N-ABLE

HEAD NERDS

Playbook für Security Sales

Schützen & Wachsen: Chancen in der Cybersicherheit optimal nutzen

Aufbau eines Advanced Security Program

Dieses Digitale Playbook für Security Sales gibt MSPs eine wertvolle Hilfestellung beim Aufbau eines erfolgreichen Cybersecurity-Geschäfts. Es bietet eine Übersicht über die wichtigsten traditionellen Programme, die von MSPs erfolgreich beworben und verkauft werden, sowie Beispiele für Preisgestaltung, Verkaufsskripte und Marketingmaterialien, die Sie individuell anpassen können.

HAFTUNGSAUSSCHLUSS

Einleitung

Die richtige Preisgestaltung ist für viele MSPs nach wie vor eine der größten unternehmerischen Herausforderungen. Als Head Nerd im Bereich Vertrieb und Marketing erhalte ich oft Fragen von MSPs wie:

- „Wir hätten Interesse daran, [Name des Sicherheitsprodukts] in unser Angebot an Sicherheitslösungen aufzunehmen, aber das Preismodell für den Endkunden ist uns noch nicht ganz geheuer und hält uns doch irgendwie davon ab, es auf den Markt zu bringen."
- „Haben Sie Material zu den Vermarktungspreisen/-strategien für [Name des Sicherheitsprodukts]?"
- „Mein Kunde interessiert sich für [Name des Sicherheitsprodukts], aber ich bin mir nicht sicher, was ich dafür verlangen soll."

Also haben wir diesen Leitfaden zusammengestellt, um MSPs Strategien an die Hand zu geben, wie sie am besten mit diesen Arten von Vertriebs- und Preisanfragen umgehen können.

Die in diesem Leitfaden enthaltenen Tipps können auf JEDE Art von Produkt oder Dienstleistung angewendet werden, die ein MSP potenziell verkaufen möchte.

Ich hoffe, dass Ihnen dieses Playbook weiterhilft! Happy Selling!

Stefanie Hammond

Head Nerd – Vertrieb und Marketing

n-able.com/de/team-member/stefanie-hammond

So bauen Sie ein Advanced Security Program

für den traditionellen Managed-Services-Kunden auf

Was ist das eigentlich?

Ein Programm, das einen umfassenderen Sicherheitsansatz verfolgt, indem es eine Reihe robusterer Dienstleistungen rund um Sicherheit, Gefahrenerkennung und -abwehr enthält, die über den Endbenutzer und den Endpunkt hinausgehen und alle Komponenten der Netzwerkumgebung eines Unternehmens umfassen, einschließlich Netzwerkgeräte, SaaS, VPN, Firewalls und die Cloud.

Zielgruppe für das Advanced Security Program

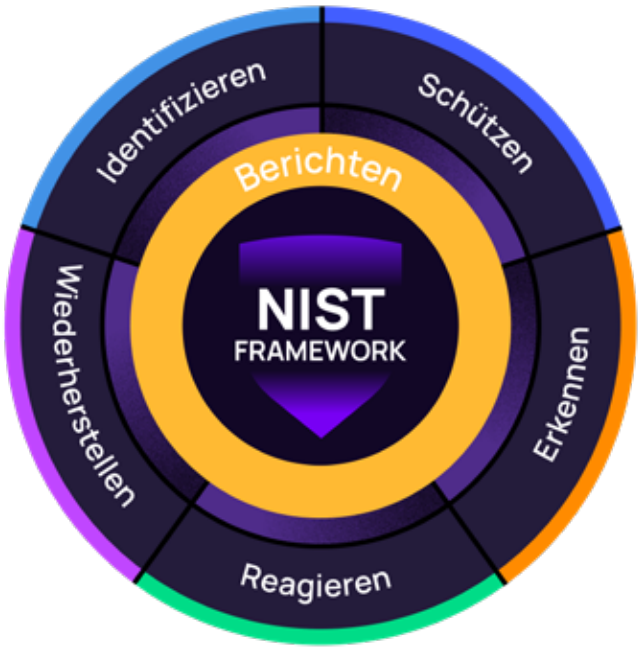
Der ideale Kunde für das Advanced Security Program ist:

- Eine Organisation, die keinen eigenen internen IT-Administratoren und keine IT-Mitarbeiter beschäftigt
- Eine Organisation, die in einer Branche tätig ist, für die Sicherheitsrichtlinien gelten, und die daher verpflichtet ist, die Einhaltung dieser Richtlinien gegenüber einer Prüfstelle nachzuweisen, z. B.:
  - Bankwesen
  - Finanzwesen
  - Gesundheitswesen
  - Bildungswesen
  - Lokale und staatliche Behörden
- Eine Organisation, die es gewohnt ist, Budgets für IT bereitzustellen, und die sich der Bedeutung eines umfassenderen Pakets an Sicherheitsdiensten bewusst ist
- Eine Organisation, die ihr Return-to-Operations-Ziel (RTO) als mittel oder hoch einstufen würde – was bedeutet, dass es sich um ein vollständig digitalisiertes Unternehmen handelt, das im Falle eines Cyberangriffs nicht auf manuelle Prozesse zurückgreifen kann. Daher wäre es dringend erforderlich, die Mitarbeiter und das Geschäft so schnell wie möglich wieder online zu bringen, damit die Organisation rasch wieder Umsatz generieren kann.

- Eine Organisation, die in Bezug auf die Risikosegmentierung als Unternehmen mit mittlerem/mittlerem bis hohem/hohem Risiko einzustufen ist. Das heißt:
  - Sie ist, gemessen am Jahresumsatz und der Anzahl der Mitarbeiter, eher groß
  - Sie sammelt und speichert eine erhebliche Menge an Daten – Finanzdaten, personenbezogene Daten, sensible geistige Eigentumsrechte – und die Mitarbeiter haben Zugriff auf diese Datenspeicher
  - Sie hat eine Reihe strategischer Partnerschaften und daher haben die Mitarbeiter möglicherweise Zugriff auf ihre sensiblen Systeme oder die Daten der Partner
  - Die Auswirkungen eines Cyberangriffs wären gravierend und könnten wohl zum Zusammenbruch der Organisation führen

Im Advanced Security Program enthaltene Dienste und Funktionen

Wie das Essential Security Program wurde auch das Advanced Security Program gemäß dem NIST Cybersecurity Framework entwickelt.



IDENTIFIZIEREN: Bestandserkennung für Netzwerktransparenz

- Monatliche Bewertung des Sicherheitsrisikos
- Bestandserkennung (mithilfe einer **RMM-Plattform wie N-central oder N-sight** und einem Produkt wie **Ranger von SentinelOne**)
- Software-Inventarisierung & Lizenzverwaltung (mithilfe einer **RMM-Plattform wie N-central oder N-sight** und **Passportal**)
- Hardware-Bestandsaufnahme & Bestandsmanagement (mithilfe einer **RMM-Plattform wie N-central oder N-sight** und **Passportal**)
- Überwachung der Infrastruktur-leistung (Server, Desktops, Firewalls, Switches/Router, alle Betriebssysteme)

SCHÜTZEN: Alle Systeme und Personen

- Geräteoptimierung
- Routinemäßige vorbeugende Wartung der Infrastruktur (Server, Firewalls, Switches/Router)
- Patch-Management für Endpunkte: Mac, Windows + Drittanbieter (über RMM)
- Wartung & Verwaltung der zentraler Anwendungen (falls zutreffend)
- Websicherheit (**einsetzbares N-able-Produkt: DNS Filter**)
- E-Mail-Sicherheit, E-Mail-Filterung und -Schutz (**einsetzbares N-able-Produkt: Mail Assure**)
- Passwortverwaltung und -sicherheit (**einsetzbares N-able-Produkt: Passportal**)
- Einführung und Durchsetzung von 2FA/MFA
- Darknet Monitoring (**einsetzbares N-able-Produkt: N-able MDR**)
- Festplattenverschlüsselung für Geräte
- Schwachstellenmanagement
- Erweiterte Gefahrensensibilisierung der Mitarbeiter durch Schulungen
- Endpoint Detection & Response (**einsetzbares N-able-Produkt: SentinelOne EDR Complete**)
- Erstellung und Durchsetzung von Zugangskontrollen für Daten
- Erstellung und Durchsetzung von Anwendungssteuerung und Sicherheitskontrolle
- Erstellung und Durchsetzung von Sicherheitsrichtlinien
- Empfehlung und Durchsetzung von Sicherheitskontrollen
- Backup – Workstation (**einsetzbares N-able-Produkt: Cove Data Protection**)
- Backup – Server (**einsetzbares N-able-Produkt: Cove Data Protection**)
- Backup – Microsoft 365 (**einsetzbares N-able-Produkt: Cove Data Protection**)
- Standby-Image mit Hyper-V-, ESXi- und/oder Azure-Zielen (**einsetzbares N-able-Produkt: Cove Data Protection**)
- Backup-Wiederherstellungstests (**einsetzbares N-able-Produkt: Cove Data Protection**)

ERKENNEN: Abweichende Aktivitäten

- Endpoint Detection & Response (**einsetzbares N-able-Produkt: SentinelOne EDR Complete**)
- Managed Detection Services für Cloud-Dienste (M365, Google, Salesforce, Azure, AWS) (**einsetzbares N-able-Produkt: N-able MDR**)
- Syslog-Überwachung und Protokollsammlung (**einsetzbares N-able-Produkt: N-able MDR**)

REAGIEREN: Auf erkannte Bedrohungen

- Das eigene Reaktions- und Behebungsprotokoll des MSP oder das Reaktions- und Behebungsprotokoll über **N-able MDR** (für alles, was im MSA inbegriffen ist)

WIEDERHERSTELLEN: Systemfunktionalität, Mitarbeiterproduktivität und Datenverlust

- Backup – Workstation – Kritische Dokumente (**einsetzbares N-able-Produkt: Cove Data Protection**)
- Backup – Server (**einsetzbares N-able-Produkt: Cove Data Protection**)
- Backup – Microsoft 365 (**einsetzbares N-able-Produkt: Cove Data Protection**)
- Backup-Wiederherstellungstests (**einsetzbares N-able-Produkt: Cove Data Protection**)
- Standby-Image mit Hyper-V-, ESXi- und/oder Azure-Zielen (**einsetzbares N-able-Produkt: Cove Data Protection**)
- Disaster Recovery-Planung
- E-Mail-Archivierung (einsetzbares N-able-Produkt: Mail Assure)
- 365 Tage Datenaufbewahrung der gesammelten MDR-Daten (angeboten über N-able MDR Advanced)
- Endpoint Detection & Response (**einsetzbares N-able-Produkt: SentinelOne EDR Complete**)

BERICHTEN: Treuhänderische Verantwortung und Rechenschaftspflicht

- Monatlicher Bericht, einschließlich der Ergebnisse der regelmäßigen Wiederherstellungstests
- Compliance-Insights (**angeboten über N-able MDR Advanced**)
- Lebenszyklusplanung für Bestände
- Vierteljährliche Übersicht für die Geschäftsführung

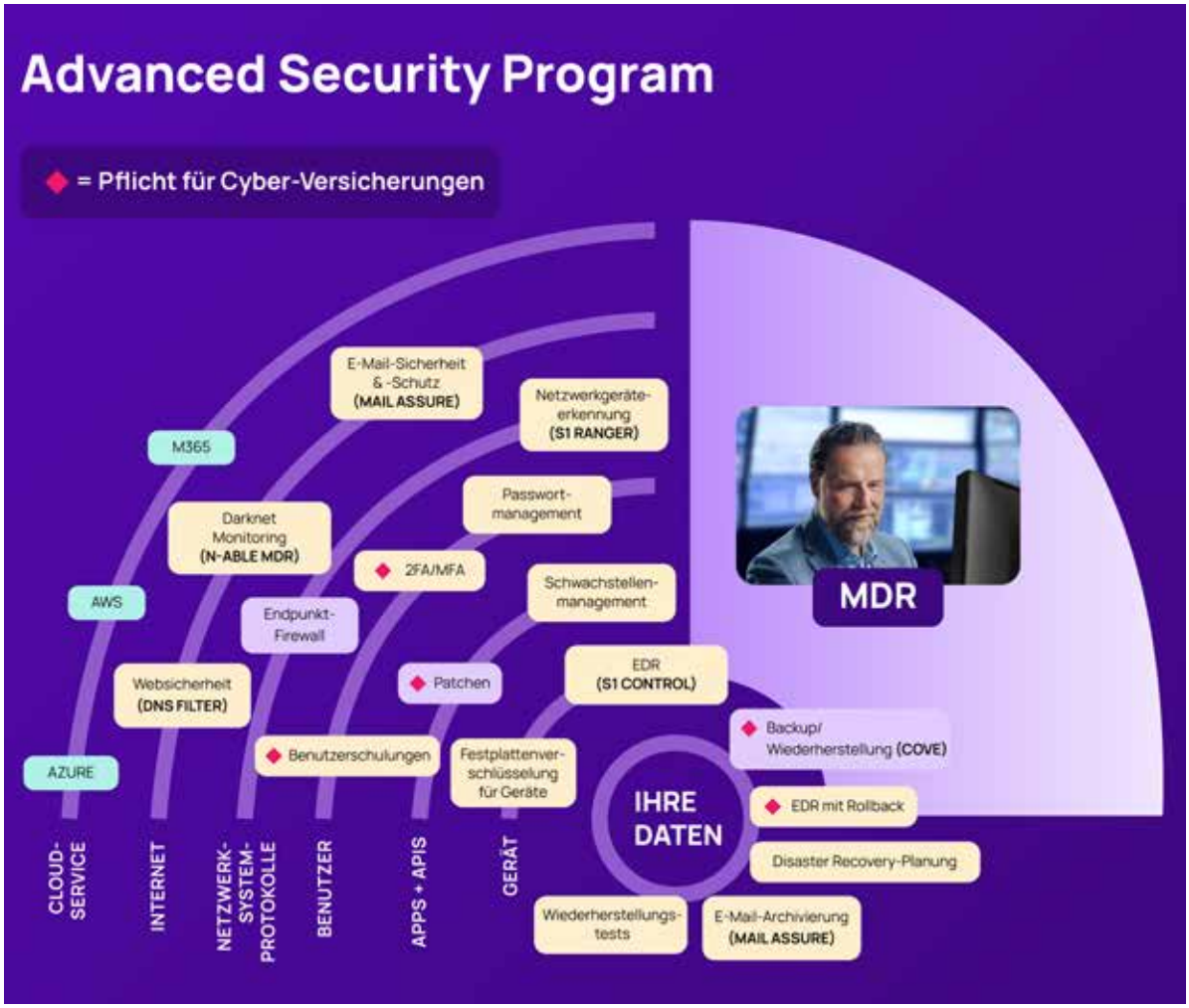
Support-Dienstleistungen:

- Alle Helpdesk-Anrufe sind gemäß SLA/MSA des MSP enthalten
- Sämtliche reaktive Unterstützung per E-Mail, Chat sowie Anrufe im Notfall ist gemäß SLA/MSA des MSP enthalten
- Support-Anrufe bezüglich der Unterstützung beim Lieferantenmanagement sind gemäß SLA/MSA des MSP enthalten
- Wiederherstellungsdienste zur Wiederherstellung kompromittierter Geräte und Daten mithilfe vorhandener Backups – mit Priorität, Dringlichkeit und ausgehandeltem SLA basierend auf Ressourcen, Datenvolumen und Gerätetypen.

Nicht inbegriffen:

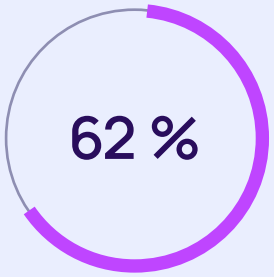
- Alles, was nach einem Cyberangriff als „Reaktion auf Vorfälle“ gilt und über die Reaktionen des N-able MDR SOC-Teams hinausgeht, ist nicht im Leistungsumfang enthalten und wird nach Zeit- und Materialaufwand abgerechnet

Um sich diese Liste in Excel anzusehen, können Sie HIER die Security Services Program Matrix aufrufen



Preisgestaltung für das Advanced Security Program

Ab 225 USD/Monat



(62 % Bruttomarge)*

*Nur Beispiel: Bruttomarge nicht garantiert.

Die monatlichen Preise beginnen bei 225 USD pro Benutzer* und beinhalten:

- Kosten für Ihren RMM-Agenten (N-central, N-sight oder RMM-Toolkit Ihrer Wahl)
- Kosten für den SentinelOne „Ranger"-Agent
- Kosten für SentinelOne EDR „Control" EDR-Agent
- Kosten für N-able MDR Advanced-Agent
- Kosten für N-able MDR 365 Tage Datenaufbewahrung
- Kosten für Cove Data Protection Workstation
- Kosten für Cove Data Protection Server
- Kosten für Cove Data Protection Wiederherstellungstests/Standby Image
- Kosten für Cove Data Protection für Microsoft 365
- Kosten für den N-able Mail Assure-Agenten
- Kosten für N-able Mail Assure-Archivierungskapazität
- Kosten für den N-able DNS Filtering-Agenten
- Kosten für die N-able Passportal „Site"-Lizenz
- Arbeitskosten für die Durchführung routinemäßiger vorbeugender Wartungsarbeiten an sämtlichen Servern, Netzwerkgeräten und Workstations (bei einem geschätzten Gesamtaufwand von 60–90 Minuten pro Monat)
- Arbeitskosten für unerwartete Supportanfragen wie Helpdesk-Anrufe, E-Mails, Chats, Lieferanten-management usw. und Notfallarbeit (bei einem geschätzten Gesamtaufwand von 90 Minuten pro Monat)
- Arbeitskosten für die Vorbereitung und Durchführung der viertel-jährlichen Übersichtsbesprechung mit der Geschäftsführung (ausgehend von insgesamt 20 Stunden/Jahr)

- Arbeitskosten für die Vorbereitung und Durchführung von Advanced Security-Schulungen (ausgehend von insgesamt 8 Stunden/Jahr)
- Arbeitskosten für die Vorbereitung und Durchführung der monatlichen Risikobewertung
- Arbeitskosten für die Umsetzung der Empfehlungen des N-able MDR SOC-Teams – sobald eine Bedrohung neutralisiert wurde – sofern diese außerhalb des definierten Leistungsumfangs liegen

Annahmen/Vorbehalte:

- *Die oben genannten Preise basieren auf der Verwendung der Lösungen von N-able und den UVP von N-able in USD ab Mai 2024. Kosten und Preise können variieren, wenn der MSP andere Sicherheitstools und RMMs verwendet, was den letztendlichen monatlichen Preis, der dem Kunden in Rechnung gestellt wird, beeinflussen kann.
- In der Berechnung verwendeter Stundensatz inklusive Gemeinkosten = 50 USD/Std.
- Unvollständige Kostenkalkulation, da die Kosten für das Toolset zum Schwachstellen-management fehlen und für den Endpreis berücksichtigt werden müssen.
- Unvollständige Kostenkalkulation, da die Kosten für das Toolset zur Risikobewertung fehlen und für den Endpreis berücksichtigt werden müssen.
- Die Schätzungen der Arbeitszeit basieren auf Durchschnittswerten. Je nach Auto-matisierungsgrad des MSP kann sich dies direkt auf die monatliche Bearbeitungszeit auswirken. Dieser Faktor wird in der Kostenstruktur und dem Endpreis für den Kunden entsprechend berücksichtigt.
- Wiederherstellungsdienste zur Wiederherstellung kompromittierter Geräte und Daten mithilfe vorhandener Backups – mit Priorität, Dringlichkeit und ausgehandeltem SLA basierend auf Ressourcen, Datenvolumen und Gerätetypen.

Nicht inbegriffen:

- Alles, was nach einem Cyberangriff als „Reaktion auf Vorfälle“ gilt und über die automatischen Reaktionen und SOC-Eingriffstaktiken des N-able MDR-Teams hinausgeht, ist nicht im Leistungsumfang enthalten und wird nach Zeit- und Materialaufwand abgerechnet oder von einem bestimmten Stundenkontingent abgezogen.

N-able bietet MSPs und IT-Serviceanbietern leistungsstarke Software zur Überwachung, Verwaltung und Absicherung von IT-Infrastrukturen und Netzwerken. Unser Angebot umfasst eine skalierbare Plattform, eine sichere Infrastruktur, Tools für die einfachere Verwaltung komplexer IT-Umgebungen und Ressourcen für die digitale Transformation. Wir unterstützen unsere Partner in jeder Wachstumsphase beim Schutz ihrer Kunden sowie beim Ausbau ihres Angebots – durch das ständig wachsende flexible Portfolio an Integrationen führender Anbieter. n-able.com/de

---