



HEAD NERDS

Security Sales Playbook

Defend & Prosper: Maximizing the Cybersecurity Opportunity

January 2026

This Security Sales Digital Playbook is designed to help MSPs build a successful cybersecurity practice. It will include an outline of top traditional and co-managed programs we see MSPs successfully promote and sell, along with sample pricing, sales scripts, and marketing collateral pieces that you can customize.

LEGAL DISCLAIMER

This document is provided for informational purposes only and should not be considered legal advice. Information and views expressed in this document may change and/or may not be applicable to you. N-able makes no warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information contained herein.

N-ABLE DISCLAIMS ALL WARRANTIES, CONDITIONS, OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON THE DOCUMENTATION, INCLUDING WITHOUT LIMITATION NONINFRINGEMENT, ACCURACY, COMPLETENESS, OR USEFULNESS OF ANY INFORMATION CONTAINED HEREIN. IN NO EVENT SHALL N-ABLE, ITS SUPPLIERS, NOR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY, EVEN IF N-ABLE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

The N-ABLE, N-CENTRAL, and other N-able trademarks and logos are the exclusive property of N-able Solutions ULC and N-able Technologies Ltd. and may be common law marks, are registered, or are pending registration with the U.S. Patent and Trademark Office and with other countries. All other trademarks mentioned herein are used for identification purposes only and are trademarks (and may be registered trademarks) of their respective companies.

Table of Contents

Introduction	05	In Conclusion	30
Part 1: Developing Your Security Programs	08	Building a Co-Managed MDR	31
Traditional Managed Services Customer Type	09	Co-managed IT Services Customer Type	31
Building an Identity Protection Program	10	What is Co-managed MDR Program?	32
Target Customer for The Identity Protection Program	10	Why would an IT administrator Be Interested in this Program?	32
Why all the focus on Microsoft 365?	11	Customer Benefits	32
Services and Features Included in the Identity Protection Program	13	Services Included in a Co-managed MDR Program	33
Pricing the Identity Protection Program	17	Telemetry Data – Supported Systems Included in a Service	35
Building an Advanced Security Program	19	Pricing a Co-managed MDR Program	36
Target Customer for the Advanced Security Program	19	Co-managed MDR Training Resources	38
Services and Features Included in the Advanced Security Program	20	Part 2: Developing Your Go-To-Market and Sales Strategy	39
Pricing the Advanced Security Program	25	Developing Security Campaigns	40
A Few Cautionary Notes About Pricing	27	Developing a GTM and Sales Strategy for Selling an Identity Protection and/or an Advanced Security Program	41
The Benefits of Bundling and Program Standardization	28	Step 1: Defining the Ideal Customer Profile (ICP) and Target Audience	41
		Step 2: Identify the Problem	41

Table of Contents

Step 3: Do Your Research	42	Step 2: Identify the Problem	89
Step 4: Creating Key Messaging and Defining Your Value Prop	45	Step 3: Do Your Research	90
Step 5: Selecting the Appropriate Marketing Channels	48	Step 4: Creating Key Messaging and Defining Your Value Prop	91
Layered Security Marketing Collaterals	49	Step 5: Selecting the Appropriate Marketing Channels	94
Step 6: Create the Sales Plan	50	Co-managed MDR Marketing Collateral	94
Developing a Sales Plan to Target Existing Customers	50	Lunch and Learns	96
Developing a Sales Plan to Target New Customers	59	Step 6: Create the Sales Plan	98
Layered Security Sales Scripting for Outbound Call Campaign	60	Co-managed MDR SDR Sales Scripting for Outbound Call Campaign	99
Objection Handling Techniques and Response for Your Layered Security Programs	65	Objection Handling Techniques and Response for Co-managed MDR	103
Step 7: Setting Your Go-To-market Sales and Marketing Goals	87	Step 7: Setting Your Go-To-Market Sales and Marketing Goals	123
Developing a GTM and Sales Strategy for Selling a Co-Managed MDR program	88	Keys to Marketing and Sales Success	124
Step 1: Defining the Ideal Customer Profile (ICP) and Target Audience	88		

Introduction

Proper pricing tends to remain a top business challenge for many MSPs. As the Head Nerd responsible for Sales & Marketing, I often field questions from MSPs like:

- ▲ “We are interested in adding [enter security product] to our security tech stack, but we are not quite comfortable yet on the retail costing model and it’s holding us back a bit from going to market.”
- ▲ “Do you have any material around go-to-market pricing/packaging on [enter security product]?”
- ▲ “My customer is interested in [enter security product], but I’m not sure how I should be pricing it.”

So, this playbook was created to provide MSPs with strategies on how to best address these types of sales and pricing inquiries.

The guidance provided in this playbook can be applied to ANY type of product or service that an MSP might be trying sell. When it comes to figuring out the pricing of any product or solution that an MSP is interested in taking to market—the first question I always ask is:

Who you are selling this product or service to?

Depending on what type of organization an MSP is selling to, that is what will help determine what they should be charging.

When looking at the MSP space, there are two distinct customer types that MSPs could be selling to: (see next page)

A Traditional Managed Services Customer

This is defined as an organization where there is no dedicated, internal IT administrator in-house, so your MSP acts as their outsourced IT department, and therefore assumes 100% responsibility for the care, maintenance, and protection of their network.

A Co-managed IT Services Customer

This is defined as an organization where there IS an IT administrator or IT department in existence within the organization, and so it is that person or that IT department who is then ultimately responsible for the care, maintenance, and protection of the organization's network—not the MSP. In a co-managed IT services model, the MSP offers to help out and fill a void by taking over the management of one or two key functions or specific components, but not the entire network environment.

And this is an important distinction to make, because depending on what type of organization the MSP is targeting, whether there is the presence of an internal IT administrator or not, will determine what they should sell them and consequently what they should charge them.

As an example, let's quickly look at how an MSP would price a new security solution like MDR.

Pricing for the Traditional Managed Services Customer

With this type of customer, an MSP wouldn't price and sell MDR (or EDR, or Backup etc). as an individual service, all on its own. MDR would not be sold in a silo. Rather, the MSP would include MDR as part of their top-tier layered security program instead. This would be a package that is offered to any medium- to high-risk organization that resides in a regulated industry that has compliance standards it needs to adhere to. So if the MSP is speaking to a customer that is required to demonstrate and prove compliance, then their top-tier security package should be positioned, that includes MDR.

For the traditional managed services customer, it is this complete bundle set of security services that should be sold to them, because ultimately it is the MSP that is accepting and shouldering the cybersecurity risk on behalf of their customer. And if this is the case, then the MSP will want to implement a layered approach with respect to security, because no singular product on its own can provide adequate protection to prevent and recover from cyber-attacks.

So in this case, MDR is that final layer that gets added into the overall security bundle to provide deeper visibility, and heightened threat hunting and detection services, as it can help provide a faster mean time to incident detection—thereby providing a faster mean time to response and a faster mean time to remediation for those organizations that can't tolerate lengthy downtime and where the breach impact needs to be minimized.

Pricing for the Co-managed Customer

But pricing is looked at very differently when you are speaking with a co-managed IT services client. In this type of scenario, it is appropriate to sell your services in an a la carte format. MDR can be sold separately to a mid- or upper-enterprise organization, because in the co-managed model, the MSP is just augmenting the in-house IT team and providing a single service that the MSP will manage. In this scenario, the MSP is not in charge of the organization's network like they would be in the traditional managed services model. Rather, the overall network performance, safety and functionality is the responsibility of the internal IT Director instead.

So it is important to recognize who the MSP is selling to so that they can design their security programs and pricing schemes correctly, because when done appropriately, it can have a profound impact on the MSP's MRR, average deal size, and their overall managed services revenue.

And this playbook was designed to help MSPs with this endeavor and has been divided into two sections. Section 1 is dedicated to program design and pricing theories for each cohort type, as each customer type has its own distinct methodology. While Section 2 is dedicated to building your go-to-market sales and promotional strategies to build awareness and interest in your target customer segment.

I hope you find this playbook helpful! Happy selling!



Stefanie Hammond

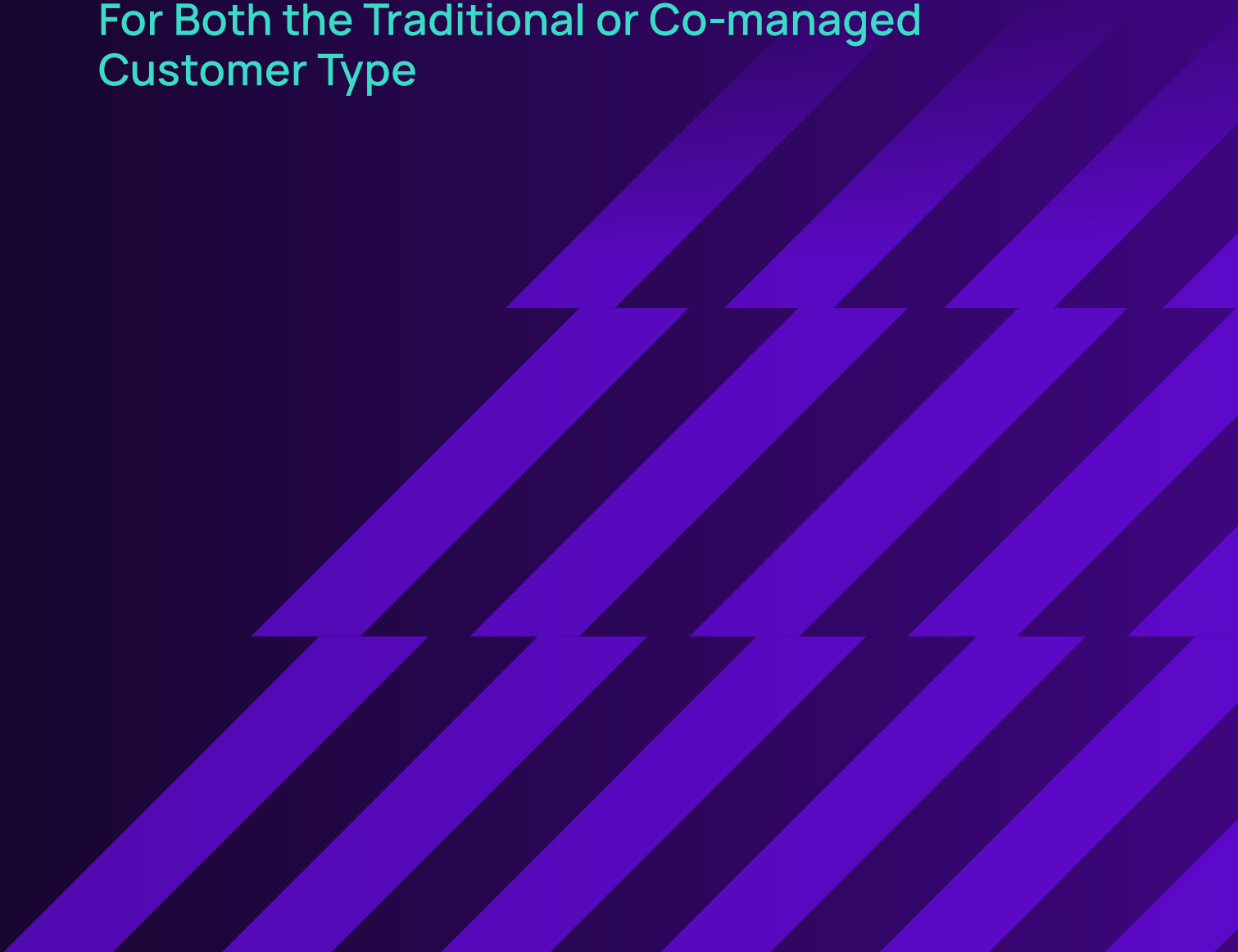
Head Nerd – Sales and Marketing

Stefanie.hammond@n-able.com

Part 1

Developing Your Security Programs

For Both the Traditional or Co-managed
Customer Type

A series of parallel diagonal stripes in a lighter shade of purple, running from the bottom left towards the top right, covering the lower half of the page.

Although this playbook was originally designed to answer the question: “How do I price [enter security product name]?”, you cannot begin to set your monthly price until you have defined:

1 Your target audience

2 Determined what features and services you intend to sell them.

Only once these two requirements have been defined, can you begin to tackle the pricing question.

So, Part 1 of this playbook is dedicated to developing your security programs and we will start with reviewing how to build security programs targeted at your traditional managed services customer-type.



Traditional Managed Services Customer Type

The traditional managed services customer is defined as an organization where there is no dedicated, internal IT administrator in-house, so your MSP acts as their outsourced IT department, and therefore assumes 100% responsibility for the care, maintenance, and protection of their network. If there is a person employed by the organization to handle the day-to-day administration of the company's network, then this would be classified as a co-managed customer

There are two program tiers that an MSP can develop, targeting the Traditional Managed Services Customer-type—**The Identity Protection Program** and **The Advanced Security Program**.

Building an Identity Protection Program

for The Traditional Managed Services Customer

What is it?

An entry-level program that offers a foundational base of security protection by incorporating a core set of security services that are centered on the end-user and the endpoint. It targets organizations that utilize Microsoft 365 as their primary productivity platform and is considered the minimum viable program that all break/fix and non-managed services customers are enrolled into.

Target Customer for the Identity Protection Program

The Ideal Client Profile for the Identity Protection Program is:

- ▲ An organization that has no dedicated, internal IT administrator or staff in-house
- ▲ An organization that does not reside in a highly regulated industry, and therefore does not have as stringent a requirement to demonstrate or prove compliance
- ▲ An organization that relies heavily upon Microsoft 365 as their primary productivity platform and storing larger amounts of data
- ▲ An organization that currently only subscribes to a break/fix or a la carte model of support, and is therefore not accustomed to allocating budget towards IT—so an Advanced Security program would be a more difficult sell in the near-term
- ▲ An organization, from a risk segmentation perspective, would be classified as a medium-risk business—meaning:
 - ▲ They would be typically smaller in size in terms of annual revenues and number of employees

- ▲ They have a limited number of strategic partnerships
- ▲ The breach impact would be lower should they succumb to a cyber-attack, but they still require the ability to quickly recover and return to work as they can only tolerate a small amount of downtime

Although these types of customers are considered smaller and exposed to a lesser amount of risk, smaller businesses are actually 3x more likely to be targeted by threat actors than larger companies, as the threat actors are very much aware that it is the smaller companies that are not making the proper investments in their cybersecurity protection coverage like they should, and many MSPs are failing to mandate that these smaller organizations enroll in any type of cybersecurity package - rather, they continue to accommodate these organizations in a break/fix or a la carte support model. So although they may be considered lower-risk from a risk segmentation perspective, there is still a minimum level of security protection coverage that should be implemented and enforced by the MSP - hence why the Identity Protection Program has been developed.

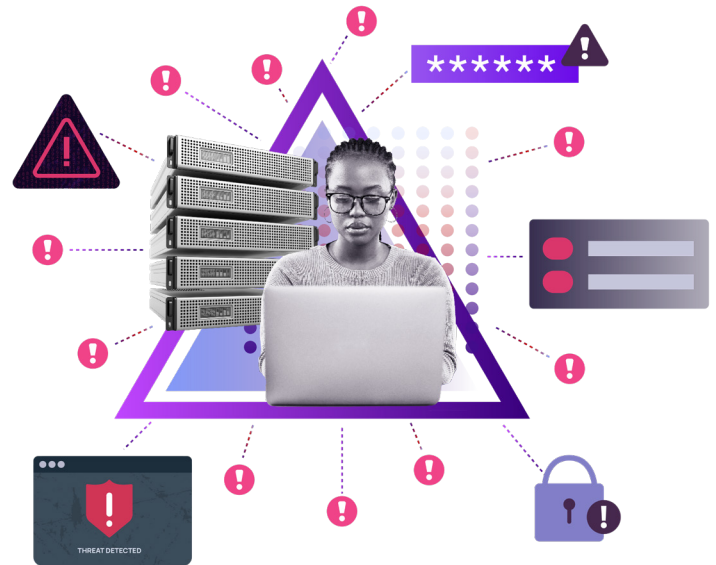
Why All the Focus on Microsoft 365?

Ultimately, this program would be beneficial to ANY customer who utilizes Microsoft 365, and heavily relies on the platform for productivity and collaboration benefits, as well as for storing their highly valuable company and customer information.

Microsoft is currently used by over 3.7 million companies around the world, but the sweet spot for Microsoft 365 customers are those small-to mid-size businesses, that typically have fewer than 50 employees. This aligns very well to the majority of an MSP's traditional managed services target client. And so with this rise in popularity, and with the large amounts of high-value data being stored in Microsoft 365, it is motivating cybercriminals to want to break into a user's Microsoft 365 account so they can gain access to the data, and exfiltrate it so they can eventually profit from it.

And while one of Microsoft 365's main selling points is its suite of integrated services like Outlook for email, OneDrive for cloud storage, and SharePoint and Teams for collaboration, which combined makes for a fantastic user experience, unfortunately with this level of integration, new management complexity and increased risk are introduced, which can lead to increased security gaps and deficiencies that attackers can then exploit. As result of this integration convenience, it has created a broader attack surface and has introduced a number of different entry points that cybercriminals can leverage to initially infiltrate the environment to steal an organization's confidential data and intellectual property.

Because once an attacker has secured this initial access, they can then use this access to delve further into the organization's network environment where the attacker would be free to move about laterally within the network to conduct their reconnaissance work to see what other valuable information might be worthwhile to steal or what kind of damage they could instigate.



Or, they could use their new access knowledge they have gained and sell it to other criminal cybergroups who may have their own motives for targeting this particular organization, where they could then launch their own set of attacks.

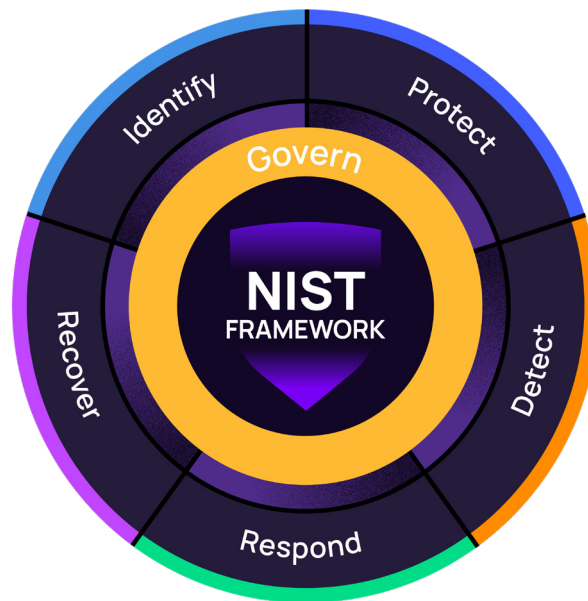
And the most dire consequence from all of this is: Without having proper Microsoft 365 security monitoring and threat detection in place, along with other important security services, the organization would be completely unaware that anything at all is happening. So, it has become increasingly more and more critical for MSPs to implement monitoring and threat detection services of their customers' Microsoft 365 accounts, so they can have the proper vision and insight that is needed. Because time is of the essence in any type of cyberattack. When you look at a ransomware attack, it can spread very quickly and may only take a few seconds for it to start encrypting files. Speed plays a vital role in catching successful identity attacks before they can escalate to data theft or ransomware deployment. Threats need to be responded to right away and they need to be acted on immediately.

So, when speaking to customers about their business' risks, it is important to convey to them that one of the biggest risks to their organizational and employee productivity is the very productivity platform that they rely on for their business. Unfortunately, Microsoft 365 has become a very popular attack target for cybercriminals, and to combat this threat, MSPs should consider launching a security program focused on monitoring and securing their Microsoft 365 estate and users' identities, to prevent attackers from causing harm and damage to the business.

Source: <https://e2e-assure.com/managed-threat-detection-and-response/top-attacks-against-m365>

Services and Features Included in the Identity Protection Program

The Identity Protection Program has been developed to align with the NIST Cybersecurity Framework and incorporates the 6 key functions outlined below.



IDENTIFY: Asset Discovery for Network Visibility

- ▲ Quarterly Security Risk Assessment
- ▲ Asset Discovery (using an [RMM platform like N-central or N-sight](#))
- ▲ Software Inventory & License Management (using an [RMM platform like N-central or N-sight](#) and [Passportal](#))
- ▲ Hardware Inventory & Asset Management (using an [RMM platform like N-central or N-sight](#) and [Passportal](#))
- ▲ Infrastructure Performance Monitoring (Servers, Desktops, Firewalls, Switches/ Routers, All O/S)
- ▲ Microsoft License Management : License Assignments, unassignments, service configurations (N-able potential product: [Cloud Commander](#))

PROTECT: All Systems and People

- ▲ Device Optimization
- ▲ Routine Infrastructure Preventative Maintenance (Servers, Firewalls, Switches/Routers)
- ▲ Endpoint Patch Management: Mac, Windows + Third Party (via RMM)
- ▲ Key Application Maintenance & Management (if applicable)
- ▲ Web Security (N-able potential product: [DNS Filter](#))
- ▲ Mail Security, Mail Filtering & Protection (N-able potential product: [Mail Assure](#))
- ▲ Microsoft 365 Breach Monitoring & Prevention (N-able potential product: [Adlumin Identity Threat Detection and Response \(ITDR\)](#))
- ▲ Vulnerability Scanning & Management – Endpoint (RMM)
- ▲ Password Management & Security (N-able potential product: [Passportal](#))
- ▲ 2FA/MFA implementation and enforcement (N-able potential product: [Cloud Commander](#))
- ▲ Endpoint Detection & Response (N-able potential product: [SentinelOne EDR](#))
- ▲ Data Protection (N-able potential product: [Cove Data Protection](#))
- ▲ Employee Security Awareness Training
- ▲ Microsoft User Management – Applying/editing permissions (N-able potential product: [Cloud Commander](#))

DETECT: Unusual Activity

- ▲ Endpoint Detection & Response (N-able potential product: [SentinelOne EDR CONTROL](#))
- ▲ Mail Monitoring – Malware & Phishing Detection & Blocking (Mail Assure)
- ▲ Microsoft 365 Breach Monitoring & Prevention (N-able potential product: [Adlumin Identity Threat Detection and Response \(ITDR\)](#))

RESPOND: To Detected Threats

- ▲ Either using the MSP's own EDR response protocol or [SentinelOne's Vigilance Service](#), as per their SLA/MSA (N-able potential product: [SentinelOne EDR](#))
- ▲ 24/7 SOAR & SOC Response & Remediation via Adlumin Identity Threat Detection and Response (ITDR) (for what is in-scope per MSA for Microsoft 365)

RECOVER: System Functionality, Employee Productivity and Data Loss

- ▲ Backup - Server (N-able potential product: [Cove Data Protection](#))
- ▲ Backup -Microsoft 365 + Teams (N-able potential product: [Cove Data Protection](#))
- ▲ Endpoint Detection & Response - Rollback (N-able potential product: [SentinelOne EDR CONTROL](#))
- ▲ Regular Backup Testing
- ▲ 30-Day Log Data Retention for Adlumin Identity Threat Detection and Response (ITDR)

GOVERN: Fiduciary Responsibility and Accountability

- ▲ Monthly Report
- ▲ Asset Lifecycle Planning
- ▲ Semi-Annual Executive Business Reviews
- ▲ Microsoft License Management & Reporting & Planning (N-able potential product: [Cloud Commander](#))

Support Services:

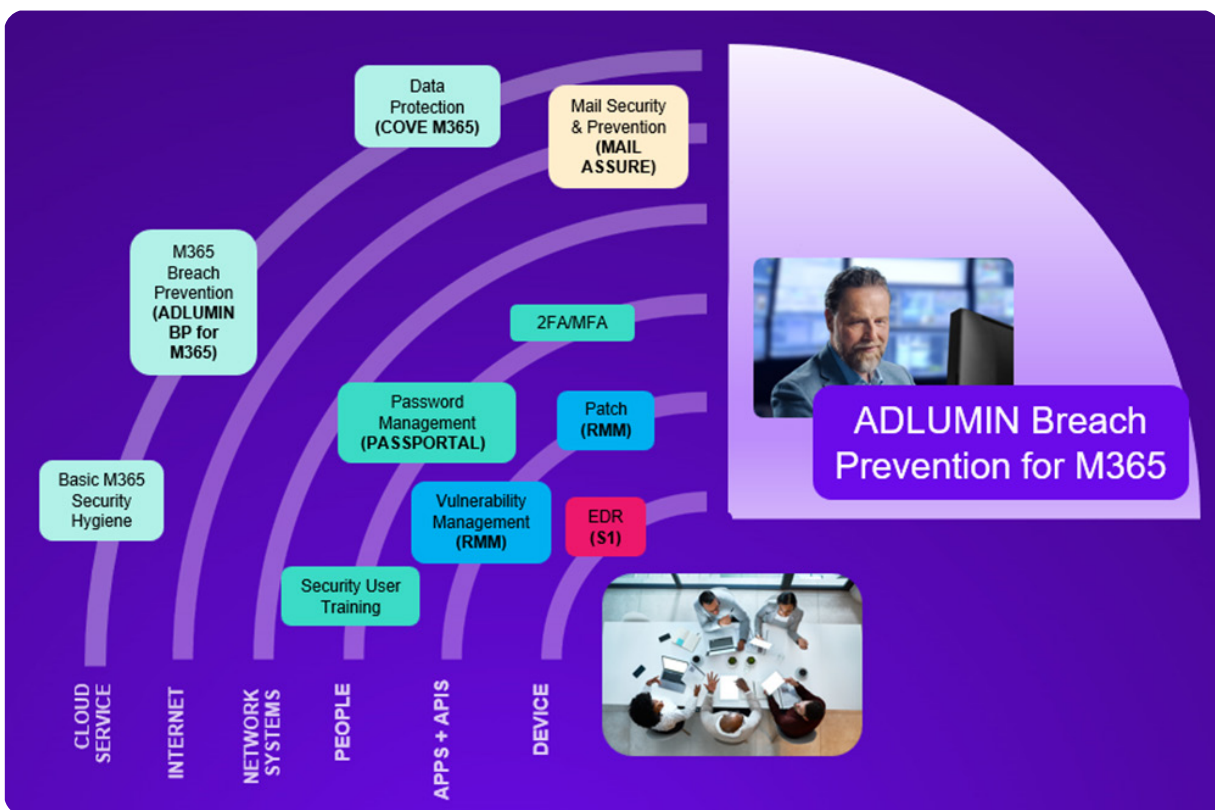
- ▲ The only included support is what is provided by the SentinelOne Vigilance team when a threat on the endpoint is detected, plus limited time for the MSP to implement recommendations put forth by the SentinelOne Vigilance team
- ▲ Restore services will be provided to recover compromised devices and data using existing backups, but there is no specified SLA, and this recovery will be on a “best effort” basis.
- ▲ Microsoft End-User Support – ex. Password Resets, reset MFA, user mailbox management - INCLUDED

Out of Scope Items:

- ▲ All helpdesk calls are out of scope and billed on a time and material basis
- ▲ All reactive, email, chat and emergency support calls are out of scope and billed on a time and material basis

- ▲ All vendor management assistance support calls are out of scope and billed on a time and material basis
- ▲ Anything considered 'Incident Response' following a cyber-attack, beyond what automatic responses are provided by the SentinelOne Vigilance team are out of scope and billed on a time and material basis

To view this list within Excel, you can access the Security Services Program Matrix [HERE](#)



Pricing the Identity Protection Program



*Sample only: gross margin not guaranteed.

Monthly pricing would start at \$100 USD/user*, and includes:

- ▲ Cost of your RMM agent (N-central, N-sight, or preferred RMM toolkit)
- ▲ Cost of Cloud Commander
- ▲ Cost of SentinelOne EDR, EDR agent + Vigilance SOC Service (if using)
- ▲ Cost of Adlumumin Breach Prevention for Microsoft 365
- ▲ Cost of Cove Data Protection Server
- ▲ Cost of Cove Data Protection for Microsoft 365
- ▲ Cost of N-able Mail Assure agent
- ▲ Cost of N-able DNS Filtering agent
- ▲ Cost of N-able Passportal 'Site' license
- ▲ Labor costs to prepare and deliver semi-annual Executive Business Review Meeting
- ▲ Labor costs to prepare and deliver Basic Training Services (2 hours/year included – assumed training is delivered by MSP)
- ▲ Labor costs to prepare and deliver quarterly risk assessment
- ▲ Labor costs to ensure regular backups are successfully run, including troubleshooting and simple file/folder recoveries
- ▲ Small amount of MSP labor is included to implement recommendations provided by the SentinelOne Vigilance team when a threat on the endpoint is detected
- ▲ Restore services to recover compromised devices and data using existing backups, but there is no specified SLA, and this recovery will be on a "best effort" basis.

Assumptions/Caveats:

- ▲ *The pricing above is based on using N-able's solutions and N-able's USD MSRP pricing as of June 2025. Cost and pricing may be different if MSP is utilizing a different set of security toolsets and RMM, which can impact the final monthly price being charged to the customer.
- ▲ Fully Burdened Labor Rate used in calculation = \$50USD/hr
- ▲ Incomplete costing due to Risk Assessment toolset cost missing, and will need to be factored in for final price
- ▲ Incomplete costing as Identity Protection Program does not include any reactive or emergency labor outside what has been budgeted for the SentinelOne Vigilance Service (if using)

Out of Scope Items:

- ▲ All helpdesk calls are out of scope and billed on a time and material basis or pulled from a block of hours
- ▲ All reactive, email, chat and emergency support calls are out of scope and billed on a time and material basis or pulled from a block of hours
- ▲ All vendor management assistance support calls are out of scope and billed on a time and material basis or pulled from a block of hours
- ▲ Anything considered 'Incident Response' following a cyberattack, beyond what automatic responses are provided by the SentinelOne Vigilance team (if using) and Adlumin Identity Threat Detection and Response (ITDR) are out of scope and billed on a time and material basis or pulled from a block of hours



If you require assistance creating your own pricing structure for the Identity Protection Program, you can [access our Costing Calculator](#)

Building an Advanced Security Program

for the Traditional Managed Services Customer

What is it?

A program that takes a more comprehensive approach to security by incorporating a more robust set of security and threat detection and response services that extends beyond the end-user and the endpoint, but encompasses all components of an organization's network environment, including network devices, SaaS, VPN, firewalls and the cloud.

Target Customer for the Advanced Security Program

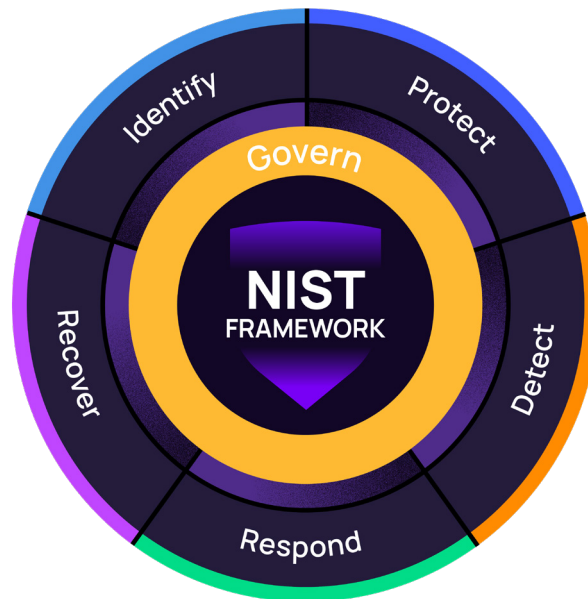
The Ideal Client Profile for the Advanced Security Program is:

- ▲ An organization that has no dedicated, internal IT administrator or staff in-house
- ▲ An organization that does reside in a regulated industry, and therefore does have a requirement to demonstrate or prove compliance to auditors such as
 - ▲ Banking
 - ▲ Healthcare
 - ▲ Local and State government agencies
 - ▲ Financial
 - ▲ Education
- ▲ An organization that is accustomed to allocating budget towards IT and has a higher awareness of their need for a more comprehensive set of security services
- ▲ An organization that would rate their Return To Operations (RTO) objective as Medium or High – meaning that they are a fully computerized firm, with no manual processes that they could fall back on, should they suffer a cyber-attack. As a result, there would be urgency to get the employees and the business back online as soon as possible, so the organization could begin generating revenue again.

- ▲ An organization - from a risk segmentation perspective - would be classified as a Medium/Medium-High/High risk business – meaning:
 - ▲ They are larger in size in terms of annual revenues and number of employees
 - ▲ They collect and store a large amount of data – financial data, PII, sensitive IP – and employees have access to these data stores
 - ▲ They have a number of strategic partnerships and therefore the employees potentially have access to their sensitive systems or the partner data
 - ▲ The breach impact would be high should they succumb to a cyber-attack, where it could likely result in an extinction event for the organization

Services and Features Included in the Advanced Security Program

As with the Identity Protection Program, the Advanced Security Program has also been developed to align with the NIST Cybersecurity Framework.



IDENTIFY: Asset Discovery for Network Visibility

- ▲ Monthly Security Risk Assessment
- ▲ Asset Discovery (using an [RMM platform like N-central or N-sight](#) and a product like [SentinelOne's Attack Surface Management](#))
- ▲ Software Inventory & License Management (using an [RMM platform like N-central or N-sight](#) and [Passportal](#))
- ▲ Hardware Inventory & Asset Management (using an [RMM platform like N-central or N-sight](#) and [Passportal](#))
- ▲ Cloud & Infrastructure Performance Monitoring (Servers, Desktops, Firewalls, Switches/Routers, All O/S, Cloud devices within Microsoft/Azure) (N-able RMM & Cloud Commander)
- ▲ Microsoft License Management – License assignments, unassignments, service configurations (N-able potential product: [Cloud Commander](#))

PROTECT: All Systems and People

- ▲ Device Optimization
- ▲ Routine Infrastructure Preventative Maintenance (Servers, Firewalls, Switches/Routers)
- ▲ Account Governance & Access Credentials Management (Cloud Commander/Passportal)
- ▲ Microsoft User Management – Applying/editing permissions (Cloud Commander)
- ▲ Microsoft Exchange Online Management (Cloud Commander)
- ▲ Microsoft Teams Management (Cloud Commander)
- ▲ Azure Health Monitoring & Resource Management (Cloud Commander)
- ▲ Intune and WIN365 Monitoring, Configuration Management and Enforcement (Cloud Commander)
- ▲ Secure Configuration Management (RMM/Cloud Commander)
- ▲ Endpoint Patch Management: Mac, Windows + Third Party (via RMM)
- ▲ Key Application Maintenance & Management (if applicable)
- ▲ Web Security (N-able potential product: [DNS Filter](#))
- ▲ Mail Security, Mail Filtering & Protection (N-able potential product: [Mail Assure](#))
- ▲ Password Management & Security (N-able potential product: [Passportal](#))
- ▲ 2FA/MFA implementation and enforcement for all on-premis and Intune devices (Cloud Commander)
- ▲ Dark Web Monitoring (N-able potential product: [N-able MDR](#))
- ▲ Internal/External IPS/IDS
- ▲ Internal/External Penetration Testing
- ▲ Device Disk Encryption

- ▲ Vulnerability Monitoring & Management – Hardware, Network, Access Points & Compliance
- ▲ Software Vulnerability Monitoring & Management
- ▲ Advanced Employee Security Awareness Training
- ▲ Endpoint Detection & Response (N-able potential product: [SentinelOne EDR COMPLETE](#))
- ▲ Data Access Controls and Enforcement
- ▲ Application Control Security Control and Enforcement
- ▲ Security Policy Creation and Enforcement
- ▲ Security Controls Recommendations and Enforcement
- ▲ Backup -Workstation(N-able potential product: [Cove Data Protection](#))
- ▲ Backup – Server (N-able potential product: [Cove Data Protection](#))
- ▲ Backup – Microsoft 365 (N-able potential product: [Cove Data Protection](#))
- ▲ Standby Image with Hyper-V, ESXi and/ or Azure Targets (N-able potential product: [Cove Data Protection](#))
- ▲ Backup Recovery Testing (N-able potential product: [Cove Data Protection](#))

DETECT: Unusual Activity

- ▲ Endpoint Detection & Response (N-able potential product: [SentinelOne EDR COMPLETE](#))
- ▲ Managed Detection Services for Cloud Services (M365, Google, Salesforce, Azure, AWS) (N-able potential product: [N-able MDR](#))
- ▲ Syslog Monitoring and Log collection (N-able potential product: [N-able MDR](#))

RESPOND: To Detected Threats

- ▲ MSP's own Response & Remediation Protocol or Response & Remediation Protocol via [N-able MDR](#) (for what is in-scope per MSA)

RECOVER: System Functionality, Employee Productivity and Data Loss

- ▲ Backup - Workstation-Full Workstation (N-able potential product: [Cove Data Protection](#))
- ▲ Backup - Server (N-able potential product: [Cove Data Protection](#))
- ▲ Backup -Microsoft 365 ([Cove Data Protection](#))
- ▲ Backup Recovery Testing (N-able potential product: [Cove Data Protection](#))
- ▲ Standby Image with Hyper-V, ESXi and/or Azure Targets (N-able potential product: [Cove Data Protection](#))
- ▲ Disaster Recovery Planning
- ▲ Mail Archiving (N-able potential product: [Mail Assure](#))
- ▲ 365 Day Log Retention of MDR log data collected (offered through N-able MDR Advanced)
- ▲ Endpoint Detection & Response - Rollback (N-able potential product: [SentinelOne EDR COMPLETE](#))

GOVERN: Fiduciary Responsibility and Accountability

- ▲ Monthly Report, including results of scheduled recovery testing
- ▲ Microsoft License Management Reporting & Planning (Cloud Commander)
- ▲ Compliance Insights ([offered through N-able MDR Advanced](#))
- ▲ Asset Lifecycle & Refresh Planning – onpremise and Azure devices (RMM/ Cloud Commander)
- ▲ Quarterly Executive Business Reviews
- ▲ Compliance Policy Creation, Management & Enforcement of Microsoft Cloud Devices (Cloud Commander)
- ▲ End-User Microsoft 'Secure Score' Compliance Reporting & Remediation of Risky User Activity (Cloud Commnader)

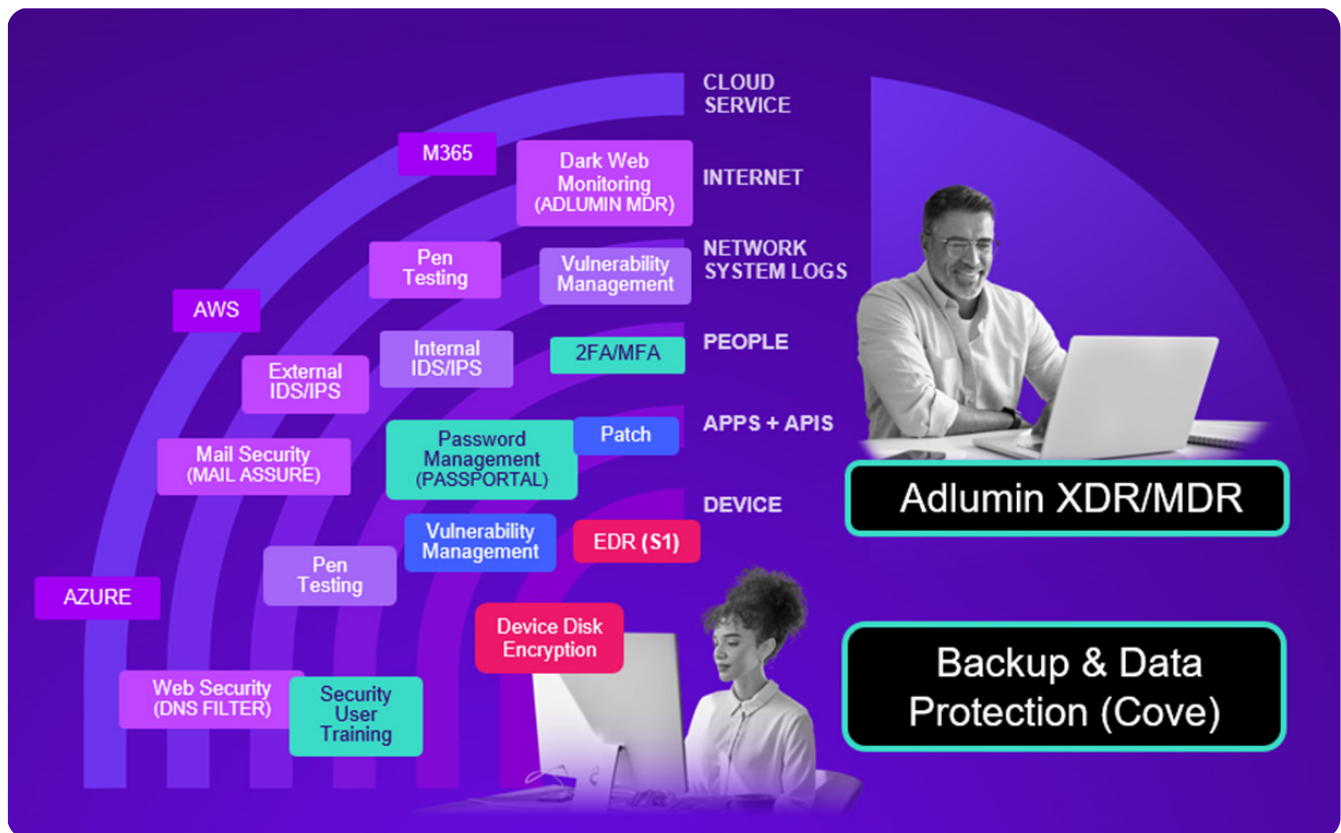
Support Services:

- ▲ All helpdesk calls are included, as per MSP's SLA/MSA
- ▲ All reactive, email, chat and emergency support calls are included, as per MSP's SLA/MSA
- ▲ All vendor management assistance support calls are included, as per MSP's SLA/MSA
- ▲ Restore services to recover compromised devices and data using existing backups, with priority urgency and negotiated SLA based on resources, data volume and device types.

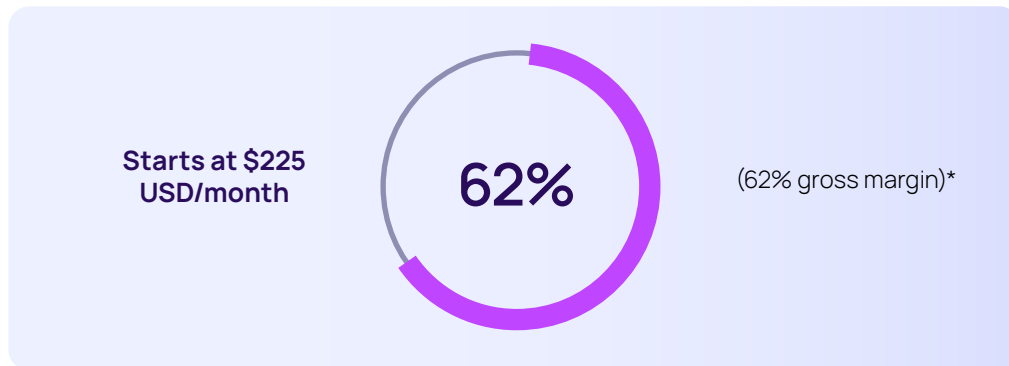
Out of Scope Items:

- Anything considered 'Incident Response' following a cyberattack, beyond what responses are provided by the Adlumin MDR SOC team are out of scope and billed on a time and material basis

To view this list within Excel, you can access the Security Services Program Matrix [HERE](#)



Pricing the Advanced Security Program



*Sample only: gross margin not guaranteed.

Monthly pricing would start at \$225 USD/user*, and includes:

- ▲ Cost of your RMM agent (N-central, N-sight, or preferred RMM toolkit)
- ▲ Cost of Cloud Commander
- ▲ Cost of SentinelOne Attack Surface Management agent
- ▲ Cost of SentinelOne EDR 'Complete' EDR agent
- ▲ Cost of Adlumin MDR Advanced agent
- ▲ Cost of Adlumin MDR 365 day log retention
- ▲ Cost of Cove Data Protection Workstation
- ▲ Cost of Cove Data Protection Server
- ▲ Cost of Cove Data Protection Recovery Testing/Standby Image
- ▲ Cost of Cove Data Protection for Microsoft 365
- ▲ Cost of N-able Mail Assure agent
- ▲ Cost of N-able Mail Assure Archiving capabilities
- ▲ Cost of N-able DNS Filtering agent
- ▲ Cost of N-able Passportal 'Site' license
- ▲ Labor costs to conduct routine preventative maintenance activities on all servers, network devices and workstations (assuming 60-90 minutes total/month)
- ▲ Labor costs to budget for unexpected reactive support like: Helpdesk calls, email, chat, vendor management etc and emergency labor (assuming 90 minutes total/month)
- ▲ Labor costs to prepare and deliver quarterly Executive Business Review Meeting (assuming 20 hours total/year)

- ▲ Labor costs to prepare and deliver Advanced Security Training Services (assuming 8 hours total/year)
- ▲ Labor costs to prepare and deliver monthly risk assessment
- ▲ Labor costs to implement recommendations provided by the Adlumin MDR SOC Team – once a threat has been neutralized – that is outside the scope of engagement

Assumptions/Caveats:

- ▲ *The pricing above is based on using N-able's solutions and N-able's USD MSRP pricing as of June 2025. Cost and pricing may be different if MSP utilizes a different set of security toolsets and RMM, which can impact the final monthly price being charged to the customer.
- ▲ Fully Burdened Labor Rate used in calculation = \$50 USD/hr
- ▲ Incomplete costing due to Vulnerability Management toolset cost missing, and will need to be factored in for final price
- ▲ Incomplete costing due to Risk Assessment toolset cost missing, and will need to be factored in for final price
- ▲ Labor time estimates included are based on averages, and depending on how automated or how manual an MSP is operationally, it will impact the monthly management time included in cost structure and final price communicated to customer
- ▲ Restore services to recover compromised devices and data using existing backups, with priority urgency and negotiated SLA based on resources, data volume and device types.

Out of Scope Items:

- ▲ Anything considered 'Incident Response' following a cyber-attack, beyond what automatic responses and SOC intervention tactics are utilized by the Adlumin MDR team, are out of scope and billed on a time and material basis or pulled from a block of hours



If you require assistance creating your own pricing structure for the Identity Protection Program, you can [access our Costing Calculator](#)

A Few Cautionary Notes About Pricing

- ▲ As tempting as it may be to base your pricing on how the competition is charging, conduct your own pricing exercise, utilizing your own software and labor costs, and program margin goals. Resist the urge to price based on what the competition is charging, as it is difficult to compare programs
- ▲ Don't aim to be the cheapest in your market—strive to sell on value, and weaponize your competitor's cheaper price, if you are questioned
- ▲ By specializing in security, and bringing a security focus into the program development and marketing activities, this will allow your MSP to differentiate yourself from your competitors and focus on the benefits and outcomes of your programs, instead of the monthly price being charged
- ▲ Don't price your programs based on what you 'think' your customers can afford—don't pre-object on behalf of your customers before even speaking with them.
- ▲ Go out and have that security and risk conversation with your customers and educate them on the changes that are being implemented as a result of the changing threat landscape. Proper cybersecurity does cost money, and it should be seen as an investment, rather than a cost
- ▲ Security is no longer an IT problem, but it is a business risk that needs to be managed, and Business Owners and CEOs have a fiduciary responsibility to take the proper measures to prevent the loss in value in the business, and your Advanced Security Program can assist with protecting the organization's business value



- ▲ Don't price per device - price by user instead. From a positioning and messaging standpoint, you are protecting and educating USERS with your security programs, so you want the focus of your sales conversations and messaging to be on the USERS, not on the technical tidbits you are managing
- ▲ Employees are generally the ones behind breaches occurring, so you are relying on your security programs to do what is necessary to bubble wrap and protect the end-users from clicking on something they shouldn't or behaving in an unsecure way that can allow an attack to take place

- ▲ People are the most expensive asset of any organization, so your goal is to do what you can to keep them safe, protected, productive and working
- ▲ Also, make sure you understand what goes into your fully burdened labor rate. A fully burdened labor rate is the full cost of an hour's worth of work and includes (among other things): Hourly wage, all payroll taxes, vacation pay, health insurance, supplies, meals training, and any other benefits or expenses related to an individual's employment. If you are unsure how to calculate your fully burdened labor rate, please consult with your bookkeeper or accountant to help calculate this for you
- ▲ Be honest in the amount of direct labor and HR time that is needed to deliver your security programs. Skimping on time estimates to reduce the monthly price, so it fits into a customer's monthly budget, only hurts your profitability and revenue levels. If you find that there is 'too much time' or too much labor that needs to be included in your programs where it appears to be inflating the monthly price, then it might be time to look internally and see where automation and optimization and toolset standardization could be better achieved
- ▲ Ensure you have implemented a process and a cadence around communicating regular price increases to your customers. Your costs increase ever year, so you need to be sure that you are implementing regular price increases for your customers or else your profitability levels will begin to erode. Include a clause about standard price increases into your new customer contracts and in all renewal opportunities with existing customers

The Benefits of Bundling and Program Standardization

- ▲ When it comes to selling security to a traditional managed services client, as outlined in the above program packages, we want to focus on selling a standardized set of 'bundled services' in a packaged format, verse selling individual services in an a la carte manner or bespoke type of programs
- ▲ There are significant benefits that can be reaped by standardizing your offerings and selling them in a bundled way.
- ▲ It **provides consistence** and keeps every customer on the same program with the same set of services, feature-sets, that are supported by the same technology stack
- ▲ Streamlines the onboarding, service delivery and support processes and will help to reduce the overall mean time to resolution: Standardization on a specific security stack makes it easier for the MSP to onboard, service and support their customers, as the tech stack is the same across the board, and every customer receives the same set of services

- Improves technician efficiency and training** because there is standardized technology stack, it makes it much easier for the techs to stay up to date on their training and to remain current on the latest updates and feature-sets contained within each product that makes up their security stack. They are not wasting cycles attempting to stay knowledgeable on 3-4 different AV/EDR products and 3-4 different backup products etc. They can focus their efforts and valuable time improving their proficiencies and expertise in a single set of tools.



- Positions the MSP as the expert and authority** as it relates to security. As the MSP, you can promote the fact that you have surveyed the threat landscape and have researched and vetted the best security toolsets available to properly manage and protect their network, and this is the toolset you mandate all of your customers be enrolled in to best mitigate their cyber-risk.
- It promotes flexibility.** As a result, affords the MSP the flexibility and luxury to adjust the security stack or amend the product mix as necessary, if the threat landscape warrants it. Selling a bundled set of services in a standardized way removes the notion of having to get the customers' permission first, before making any changes. The MSP is free to introduce new products or services as required, to continue providing the best chances of thwarting cyberattacks and potential breaches
- By not bundling, and by continuing to offer services in a bespoke or a la carte model, it not only increases your customers' risk, but also increases your risk as their MSP**
- If you allow your customers to deviate from your new security standards, and they end up suffering a cyber-attack as a result, they will likely be very upset and will be looking to point the finger at someone to blame – and as their MSP, you will be that target for their anger and frustration because their perception is that they are paying you to take care of them, and you didn't, because you allowed a threat actor to get through. So your MSP can suffer reputational damage as a result of your noble desire to accommodate their own preferred path to support, instead of mandating that they be enrolled in one of your standard cybersecurity programs**
- Also by neglecting to bundle and continuing to allow your customers to create their own set of services, you are impeding your ability to scale, and you are sacrificing the ability to obtain consistent contract margins and higher MRR and ACV for your MSP**

In Conclusion

The key takeaway from this entire section is:

- ▲ If you are going to spend your valuable time creating a marketing and sales campaign targeted at the traditional managed services customer that only focuses on selling MDR, or EDR, or backup, on its own, in a non-bundled way, then you are not making the most of the sales opportunities that you will be generating
- ▲ Instead, dedicate the effort and expense into selling a bundled set of services (like your Identity Protection or Advanced Security Program) that provides higher value, improved security coverage, and improved cyber resiliency protection
- ▲ This is a difference between making this a technical sale, where you are just reselling a toolset, which offers only minimal levels of profitability, versus turning this into a value-based sales motion
- ▲ If you are going to engage with a traditional managed services prospect or customer anyway, then you don't want to waste the opportunity before you. Leverage the opportunity to speak to your customers about your Advanced Security Program (or Identity Protection Program) and not just a singular product, and benefit from higher contract values and improved MRR, while also working towards reducing and mitigating your risk as their MSP



For additional information around how to build and price your layered security programs targeted at the traditional managed services customer-type, please visit [N-ableU](#) to access on-demand recordings of:

Masterclass

[Threat Ready: Building Resilience in the Face of Risk \(Advanced Security Program\)](#)

Masterclass

[Protecting What Matters Most: The Identity Plane \(Identity Protection Program\)](#)

Building a Co-Managed MDR

for Mid and Upper-Enterprise Organizations

What is it?

A program where the MSP partners with the internal IT department to proactively provide managed threat detection, investigation and containment services based on a turnkey mix of security toolsets and platforms, while leveraging a team of security experts within a SOC setting who are monitoring and responding to security threats on a 24/7/365 basis.

Co-Managed IT Services Customer Type

As outlined in the introduction of this security sales playbook, a co-managed IT services customer is defined as an organization that employs a dedicated, in-house IT administrator or IT department, and where it is this IT Administrator or department that is ultimately responsible for the care, maintenance, and protection of the organization's network—not the MSP. Rather, in the co-managed IT services model, the MSP augments the in-house IT team by filling a void by offering to take over the management of one or two key components, but generally does not take on the management responsibility of the entire network environment. This is an important distinction, because if there is NO dedicated in-house IT Administrator employed by the organization, then this would be considered a traditional managed services opportunity instead.

When it comes to building and selling programs that are targeted at mid- and upper-enterprise customers, it is very different from the model that was discussed in the previous section. In the co-managed market, you CAN sell your services in a silo – you can sell a la carte. And while there are a variety of different services that can sold in this manner, for the purposes of this playbook, we will focus on one program offering – the co-managed MDR program. If you are interested in learning more about other top co-managed programs that you can build and take to market, please refer to our [Co-Managed Digital Playbook](#).

What is a Co-Managed MDR Program?

A program where the MSP partners with the internal IT department to proactively provide managed threat detection, investigation and containment services based on a turnkey mix of security toolsets and platforms, while leveraging a team of security experts within a SOC setting who are monitoring and responding to security threats on a 24/7/365 basis.

Why Would an IT Administrator Be Interested in This Program?

Customer Benefits

- ▲ Can help an organization reduce their cyber-risk by solving a number of security challenges if they are not equipped to effectively handle cyber threats on their own due to lack of knowledge, experience, expertise or skillsets
- ▲ Can provide a high level of business continuity and time savings in the event of a cyberattack by supplementing the existing internal IT team and acting as their front-line response by immediately starting the remediation process on their behalf
- ▲ Allows the internal IT team to focus on its core competencies and strategic projects by offloading the security burden and the day-to-day security operations to the MSP's SOC team instead, thereby making the MSP responsible for the ongoing monitoring, detection, investigation, and mitigation of malicious threat events
- ▲ Can help the organization demonstrate and maintain compliance by providing a mechanism and a process to collect and aggregate logs from across the organization's entire estate including: endpoint, identity, cloud, network, or anything with a syslog output,
- ▲ Can provide full transparency, visibility and equitable access to all data and reporting for better decision-making capabilities on future technology improvements and spending
- ▲ Can provide a bridge to their existing technology stack and mitigate risk as the organization develops and implements their technology roadmap or consolidates disparate technology when it comes to M&A
- ▲ More cost effective as the internal IT team can rely upon the MSP's SOC team to handle their advanced security requirements without having to hire and managed the security software, operations and personnel themselves

Services Included in a Co-Managed MDR Program

- ▲ MSP will provide a cybersecurity assessment or network health review to determine baseline, and offer ongoing assessments for transparency and accountability at a regular cadence
- ▲ MSP will create an incident response plan and incident response playbook that will outline the rules of engagement between MSP's SOC team and the internal IT department (as part of the onboarding process)
- ▲ Use of MSP's Security Incident Event Management (SIEM) Platform that provides the ability to ingest data from a multitude of data sources and API integrations, including: endpoint, identity, cloud, network, or anything with a syslog output – without any data ingest fees
- ▲ 24/7/365 real-time monitoring and detection of cyberthreats utilizing:
 - ▲ User & Entity Behavior Analytics (UEBA) to identify, detect, analyze, and prioritize anomalous behavior
 - ▲ AI and machine learning to detect known and unknown threats—specifically when determining an insider threat, account takeover, privilege abuse or misuse
 - ▲ 'Honeypots' to provide organizations with another way to detect threat actors that may already be in their environment in order to quickly stop them before they access critical systems or data
 - ▲ Darknet Exposure Monitoring to search for confidential information and leaked accounts on the deep and dark web, so if a business account is found to be leaked, then notifications will be sent out and password resets will be implemented to protect the user
 - ▲ Perimeter Defense Monitoring to look for: port changes, certificate issues, known vulnerabilities



- ▲ Front-line, first-line response, remediation and containment when a threat is detected either via SOAR (Security Orchestration Automation & Response) or human security operator intervention
- ▲ Customizable dashboard access
- ▲ Live and on-demand reporting for visibility, accessibility and transparency purposes
- ▲ Monthly review meetings
- ▲ 365-day retention of log data (or longer, but at an additional cost)
- ▲ Compliance services include:
 - ▲ One-touch compliance reporting, framework verification and executive reports to demonstrate adherence and to streamline an organization's compliance efforts
 - ▲ Automated PCI DSS, NIST and HIPAA Compliance which includes the following actions:
 - ▲ Automatically tracks and records all access and combines compliance details across the entire enterprise
 - ▲ Determines and views all privileged accounts at local and domain levels quickly and easily
 - ▲ PCI DSS device log management
 - ▲ Daily of logs and retainment of log monitoring audit trail for 1 year to keep organization fully PCI compliant
 - ▲ Review of the organization's Active Directory GPO policies for PCI violations and poor security practices

Telemetry Data – Supported Systems Included in Service

Supported Systems

◆◆ Integrations

Cloud

- AWS
- Azure
- Google
- Oracle Cloud
- Salesforce

Email Security

- Abnormal Security
- Azure (Azure & Office365)
- Google (Google Workspace)
- KnowBe4
- 1Password
- Proofpoint Enterprise/Essentials
- Zix

Endpoint

- Bitdefender
- Carbon Black Endpoint and Response
- Carbon Black App Control
- Cisco AMP
- CrowdStrike
- Cylance
- Endpoint Security Devices
- Huntress
- Malwarebytes
- Malwarebytes OneView
- NinjaOne
- Palo Alto Networks Cortex
- SentinelOne
- Sophos
- TrendMicro WFBS
- Webroot

◆ Adlumin MDR

◆ Adlumin MDR Advanced

◆◆ Agent Telemetry

- Windows7+
- Win Server 2008+
- MacOS 10.15+
- Linux
 - RHEL 6.0+
 - Ubuntu 14.0+
 - Centos 7.0+
 - SUSE 11.4+
 - Amazon Linux

◆◆ Perimeter Devices

Anything that sends Syslog Events

- Acronis
- AWS
- Bitwarden
- Cisco Meraki
- Cisco Umbrella
- Darktrace
- Duo
- Firewall
- JumpCloud
- Netskope
- Network Security Devices
- Okta
- Oracle Cloud
- Salesforce
- VPN

For additional reading to learn more about Adlumin MDR and its functionality:

▲ Adlumin MDR:

<https://www.n-able.com/products/managed-detection-and-response>

▲ Introducing Adlumin MDR:

<https://www.n-able.com/resources/introducing-mdr>

▲ Key feature of Adlumin MDR:

<https://www.n-able.com/resources/key-features-of-n-able-mdr>

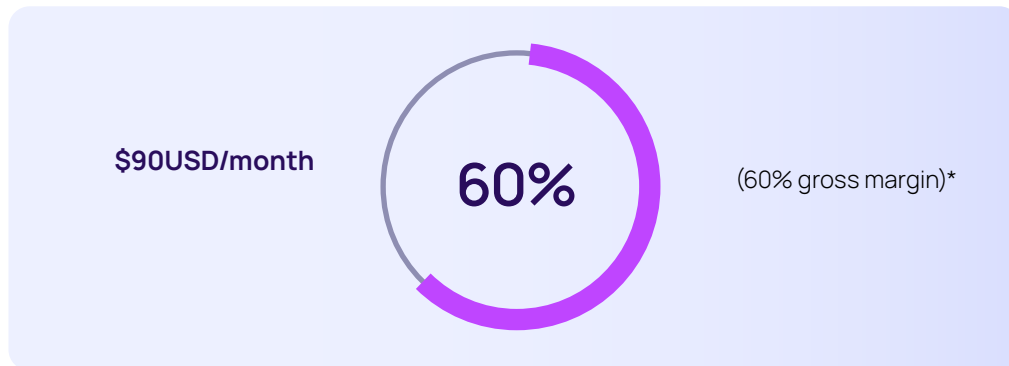
▲ XDR vs MDR:

<https://www.n-able.com/resources/xdr-v-mdr>

▲ Security Re-invented: Omega Systems' Transformation with Adlumin MDR:

<https://www.n-able.com/resources/security-reinvented-omega-systems-transformation-with-n-able-mdr>

Pricing the Advanced Security Program



*Sample only: gross margin not guaranteed.

Monthly Pricing Would Start at \$90 USD/user*, and Includes:

- ▲ Cost of your RMM agent (N-central, N-sight, or preferred RMM toolkit)
- ▲ Cost of SentinelOne 'Complete' EDR agent
- ▲ Cost of Adlumin MDR Advanced agent
- ▲ 365-day retention of log data
- ▲ MSP labor for tasks to be completed outside of MDR SOC team – as per rules of engagement determined during onboarding process

*The pricing above is based on using N-able's solutions (RMM, SentinelOne, Adlumin MDR) and N-able's USD MSRP pricing as of June 2025. Cost and pricing may be different if MSP utilizes a different set of security tools and RMM.

Out of Scope Items:

- ▲ Creation of custom detections and SOAR actions for unique environments (additional T&M charge)
- ▲ Email and browser security or support
- ▲ Incident response actions that require remediation or mitigations applied outside of MDR
- ▲ DNS filter / content filtering not included – additional charge for those security toolsets
- ▲ Vulnerability management, penetration testing not included – additional charge for those actions

Support Entitlements–In-Scope vs. Out-of-Scope Support Elements:

- ▲ SOAR playbook of automated responses, is included in the monthly fee
- ▲ Human intervention is also included in the monthly fee to:
 - ▲ Neutralize and stop the breach
 - ▲ Give an explanation on how and why the breach occurred
 - ▲ Give recommendations on what actions are needed next to ensure the same breach doesn't happen again
- ▲ Monthly fee does not include completing the actual work to implement the recommendations provided-that is considered incident response and would be a billable service for the MSP OR the MSP can advise the internal IT department on what actions are required next to complete a full recovery

Co-Managed MDR Service Sample Statements of Work (SOW)

To help to better define the roles and responsibilities for each team, we have created a sample SOW for you to customize:

You can access the sample Co-managed MDR Service Statement of Work [HERE](#)

Co-Managed MDR Training Resources

If your MSP is looking for additional assistance on how to leverage Adlumin MDR, our Head Nerd Team can assist

Co-Managed MDR Boot Camps:

- ▲ SIEM > SOC > SOAR > Compliance:
Can you Build It All In One Day?
- ▲ Accelerate Your Growth with
Adlumin MDR
- ▲ [Live Product Demos](#)

[Register Here](#)

For N-able Partners, you can access these Boot Camps on demand within our [N-ableME](#)

For live product demo of MDR

[https://www.n-able.com/
product-demos](https://www.n-able.com/product-demos)



For additional information around how to build and price your co-managed MDR program, please visit N-ableU to access the on-demand recording of:

Co-managed Services - Part 1 - Top Programs & Pricing



If you require assistance creating your own pricing structure for MDR, you can [access our Co-managed Costing Calculator](#)

Part 2:

Developing Your Go-To-Market and Sales Strategy

Developing Your Go-To-Market (GTM) Strategy

Once you have designed your security programs, you can then begin building each co-hort's go-to-market (GTM) strategy.

An MSP's GTM strategy is a step-by-step plan for launching a new product or service, or it can be used to expand into a new marketing with an existing product or service.

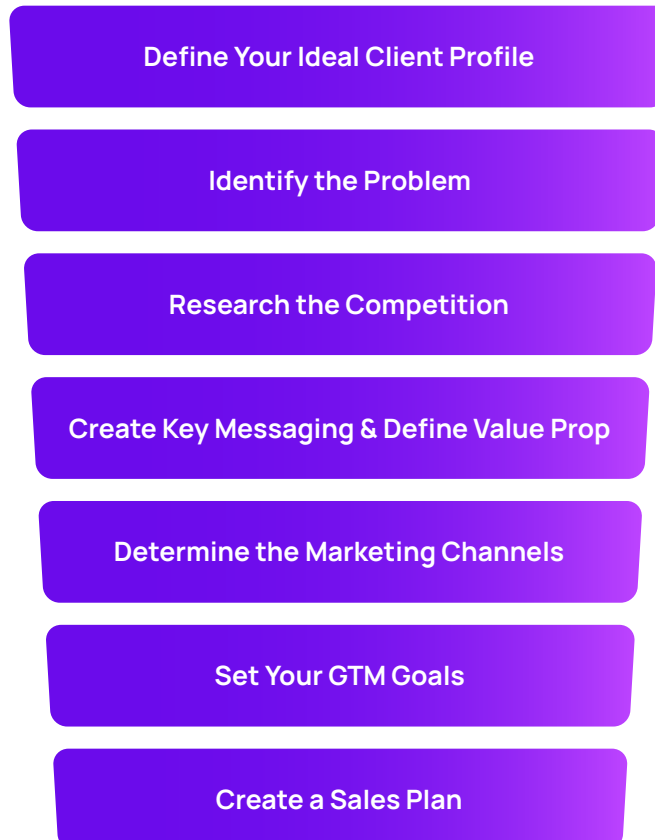
Your GTM strategy is typically tailored for a specific launch, focused on a certain activity or campaign, over a prescribed period of time.

There are 7 steps to crafting your GTM strategy to help launch your new security services. The details of each step will differ depending on who the MSP is targeting.

To help you formulate your GTM strategy, we have created a Go-to-Market Planning Guide for you to use to help document your plans and ideas. **You can access the GTM Planning Guide [HERE](#).**

FIGURE 1

Developing Security Campaigns



Developing a GTM and Sales Strategy for Selling an Identity Protection and/or an Advanced Security Program

Step 1: Defining the Ideal Client Profile (ICP) and Target Audience

Section 1 of this playbook details the ideal client profile for both the Identity Protection Program and the Advanced Security Program. But the primary differentiating factor between the two audiences is whether the customer resides in a regulated industry or not.

If the customer or prospect you are speaking with resides in regulated industry and is required to demonstrate and prove compliance to auditors, then the Advanced Security Program should be positioned, as this is the program that has been designed to best support organizations from a security and compliance perspective.

Step 2: Identify the Problem

In this step, the MSP will want to identify the purchasing triggers and pain points of their traditional managed services target audience to help create key messaging and value prop statements needed to help promote their Identity Protection and/or Advanced Security Programs.

Your Security Programs aim to solve the top security challenges experienced by Business Owners/CEOs and the Executive Leadership team. We can think of these as being the 'purchasing triggers' that we need to help solve via one of our security programs.

Potential Purchasing Triggers

- 1 Has the prospect experienced a potential or a confirmed breach via their existing MSP, where that experience has caused them to question the skillsets, capabilities, processes, and/or procedures of their MSP?
- 2 Has the prospect experienced a failed or unacceptably slow recovery of data or devices after an incident?
- 3 Does the prospect have concerns that their existing MSP is not well equipped to help them prevent an attack that could potentially lead to lost or stolen company data?
- 4 Does the prospect have concerns that their network and data are not as secure or as protected as they should be from online threats?
- 5 Does the prospect have concerns that their employees are lacking proper security awareness training, because it is a service that their MSP is currently not delivering or offering?
- 6 Does the prospect operate a hybrid workforce and have concerns around how to keep their employees and their organization's network and data safe and secure while their employees work remotely?
- 7 Does the prospect require cyber liability insurance, but is unsure how to complete the application process or what is needed to qualify for cyber liability insurance?
- 8 Does the prospect have concerns that their existing MSP is not sufficiently knowledgeable about their industry and what is needed to help them demonstrate and prove compliance, should they be audited or experience a cyberattack or breach?
- 9 Has the prospect been mandated by their compliance regulations that they must enhance their existing security protocols, as they have been found to be weak and/or non-compliant?
- 10 Does the prospect express concerns that they never hear from their current MSP, and are feeling 'forgotten'?

Step 3: Do Your Research

To determine where and how to best position your new layered security programs, you will want to conduct both external and internal research first to see what sort of competition you might be up against and where your sales opportunities lie.

External Research: Used to Target Net New Customers to Your MSP

Questions to be considered include:

- ▲ What are other MSPs in your market currently offering from an outsourced perspective?
- ▲ How do their security bundles compare to yours?
- ▲ What vertical markets, role types, geographic regions are your competitors targeting?
- ▲ How well is your competition doing at promoting their security programs?
- ▲ What kind of marketing and promotion activities are you seeing being advertised as it relates to their security services?

To help with this research, it would be good to review your competition's websites and social media feeds like LinkedIn and Facebook to see if there are mentions of a dedicated security focus in their material. This research will be useful for when you decide that you are ready to starting targeting net new organizations for your MSP.

Internal Research: Used to Identify Upsell/Cross-Sell Opportunities Within Your Existing Customer Base

Then, you will want to conduct some internal research to evaluate where your existing customers currently sit from an advanced security perspective, as this will help you to develop a plan to cross-sell/upsell those customers into one of your new security programs to improve the monthly fee they are currently spending with you.

To help with this exercise, you are encouraged to create a Services Whitespace Matrix. The purpose of this matrix is to quickly identify what customers are buying what services from you, and conversely, to see what services your existing customers are currently NOT buying from you. And then for each customer, you would tally up their monthly spend.

Depending on the amount of whitespace identified (meaning more whitespace, the less number of services the customer is currently paying for, and therefore the greater the sales opportunity that exists), will help set priorities around which of your existing customers you should be reaching out to schedule a meeting with first. The goal of these meetings is to upgrade and standardize all your existing customers into either your Identity Protection or Advanced Security Program based on the Ideal Client Profile defined back in Step 1 for each program level. (i.e. if they operated in a regulated industry = Advanced Security Program ; if they operate outside of a highly-regulated industry = Identity Protection Program).

It's very easy to create a Services Whitespace Matrix:

- 1 Open Excel and start a new spreadsheet
- 2 Along the top, list out every single MRR service you sell individually
- 3 Down the side, list out all of your customers
- 4 For each customer, check off those services that they are paying for today
- 5 Tally up their MRR spend with you

When completed, you should have something that looks like the illustration below. Goal is to use this chart to start calling customers to book meetings to discuss enrollment into one of your new MSP security program.

Customer Whitespace Opportunities Matrix

Customer Name	Service 1	Service 2	Service 3	Service 4	Service 5	MRR Value
ABC	X		X			\$
DEF		X		X	X	\$
GHI	X	X	X		X	\$
JKL						\$
MNO		X				\$
PQR				X		\$
TUV	X		X			\$
WXY						\$
ZZZ			X		X	\$

Step 4: Creating Key Messaging and Defining Your Value Prop

This involves taking the pain points/purchasing triggers that have been identified back in Step 2 and pairing each of those purchasing triggers with a top benefit of your outsourced security programs. Combining these pieces together, will help you create the key messaging that can be used in your sales and marketing messaging and layered security campaigns.

Here are some examples of security-specific messaging statements that can be used to build a layered security marketing and sales campaign.

Purchasing Trigger #1 – The Prospect has experienced a potential or confirmed breach where they are now questioning their existing MSP's capabilities.

Key benefit your layered security program can provide: With the advanced security program, and the layered approach taken to developing the program, a holistic philosophy was implemented to safely secure an organization's network. Through the use of the right toolsets, employing the right people and leveraging the correct cybersecurity best practices, the aim is to provide confidence and remove uncertainty.

Key Message

"Have you experienced a security incident or cyberbreach in the past? Do you have concerns that you could be targeted again? Look for a partner that can help you regain trust and confidence in your security measures. With our advanced security program, we have the toolsets and the skilled security professionals that you can rely on to provide the highest level of protection coverage you require. We can detect and neutralize a threat within seconds, before it can compromise your network, impact your employees or wipe out your data."

Purchasing Trigger #2 – The Prospect has concerns that their employees are lacking proper security awareness training as it is a service that their existing MSP is currently not providing or doesn't offer.

Key benefit your layered security program can provide: Security awareness training is a cornerstone of your advanced security program as it is critical to build a human firewall to help reduce breaches.

Key Message

"Your employees are your first line of defense when it comes to properly securing your network and protecting your organization's critical data. Arm them with the correct knowledge to help defend against phishing attacks and cyber threats. Consider enrolling in our advanced security program where we emphasize the importance that regular security awareness training can play in reducing your organization's cyber risk by changing employees' behavior and equipping them with the essential skills needed to safeguard your sensitive data and assets."

Purchasing Trigger #3 – The Prospect operates a hybrid workforce and is worried about how to keep their employees and organization's network and data safe while employees are working remotely.

Key benefit your layered security program can provide: With the advanced security program, and its proactive threat monitoring, detection and response capabilities, organizations can confidently embrace the hybrid work model, without compromising their overall network security.

Key Message

"The hybrid work model has become a mainstay for many businesses operating today. While employees enjoy the freedom and flexibility the model provides, the steps required to keep remote and hybrid workers safe online are constantly evolving. Through enrollment in our advanced security program, we can provide the protection coverage your employees need to work from anywhere and remain productive, without compromising on security. Safeguarding your organization's data while providing a seamless remote work environment for our employees is our #1 priority."

Purchasing Trigger #4 – The Prospect has concerns that their existing MSP is not sufficiently knowledgeable about their industry, and what is needed from a compliance perspective to help them demonstrate and prove compliance, should they be audited or experience a cyberattack or breach.

Key benefit your layered security program can provide: Through enrollment in the Advanced Security Program, that includes the MDR service and compliance insights, you will be able to proactively help customers in regulated industries demonstrate and prove compliance when required.

Key Message

"In today's highly regulated landscape, demonstrating and providing compliance can seem like a complicated issue, but we can simplify it for you. With our [XX] years in the [INSERT INDUSTRY], we have curated a deep understanding of its unique regulatory requirements and compliance challenges. Our team of security and compliance consultants not only remain up-to-date with the latest industry standards, but through enrollment in our Advanced Security Package that includes Compliance Insights, we can properly prepare your organization for audits while helping you avoid potential cyberincidents. We truly understand the [INSERT INDUSTRY] and its demands, so you can have the confidence and peace of mind that your compliance needs will continually be met."

Purchasing Trigger #5 – The customer or prospect is looking to acquire cyber liability insurance, but is unsure how to complete the application or what is needed to qualify for cyber liability insurance.

Key benefit your layered security program can provide: No organization when they experience a cyberattack or data breach wants to be told that their cyber liability insurance payout is going to be denied, due to failure to meet certain requirements. With the advanced security program, it has been designed to align to the cyber liability insurance application requirements to provide peace of mind that should an organization experience a data breach and require financial assistance to properly recover, will have their claim promptly paid out.

Key Message

"Cyber liability insurance is quickly becoming a key piece in helping organizations mitigate their downtime and financial risks when it comes to recovering from a cyberattack or data breach.

Continuation...

Also, many different compliance regulations are now mandating it for their respective industries. But without having the correct cloud, network and endpoint security protection in place, you could be in serious jeopardy of having your cyber liability claim denied, which could put your organization in serious financial hardship. With our support, we can guide you through the application process and help you understand the cyber liability insurance qualification requirements so you can feel confident that your organization has the proper protection coverage it needs.”

Step 5: Selecting the Appropriate Marketing Channels

This step is all about deciding what marketing channels will be the most appropriate to use to help build awareness and promote your layered security program offerings to both your existing customers, as well as when you begin targeting net new organizations for your MSP.

Marketing channels refers to the different types of content you will use to create demand for your services to help move potential customers through the marketing and sales funnel until they hopefully become a new, signed contract.

Examples of different types of marketing channels include:

- ▲ Social media
- ▲ Paid search ads
- ▲ Email
- ▲ SEO optimized content to drive traffic to your website like blog posts

Layered Security Marketing Collateral

To help market and promote your layered security programs, we have created several campaigns and collateral pieces for you to brand and customize, and these can be found within our [N-able MarketBuilder](#) platform.

PLEASE NOTE: This platform is available to every N-able partner.



Within MarketBuilder, you can find the following campaigns:

- ▲ [Layered Security Campaign](#)
- ▲ [IT Support Essentials Campaign](#)
- ▲ [IT Compliance Campaign](#)
- ▲ [Cybersecurity Awareness](#)
- ▲ [Cyber Insurance Campaign](#)
- ▲ [Hybrid Workforce Campaign](#)
- ▲ [Managed Security Campaign](#)
- ▲ [Managed Security Campaign \(UK Partners\)](#)
- ▲ [The essential 8 \(Australian Partners\)](#)

Plus there are several verticalized campaigns targeting:

- ▲ [Healthcare](#)
- ▲ [Healthcare Campaign \(Canadian Partners\)](#)
- ▲ [Healthcare Campaign \(UK Partners\)](#)
- ▲ [Dental](#)
- ▲ [Financial Services Companies](#)
- ▲ [Insurance](#)
- ▲ [Local Government](#)

And each of campaign contains:

- ▲ Sample Emails
- ▲ Landing Page
- ▲ Social Media Posts
- ▲ Sell Sheet
- ▲ Presentation Deck
- ▲ Word Docs (to gain access to the verbiage, but utilize your own branding)

One useful piece within MarketBuilder as it relates to SEO optimization that should be highlighted is that for each MarketBuilder campaign, it provides sample keywords to include in any content you create that will help your website be found by prospects searching for IT, security and compliance support on the web.

Looking in MarketBuilder, sample Keywords and phrases that could be included in your marketing copy for your layered security campaigns includes:

- ▲ Risk Management
- ▲ Network Security
- ▲ Advanced Cybersecurity
- ▲ Cybersecurity
- ▲ Compliance consulting

The different marketing channels you decide to use to promote your layered security programs will depend on your target audience and where your potential customers are in their buying journey

Step 6: Create the Sales Plan

The primary goal of this security sales playbook is to help you build and ultimately sell one of your new layered security programs. So, step 6 of your GTM plan is mapping out what your sales strategy will look like. Initially, you will want to create two separate sales plans—one targeting your existing customers and another one targeting net new organizations.

Developing a Sales Plan to Target Existing Customers

Embrace the Power of the Executive Business Review

If selling security-centric managed services programs is relatively new for you, it is recommended that you focus on targeting your existing customers first, based on the direction provided from the Services Whitespace Matix exercise that was completed back in Step 3.

Your existing customers already know your organization and the quality work that you do—you have built a relationship with them (and hopefully a partnership). As a result, these are the perfect set of businesses to 'practice' on. They can ideally provide you with constructive feedback and advice that you can incorporate into your sales and technical processes, for when you begin selling to organizations that are not familiar with your MSP at all.

As an example, your existing customers can help prepare you and your team for the various objections you will likely hear, so that you can practice how to address the push back you may receive, especially when you introduce the new pricing structure around your redesigned programs.

You can also use your existing customers to help your team iron out the technical deliverables and onboarding processes if these have changed. You can leverage these customers to provide real-world training for your techs and service desk staff, especially if you have introduced new technologies into your security tech stack that you may not have been using previously.

From a marketing perspective, after a period of soaking time, you can solicit testimonials and reviews from your existing customers and develop case studies that can be posted to your website and social media feeds that can then be referenced when you are ready to start selling to net new clients.

To help with this exercise, we have created a set of campaigns within [MarketBuilder](#) that can be used when targeting existing customers. These campaigns can be used to help line up those initial meetings with your existing customers to discuss your new set of programs with them. These can also be used in conjunction with the Layered Security Marketing Campaigns mentioned in the previous section:

- ▲ [Re-engagement – Managed Services Campaign](#)
- ▲ [Virtual Chief Information Officer \(vCIO Campaign\) – Managed Services](#)
- ▲ [Executive Business Review – Managed Services](#)

We also have a Head Nerd Boot Camp focused on how to structure and deliver Executive Business Reviews (if this is something your MSP doesn't perform regularly). It is called: Cracking the Code to Building Loyal Customers and can be found within [N-ableU](#).



As you begin lining up review meetings with your customers, there are a few strategies that can be employed to help jumpstart the security conversation. These strategies will help to position your new security-centric packages and provide you with the opportunity to explain why it is necessary that they be transitioned over to one of these new packages as soon as possible.

Conversation Starters to Introduce Your Layered Security Services to Existing Customers

Strategy #1: Discuss the ever-changing threat landscape

Review the latest Cybersecurity Reports to remain update on the Current Threat Landscape such as:

2025 Verizon Data Breach Investigations Report:

<https://www.verizon.com/business/resources/reports/dbir/>

2024 Microsoft Digital Defence Report:

<https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024>

"Mr. Customer: I'm sure you're hearing and reading in the news how prevalent security attacks are becoming. Security data breaches are getting to be more and more commonplace these days. According to the 2024 IBM Cost of Data Breach Report, it reported that that global cost of a data breach increased 10% in 2024, costing organizations on average of USD \$4.88 million – which has been the biggest jump since the pandemic. This was driven by increased business disruption and post-breach customer support and clean-up expenses.¹

Looking at some other stats:

- ▲ There are nearly 20 ransomware attempts reported every second.²
- ▲ Ransomware continues to be a significant threat to businesses of all sizes, but is disproportionately affecting smaller organizations—in larger organizations, Ransomware is a component of 39% of breaches, while SMBS experienced Ransomware-related breaches to the tune of 88% overall.³
- ▲ When it comes to cybersecurity threats, social engineering continues to be another top threat targeting organizations—more than 90% of cyberthreats in 2024 were social engineering threats preying on human nature, getting users to click on malicious links, share passwords or download malware. ⁴
- ▲ And these cybercriminals are relentless as the average time between cyberattacks is a mere 39 seconds.⁵

So, seeing all of this unfold, it has become evident that we need to update our monthly services packages to make them more security-centric to provide better protection coverage, as we do not want any of our customers to fall victim to a cyberattack and becoming a statistic.

Unfortunately, what we had been recommending previously is no longer sufficient, and so we now need to update our security recommendations to accommodate this ever-changing threat landscape.

As such, I would like to schedule some time with you to review what you currently have in place and explain what we will be adding to your monthly package to help reduce your risk of attack.

1 <https://www.ibm.com/downloads/documents/us-en/107a02e94948f4ec>

2 2021 Cybersecurity Statistics The Ultimate List of Stats, Data and Trends," PurpleSec LLC. <https://purplesec.us/resources/cyber-security-statistics/> (Accessed May 2021).

3 2025 Verizon Data Breach Investigations Report <https://www.verizon.com/business/resources/reports/dbir/> (Accessed July 2025)

4 <https://www.gendigital.com/blog/insights/research/q2-2024-cybersecurity>

5 <https://www.getastra.com/blog/security-audit/cyber-security-statistics/#:~:text=160%20Cybersecurity%20Statistics%202025%20%5BUpdated%5D&text=Search%20for%3A160%20cybersecurity%20stats%20for%202025>.

How to Educate Prospects and Customers About the Current Threat Landscape to Help Them Adapt to This New Era of Cybersecurity

**This comes from the [Verizon Data Breach Investigations Report](#).

It is a very different world that we are all living in today, and it continues to evolve daily. With the rise of hybrid and remote work environments, organizational networks have become increasingly more and more complex. This shift has significantly expanded the attack surface, creating more entry points that cybercriminals can exploit to gain unauthorized access into corporate environments.

This increase in the number of different infiltration points puts each of the different layers surrounding a company's employees and data and the outside world increasingly more at risk of being breached, so it is important to educate prospects and customers that your services must now go beyond traditional defenses to proactively address this dynamic threat landscape and must now include services to prevent, detect, thwart, and neutralize a wide range of different threat vectors – each designed with the singular goal of breaching your customers' networks to disrupt operations and exfiltrate sensitive data.

So, when we look at the most prevalent ways that cybercriminals are leveraging to access company networks:

1 System Intrusion Attacks (Purple Blocks)

These are complex attacks that leverage malware (in the form of ransomware) and/or hacking attempts (via the use of stolen user/password credentials) to gain access into a victim's network. Also includes attempts to exploit unpatched vulnerabilities found in such software assets like: Web applications, VPN software and Desk Sharing Software. Vulnerability exploitation remains one of the most common root causes of ransomware attacks as ransomware threat actors are finding that unpatched vulnerabilities are a very lucrative path to gaining access to company's network to initiate a breach.

2 Social Engineering Attacks (Light Green Blocks)

This includes attacks like Pretexting, Business Email Compromise, and Phishing. For Pretexting and Business Email Compromise attacks, this is when threat actors target users with existing email chains and context to trick victims into doing something, because the recipient of the email believes 'the ask' is legitimate. The employee believes 'the ask' is coming from someone of position and authority within their company—like a CEO/CFO or Accounting Manager. So, believing the email is legitimate, they will use the email to act on instructions like: Update a certain bank account associated with a deposit or they will act on instructions to wire money out of the company to pay a fake, outstanding invoice—when in reality, these company figure-heads made no such requests. It is the result of their email accounts getting compromised somehow, and it was the cybercriminal that sent out the email and made the request.

3 Basic Web Application Attacks (Blue Block)

This is where threat actors use compromised credentials to gain unauthorized access to cloud-based email and collaboration accounts. With these types of attacks, threat actors are leveraging devices with default, simplistic and easily guessable credentials to gain access into a victim's network or gain access to their personal, financial, and other valuable data. These types of attacks are typically not terribly complicated attacks—they are the result of the organization having either unprotected or poorly protected web applications in place, making it fairly simple for threat actors to get into the victims' environment by either acquiring the necessary credentials through brute forcing them, buying them or reusing them from previous successful breaches.

4

MFA Bypass (Pink Block)

Despite having MFA in place, it is not foolproof. Cybercriminals have developed techniques to bypass it to gain entry into a company's environment, so it has become another attack path that organizations and MSPs need to contend with and monitor.

5

Human Errors/Honest Mistakes (Light Purple Blocks)

These are simple mistakes that employees could make, but are unintentional in nature. Mistakes like: A System Admin misconfiguring something that inadvertently allowed a threat actor in, or a employee accidentally sending something out to the wrong recipient, or events like laptops being lost or stolen where a data breach was reported because someone accessed the data on the device that they shouldn't have been able to.

6

Privilege Misuse (Red Blocks)

Breaches that occur due to unapproved or malicious use of legitimate privileges or where employees steal company data for their own personal or financial benefit.

7

Denial of Service Attacks (Dark Green Blocks)

These types of attacks aim to overload a device, a website or a network, with the goal of degrading its performance or making it completely inaccessible by its intended users. DoS attacks work to compromise the availability of the organization's network and its systems, and they can target different points of the infrastructure and can manifest themselves in several different forms. As these types of attacks are relatively cheap to execute, and come with a high rate of success, they are posing greater risks to business availability than ever before.

8

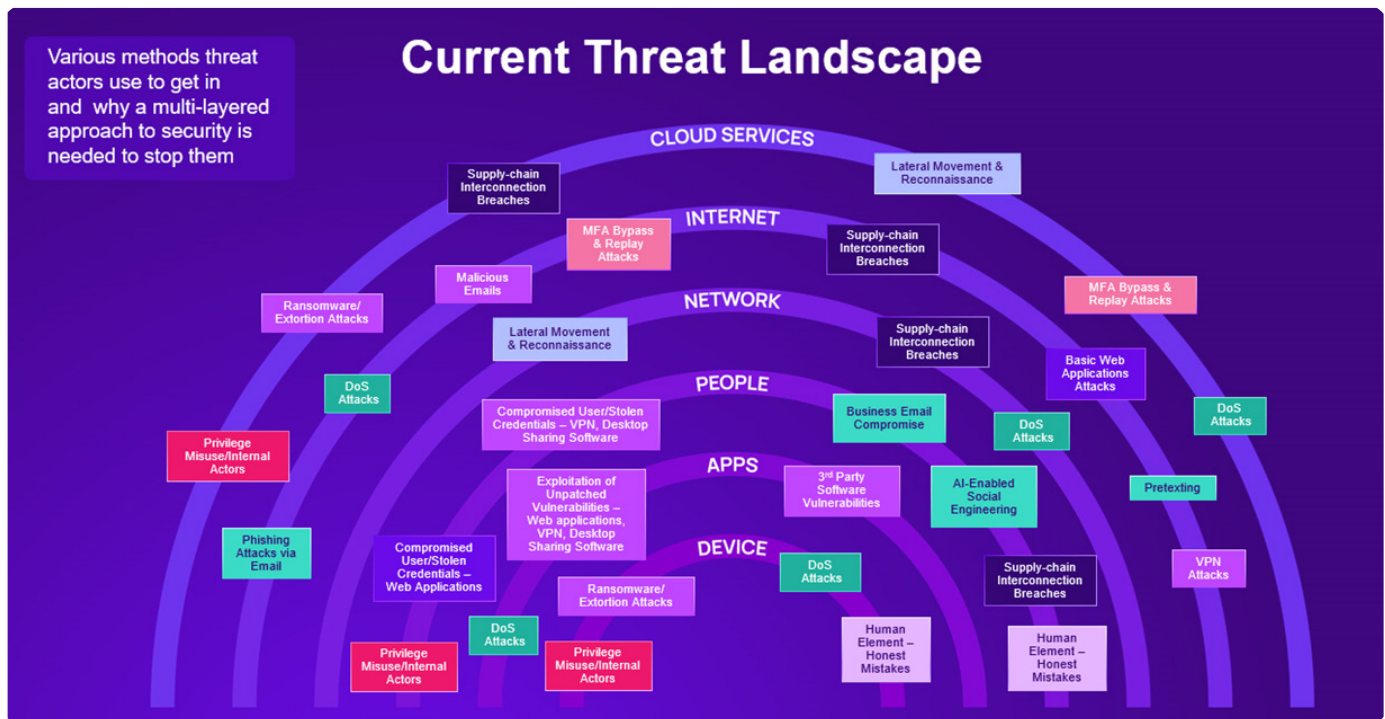
Supply Chain Interconnection Breaches (Dark Blue Blocks)

This kind of breach occurs when a business partner was the point of entry and the gateway for the breach. It fails to recognize how interdependent organizations can be on one another, and how important it is for organizations to comprehensively vet any future strategic partner, especially the security standards and protocols they subscribe to. If the strategic partner's security standards are lacking, they represent a huge hole in the other organization's cybersecurity defenses. So, when a customer tells you that they are too small or who would want their data, ask them what kind of vendor or supplier relationships they have place? Although they may not be the intended target, threat actors may be very interested in who they have close business dealings with-so it is critical that your customers not be the weak link and the gateway into the vendor/supplier's network.

9

Lateral Movements/Reconnaissance (Light Blue Blocks)

It is one set of challenges to do what you can to keep the threat actors out of your customer's network and away from their data, but if they are still able to get in, masked as a legitimate user—the challenge now becomes: How do you find them? How do you track them to see what they are up to? It is possible that threat actors can make their way into the network unknowingly and not cause any real problems in the beginning because they are focused on quietly doing their pre-attack prep work to see what kind of data they can find, and where that important data is being stored. Without proper security monitoring in place for this type of scenario, it could be months before anyone becomes aware of the threat actor's existence—so this could become a real blind spot for organizations if they are not watching for this.



Strategy #2: Leverage YOUR knowledge of THEIR industry

"Mr. Customer, I know that you are part of XYZ industry and unfortunately, we haven't been doing a great job advising our clients on how to best help them adhere to the various compliance standards and regulations by which businesses in your vertical need to abide.

We are looking to change this through the introduction of our new Advanced Security Program that includes monthly compliance insights. This is a new program on which we are standardizing all our clients.

I would like to schedule some time with you to review what you currently have in place today, and explain what we will be adding to your monthly package to help you better adhere to the compliance standards that are in place for your industry."

Strategy #3: Leverage COMPLIANCE to highlight WHY things need to change

"Mr. Customer, as a business operating in XYZ industry, compliance standards state that organizations in this vertical need to collect and aggregate log data from their network, and then be able to show proof that they can use that log data to investigate an incident on their network should a breach occur.

As your MSP, one of our jobs as your cybersecurity advisor is to be able to help you prove that you can demonstrate compliance when you are asked to do so. With the existing security package you are enrolled in, we are unable to accomplish this for you, so you are at risk of being labeled "non-compliant" and could possibly face fines.

We don't want this to happen to you. Therefore, we need to transition you to our new Advanced Security Package where we can implement the right set of toolsets, processes, and security controls so, in the event of a breach, we can extract the necessary data needed to investigate the attack.

Unfortunately, organizations that operate in regulated industries don't get a choice as to whether or not they wish to be compliant. So, I would like to set up a time for us to meet so we can review what these new changes will be, and what the new security controls will look like moving forward."

Strategy #4: Leverage cyberinsurance to introduce your new security programs

Are you finding that your customers are coming to you with a cyber liability insurance questionnaire in hand, and they are looking for your help to complete?

Or maybe you start to make cyberliability insurance for their business a requirement of all of your customers, if they are to remain a client of yours?

The items referenced on the cyberinsurance questionnaire are the same security control items being requested for compliance purposes and align to the features and services that have been included in the Essentials and Advanced Program.

As a result, if a customer comes to you requesting help filling out their cyberinsurance questionnaire—and you know that they are not enrolled in one of your layered security programs—then this is your opportunity to start that conversation with them about one of your new security programs.

Explain that insurance companies mandate that a certain set of requirements are to be in place to prevent and promptly recover from cyberattacks, and if an organization doesn't abide by these requirements, it can invalidate their insurance policy, and this is something you never want the customer to have to experience.

So, politely explain that they will need to be enrolled into one of your layered security programs first, as you will be unable to complete the questionnaire accurately until that transition takes place.

Strategy #5: Ask about future projects or expectant changes in their business

"Mr. Customer, do you have any upcoming projects that you are planning or expecting any significant changes in your business that might impact your cybersecurity requirements or expose your organization to increased risk?"

If so, we should schedule a time to meet to discuss what those anticipated changes are so we can ensure they are in line with our own security recommendations. This will ensure that we implement the correct cybersecurity protection coverage to accommodate these upcoming changes so that you remain secure."

This is a backdoor way to bring about the security and risk conversation as you can incorporate your security upgrades into the overall project design. As you are talking about what the various steps are to implement the different phases of the project, you can align the security conversation alongside those phases.

Developing a Sales Plan to Target Net New Customers

Once you have standardized all of your existing customers onto either your Essentials or Advanced Security Program, you are ready to start targeting net new organizations with your security services!

This is where launching a campaign targeting those organizations that have made your 'Dream List' and inviting them to an in-person event (like a Lunch N Learn) or a virtual webinar will work well as it will give your sales team a purpose and a dedicated focus. Instead of having just a general outbound calling campaign to talk about security and compliance, your sales team can call on prospects to invite them to your event. It will give them something tangible, educational and fun to promote.

A sample sales plan could be:

- ▲ Business Owner, sales leadership, sales teams, Sales Development Representatives (SDRs) work together to create a prospect list of companies and individuals to call to invite to the event
- ▲ The SDRs (or other sales-designate) proceed with a proactive, outbound calling campaign to invite prospects to the event
- ▲ At the event, the sales team is responsible for introducing themselves to prospects, building interest and attempting to schedule 1:1 discovery meetings with potential customers post-event
- ▲ Salesperson and/or Business Owner attends the initial discovery meeting to determine if there is a need for one of their layered security programs, and if there is a good fit between the two organizations
- ▲ And if there is a good fit, the Salesperson/Business Owner would proceed by moving forward into the next phase of the sales process, where they would time to book a cyber and business assessment to get a better understanding of their cyber risk exposure

Layered Security Scripting for Outbound Call Campaign

If you do not plan on hosting a prospect event, this playbook also includes additional sample scripting that the SDR team can use to proactively call on prospects to discuss your layered security services offering.

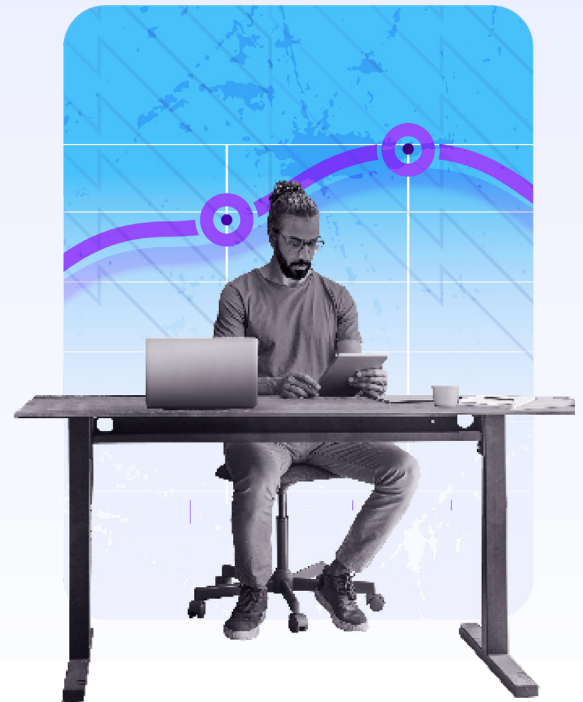
For continued growth, it is useful to have someone dedicated to calling your Dream List of Prospects to help book appointments for yourself or your Account Executives.

If you currently do not have a telemarketing motion established for your MSP and are interested in building one, we have created a Head Nerd Boot Camp that focuses specifically on this topic called:

Cracking the Code to Lead Generation Part 2: Building a Tele-sales Strategy

[Register Here](#)

For N-able Partners, you can access this Boot Camp on demand within our [N-ableME](#).



The goal of this initial call is for the SDR to book an appointment for either the MSP Business Owner or for the Account Executive with the Business Owner/CEO and C-suite team of the prospect's organization to explore if there is a need for your set of security services.

Conversation Starters to Introduce Your Layered Security Services to Prospects

Strategy #1: Inquire about past security incidents

"Mr. Prospect, have you experienced a security incident in the past?"

If so, what was the experience like for you and your team?

On a scale of 1-10, how well do you feel it was handled by your existing MSP?

With our advanced security program, and the tools, people, and processes we have in place, our protection coverage is extensive.

Let's set up a time where we can explain how our services are designed to detect and neutralize a threat within seconds, before it can compromise your network, impact your employees, or wipe out your data."

Strategy #2: Leverage the compliance angle to differentiate your MSP from the competition

Question #1:

"Mr. Prospect, I know that you are part of XYZ industry. How is your existing MSP helping you adhere to the compliance standards that businesses in your vertical need to abide by? And what measures do they have in place to help you demonstrate compliance in the event of a breach?"

Question #2:

"Mr. Prospect, I know that you work with and store valuable customer personal data. What measures does your existing MSP have in place to help mitigate your data disclosure risks from those that might be interested in stealing this type of PII data?"

Continuation...

Question #3:

"Is your current MSP having the compliance conversation with you?"

"Mr. Prospect, we never want our customers to have to face punitive penalties as a result of not having the proper security protocols in place. Let's setup a time to meet to review your existing setup and we can explain how we help our customers demonstrate and prove compliance when they are visited by auditors."

Strategy #3: Focus on the employees and what the incumbent MSP is doing (or not doing) to increase their security posture, so they are not the catalyst to a data breach

"Mr. Prospect, were you aware that 74% of data breaches are caused by people?*

People either make a mistake (doing something incorrectly or not doing something as they should), misuse privileges, use stolen credentials, or fall victim to social engineering and/or phishing techniques.

End-users are a real source of risk for any organization. If we didn't have end-users, we wouldn't be experiencing the heightened levels of security issues we are dealing with today. And without the right protection measures in place, the inherent risk that end-users bring to the table will only continue to keep the organization exposed.

What protection measures does your current service provider have in place to lessen the risk of your employees being the catalyst to a data breach for your organization?"

Strategy #4: Leverage the assessment to highlight gaps in the prospect's security protection coverage that may have been missed by the competition.

Question #1:

"Mr. Prospect, do you any have concerns over how potentially exposed your network might be to an attack?"

Continuation...

Question #2:

"Mr. Prospect, do you have any concerns over how well your current service provider is helping your organization avoid an attack?"

"Mr. Prospect, if yes: Let's setup a time to run a cybersecurity assessment on your network to see where there might be gaps in your protection coverage that your current service provider might have missed.

As part of our assessment process, we can provide you with an overall Network Health Score to confirm how well-positioned your network is in avoiding an attack, as well as how quickly your organization can recover should a data breach occur."

Strategy #5: Leverage the cyber-insurance angle to spark the security conversation to help differentiate your MSP from the competition and weed out prospects that may not be a good fit.

Question #1:

"Mr. Prospect, do you currently carry cyberliability insurance for your business?"

Question #2:

"Mr. Prospect, does your current MSP require that your organization carry cyberliability insurance?"

How the prospect answers this question is one of the best indicators to help you potentially qualify-out prospective customers who may not be a good fit for your services. If the prospect tells you that they don't currently have cyber liability insurance, and that they don't plan to purchase it, then this is a red-flag to stop pursuing them as a potential customer altogether.

Or if the prospect tells you: "I'm hiring you to protect me. So I don't need cyberinsurance. It's on you", this is another red flag where you should take pause before proceeding.

This is where education will be key, as it is evident that there are some misconceptions here that their existing MSP has failed to correct. You will want to educate the prospect on what an MSP's role is when it comes to cybersecurity and where an MSP's responsibilities lie verses where their responsibilities lie in preventing and recovering from an attack, should one occur. Security and risk mitigation is a SHARED responsibility and not all security incidents are preventable, hence the need for cyber liability insurance protection coverage.

Continuation...

An MSP's responsibility is to put in place the correct set of security measures to best mitigate the prospect's chances of falling victim to an attack. And if the prospect does happen to suffer an attack (as nothing provides a 100% guarantee to preventing an attack) then it is through the MSP's advanced security program where they will be able to have them recover as quickly as possible, post-attack, minimizing the length of downtime they'll experience.

It is the prospect's responsibility to carry a proper amount of cyber liability insurance coverage to help pay for the remediation services, if needed, because it is impossible for the MSP to be able to stop everything, even with the best cyberhygiene controls in place.

So, if the prospect still tells you 'no' after this conversation, then you may want to think seriously if this is the type of account you wish to have on the books.

A possible response to provide to the prospect:

"Mr. Prospect, unfortunately, it doesn't appear that our organizations will be a good fit for one another, as we seem to have differing views on how to deal with the cybersecurity risk your organization is currently exposed to.

We run our MSP, and manage our customer's network environment, in a certain way, where security is at the forefront of everything that we do. While I respect your decision as to relates to your stance around security and cyber liability insurance, we are not able to assume the risk your organization would impose on our MSP and our currently clients. But thank for your time and your initial interest in our MSP."

This statement alone could go a long way in helping you change the perspective of your prospect, and actually win the client over, as you are detailing how very different you operate your MSP and how you take care of YOUR customers verses how their existing MSP is treating and taking care of them.

Objection Handling Techniques and Response for Your Layered Security Programs

During the traditional managed services customer sales process, you will likely receive pushback or hear concerns from the Business Owner/CEO. To help you prepare, we have listed below the most common objections you may come across, with some possible sample responses for each.

Tip: Do what you can to capture your prospect's direct quotes as you are speaking with them so you can add these to your proposal that you present to your prospect during the closing stage

12 Most Common Objections

"I thought I was already protected? Are you saying I'm not?"

"I thought you were already taking caring of that?"

"Why do I need to change my services?"

"This sounds much more expensive compared to what I was paying before."

"This doesn't sound worth it to me."

"I can get it cheaper elsewhere." or
"Another MSP is only charging \$X."

"Can I remove some services to better fit my budget?"

"What's wrong with EDR? Now you are saying I need to buy another product?"

"It won't happen to us—we are too small."

"It won't happen to us. Who would want our data?"

"I'll take my chances and pay the ransom and claim through my insurance."

"No. I won't switch/ won't pay for this new program."

OBJECTION #1 & 2:

“I thought I was already protected? Are you saying I’m not?”

“I thought you were already taking care of that for me?”

Sample Response

“You were protected and I was taking care of this for you. But as the threat landscape evolves, so does the technology that is needed to continue providing proper, comprehensive protection coverage—so the services that I provide to my customers have to evolve as well to keep ahead of the bad actors that are out there.

This is just a business to them and they are making a lot of money as result. In 2023, the average ransomware payment was \$1.54 million—almost double the 2022 figure of \$812k¹. But, once you factor in a variety of other costs beyond just the ransomware payment, it can add up to be 7x² the basic ransom demand.

To ensure this doesn’t happen to you and your business, our security packages needed to change, and we now need to enforce stronger measures—not only ourselves as your MSP, but across all of our customers as well.”

¹ <https://www.varonis.com/blog/ransomware-statistics>

² <https://www.netapp.com/blog/ransomware-cost/#:~:text=In%20fact%2C%20the%20average%20ransom,cost%20of%20a%20ransomware%20attack>

OBJECTION #3:

“Why do I need to change my services that I have with you?”

Sample Response

“Things are very different now than what they were 3-5 years ago.

Statistics show that 60% of SMBs go out of business 6 months following a cyberattack,* and we do not want to be a contributing factor to that.

So, what we had recommended as security best practices even last year isn’t what we are recommending to our clients today.

And we will very likely be having this same conversation again next year—where I might have to implement some new security services or make other changes as ransomware attacks, business email compromise, and phishing tactics become more and more sophisticated.

So, as a result of this everchanging threat landscape, as your MSP, I need to keep up to date and keep amending my recommendations to keep our customers’ networks, their employees, and their data as safe and secure as possible.”

*<https://purplesec.us/security-insights/top-cyber-attacks-2022/#Breaches>

Continuation...

The Layered Network illustration can be used to help educate customers around WHY the set of security services now being recommended is changing from what had been recommended previously; and as a result, these new recommendations are impacting the security packages that are now being promoted in market.

When looking at the customer journey with respect to security, 5-10 years ago, the traditional MSP's answer to security was: AV/patch/firewall/and backup. At that time, those services were sufficient, as threats were not as sophisticated, and people were working in offices behind corporate firewalls. But in today's threat landscape, it is no longer enough.

Looking at our layered network diagram, with the old approach of AV/patch/Firewall/backup, there are layers that are left under-protected, and there are layers that are completely unprotected—namely the cloud layer, the internet layer, and the people layer specifically. This has created significant gaps in a customer's security coverage, so the old minimum standard for essential security has to be upgraded, and MSPs need to develop and promote a more comprehensive suite of security services, to plug these gaps that have now surfaced. And the focus needs to extend beyond the endpoint as well.

New Recommendations:

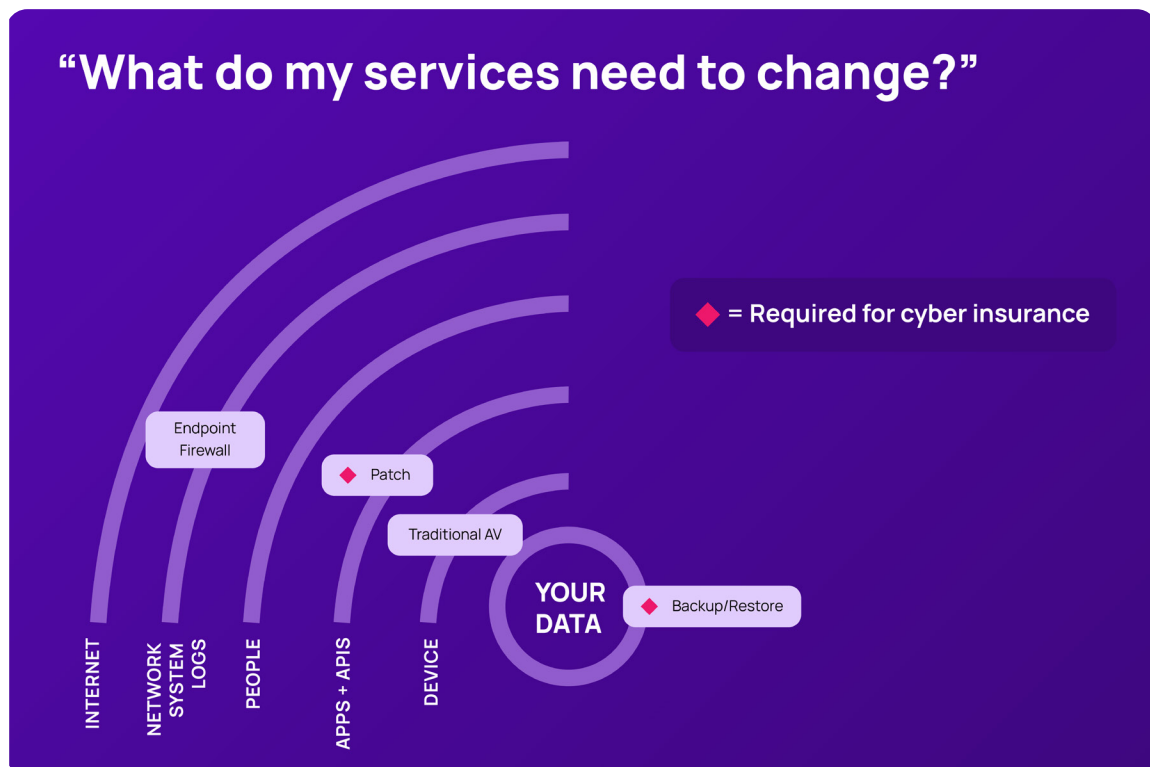
- ▲ **Device Level Changes:** Replacing traditional AV at the device level with a next-gen AV like [EDR](#) to provide a broader, more advanced protection coverage against zero-day threats, and which also includes rollback capabilities to get the device back to a pre-attack, healthy state, should something get through
- ▲ **Internet Level – adding in:**
 - ▲ Mail Security with Email filtering and spam protection
 - ▲ Web Security/DNS/URL filtering and
 - ▲ Dark Web Monitoring
- ▲ **Network Level – adding in:** Network Device Discovery (using something like [SentinelOne's Attack Surface Management](#) product) that will providing alerting whenever any new, unknown devices have appeared on the network like IoT devices, camera systems etc.that might be trying to gain access into the network
- ▲ **People Level – adding in**
 - ▲ [Password management](#)
 - ▲ MFA
 - ▲ Security User Training

Continuation...

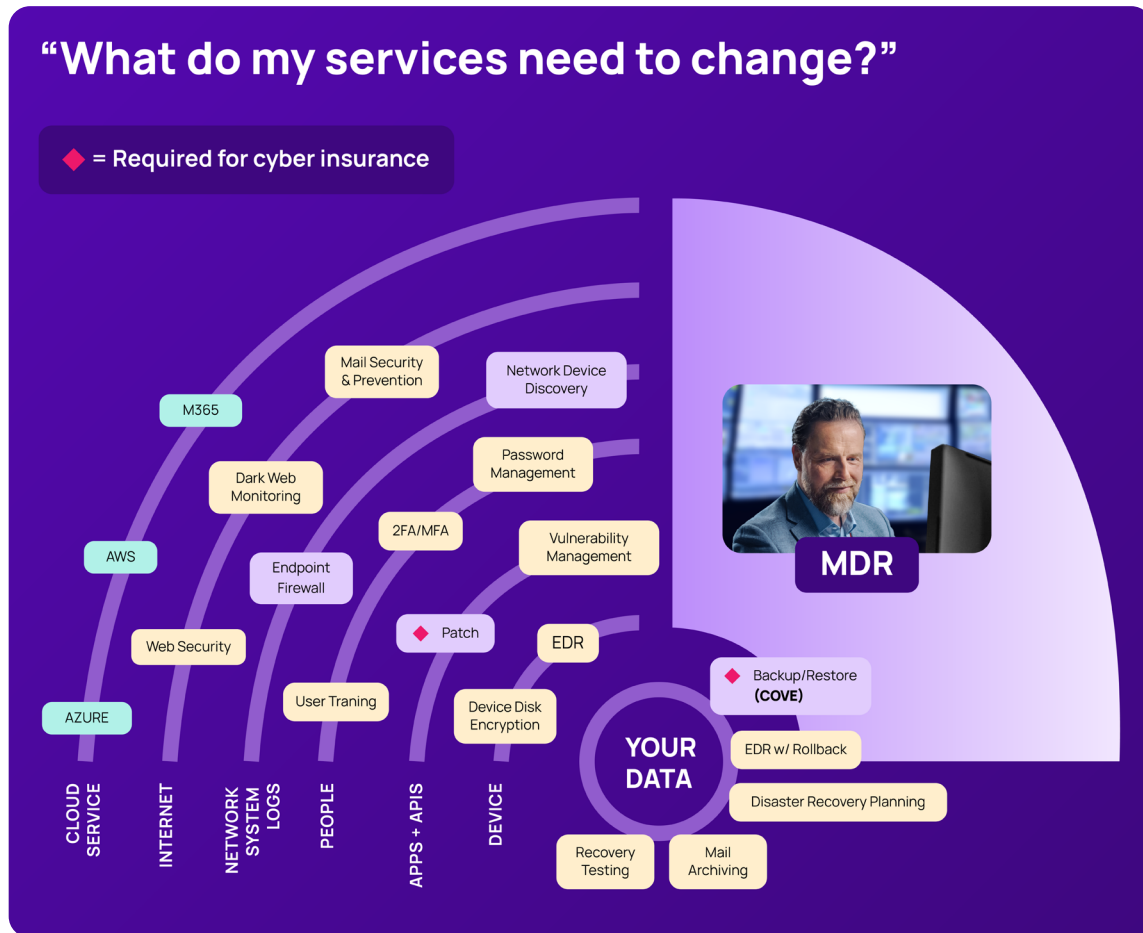
- ▲ Application Level – adding in:
 - ▲ Vulnerability Management
 - ▲ Backup recovery testing with the possibility of implementing standby system
- ▲ Cloud Level – adding in: [Managed Detection and Response](#) to provide heightened visibility, monitoring and detection capabilities, and to extend monitoring and detection from beyond the endpoint

A layered approach to security provides the best defense against cyberattacks as each security solution on its own contains its own set of limitations. The goal is to implement as many hurdles as possible to make it as difficult as possible for threat actors to get through and gain a foothold. Then the MDR is implemented to provide the 'alarm bells' if it detects unusual behavior. Therefore it is not recommended that any security product be sold and implemented in a silo, as nothing on its own can provide 100% guaranteed protection from an attack. A bundled approach/suite of services is needed to truly protect the networks of your highest-risk customers and prospects.

The Layered Network: Old Security Recommendations - Gaps are present – layers left under-protected AND unprotected



Today's Recommended Security Program: Aims to close the gaps to ensure ALL layers are sufficiently protected



OBJECTION #4&5:

“This sounds much more expensive compared to what I was paying before.”

“This doesn’t sound worth it to me.”

Sample Response

- ▲ Demonstrate ROI to help your customer understand the total costs that can be incurred by not moving to your new security package and to demonstrate that it is cheaper to prevent than to pay out
- ▲ Ransomware payment represents only 15% of the total cost of the ransomware attack¹

- ▲ 66% of businesses suffered significant revenue loss post attack¹
- ▲ 53% of businesses reported their brand suffered post-attack²

1 <https://www.bleepingcomputer.com/news/security/ransom-payment-is-roughly-15-percent-of-the-total-cost-of-ransomware-attacks/>

2 https://www.cybereason.com/hubfs/dam/collateral/ebooks/Cybereason_Ransomware_Research_2021.pdf

Showing ROI Via Cost of Downtime Exercise (per day)

Downtime Cost = Lost Employee Productivity + Lost Revenue + Costs to Recover + Cost of Intangibles

A copy of the ROI Downtime Calculator can be accessed [HERE](#)

Step 1: Calculate Cost of Lost Employee Productivity (USD)

ROI - Cost of Downtime - Security Angle	
Employee Productivity Costs	
Department Impacted by Downtime	ALL
# of Employees in Company	40
# of Employees in Affected Department	40
Average % of lost productivity	100%
Average Cost of Employees per hour	\$50
# of Total Downtime Hours	160
Employee Productivity Costs	\$320,000.00

Example:

- ▲ Accounting firm prospect with 40 employees
- ▲ Average wage cost = \$50/hour

Continuation...

- ▲ Situation: An employee clicks on a link in a phishing email they received, which sparked a chain reaction and caused all employees to be locked out
- ▲ Assumption: Length of downtime incident is 30 days
- ▲ Total # of downtime hours is: $8 \text{ hours a day} \times 5 \text{ days a week} \times 4 \text{ weeks} = 160 \text{ hours}$

Employee Lost Productivity costs = \$320,000

Step 2: Calculate Lost Revenue Costs (USD)

Lost Revenue Costs	
Gross Annual Revenue	\$1,000,000.00
# of working days per year for the business	240
# of working hours per day	8
What % of lost business is irrecoverable?	100%
Lost Revenue Per Day	\$4,166.67
Lost Revenue Per Hour	\$520.83
Lost Revenue for Duration of Outage	\$83,333.33

- ▲ Prospect's Annual Gross Revenue = \$1M/year
- ▲ Assumption: Number of working days per year is = 240 days
- ▲ Assumption: Number of working hours per day = 8
- ▲ Assumption: % of lost business potentially irrecoverable = 100%

Lost Revenue for Duration of Outage = \$83,333

Step 3: Calculate Remediation Costs (USD)

Remediation Costs	
Total # of Labor Hours to reach full recovery	\$160
Hourly Labor Rate for Recovery Services	\$150
Total System Recovery Cost (Remediation Costs)	\$24,000
Total Cost of Downtime	\$427,333,33
Total Cost of Downtime/Hour	\$2,670.83

- ▲ Total # of Downtime Hours (from above) = 160 hours
- ▲ T&M bill rate = \$150/hr

Total System Recovery Costs i.e. Total Remediation Costs = \$24,000

Total Cost of Downtime = Cost of Lost Employee Productivity + Lost Revenue + Remediation Costs = \$427,333

Hourly Downtime Cost = \$2670/hour

Step 4: Calculate the Costs of Intangibles

Other Costs to be Factored In (In the Event of Security Breach)	
Cost of Ransomware Project	\$1,540,000.00
External Forensics	
Regulatory Fines & Penalties (HIPAA, PCI)	
Crisis Communication Expenses / Notification Costs	
Attorney & Legal Expenses	
Higher Insurance Premiums	
Consultancy Costs + Employee Security Training Fees	
Infrastructure Improvements	
Collateral Damage	
Attack Re-occurrence Potential	
Loss of Sales/Customers	
Reputational Damage and Damage to Brand & Business	
Total Costs of Security Breach	\$1,967,333,33

**BREACH
COSTS**

- ▲ Cost of the Ransomware Payment is only 1 type of cost that is incurred when a security breach happens
- ▲ Average Cost of Ransomware Payment in 2023 = \$1,540,000¹ <https://www.varonis.com/blog/ransomware-statistics>
- ▲ Other potential costs that could be incurred when a security breach happens:
 - ▲ **Regulatory Fines** - depending on the industry, your customer could be accessed fines because they didn't take the proper precautions or invest in the proper measures to protect their customers personal data
 - ▲ **Customer Crisis Communication Costs** - customers whose information is believed to have been compromised must be notified in writing to be on alert for fraudulent charges. So, these are additional costs that will need to be incurred for the printing and posting of customer letters and the HR costs of handling customer complaints afterwards

Continuation...

- ▲ **Regulatory Fines** - Depending on the industry, your customer could be assessed fines because they didn't take the proper precautions or invest in the proper measures to protect their customers personal data
- ▲ **Attorney Fees and other Legal Costs** incurred from class action lawsuits and settlements launched by aggrieved customers upon finding out that their data has been stolen and compromised. These lawsuits can cost businesses tens of millions of dollars to settle
- ▲ **Higher Insurance Premiums** and larger deductibles potentially to be levied by their insurance company after a cyberattack
- ▲ **Consultancy Costs and Employee security training fees** will likely need to be incurred to teach employees what to look for so they don't cause another breach to take place
- ▲ **Infrastructure Improvements, upgrades, new security technologies** to fix exposed vulnerabilities in the organization's security infrastructure and to bolster their existing cybersecurity protection coverage
- ▲ **Collateral Damage** - The breach could potentially impact and cause harm to other organizations in that customer's supplier and customer-chain that could have lasting damage
- ▲ **Re-attack Risks** - The potential to be threatened again, and incurring these same costs all over again
- ▲ **Reputational damage to brand and business**, which could lead to loss of sales and customers

Step 5: Total Cost of Security Breach

Total Cost of Security Breach = Total Cost of Downtime + Potential Ransomware Payment + Cost of Intangibles

According to IBM Study, cost of intangibles could amount to: \$4.62 million* (does not include ransomware payment)

1 <https://www.netapp.com/blog/ransomware-cost/#:~:text=In%20fact%2C%20the%20average%20ransom,cost%20of%20a%20ransomware%20attack>

Total Cost of Security Breach = \$427,333 + \$1,540,000 + \$4,620,000

Total Cost of Security Breach = \$6,587,333

Step 6: Calculate ROI

ROI:	
# of Employees	\$40
Monthly Managed Services Program Price	\$250
Monthly Security Program Costs	\$10,000
Annual Managed Services Program Costs	\$120,000
Annual Savings	\$1,847,333.33

- ▲ Looking at it from an ROI perspective:
- ▲ Advanced Security Program Monthly Cost = \$250/month
- ▲ 40 user organization
- ▲ Monthly Cost of Advanced Security Program = \$10,000/month

Annual Cost of Advanced Security Program = \$120,000/year

ROI Response:

"Comparing the costs between our Advanced Security Program—that has an annual fee of \$120,000 year to properly protect your 40 employees—verses the costs associated with a potential security breach that could easily exceed \$6 million or more and could also include the risk of you losing your entire livelihood and the livelihood of your staff and employees, it is worthwhile to focus on prevention and recovery strategies to mitigate your risk, than to be forced to pay out after the attack happens."

Or – if you are getting pricing pushback, consider that this customer may not be a good fit for an Advanced Security Program.

Or, maybe you haven't done an adequate job of quantifying the risk for them, so they don't see the value in your cybersecurity services. To help a prospect or customer understand and see the benefits of improving their overall security posture, it starts by rejuvenating the security conversation and having it centered around RISK, not security. Risk isn't a bad word and it isn't a topic of discussion that MSPs should be afraid to have with their customers and prospects.

Continuation...

Risk is healthy and you have to acknowledge it. You can't allow your prospects and customers to stick their heads in the sand and say, "I don't have any risk—cyberattacks won't happen to me." Because that isn't a true statement. In our world today and the dynamic threat landscape we are experiencing, it's not about IF a company will suffer an attack, but more about WHEN.

You want to have a discussion with the prospect to help them determine their own respective Risk Exposure Rating, and once you can help them identify their Risk Exposure Rating, you will have a better idea as to which program offering they are a better fit for—either your Identity Protection Program or your Advanced Security Program—because not every organization will be suited for your top-tier Advanced Security Offering.

So, how do you quantify a company's risk exposure? We can look at this as an equation, where an organization's Risk Exposure is calculated as = Likelihood of Attack x Impact of the Attack or Breach.

And where the risk exposure rating is the highest, that organization will require a more robust set of security services, and will be a good candidate for your advanced security program.

So, when we look at the likelihood of a business being attacked, here we are looking at:

- ▲ The overall attractiveness of the organization to threat actors. Meaning how large are they? How many employees do they have? How much revenue do they generate every year?
- ▲ What does their supply chain look like? What kind of partnerships have they forged within their industry? Or what kind of partnerships are they looking to develop within their industry? How valuable and profitable are those partnerships to the growth and success of the business? If they are an organization that leverages a number of different suppliers, the prospect's attack surface has greatly expanded because they are now exposed to the risk that THEIR suppliers may have—especially if their suppliers don't appreciate the value behind good proper cyberhygiene. Unfortunately, if one of their vendors is compromised, their operations could be compromised as well and experience massive disruption as a result. So, if your prospect uses and relies on a number of different suppliers to manage their business and deliver their services, not only do they need to worry about their own internal security, but they also need to be worried about the risk exposure they face from those organizations in their supply chain—their risk exposure increases. If one of their suppliers suffers an attack, they become vulnerable to suffering from that attack as well through business association.

Continuation...

- ▲ What vertical or industry do they operate in?
- ▲ Do they have to adhere to any sort of compliance standards?
- ▲ What kind of data does the organization collect and store? What kind of intellectual property are they amassing? Who has access to this data?

And when we look at the Impact that the attack or the breach could have on the business:
Here we are looking at:

- ▲ What would be the loss in sales and revenue, if the business was breached and their doors were closed for a period of time?
- ▲ What would the end-customer impact be, especially if the organization wasn't able to perform their business-critical work? How significant would the impact on the business be if their end-customers lost patience from the disruption and opted to take their business elsewhere and jump to another competitor as they don't want to deal with or be inconvenienced by, the disruption in service?
- ▲ What would the hit be to their overall market competitiveness, if their data and intellectual property was stolen and sold to their biggest competitors? Or if that stolen data couldn't be easily replicated again?
- ▲ What would be the extent of the damage they could suffer from any supplier relationships they might have in place? Or are looking to get established in the future?

When dealing with each of these different scenarios with your customer, you would want to ask the customer to assign a rating to each—and that rating would be either LOW, MEDIUM or HIGH. The more MEDIUM and HIGH ratings that are assigned to each scenario, the higher the likelihood and the greater the chances of that business falling victim to a breach. And if the breach impact and the consequences of the breach would be significant as well, then the higher the overall risk exposure rating would be for that organization. The higher the overall risk exposure rating, then the better the fit that business would be for your high-end, advanced security program, and this would be the program that your customer would need to be enrolled in to best mitigate their risk of attack. i.e. If your prospect or customer can say 'YES' to many of these scenarios above, then they are at risk, and they need to be agreeable to allowing you to put the proper security measures in place that are needed to mitigate their business risk.

Subsequently, if the customer or prospect seems to have a few 'Nos' when going through this risk assessment-especially if they operate outside of a highly regulated industry-then they would make an excellent candidate for your Identity Protection Program instead

Assessing a prospect's Risk Exposure Rating

Determine the best businesses to target

Calculating Risk

Risk Exposure = Likelihood of Attack x Impact of Attack/Breach

• Likelihood of the Customer Being Attacked:

- Overall attractiveness?
- Supply chain and partnerships?
- Industry/market vertical?
- Compliance adherence standards?
- Type of data collected and stored?

• Impact of the Breach on the Customer:

- Revenue/sales loss?
- End-customer desertion impact?
- Market competitiveness?
- Damaged supplier relationships?



The Risk Exposure = the better the fit for a high-end security program



Top risk characteristics and industries for an advanced security program

- Has financial, health, PII data, or sensitive IP
- Employees have access to sensitive systems or partner data
- Data that would be very attractive to adversaries
- Possible extinction event for that business
- Regulated industries:
 - Banking
 - Financial
 - Healthcare
 - Education
 - Manufacturing
 - Local and state governments



HIGH RISK BUSINESS

LIKELIHOOD = HIGH
IMPACT = HIGH
AN ADVANCED SECURITY PROGRAM IS NEEDED

OBJECTION #6:

“I can get it cheaper elsewhere.” OR “Another MSP is only charging \$X/month.”

- ▲ Possibility: The competitor's program is missing key features and services in their offering and it's the lack of those key features that could be resulting in the price gap
- ▲ Recall from the Layered Security Illustrations: There are 6 key layers that need to be addressed when it comes to properly protecting an organization's critical data and keeping it secure and all 6 layers requires its own specific security tool sets

1. Perimeter/Internet level 2. Network level 3. End-User level	4. Applications level 5. Device level 6. Cloud Layer
--	--
- ▲ If a competitor is saying they can deliver a cybersecurity program for far less than what you are charging them, you should be concerned as to what is actually being done across all six layers
- ▲ Or, the competitor is severely underestimating the labor component involved in successfully deliver their version of the program
- ▲ Or, the competitor is significantly sacrificing margin and their overall profitability levels to win the deal, which is not sustainable long term in building a successful business
- ▲ Recall: Best-in-Class MSPs are generating anywhere between 60-80%+ gross margin on their cybersecurity programs, so these programs should cost more as MSPs should be charging a premium for the security programs they offer
- ▲ To overcome this objection, weaponize the competitor's lower price and use the opportunity to highlight not only your comprehensive security toolset, but the skilled people you employ and the qualifications they possess, and the best practices and processes you adhere to as well due to the various compliance and security regulations that you subscribe to

Sample Response:

“Our monthly fee reflects what is truly needed to properly protect, detect, remediate and recover from cyber-related issues for our customers. Proper risk mitigation is a combination of implementing the right toolsets, with the right processes and procedures, and I worry that the price you are being quoted doesn't contain everything that is being recommended by compliance standards and cyber liability insurance providers today.”

OBJECTION #7:

“Can I remove some of the services you have included in the program that I don’t think really need, so that the monthly price fits better into our budget?”

- ▲ Short Answer: No, it is strongly recommended that you do not allow customers the opportunity to remove services for budgetary reasons
- ▲ It is not advisable to allow customers to dictate their own path to support
- ▲ Recall the layered security diagram—and the 6 layers that surround your customer’s employees and its critical data—if an MSP allows their customers to remove services because of budgetary concerns, they are creating gaps in the customer’s protection coverage, which will increase the risk of malware or a virus getting through
- ▲ The programs have been designed so that each of the 6 layers has appropriate protection coverage to build the strongest defense possible, and will also allow for quicker recovery when something happens (because it is about WHEN, NOT IF, something happens)
- ▲ Goal of the traditional security program is to get employees back to work with as minimal damage and minimal impact as possible
- ▲ If price or budget is a concern, especially if this objection is being voiced by any of existing break/fix or a la carte/reactive customers, then position the Identity Protection Program as that program was designed to act as the minimum viable security program that customers can be enrolled into
- ▲ If the MSP allows for the removal of services to fit some pre-conceived price point, they are opening the door to increased risk and liability for themselves and their customers
- ▲ Not only are there costs to the customer by refusing to elevate their security posture (recall from the ROI exercise we reviewed earlier), the MSP could incur financial costs as well if a minimum standard of security is not enforced such as:
 - ▲ **Revenue Loss** – With average remediation time of 30 days and costing roughly \$24,000 or more (from our previous ROI/Cost of Downtime example) this is a significant, unexpected cost to a small business. Often times MSPs will heavily discount this bill or waive it altogether as they feel bad that their customer got infected
 - ▲ **Reputation Loss** – Just like with a customer who gets breached and may experience a loss in reputation depending on how it plays out, the MSP could experience a reputation loss as well, and come to be known as the MSP who allowed a breach to happen. This could be especially harmful if the MSP resides in a vertical or industry specific MSP

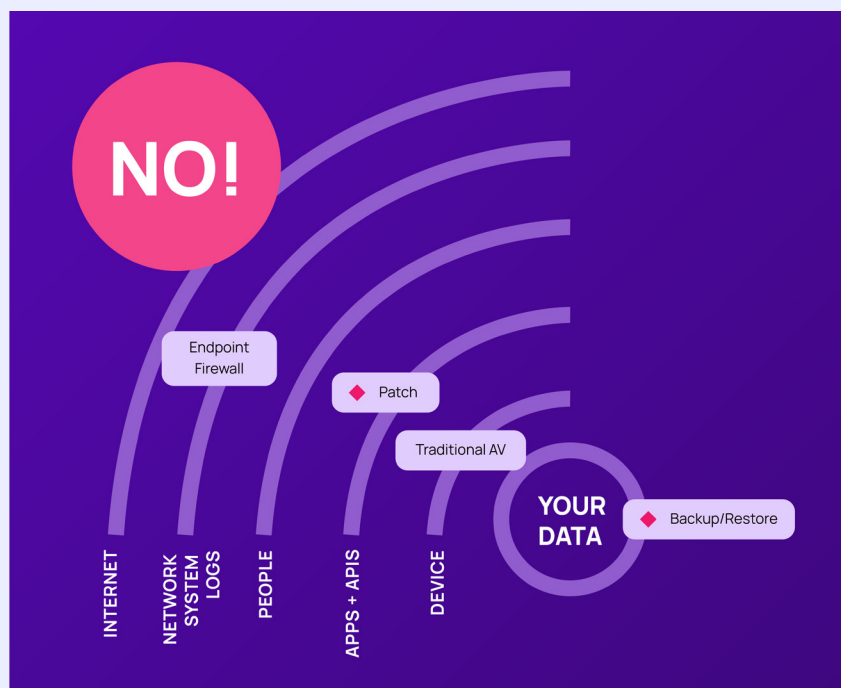
Continuation...

- ▲ **Liability Costs/Fines** – The MSP could be fined or sued and be found negligent, which could result in an extinction event
- ▲ **Opportunity Costs and Lost Sales** due to the loss of other potential business the MSP might have been able to generate for their MSP during this time, but had to miss out on as their most experienced techs were pulled away to assist the breached client and help them recover
- ▲ **Operational Costs** – By allowing customers to remove services from the minimum package, it will make it more difficult to track, bill, support and manage customers on a day-to-day basis as every customer would be a bit different, causing the MSP to forfeit many of the service optimization and efficiency benefits that are gained from a program standardization perspective

Sample Response:

“60% of small and medium-sized businesses go under 6 months following a cyberattack¹, and this is a fate we do not want to happen to any of our customers. We have designed our security programs to ensure that every layer that sits between your employees, the data they are accessing, and the outside world is properly protected. If we remove a service, we are creating a hole in this protection coverage, thereby increasing the odds of you falling victim to an attack.”

¹ <https://purplesec.us/security-insights/top-cyber-attacks-2022/#Breaches>



OBJECTION #8:

“What’s wrong with the endpoint detection and response product you told me about during our last QBR? You told me then that I needed it, and now you are telling me that I need to buy yet another product? Seems like a cash-grab to me.”

This objection is for any MSP that might still be selling security on a product-by-product basis versus selling a complete security bundled solution. This response can be used to help get the MSP out of this situation.

Sample Response

“Endpoint Detection and Response (EDR) is still necessary, but it is only one piece of the entire security suite we are now recommending to our customers. As your MSP, I need to be protecting your organization on a 24/7/365 basis, and I need to ensure that your business does not suffer any unnecessary, long-term downtime that could impact your revenue and your reputation. Our aim is to keep your business up and running, operationally safe and secure—and so that requires us to expand our coverage beyond just protecting the endpoint.

Unfortunately, with just an endpoint detection/protection piece in place, we don't see everything that is happening across the entire network. Endpoint protection only sees what is happening on the endpoint, and the endpoint isn't always the infiltration point for a threat actor. So, in the event of a breach, it can't give us the full picture of how it started or what happened, and we need that from a forensics standpoint, especially if you need to file a claim and get your cyber liability insurance company involved.

So, by including other software pieces to protect the layers beyond the endpoint, and then incorporating our more holistic managed detection and response service over top of that, this provides more expansive coverage and higher levels of visibility that will help us when we have to help you recover from a cyberattack or data breach. Having an EDR agent alone on the endpoint is no longer sufficient to provide us the full visibility and breadth of coverage and data we now require.

So bottom line: We no longer sell any product in a silo, as we recognize that nothing is 100% foolproof in preventing an attack. Moving forward, our approach is to layer a variety of services and security toolsets together into what we are calling our Advanced Security Program, as that is the best defense to help mitigate our customers' cyber risk and lessen the chances of them succumbing to an attack.”

OBJECTION #9 & 10:

“It won’t happen to us. We are too small and we have never been breached before.”

OR

“It won’t happen to us. Who would want our data?”

- ▲ “Security through obscurity is not a security strategy for smaller businesses.” Charles Weaver – MSP Alliance
- ▲ A customer hoping that they won’t get breached due to their size, or the fact that they have never been breached before, is not a protection strategy that your MSP should accept
- ▲ Customer size no longer matters-according to CISA, they are finding that smaller businesses are 3x more at risk of being attacked than larger ones
(Source: <https://www.cisa.gov/news-events/news/accelerating-our-economy-through-better-security-helping-americas-small-businesses-address-cyber>)
- ▲ Every business is open to being attacked
- ▲ It could be that the business may not be the intended target, but bad actors might want access to the suppliers and the vendors that the customer has business dealings with, and therefore the customer could act as a potential gateway to those other more desirable vendors.
- ▲ So, education is needed to help the customer see that although they may ‘think’ an attack may never happen to them, the current state of their network does not meet your MSP’s new security standards that have been set for all customers, and therefore their network security needs to be hardened to avoid becoming the ‘weak link’ in the chain to their suppliers and business partners they interact with
- ▲ Or, if the customer pushes back and says they don’t need to enroll in one of your layered security programs because no one would want their data, again education is needed
- ▲ The threat actors don’t care about the data they are stealing, they are only concerned about the ransom money they could collect, but they know that the customer cares about their data, and that is what they are preying on
- ▲ Smaller customers are easy targets and quick wins for the bad guys because of the way they have been accommodated in the past by MSPs

Continuation...

Sample Response

"Cyberattacks against small businesses have actually been on the rise in recent years as their lax approach to security makes them attractive prey. In fact, certain types of attacks, social engineering attacks like phishing, are much more commonly aimed at smaller businesses.¹

DYK?

- ▲ Companies with fewer than 100 employees received 350% more social engineering attacks, such as phishing, than larger enterprises²
- ▲ And in 2023, small businesses were hit hard by cyberattacks, with more than 40% reporting an attack³

And the sad part is that, generally, smaller businesses are not financially prepared for an attack and many lack adequate cyber insurance. As a result, a successful attack against a smaller business could potentially put them out of business, and that is what we strive to avoid for our customers with our security programs."

¹ <https://www.strongdm.com/blog/small-business-cyber-security-statistics> (accessed March 2024)

² <https://www.embroker.com/blog/cyber-attack-statistics/>

³ <https://www.embroker.com/blog/cyber-attack-statistics/>

OBJECTION #11:

"I'll take my chances and pay the ransom and then make a claim through my insurance company."

- ▲ If you receive this type of response from a customer, think seriously about continuing that relationship as this is a red flag. You cannot allow a client to rely solely on their insurance company to bail them out
- ▲ The cyber insurance industry is changing due to the increased number of attacks and the increased payouts they have been forced to make, so they are starting to change the rules of engagement
- ▲ If an organization gets ransomed and they need to file a claim to pay that ransom, the insurance company will likely want to conduct an investigation first, which will take time

Continuation...

- ▲ Remind the customer of this, and remind them that downtime will cost their organization money in terms of lost sales and lost productivity
- ▲ And when the insurance company conducts their investigation, their goal is to try to determine who the negligent party could be and who may be at fault
- ▲ Your goal as their MSP is to not be labeled as that negligent party, nor do you want your customer to be labeled negligent which could result in having their claim denied
- ▲ And not implementing the right security measures could be a reason that the insurance company invalidates the customer's insurance and deny the claim
- ▲ Both the MSP AND the customer have to abide by certain requirements set forth by the cyber liability insurance companies to increase the chances of having a claim paid:
 - ▲ MSPs have to prove that they are having the cybersecurity and risk conversation with all of their customers in order to have their own cybersecurity insurance policies renewed
 - ▲ If the MSP is not having the cybersecurity liability and risk discussion with their customers or if they not mandating that their customers enroll in one of their new security programs, or if they are allowing their customers to decline their security program without having them sign a release or waiver of liability, then the insurance company has identified their negligent party and there is a high probability the claim may be denied as the MSP cannot prove that they did their due diligence and took the proper steps to protect their customer
 - ▲ From the customer's perspective, they need to demonstrate that they have taken the proper protection measures to do what they can to properly care for and secure their network
 - ▲ If it is proven that the MSP offered to enroll them in one of their cybersecurity packages (that aligns to the cyber liability insurance application requirements) but the customer declined that protection coverage, then again, the insurance company has found their negligent party and may possibly refuse to pay the claim
- ▲ So, by enforcing enrollment in one of the structured security programs, both the MSP and the customer have demonstrated that they have taken the proper steps to protect themselves from a cyberattack, thereby increasing the chances that the insurance company will pay the claim

OBJECTION #12:

“No. I won’t switch to your new program nor will I pay for these new services.”

Sample Response #1

If this is a legal or a healthcare client that is giving this pushback, one possible response could be:

- ▲ “Mr. Customer, your job is to protect your clients. So is mine. But you’re not letting me do my job by refusing to enroll in my new advanced security program I have developed to better protect my customers. I feel like you’re not taking my job seriously as your technology security advisor when I bring you recommendations that will protect your employees and your business. I do need you to sign this new agreement for our new cybersecurity program that we are standardizing and enrolling all of our clients into moving forward.”

If you continue to get pushback and the client won’t sign the new contract at this meeting, then ask as follow-up:

- ▲ “If you feel that you are not able to sign this new agreement today, then when? Is this something you can sign in the next 60-90 days?”

Hopefully they will reconsider what you are asking them, especially if you can give them a small window to adjust and get used to the idea of the new changes you are implementing

Sample Response #2

If the customer still refuses to sign the new agreement, then you may decide to remove them as a client of yours, as they are no longer a good fit for your business

- ▲ “I respect your decision, but unfortunately this is something we cannot support as it poses a significant amount of risk that we do not want to be associated with. Our job is to protect our clients and their business, and by not enrolling in our recommended security program, you are hampering our ability to do what is needed according to security and compliance best practices. In this instance, you may be better suited to work with another MSP who does not align themselves to the recommended security standards that we do, and we would be happy to help you make that transition over to another MSP.”

Ultimately let the decision be theirs, but do not let this issue linger beyond the 60-90 day mark, as you are putting your MSP at risk.

Step 7: Setting Your Go-To-Market Sales and Marketing Goal

It will be important to create goals and track them in order to measure the sales success as it relates to promoting your layered security programs. Without setting goals, it will be difficult to tell how well your strategy is working.

Some simple Key Performance Indicators (KPIs) that you could track to gauge the success of your layered security sales and marketing efforts:

Existing Customers:

- ▲ Increased MRR over campaign length – Started MRR vs. Target MRR Growth
- ▲ # of customers converted from break/fix or a la carte programs into new standardized security program
- ▲ # of customers churned as a result of refusal to sign new contracts
- ▲ MRR lost as a result of churned customers
- ▲ Net MRR gained/lost from churned clients vs. converted clients

New Customers:

- ▲ # of new customers enrolled into new standardized security program
- ▲ Total value of new security program contracts signed?
- ▲ #Increase ACV (average contract size) from new customers enrolled into new standardized security program
- ▲ Closing rate for new security contracts
- ▲ Length of time to close new security contracts

Developing a GTM and Sales Strategy for Selling A Co-Managed MDR Program

Step 1: Defining the Ideal Client Profile (ICP) and Target Audience

If you decide that your MSP is well-positioned to offer a co-managed MDR service to your customers and prospects, it will be important to target and attract the right type of customer to help make your MDR offering as successful as it can be.

So, for your co-managed MDR program, what does the Ideal Client Profile look like?

- ▲ There has to be an IT Leader in-house, like an IT Admin, IT Director, CTO, etc.
- ▲ There has to be someone within the organization that the MSP can collaborate with, and who knows all about the network setup and critical applications being used by the employees.
- ▲ Typically has 100 or more employees
- ▲ Geared towards internal IT departments that are comprised of:
 - ▲ Solo individuals
 - ▲ A team of only generalists who are lacking security specialization or expertise
 - ▲ An organization that is looking to expand and hire internal security personnel, but cannot find or afford them
- ▲ Key Verticals/Industries that would appreciate the co-managed MDR model:
 - ▲ Healthcare establishments
 - ▲ Manufacturing
 - ▲ Large legal firms
 - ▲ Large accounting offices

- ▲ Small banks and other financial institutions
- ▲ Any other organization that resides in a regulated industry and has compliance standards it must comply with and where the breach impact would be consider high
- ▲ Other professional services organizations that collect and store sensitive customer data that would make the organization a target for attack and are lacking key staff to help implement and manage their company's security stack

Once the MSP has defined their Ideal Client Profile and target audience for their MDR service, this profile can be used to begin creating prospect lists of company names to target from a marketing and sales perspective.

Resources that can help with this step include:

- ▲ A review of your CRM to see if there are existing clients that might fit
- ▲ Online job sites like Indeed, Glassdoor, ZipRecruiter, LinkedIn to see what companies are looking to hire additional security engineers or cybersecurity specialists where you could speak with them about the co-managed MDR services model
- ▲ LinkedIn
- ▲ Google
- ▲ Chamber of Commerce
- ▲ Referrals
- ▲ Networking Events and Trade Show

Step 2: Identify the Problem

In this step, the MSP will want to identify the purchasing triggers and pain points of their target audience to help create key messaging and value prop statements needed to help promote and sell a co-managed MDR services program.

The co-managed MDR program aims to solve the top security challenges experienced by internal IT departments and the organizations they work for. We can think of these as being 'purchasing triggers' of the internal IT administrator:

- ▲ **Increasing prevalence and sophistication of cyberthreats.** As cybersecurity threats continue to evolve, they are becoming increasingly more and more sophisticated and prevalent, making it difficult for internal IT departments to manage it all with any degree of confidence

- ▲ **Increasing Network Complexity.** With changing technology trends, networks are becoming increasingly more and more complex, making it difficult for the internal IT team to properly manage and secure it all. This is especially true when it comes to cloud deployments. Cloud security has become a potential weak point because internal IT doesn't understand what is needed to secure it appropriately
- ▲ **Increasing Compliance Demands.** Companies in regulated industries are experiencing increasing compliance demands, and failure to comply can invoke punitive penalties from different regulatory bodies. But internal IT is lacking the proper security monitoring and reporting toolsets to demonstrate and prove compliance, should they be audited.
- ▲ **Lack of Skilled Cybersecurity IT Talent.** With the increased sophistication of cyberattacks and the ever-changing threat landscape, internal IT requires specialized cybersecurity expertise, but no one in-house has it, nor do they have the budget to hire to acquire it.
- ▲ **Difficulty Finding Skilled Cybersecurity Talent.** With the increased sophistication of cyberattacks and the ever-changing threat landscape, internal IT recognizes they now require specialized cybersecurity expertise in-house, and while attempting to hire, they cannot find the skilled security individuals they need to fill their requisitions.

Step 3: Do Your Research

To determine if there is a market in your area for co-managed MDR services, you will want to conduct some research to see what sort of competition you might be up against. Questions to be considered include:

- ▲ What other MSPs in your market are offering a co-managed MDR service?
- ▲ How does their MDR offering compare to yours?
- ▲ What vertical markets, role types, geographic regions are your competitors targeting?
- ▲ How well is your competition doing at promoting their co-managed MDR service?
- ▲ What kind of marketing and promotion activities are you seeing being advertised as it relates to their co-managed MDR service?

To help with this research, it would be good to review your competition's websites and social media feeds like LinkedIn and Facebook to see if there are mentions of the co-managed services model in their material.

Step 4: Creating Key Messaging and Defining Your Value Prop

This involves taking the pain points/purchasing triggers that have been identified back in Step 2 and pairing each of those purchasing triggers with a top benefit of your co-managed MDR service. Combining these pieces together, will help you create the key messaging that can be used in your sales and marketing messaging and MDR campaigns.

Here are some examples of co-managed MDR-specific messaging statements that can be used to build an MDR marketing and sales campaign.

Purchasing Trigger #1 – Increasing prevalence and sophistication of cyberthreats

Key benefit your MDR service can provide – With an MDR service, the MSP can augment the internal IT team and assume the 24x7x365 security responsibility, providing peace of mind and a higher level of business continuity in the event of a cyberattack.

Key Message

“Did you know? There are nearly 20 ransomware attempts made every second, and the average time between cyberattacks is a mere 39 seconds. Adversaries don’t sleep and it is impossible to have eyes everywhere on everything at all times. When a cyberincident occurs, the clock is your enemy!

Leverage our SOC and our team of cybersecurity experts to provide around the clock protection coverage to ensure that your organization remains safe and secure.”

<https://www.verizon.com/business/en-nl/resources/reports/dbir/>

Purchasing Trigger #2 – Increasing network complexity

Key benefit your MDR service can provide – With an MSP's breadth and depth of experience working with different companies and different IT environments, they can offer a broader perspective and provide valuable insights on how to best manage and secure it all—with the MDR service playing a key role.

Key Message

"Technology trends are constantly evolving and networks are becoming increasingly more complex to properly secure and manage. Are you having difficulty keeping up with it all? Leverage our experience that comes from working with a vast array of different companies and different IT environments—including cloud environments—and allow us to offer a broader perspective on what is required to properly protect your organization's data from outsiders, no matter where on your network it resides."

Purchasing Trigger #3 – Increasing compliance demands

Key benefit your MDR service can provide – With an MDR service, enterprise companies can gain access to the compliance expertise they need as the MSP can step in with the proper security monitoring toolsets and reporting features to manage the compliance risk for them.

Key Message

"How confident are you that your organization would pass its compliance audit, should you be audited? Do you have the proper security monitoring and reporting toolsets in place to demonstrate and prove compliance, should a security incident occur on your network? Compliance isn't an option. Partner with us to gain the compliance intel you need to help your organization avoid costly punitive penalties."

Purchasing Trigger #4 – Lack of skilled cybersecurity IT talent

Key benefit your MDR service can provide – With an MDR service, enterprise companies can gain access to the skilled cybersecurity expertise they require, as the MSP can step in to manage the network and cloud security for them in a more cost-effective model.

Key Message

“Having concerns around what is needed to properly secure and protect your organization’s network from cybercriminals, but don’t have the expertise in-house or the budget to hire skilled cybersecurity personnel?

Consider leveraging our MSP to provide the cybersecurity specialization you require. We can act as an extension of your in-house IT department and provide the safety and security you are looking, in a more cost-effective model for your business.”

Purchasing Trigger #5 – Difficulty finding skilled cybersecurity talent

Key benefit your MDR service can provide – With an MDR service, enterprise companies can offload the hiring and management stress, and can save time, money and effort in trying to source and hire the skilled cybersecurity expertise they need, by partnering with an MSP who can manage the organization’s network and cloud security on their behalf. By partnering, the enterprise company can gain access to a pool of around-the-clock cybersecurity analysts quickly and easily, at a fraction of the cost of building a team of cybersecurity experts themselves—especially if they are challenged finding the talent they need.

Key Message

“Are you struggling trying to find and hire the skilled cybersecurity staff to join your team to help you grow? Consider offloading that responsibility to us. By partnering with our MSP, you can quickly and easily gain access to an entire network of around-the-clock, qualified cybersecurity personnel, that can provide the safety and security you are looking for, at a fraction of the cost of building a team of cybersecurity experts yourself.”

Step 5: Selecting the Appropriate Marketing Channels

This step is all about deciding what marketing channels will be the most appropriate to use to help build awareness and promote your co-managed MDR service offering.

Marketing channels refers to the different types of content you will use to create demand for your service to help move potential customers through the marketing and sales funnel until they hopefully become a new, signed contract.

Examples of different types of marketing channels include:

- ▲ Social media
- ▲ Paid search ads
- ▲ Email
- ▲ SEO optimized content to drive traffic to your website like blog posts

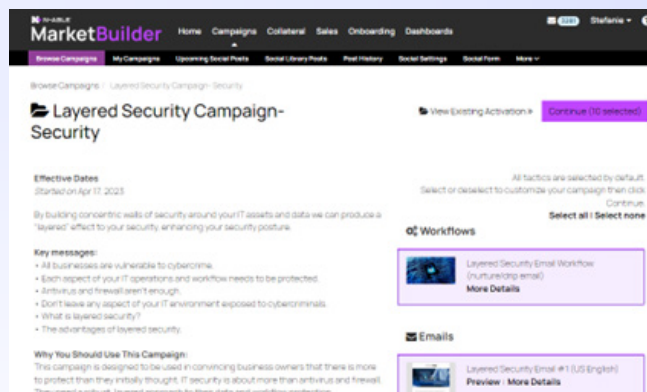
Co-Managed MDR Marketing Collateral

To help market and promote your co-managed MDR services offering, we have created several pieces of collateral for you to brand and customize. You can find an entire MDR marketing campaign within our N-able MarketBuilder, that includes:

- | | |
|----------------------|---|
| ▲ Emails | ▲ MDR Battlecard |
| ▲ MDR Landing Page | ▲ MDR Presentation Deck |
| ▲ Social Media Posts | ▲ Word Docs (to gain access to the verbiage, but utilize your own branding) |
| ▲ MDR Sell Sheet | |

N-ABLE MarketBuilder

If you are looking for formatted versions of these marketing collateral pieces, we encourage N-able partners to register for our [N-able MarketBuilder](#) platform where they can gain access to not only these co-managed MDR pieces, but much, much more.



One useful piece within MarketBuilder as it relates to SEO optimization that should be highlighted is that for each MarketBuilder campaign, it provides sample keywords to include in any content you create that will help your website be found by prospects searching for IT, security, and compliance support on the web.

Looking in MarketBuilder, sample Keywords and phrases that could be included in your marketing copy for your co-managed MDR campaign includes:

- ▲ Co-managed IT
- ▲ Supplement IT management
- ▲ Supplement IT support
- ▲ Help for internal IT teams
- ▲ Help for internal IT departments
- ▲ Help for in-house IT departments
- ▲ MDR
- ▲ Managed Detection and Response
- ▲ Advanced Cybersecurity
- ▲ Cybersecurity protocols
- ▲ Compliance consulting

The different marketing channels you decide to use to promote your co-managed MDR service will depend on your target audience and where your potential customers are in their buying journey.

Lunch and Learns

One marketing activity you may want to consider that can help build interest and awareness in your MDR service is to host a webinar or an in-person event to help educate your target audience on what a co-managed MDR services looks like. A popular concept of an in-person event is known as the 'Lunch and Learn'. Hosting a Lunch And Learn could serve has a good starting point to jump start you new co-managed MDR service for your MSP.

There are several benefits of Lunch and Learns:

- ▲ Can be used to help transform your MSP into an authority figure on the subject of MDR as you can educate prospects on the topic
- ▲ Can be used to help differentiate your MSP from the competitors in your area, if they are not offering co-managed MDR services themselves
- ▲ Having face-to-face interactions will help you to develop closer connections more quicker with potential prospects

Elements of a Good Lunch and Learn

There are several elements that can help you to have a successful Lunch and Learn event.

- ▲ **Have a good list.** This is something that was discussed back in Step 1 of building a GTM strategy for co-managed services. Spending the time to develop your ideal client profile and target audience will help you build a list of top prospects that you can market to that possess the key characteristics you desire in quality customers that you prefer to do business with.
- ▲ **Have educational content.** One of the top priorities of your event is to educate prospects and provide relevant insights that can help address key challenges and struggles they may be facing of which you can potentially help them overcome via your services. This is result of the work that was completed back in Step 2 and Step 4 of the GTM planning process-If you can demonstrate that your MSP understands the challenges facing internal IT departments today, and you can offer options to help alleviate these challenges, your attendees will be interested.

- ▲ **Plant a few friendlies** in the audience that can provide testimonials and insights to your guests. Consider asking them to take part in your presentation or to participate in a panel discussion where you can discuss how partnering with your MSP has really helped to make their IT department more productive and run more efficiently. The truth of the matter is: peers will ALWAYS be more receptive to listening to their peers and will tend to view their peers as being more credible.
- ▲ **Select a good venue** that includes good food. Don't underestimate what a good venue with good food can do at fostering connections and building relationships with prospects. This provides your MSP with the opportunity to make a great first impression with your target audience. Also promoting a nice venue that is known for its great atmosphere and food selection will also help to improve your attendance rate.
- ▲ **Be polished and professional** when it comes to your event logistics and RSVP management. Having a proper registration and RSVP process, with professional reminders in place (leveraging email and follow-up phone calls) will help to set the expectation that this is a serious and professional event your MSP is hosting.
- ▲ **Have a positive attitude.** If you have never hosted a customer event before, be prepared for some hiccups as it will likely not go perfectly the first time around. But don't let this stop your MSP from planning follow-up events. Recognize what went well, and what could go better, and adjust your processes and procedures and tactics for next time.

If you are interest hosting a prospect event to help promote your co-managed services, we have developed a 'Co-managed Services Event-in-a-Box' that you can use. This contains information to help you plan, promote and deliver a prospect event designed to introduce and help educate your target audience on the value of co-managed IT services.

Included in the 'Co-Managed Event-in-a-Box':

- ▲ [4 sample emails to encourage prospects to register for your event](#)
- ▲ [6 sample social media messages that can be posted to your MSP's social feeds to encourage prospects to register for your event](#)
- ▲ [Sample Text for a direct mail postcard, or to be included in a newsletter](#)
- ▲ [Sample Phone Scripts for the sales department to use as part of outbound call campaign to invite prospects to your event](#)
- ▲ [Co-managed IT services sell sheet](#)

- ▲ [Customizable Powerpoint presentation that can be used during the event](#)
- ▲ [An Event Planning Guide](#)
- ▲ [And Event Planning Checklist](#)
- ▲ [An Evaluation form to solicit feedback from guests](#)

Step 6: Create the Sales Plan

The primary goal of this security sales playbook is to help you build and ultimately sell your co-managed MDR program. So, step 6 of creating your GTM strategy is mapping out what your sales strategy will look like.

This is where launching your co-managed MDR service with an in-person event or webinar will work well as it will give your sales team a purpose and a dedicated focus. Instead of having just a general outbound calling campaign, your sales team can call on prospects to invite them to your event. It will give them something tangible, educational and fun to promote.

So leveraging the [sample call scripts](#) from the 'Co-managed Event-in-a-Box', a sample sales plan could be:

- ▲ Business Owner, sales leadership, sales teams, Sales Development Representatives (SDRs) work together to create a prospect list of companies and individuals to call to invite to the event
- ▲ The SDRs (or other sales-designate) proceed with a proactive, outbound calling campaign to invite prospects to the event
- ▲ At event, the sales team is responsible for introducing themselves to prospects, building interest and attempting to schedule 1:1 meetings with potential customers post-event
- ▲ Salesperson and/or Business Owner attends the initial discovery meeting to determine if there is a need for a co-managed IT MDR service, and if there is a good fit between the two organizations
- ▲ And if there is a good fit, Salesperson/Business Owner drafts and presents the proposal to start the services engagement

Co-managed MDR SDR Sales Scripting for Outbound Call Campaign

If you do not plan on hosting a prospect event, this playbook also includes additional sample scripting that the SDR team can use to proactively call on prospects to discuss your layered security services offering.

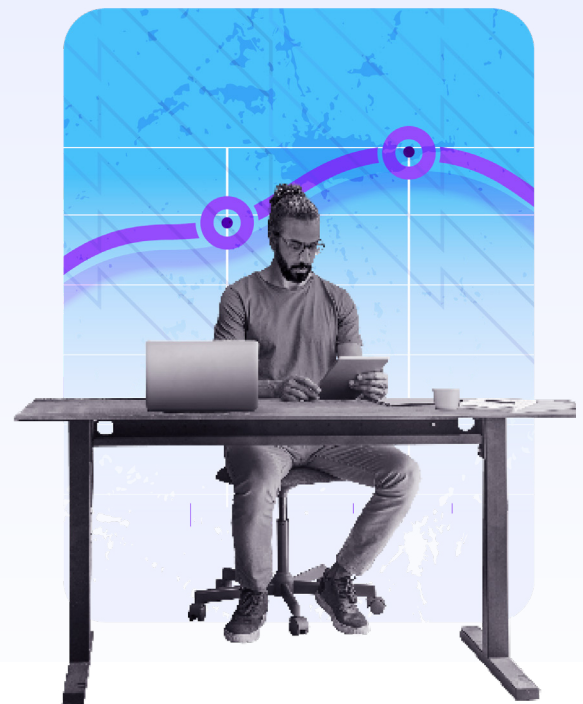
For continued growth, it is useful to have someone dedicated to calling your Dream List of Prospects to help book appointments for yourself or your Account Executives.

If you currently do not have a telemarketing motion established for your MSP and are interested in building one, we have created a Head Nerd Boot Camp that focuses specifically on this topic called:

Cracking the Code to Lead Generation Part 2: Building a Tele-sales Strategy

[Register Here](#)

For N-able Partners, you can access this Boot Camp on demand within our [N-ableME](#).



The goal of this initial call is for the SDR to book an appointment for either the MSP Business Owner or for the Account Executive with the IT Leadership and C-suite team of the prospect's organization.

SDR Opening Lines to Introduce Your MDR Services to Prospects

Opening Line #1:

"Mr. IT Administrator, with the increasing sophistication and prevalence of cyberthreats today, we are finding that many mid-and upper-enterprise IT organizations are discovering that they are not as prepared as they would like to be when it comes to handling the onslaught of attacks that are coming their way.

How equipped is your team when it comes to quickly detecting and neutralizing cyberthreats, so as not to negatively impact the productivity of the employees or the revenue-generating capabilities of the business?"

Opening Line #2:

"Mr. IT Administrator, as a business operating in XYZ industry, your organization is required to abide by [name compliance regulation]. And one of the primary requirements of this regulation states that organizations must have a process in place for network and security log collection and aggregation, so that in the event they are audited or face a cyberbreach, they are able to demonstrate that this log data can be readily relied upon for forensic investigation purposes, or else they could potentially face punitive fines and increased scrutiny.

How well equipped is your department when it comes to the log collection and aggregation requirements set forth by [insert compliance standard]?

And how confident are you that you will be able to quickly and efficiently demonstrate compliance should you be audited or fall victim to an attack?"

Opening Line #3:

"Mr. IT Administrator, how is your department currently addressing the security and data protection requirements when it comes to [name of regulation/standard]?"

On a scale of 1 to 10, how well do you feel your organization is doing when it comes to implementing and adhering to the recommend security best practices outlined by [name of regulation/standard]?"

Opening Line #4:

"Mr. IT Administrator, I see from LinkedIn that your company is looking to hire a new security analyst to join your IT team. How is that search going for you?"

Have you ever considered leveraging the services of an MSP in lieu of hiring new internal security or technical staff that you would then have to manage?"

You could offload the hiring and management responsibility over to us, and allow our team to handle the security monitoring and management on behalf of your organization."

SDR follow-up questions once rapport has been established

Once the SDR has gained success in getting the conversation started, use some of the sample follow-up questions below to continue the conversation could be:

Follow-up Questions:

"You indicated that your organization has a shortage of cybersecurity staff. Why do you think this is? What do you think are the biggest causes around this shortage?"

"Do you feel that the lack of certified cybersecurity staff on the team is putting your organization at heightened risk of cyberattacks?"

"How is the function of cybersecurity currently being handled within your department? Do you mind describing the security stack and best practices you have in place today?"

"Is your department currenting following an established cybersecurity framework like NIST or the CIS controls?"

"How confident are you that your cybersecurity measures have been implemented correctly and are being adhered to consistently within your organization? How are you tracking or auditing this?"

Continuation...

"If your organization suffered a cyberattack, how quickly (say in the number of hours) would your team be able to get all of your employees back online and back to work? Is this a timeframe that you are comfortable with?"

"If your organization suffered a ransomware attack, what reports do you have that would outline what really took place during that attack? Where is your record of truth to explain what happened within the network environment?"

"Do you find that your team is often stretched for time when it comes to properly performing their cybersecurity duties?"

"How is your IT department handling the current workload? IT and security professionals are in demand, and good ones are even harder to find and hire. Are you struggling with finding the right IT and cybersecurity specialists for your department?"

"Companies are constantly striving to find ways to stretch their budgets, especially their IT and security budgets. Are you finding that you being forced to do more, but with less money and resources to get it all done?"

"Organizations are increasingly becoming more and more reliant on the technology that runs their business. What would the impact be if your department didn't have the resources needed to handle an emergency downtime or security incident?"

SDR closing question to ask for the initial meeting

Lastly, if the SDR feels that they are building consensus with the prospect, and there is potentially a good fit, then the SDR will want to secure an initial face-to-face meeting to conduct an cyberassessment and network health overview with the IT Director and CEO of the organization:

Closing Questions:

"Mr. IT Administrator, what you can't see poses the greatest risk to your organization and there are countless areas within your environment where threats can hide before they lead to business disrupting events like ransomware shutdowns or massive data breaches.

Why don't we setup a time to review your network and conduct an assessment so we can provide you with the intel to help determine where you might be exposed that could lead to a significant attack?

And then we can discuss how we might be able to help your team—via our MDR service—close those gaps and mitigate your cyber risk?

Objection Handling Techniques and Response for Co-Managed MDR

During the MDR sales process, you will likely receive pushback or hear concerns from either the internal IT Director or the CEO. To help you prepare, we have listed below the most common objections you may come across, with some possible sample responses.

Tip: Do what you can to capture your prospect's direct quotes as you are speaking with them so you can add these to your proposal that you present to your prospect during the closing stage.

10 Most Common Objections

"Our Endpoint protection is sufficient. We don't need anything like MDR."

"We are currently already looking at different SIEM software providers to implement internally."

"We are already using an MDR service internally with someone else."

"We currently have dedicated internal security staff, so we don't need the services of an MSP at this time."

"We can do this ourselves with our technical team. We don't need the services of an MSP to assist us with this."

"You are just trying to make my team and I look bad in front of my CEO."

"We have other priorities and other technology upgrade projects that we are focused on first at the moment."

"We don't really need anything like this, as we don't reside in a regulated industry."

"This sounds like it is an expensive service. We don't have the budget for this."

"How can we know to trust you? Why should we trust you and your service?"

OBJECTION #1:

“Our Endpoint protection is sufficient. We don’t need anything like MDR.”

Sample Response Option #1:

“It is fantastic to hear that you have endpoint protection coverage on your employees’ devices. But, your employees’ devices are only one component of your organization’s environment and the endpoint isn’t always the infiltration point for the threat actor. There are several other areas of your network that require security monitoring as well for data breach prevention purposes.

As the organization’s IT Director, when an attack occurs on your network you need the ability to recover, and to recover quickly. And to do so, you need a good understanding around: What actions are needed to quickly neutralize the attack? What caused the attack to occur? And then determine what steps should be implemented to ensure that a breach like this doesn’t happen again? And this storyline requires as much data from your environment that you can get—and those data requirements extend far beyond the endpoint.

So, if you are only monitoring your employees’ endpoints, you are not capturing the complete picture to help you understand how the attacker was able to get in and access your network and your data. In addition to collecting system logs from the employees’ endpoints, logs also are needed from the other components of your organization’s ecosystem including: firewalls, routers, and switches and cloud sources like Azure, AWS, Salesforce, Google etc., as that is the only way you’ll be able to stitch together what happened.

With our MDR service, we can help extend the endpoint protection coverage you currently have in place, and provide you with this complete overview, which will not only help speed up your forensic investigation (should there be one), but will also help get your employees and your business back up and running much more quickly.”

Sample Response Option #2:

“EDR is not MDR. It is a fundamental piece of your security strategy, but it is only one piece of your overall security stack. When designing your organizational security strategy for a business of your size and the industry you are in, you want to implement the most comprehensive coverage available because you want to put in place as many hurdles as you can to make it as difficult as possible for the bad guys to get through.

Hurdles like: proper firewalls, endpoint protection, patch management, backup, MFA, email and spam protection, web filtering, end-user security training, VPNs to encrypt your connections. These are the fundamentals that have to be put in place.

On an individual basis, each of these security pieces are not powerful enough to stop the bad actors from worming their way into your network. But once you combine them together, that is when you increase their overall effectiveness in preventing access to your network and preventing attacks from happening.

Continuation...

And then what an MDR solution does is it strengthens your defenses even more and sounds the alarm bells if it detects that something is off. It provides you with heightened visibility, because it will aggregate the data that is being collected from these fundamental pieces of your security stack and will alert you to when there might be suspicious activity that needs to be investigated.

Without an MDR solution in place—working alongside your EDR—you may never know about the suspicious activity that is happening on your network, and then one day you wake up and all of your organization's data is gone, or money has been emptied out of an account.

So organizations of your size—especially those that reside in regulated industries—need stronger protection and increased visibility beyond what EDR can provide, because the earlier you can detect the suspicious activity and catch it, the less it is going to cost you, and the less of an impact the event will have on your business, and the quicker you will be able to recover.

And so our MDR service is beneficial in helping to fortify your existing security stack.”

Sample Response Option #3:

“Ok. Can I ask who on your team is responsible for demonstrating compliance within your organization?

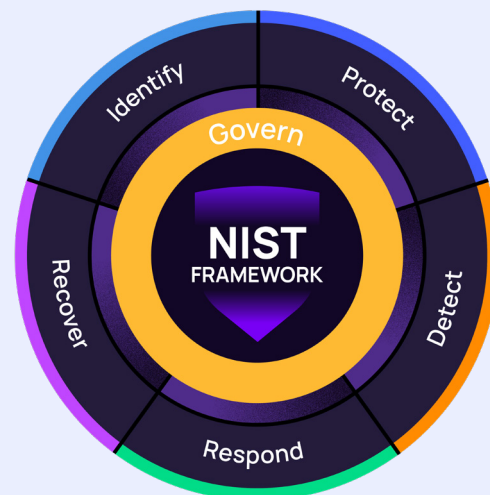
Because compliance standards state that organizations in regulated industries are required to collect system logs and show proof that they can investigate cyberincidents on their network, should a breach occur. And this requirement is coming down from the federal level, from the state level, and from different regulations that are in place.

So, organizations that reside in highly regulated compliance markets need to have a way to collect and aggregate their system logs, and we can help you achieve and maintain compliance with our MDR service.”

Sample Response Option #4:

“Well, we would like to refer to the NIST Cybersecurity Framework (CSF) 2.0 for a minute to explain why just having endpoint protection isn't sufficient coverage for organizations like yours.

We rely upon this cybersecurity framework and use it as our guide to help support our customers' security and compliance requirements, and we follow their risk mitigation and security best practices recommendations very closely.



Continuation...

Looking at this framework, there are now 6 functions associated with it, and many internal IT departments that we engage with are pretty sound when it comes to the Identify, Protect and Recover functions of the framework—where they have their network monitoring, endpoint protection and backup solutions in place

But they are experiencing some real challenges when it comes to the Detect, Respond and Govern functions of the framework, especially when it comes to the 'What happened?' and 'What happens next?' pieces of a successful cyberattack—after an endpoint gets hit with a virus, or after a device gets hit with a ransomware event. Many internal IT departments are not quite sure of the steps that are needed to investigate how an attack happened, and what needs to be done post-attack to ensure an attack like this doesn't happen again.

So to properly deal with the Detect, Respond and Govern functions, it requires toolsets beyond the endpoint protection software that has been installed on the employees' endpoints—it requires an advanced toolkit like a SIEM be put in place, to deal with the more sophisticated attacks that are becoming more and more prevalent, and to deal with the obligations that are being imposed on regulated industries to reduce their cyber risk

A SIEM is now something that many CSF frameworks, including the NIST CSF, recommend be added, on top of your existing endpoint protection coverage—and we can provide that for you through our MDR service.

A SIEM provides the ability to have centralized logging from across local AND cloud resources, all in one centralized location. So, when the forensics team asks the question of 'What happened?' you can provide them with the 'when, where, and what' intel from your SIEM platform to provide them the complete picture, not just what happened on the endpoint itself.

A SIEM also provides the real-time analysis and threat hunting capabilities, and is critical for a speedier incident response process, and enhanced compliance reporting and auditing—which is now being required for the govern function—and again, these are pieces that are not possible if there is only endpoint protection in place."

OBJECTION #2:

“We don’t really need this. We have never experienced a cyberattack or ransomware attack yet. What we have in place today appears to be working well for us.”

Sample Response Option #1:

“I’m really glad to hear this because many organizations that we work with haven’t been as fortunate. But because they were enrolled in our MDR service, we were able to get them back up and running fairly quickly, with little to no damage. Because now-a-days, it isn’t about IF an organization will experience a cyberattack, but more about WHEN, and what will the trail of destruction look like afterwards.

Just because it hasn’t happened to your organization yet, doesn’t mean it won’t eventually happen in the not-so-far-off distant future. With ransomware-as-a-service and the introduction of AI toolkits like ChatGPT, threat actors no longer have to expend a lot of time, money, or effort to catch an under-protected business.

I’m sure that updating your security policies, procedures, and toolkits will be necessary for your team at some point because security standards shouldn’t remain static. So, why put this off and increase your risk exposure if you are going to have make these types of changes in the future anyway? We are designed to act as an extension of your team and you can leverage our expertise and experience to modernize your security posture today, so that when something does happen, it will have minimal impact on your employees or on your organization.”

Sample Response Option #2:

“I’m really glad to hear this because many organizations that we work with haven’t been as fortunate. But because they were enrolled in our MDR service, we were able to get them back up and running fairly quickly, with little to no damage. And because now-a-days, it isn’t about IF an organization will experience a cyberattack, but more about WHEN, and what will the trail of destruction look like afterwards.

But if I can ask: How do you know that you have never experienced a cyber or ransomware attack before? What visibility into your network do you have?”

Because maybe the real answer is: “We have never experienced an attack before that we know of.”

Here you want to try and find out what kind of security solutions or logging toolkits are they using currently?

Because they could have suffered an attack, albeit maybe just a benign one, and one that wasn’t necessarily catastrophic in nature, but then how would they know for sure?

Continuation...

Here you want to probe to uncover what capabilities do they have (or don't have) in place from a detection and reporting perspective to help them understand what is going on within their network at all times. You want to understand what sort of monitoring and alerting tools are being used to proactively look for threat attempts and providing them with the insight and visibility they need.

If we use a car analogy here: Just because a car is driving down the road, doesn't mean that it might not have a hole in the oil pan. And if you are not proactively checking the oil pan to ensure that there isn't a hole, you will never know there is a problem until the engine ceases and you get stranded at the side of the road.

So, unless you are monitoring your car's gauges and continually checking what your oil pressure and engine temperature is, you don't actually know how well your engine is working. That is the whole reason why cars have gauges, so the driver can monitor and fix any problems that arise.

Sample Response Option #3:

"How lucky and fortunate you have been to never have experienced a cyberattack before. Having a security plan in place is step one, but have you ever had the opportunity to test that plan? Everyone has a plan until they have an incident and that's when the real challenge begins.

Because if you ever did suffer a cyberattack, what is your confidence level that your team would be able to quickly and easily handle this crisis, and, looking post-incident, what confidence do you have that your team will have to the appropriate telemetry data needed, in the event you wanted to file an incident response claim?

It is about what you are going to do when something happens, not if. And with our MDR service, we can take the guesswork out of this for you and your team. We can help you develop and implement a crisis response plan and manage this all for you and have all of the appropriate data necessary afterwards if you need file a claim."

OBJECTION #3:

“We are currently already looking a different SIEM software providers to implement internally for our team to manage.”

Sample Response Option #1:

“That is fantastic news to hear. How is your search going so far? And how much have you budgeted for this? As SIEMs can get to be pretty expensive due to the amount of data that gets collected and stored in the cloud.

And pricing can be unpredictable and fuzzy because how can you predict how many alerts are going to be coming into your SIEM platform on a daily basis?

Many of the complex customer environments we are seeing today are generating billions of alerts, and all of that data needs to get processed.

As a result, we are finding that many SIEM providers are being opportunistic and charging a lot of money for data ingestion, and companies don't really have a choice but to pay those ingestion costs.

But, with our MDR service, we charge \$0 for data ingestion and storage. We include it as part of our monthly fee, so we can provide you with a level of budget predictability when it comes to your security investment.”

Sample Response Option #2:

“That is great news to hear. Do you mind if I ask a few questions around some of the products you are considering? With the products you are evaluating now, what sort of monitoring and detection capabilities do they have?

Because with our MDR platform, it contains:

- ▲ AI and machine learning algorithms to detect known and unknown threats, specifically when it comes to determining an insider threat, account takeover, privilege abuse or misuse
- ▲ User & Entity behaviour analytics to help identify, detect, analyze and prioritize anomalous end-user behaviour in real-time, which we feel is an important piece of our platform
- ▲ Our User & Entity behaviour analytics provides the ability to be predictable about what an end-user typically does, and is useful in flagging what is normal vs what is abnormal in terms of employee behaviour, so that the abnormal behaviour can be immediately investigated to see if the actions are legit

Continuation...

- ▲ The use of 'honeypots' to spot early indicators of compromise, and to provide your organization with another way to detect threat actors that may already be in your environment, so that we can quickly stop them before they access your critical systems or data.
- ▲ Darknet Exposure Monitoring to search for confidential information and leaked accounts on the deep and dark web before it falls into the wrong hands. We can help you identify darknet compromise early on, before your data can be used to exploit you

ASK: Does your organization already subscribe to a separate dark web monitoring service? If so, we may be able to provide you with some license consolidation and cost savings, as this feature is already included in our MDR platform, at no additional cost—so why pay for redundancy?

It also includes perimeter defense monitoring where our service will monitor your organization's external IPs with regular scans to look for: Port changes, certificate issues, and known vulnerabilities—and if any issues or changes are detected, perimeter defense will trigger a detection alert that will be investigated.

Maybe we can set you up on a proof-of-concept so you can compare our solution to some of the ones you are currently looking at?

OBJECTION #4:

“We are currently already using an MDR service with someone else, so we are covered.”

Sample Response Option #1:

“That is great to hear that you already understand the importance of MDR and why your organization requires it.

Do you mind if I ask you a few questions about the MDR service you are currently using?

I'm curious to hear what their incident response process like?

Like when a threat is detected in your environment, what happens next? Does the threat get passed over to your team to handle? Or does the company that you have partnered with deal with detections?”

Continuation...

If the answer is: “When they detect a threat, they send us a ticket and forward the alert over to our team to handle.”

Sample Response:

“With our MDR service, we provide our customers with what we call the ‘Big R Response’ vs. what you are describing as their “little r response.”

Are you aware as to how fast a vulnerability can move throughout your environment? When a threat is detected by the system, time is your enemy. It needs to be neutralized and halted as quickly as possible, because it only takes minutes before your whole network and important company data could be wiped out.

If your MDR service provider sends you a ticket at 3am to warn you of an event that is happening in your environment, and you or your team are sleeping and not responding, you might be walking into a pretty serious situation when you get into work. Or what happens if the alert comes in over the weekend? Or during a holiday? The quality of life of your staff may be compromised if your team is expected to work around the clock.

It’s great that you have an MDR service in place, but if it is only an ‘alert factory’, where you are then responsible for dealing with the alerts that you receive, then that actually isn’t very helpful to your team. Because there is the risk that it may take some time before anyone on your team becomes available to address them—and who knows what damage may have occurred by then?

Let our MSP take over this function for you with our MDR service. The difference with our service is that we have a human intervention piece—a team working around the clock—that is going to take corrective action on your behalf to stop any breaches that might occur. Our dedicated SOC and cyberanalysts can augment your team and intervene to complete the actual security work for you, instead of just throwing what is detected over the fence for you to deal with.

This will afford your team a better work/life balance and improved operational efficiencies, as it will allow your team to focus on its primary activities and other strategic projects that they may be working on, instead of being continually distracted with the alert tickets coming in.”

OBJECTION #5:

“We currently have dedicated internal security staff, so we don’t the services of an MSP at this time.”

Sample Response:

“Fantastic! Do you mind if I ask a few questions to gain an understanding of what this looks like for you?”

- ▲ How many cyber specialists do you currently have on your team?
- ▲ How many hours do they each work?
- ▲ Do they work a standard 8x5 shift, or do you run multiple shifts?
- ▲ Are there any feelings being expressed where the team is feeling overwhelmed or overworked?

If so, we can help create space for them. We can be THEIR backup so that they can take holidays, vacation, personal and sick days and have it not impact the rest of the team or the organization.

And as your organization grows, scalability won’t be an issue as our team can grow alongside your team.”

OBJECTION #6:

“We can take care of this ourselves with our existing technical team. We don’t need the services of an MSP at this time.”

Sample Response Option #1:

Qualify if the internal IT director understands the differences between a Network Operations Center (NOC) and a Security Operations Center (SOC) and the roles and responsibilities of each.

Ask

- ▲ “How many people work within your IT Department?”
- ▲ “Do you have a separate SOC setup or separate security team that is independent of your NOC and NOC engineering team? Or are the same individuals responsible for both functions?”
- ▲ “Does your team operate on a 24/7 basis to ensure sufficient oversight and protection coverage?”

Continuation...

If the answer is: “We have 1 team that handles both the NOC and SOC function for our organization.”

Reality: This team is overextended

NOC and SOC personnel should be separate, as they have different skillsets, goals, and priorities

SOC Team:

- ▲ Responsible for managing the organization's security posture
- ▲ Responsible for preventing, detecting, analyzing, and responding to cyberthreats
- ▲ Monitors the network for suspicious activity and breaches
- ▲ Utilizes a SIEM

NOC Team:

- ▲ Responsible for the management of the organization's network infrastructure
- ▲ Responsible for monitoring network performance, troubleshooting issues, and maintaining network reliability and availability
- ▲ Utilizes network monitoring tools and automation

“Mr. IT Director, The NOC function and the SOC function are two very different roles, with two very different sets of priorities, goals, and responsibilities.

Why don't you consider leveraging our SOC team to take the security workload off of the shoulders of your existing team?

This will allow your NOC team to remain focused on their core set of responsibilities: Responding to employees' concerns, dealing with and troubleshooting network issues, and performing the necessary maintenance tasks that are required to keep your infrastructure running as optimally and efficiently as possible?”

If the answer is: “Our team does operate 24x7x365.”

Sample Response Option #2:

“Mr. IT Director, could you clarify what you mean by 24x7x365 coverage? Because having staff that are 'on-call' is not sufficient from a cybersecurity perspective.

Continuation...

What happens when an alert comes through at 2am? Every second counts when a threat is detected. And every second that is wasted can quickly escalate to becoming a crisis situation for you.

For sufficient security coverage and for proper risk mitigation, it is recommended that an organization have—at a minimum—6-7 dedicated security personnel, and this is assuming that no one gets sick or takes unexpected time off. And this is IN ADDITION TO your regular helpdesk and networking personnel.

Why don't you consider leveraging our team to handle the 'around-the-clock' security coverage that you require and allow your team to focus on their core set of responsibilities, while providing them with a better work/life balance? No longer will your team be required to be 'on call'. Rather you can leave the 2am threat detection, response and remediation for our team to handle on your behalf."

OBJECTION #7:

"We are planning on hiring our own team of cybersecurity specialists to join our team."

Sample Response Option #1:

"That is great to hear. But do you know how long it will take to get the team all in place and to setup your own SOC? And how expensive that endeavor will be? And what is being done in the meantime to ensure your employees and your organization's network remains safe and secure from attacks?"

Because even if you were able to hire all of your new security employees tomorrow, it will likely still take several months to get everyone ramped up and working cohesively together. So, during this timeframe, your employees and the network are still at significant risk.

A main benefit of partnering with us and enrolling in our MDR service, is that we are a turn-key solution, and will not require a substantial amount of time to ramp up. Once our MDR platform is installed and tuned, we are ready to go so this can reduce your implementation from taking a few months to just a few days when using our team. We can provide you with the immediate visibility and insight you require to start monitoring and tracking what is going on within your network, at a fraction of the cost of attempting to implement this yourself."

Sample Response Option #2:

"How is your search going? What kind of success are you having at sourcing quality cybersecurity talent? And what happens if one of your new cybersecurity analysts quits?"

Many of our customers that we support seem to be struggling with a high degree of employee turnover lately.

Continuation...

They go and make the investment in getting their new cybersecurity analysts all trained up, and then once that person gets a few years under their belt and gains some proper experience, that person gets poached by another firm, lured away by the chance to make more money.

And so now they need to start all over again, back to trying to find and hire another analyst to replace the individual who left. It seems to be a cycle that these organizations have a hard time breaking.

Whereas, if you decide to partner with us by enrolling in our MDR service, we can help address this issue of expensive and disruptive employee turnover for your organization. You can offload that responsibility to us, or we can augment the team that you currently have in place."

OBJECTION #8:

"You are just trying to make my team and I look bad in front of my CEO. You want to make us look incompetent like we don't know what we are doing."

Sample Response:

"Actually, no. We want to make you look knowledgeable and informed in front of your CEO.

Our dashboard access and response actions can be tailored based on how involved or how hands off you and your team need or want to be, and then based on your requirements, we can customize the response plan to align to what makes the most sense for you. We can setup the rules of engagement based on who will do what, when a breach occurs.

We pride ourselves on providing our customers with equitable access to all of the data—we both have access to the data in the event of a breach. You can also complete your own validation on things that might be happening in your environment, and you have authority to make your own decisions based on what the data is telling you. The service that we offer isn't like a black box where you don't know what is going on.

We provide transparency and visibility to our customers so you can see what is happening and what is being done. So in the event of a breach, if your CEO does come looking to you for answers, you can log into the dashboard and see all the notes and every single action that has been taken by our team, in chronological order, so you can give your CEO the answers they require. You will be kept up-to-date and informed as to what is transpiring and you will never be running blind. Our service allows you to trust, but verify, because you have access to all of the data—the same as we do."

OBJECTION #9:

“We can’t use an outside service because we need the ability to run our own reports, whenever we may need them.”

Sample Response:

“Because we provide equitable access to all of the data, we can provide you with the capability to generate your own reports, should you need them.

I know for organizations that reside in regulatory industries, you need to have the ability to run your own reports because you can’t just accept whatever reports a vendor may supply you with.

Or if an auditor or regulator happens to visit your location, and begins asking that you show proof that you are collecting and aggregating your system and security logs, you can log into the dashboard yourself and do a search query to get them the data that proves you are doing things correctly.

Whereas with some other services, it can become a situation where you might have to contact your MDR provider to ask them to send you a report, but it could be a couple of weeks before you can get that report and send it over to the regulators.

That isn’t a concern with our service. You can generate the report yourself, and hand it straight over to the regulator without any delays. That is the transparency that our service can provide.”

OBJECTION #10:

“We have other priorities and other technology upgrade projects that we are focused on first at the moment.”

Sample Response:

“Understandable. But in the meantime, is your network currently exposed and at risk while you are working on implementing these upgrade projects?

Traditionally, infrastructure improvement projects take time, so while your team is busy working on these initiatives, our MDR service can provide your organization with a safety net, as it can protect your existing network setup now, while being flexible to accommodate the changes that you are working towards.

Our service is both tools- and hardware-agnostic. So, you don’t need to wait to finish your technology upgrades first before you get the right security protection coverage in place.

We can work with you and your team to understand your tech roadmap, and provide you with a solution that will span that growth, all while providing you with the right set of security services you need in the meantime, so that your organization is not left vulnerable and at risk.”

OBJECTION #11:

“We have other priorities at the moment – we are in the middle of acquiring another company, so this is something that has to be put on hold for the time being.”

Sample Response:

“Our solution is great for organizations that are going through M&A, as we can provide immediate protection coverage for both organizations, while your team is busy working through the technology consolidation that generally occurs when companies are joined together.

Usually in M&A situations, there are mixed environments that you need to contend with, where the endpoints have different technologies loaded on them, or the environment has different firewalls that are being used, and our MDR service can monitor and support it all—right out of the gate—until you are able to start standardizing the new organization onto your preferred tech stack.

There isn't a need to wait for their licenses to expire or for renewals to come up to make the switch. There isn't a need to leave your newly acquired company unprotected during this transition. You can provide immediate protection as our MDR service can pull it all in, no matter what the other company is using on their endpoints or network.”

OBJECTION #12:

“We don't really need anything like this, as we don't reside in a regulated industry.”

Sample Response:

Ask a few probing questions to determine if this is truly the case:

“Do you accept credit cards?” If YES, they are regulated

“Do you fall under the Federal Trade Commission and the FTC Safeguards Rule?” If YES, ask:

“Are you aware that you fall under the Federal Trade Commission and the FTC Safeguards Rule applies to you?”

The FTC Safeguards Rule requires covered companies to develop, implement, and maintain an information security program with administrative, technical and physical safeguards designed to protect consumer information.

Continuation...

This applies to any non-banking institution that is handling finance:

- ▲ Advertising and marketing firms
- ▲ Credit and finance companies
- ▲ Privacy and security companies
- ▲ Mortgage companies and mortgage brokers
- ▲ Debt collectors
- ▲ Car dealerships

"So in fact, you actually DO reside in a regulated industry, and therefore need to comply to these standards."

OBJECTION #13:

"This sounds like an expensive service. We don't have the budget for this."

Sample Response Option #1:

If you hear this, it may help to review a simple ROI scenario to get the IT Director and CEO to understand what the true costs of a security breach are and the impact it can have on their business.

The goal of the exercise is to help educate that it will be cheaper in the long-run to partner with your MSP and enroll in your MDR service than it is to pay out after the fact.

Help them to understand that the total cost of a security breach isn't just the ransomware payment that may need to be paid if the IT Director and their team are not able to get all of the organization's data back.

- ▲ Ransomware payment – the average ransomware payment in 2023 was reported to be \$1.54 million USD¹
- ▲ Regulatory fines & penalties
- ▲ External forensics
- ▲ Crisis communication expenses
- ▲ Attorney fees & legal costs
- ▲ Higher insurance premiums levied
- ▲ Consultancy costs & employee training

Continuation...

- ▲ Infrastructure improvements
- ▲ Collateral damage
- ▲ Risk of attack reoccurrence
- ▲ Loss of sales and/or customers
- ▲ Reputational damage with possible extinction

2022 IBM study reported the average cost of a ransomware attack—taking all of these intangible costs into account, amounted to \$4.62 million USD², and that EXCLUDES the ransomware payment.

When you factor in the ransomware payment of \$1.54 million USD, total breach costs could easily exceed \$6.16 million USD.

But when you compare that to what you would be charged on an annual basis for your MDR service, you will find that it is cheaper to prevent than to payout.

1 <https://www.paloaltonetworks.com/blog/2022/06/average-ransomware-payment-update/#:~:text=The%20numbers%20are%20startling%3A%20The,rose%2071%25%20from%20last%20year.>

2 <https://www.netapp.com/blog/ransomware-cost/#:~:text=In%20fact%2C%20the%20average%20ransom, cost%20of%20a%20ransomware%20attack>

“With your current departmental and technological setup, I would hate to see your organization suffer a breach.

Is the \$90/user that I am charging per month for our MDR service really that more expensive than your organization suffering a potential security breach that could cost you well north of \$6,000,000? Or worst case, cost you your livelihood and the livelihood of your employees who depend on you?

For an annual cost of \$135,000 [125 users*\$90/user], it isn’t even possible to hire one qualified cybersecurity analyst for your organization. And to protect an organization like yours, you would need a minimum of 6-7 analysts to provide around-the-clock security monitoring and protection coverage.

So for \$135,000 per year, you are gaining access to an entire TEAM of 24x7 security personnel AND security monitoring, reporting, and log correlation software—giving you the power of a full SOC and SIEM service, at a fraction of the cost to build and implement one on your own.

And we would be working alongside you every step of the way, supporting your security and compliance requirements.”

Continuation...

Sample Response Option #2:

"We might be able to save you some money that can then be used to help partially cover the costs of our services, as we might be able to reduce some of the redundancy that may exist with respect to the security toolsets you are currently using.

As an example: Are you currently paying for a security toolset to perform dark web monitoring for you? Or is this something that you are potentially looking into?

If yes: then our MDR service INCLUDES Darknet Exposure Monitoring that can be used to search for confidential information and leaked accounts on the deep and dark web before it falls into the wrong hands. And if a business account is found to be leaked, then notifications will be sent out and password resets will be implemented to protect the user. Many cyberattacks rely on stolen credentials, so being able to help an organization identify darknet compromise early on before their data can be used to exploit them can make a real difference between a minor inconvenience and major incident.

So if you are using a dark web monitoring service already, or if this was something that you were going to look into, we can offer you some technology consolidation and license cost savings potentially."

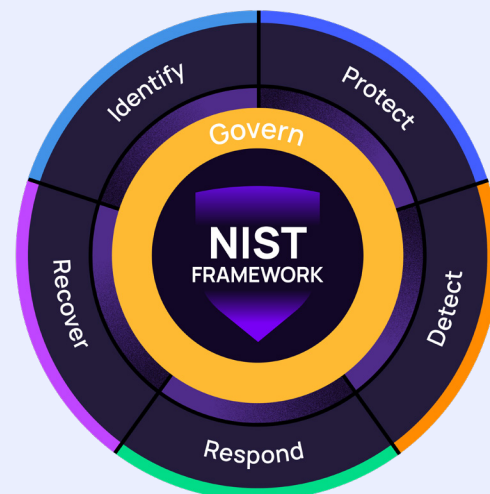
Sample Response Option #3:

"Well, we would like to refer to the NIST Cybersecurity Framework 2.0 for a minute to provide you with the justification that you can take to your Executive Team to help them understand that this is a core component of the business that they need to be involved it, and it has become something that they have no choice but to fund.

Security is no longer just a technical problem that the executive leadership team can just brush off and leave up to the internal IT department to deal with.

It has evolved to become a business risk that needs to be managed properly, with proper funding allocated towards it."

When we look at the NIST Cybersecurity Framework, it is the guide that WE rely upon to help support our customers' security and compliance requirements, and we follow their risk mitigation and security best practices recommendations very closely.



Continuation...

You may not be aware, but as of February 2024, the framework was updated to include a 6th function that is called 'Govern', and this is a change that can really benefit someone in your position. Because if you are receiving pushback from the executive team—like your CEO or CFO—where they are hesitant to implement your recommendations to improve your overall organizational security posture, then these changes to the NIST CSF are something that you can leverage to help gain the buy-in and resources that you are looking for to help fund this kind of initiative.

The inclusion of the new Govern function reinforces the message that organizations—starting at the very top at the Executive level - need to accept and be held responsible for managing their own cyber risk, and if the organization suffers a breach due to lack of due care and due diligence, then that is on them.

Business leadership has a fiduciary responsibility to do what they can to prevent loss of value in the business by implementing 'reasonable measures' to protect themselves. Our MDR can be considered one of those 'reasonable measures' to protect an organization's business value as a result of a cyberattack or data breach."

Sample Response Option #4:

"I can understand that this might not have been an arrangement that you have budgeted for. Are you currently facing insurance premium rate increases from your cyber liability insurance provider?"

Because if you are, we may be able to help you reduce those premiums by implementing our MDR service that contains security controls that go above and beyond what insurance companies are looking for. In some cases, you may be able to ask your insurance provider for a reduction in premiums by demonstrating that you have gone further than what was actually needed."

****PLEASE NOTE:** There is no guarantee when it comes to this objection handling approach, but some insurance providers reduce cyber liability insurance premiums for improved cybersecurity posture. MSPs should be encouraged to check with their cyber liability insurance provider to see if this is an option.

Sample Response Option #5:

"I can understand that this might not have been an arrangement that you have budgeted for. But would this be an opportunity where we could look at switching up the budget allocation?"

As an example: If we are able to remove this responsibility and critical function from your team's plate, does this free up your team and give you some time back that can be used elsewhere, like on other projects or strategic initiatives the company may have that you haven't been able to get around to?

Continuation...

Would you see this as providing a benefit to you? Helping you to save on labor hours so those hours could be re-allocated elsewhere? Helping you save on subscription licensing costs, so that budget could be used elsewhere within your department?

With our Co-managed MDR option, we can help your team tackle multiple priorities at once.”

OBJECTION #14:

“Why should we trust you to take care of this for us?”

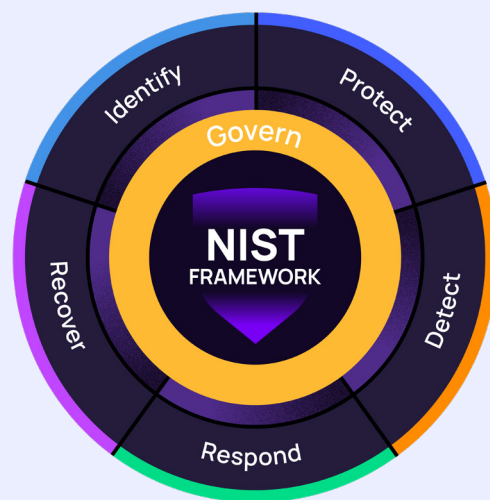
Sample Response:

“Our MSP and the MDR service that we use to support our customers’ security and compliance requirements, closely follow the risk mitigation and security best practice recommendations put forth by the NIST Cybersecurity Framework 2.0.

This is a service that we offer through a company called N-able, who has purchased a cybersecurity firm called Adlumin, and it is via Adlumin that we leverage their US-based, 24x7 enterprise-grade security operations center and their patented MDR platform that gives us the ability to provide effective security monitoring, threat hunting and detection services, vulnerability monitoring and management, proactive and timely incident response and remediation services, along with the reporting and analytics required to keep organizations secure, and safe from attackers and auditors alike.”

To check out N-able’s website:

<https://www.n-able.com/products/adlumin>



Step 7: Setting Your Go-To-Market Sales and Marketing Goals

It will be important to create goals and track them in order to measure the success of your co-managed GTM strategy. Without setting goals, it will be difficult to tell how well your strategy is working.

There are two different sets of tracking metrics to gauge the success of your co-managed services sales and marketing efforts:

1 Key Performance Indicators (KPIs) for In-person or virtual event

2 KPIs to track the overall success and growth of the entire co-managed business model

KPIs to measure the success of an in-person or virtual event



- ▲ Event Registration vs. Target
- ▲ Event Attendance vs. Target
- ▲ Event Marketing Effectiveness Metrics (email vs. SDRs vs. social)
- ▲ Number of Sales Qualified Leads Generated vs. Target
- ▲ Pipeline Generated vs. Target
- ▲ New Customers Acquired vs. Target
- ▲ Customer Acquisition Cost
- ▲ Event ROI
- ▲ Event feedback surveys received vs. # of Attendees
- ▲ Event Budget vs. Actual Spend

GOAL: Where do you want to see your co-managed services line of business in the next 12 months?

- ▲ # of new co-managed clients?
- ▲ Total value of new co-managed MRR contracts signed?
- ▲ Average Deal Size of co-managed MRR contracts
- ▲ Marketing metrics and traction in generating leads
- ▲ Sales metrics to close opportunities

Keys to Marketing and Sales Success

Regardless of what type of security program you design and take to market, a few final remarks:



1 Be sure to select the right type of customers to do business with, and aim to discern that they are a good fit for your business model.

In your planning stages, spend time thinking of your Ideal Client Profile and defining the types of companies you want to have for both customer types and be sure to communicate this ideal to everyone on your team.

2 Focus on your messaging and how you craft your value prop statements.

When creating your GTM plan for your security services, think like a CEO or a CFO and reflect on what do these types of senior executives primarily care about?

They care about:

- ▲ Profitability
- ▲ Growth
- ▲ Scalability
- ▲ Mitigating any and all exposure to risk, because risk can impede or inhibit growth for their organization

Also think about what does the IT Leadership team care most about?

They care about:

- ▲ Being able to successfully complete important IT projects in a timely manner
- ▲ Competently and efficiently handling the day-to-day tasks that are needed to properly care for their network infrastructure
- ▲ Creating and maintaining a reliable and dependable network environment in order to keep the employees' working and productive
- ▲ Keeping employee morale high and keeping their technical employees engaged and excited to come to work
- ▲ Reducing employee technical churn by creating a positive work/life balance
- ▲ Mitigating the organization's risk exposure and doing everything possible to keep the business and its critical data safe and secure

3 Take care of the marketing basics prior to launch.

Ensuring the following activities are completed and in place:

- ▲ Your website is up to date and contains the new messaging about your security services
- ▲ Your company and personal LinkedIn and Google Business profiles are updated to announce the new set of services your MSP is now offering
- ▲ You have collected sufficient amounts of social proof from existing customers and/or have created case studies to highlight how your services have helped their businesses' succeed
- ▲ You have implemented a proactive sales outreach telemarketing motion to make phone calls into prospective companies to build interest and awareness



At N-able, our mission is to protect businesses against evolving cyberthreats with a unified cyber resiliency platform to manage, secure, and recover. Our scalable technology infrastructure includes AI-powered capabilities, market-leading third-party integrations, and the flexibility to employ technologies of choice—to transform workflows and deliver critical security outcomes. Our partner-first approach combines our products with experts, training, and peer-led events that empower our customers to be secure, resilient, and successful. n-able.com

This document is provided for informational purposes only and should not be relied upon as legal advice. N-able makes no warranty, express or implied, or assumes any legal liability or responsibility for the information contained herein, including for the accuracy, completeness, or usefulness of any information contained herein.

The N-able trademarks, service marks, and logos are the exclusive property of N-able Solutions ULC and N-able Technologies Ltd. All other trademarks are the property of their respective owners.

© 2026 N-able Solutions ULC and N-able Technologies Ltd. All rights reserved.