N-ABLE

HEAD NERDS

Playbook für Security Sales

Schützen & Wachsen: Chancen in der Cybersicherheit optimal nutzen

Aufbau eines Essential 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

Dieses Dokument dient nur zu Informationszwecken und ist nicht als Rechtsberatung zu verstehen. Die hier dargestellten Informationen und Sichtweisen können sich ändern und/oder treffen nicht notwendigerweise auf Ihre Situation zu. N-able übernimmt weder ausdrücklich noch stillschweigend Gewähr noch Haftung oder Verantwortung für Korrektheit, Vollständigkeit oder Nutzen der in diesem Dokument enthaltenen Informationen.

N-ABLE LEHNT SÄMTLICHE AUSDRÜCKLICHE ODER STILLSCHWEIGENDE GEWÄHRLEISTUNGEN, KONDITIONEN UND SONSTIGE BEDINGUNGEN JEGLICHER ART, GESETZLICH ODER ANDERWEITIG, IM HINBLICK AUF DIESE DOKUMENTATION AB, UNTER ANDEREN FÜR NICHTVERLETZUNG, GENAUIGKEIT, VOLLSTÄNDIGKEIT ODER NÜTZLICHKEIT DER HIERIN ENTHALTENEN INFORMATIONEN. N-ABLE, SEINE LIEFERANTEN ODER LIZENZGEBER HAFTEN GRUNDSÄTZLICH NICHT FÜR AUS UNERLAUBTER HANDLUNG, VERTRAGLICH ODER ANDERWEITIG ENTSTANDENE SCHÄDEN, AUCH WENN N-ABLE AUF DIE MÖGLICHKEIT DES EINTRITTS SOLCHER SCHÄDEN HINGEWIESEN WURDE.

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

Die Entwicklung Ihres Security-Programms

Obwohl dieser Leitfaden ursprünglich dazu gedacht war, die Frage zu beantworten: „Wie lege ich den Preis für [Name des Sicherheitsprodukts] fest?“, können Sie Ihren monatlichen Preis tatsächlich erst festlegen, wenn Sie Folgendes definiert haben:

1. Ihre Zielgruppe
2. Welche Funktionen und Dienste Sie dieser Zielgruppe verkaufen möchten

Erst wenn Sie diese beiden Fragen beantwortet haben, können Sie sich mit der Preisgestaltung befassen.

Teil 1 dieses Leitfadens ist daher der Entwicklung Ihres Sicherheitsprogramms gewidmet. Wir beginnen mit einer Übersicht darüber, wie Sie ein Sicherheitsprogramm erstellen, das auf Ihre traditionellen Managed-Services-Kunden zugeschnitten ist.

Traditionelle Managed-Services-Kunden

Der traditionelle Managed-Services-Kunde ist eine Organisation, die keinen eigenen internen IT-Administratoren beschäftigt. Ihr MSP-Unternehmen fungiert als ausgelagerte IT-Abteilung und übernimmt daher die volle Verantwortung für die Pflege, Wartung und den Schutz des Netzwerks. Wenn eine Person bei der Organisation angestellt ist, die sich um die alltägliche Verwaltung des Unternehmensnetzwerks kümmert, dann würde dies als Co-Managed-Kundenbeziehung eingestuft werden.

Es gibt zwei Programmstufen, die ein MSP entwickeln kann und die auf den Kundentyp der traditionellen Managed Services abzielen – das **Essential Security Program** und das **Advanced Security Program**.

So bauen Sie ein Essential Security Program

für den traditionellen Managed-Services-Kunden auf

Was ist das eigentlich?

Es handelt sich um ein Einsteigerpaket, das eine Basis für den IT-Schutz bietet. Es umfasst eine Reihe essentieller Sicherheitsdienste, die auf den Endbenutzer und den Endpunkt ausgerichtet sind. Es ist sozusagen das Mindestprogramm, in das alle Kunden für Break/Fix- und nicht verwaltete Services aufgenommen werden.

Zielgruppe für das Essential Security Program

Der ideale Kunde für das Essential Security Program ist:

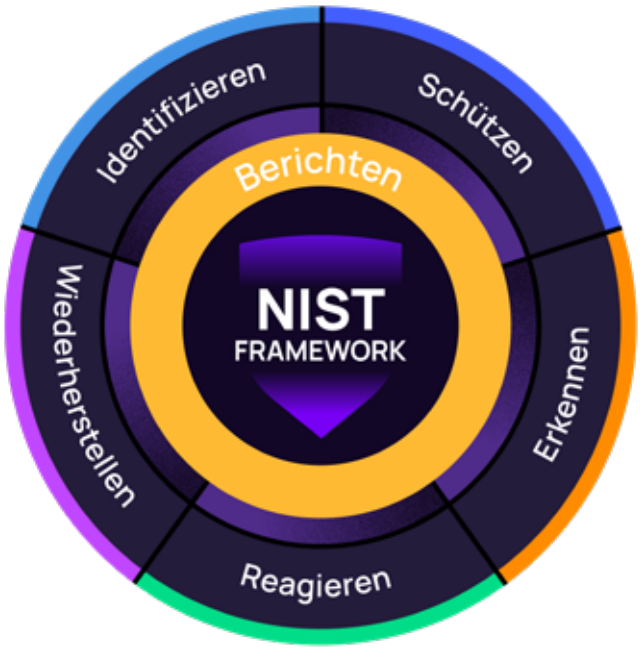
- Eine Organisation, die keinen eigenen internen IT-Administratoren und keine IT-Mitarbeiter beschäftigt
- Eine Organisation, die nicht in einer Branche tätig ist, für die Sicherheitsrichtlinien gelten, und die daher nicht verpflichtet ist, die Einhaltung dieser Richtlinien nachzuweisen
- Eine Organisation, die derzeit nur ein Break/Fix- oder ein A-la-carte-Support-Modell bezieht und daher nicht damit vertraut ist, ein Budget für IT bereitzustellen, sodass ein Advanced Security Program auf kurze Sicht schwieriger zu verkaufen wäre
- Eine Organisation, die ihr Return-to-Operations-Ziel (RTO) als niedrig einstufen würde – was bedeutet, dass sie ihre Arbeit und Geschäftstätigkeit mit Papier und anderen manuellen Methoden fortsetzen kann, während der Cyberangriff untersucht wird – wenn auch mit einigen Unannehmlichkeiten
- Die Organisation ist – in Bezug auf die Risikosegmentierung als Unternehmen mit geringem Risiko einzustufen – das heißt:
  - Sie ist gemessen am Jahresumsatz und der Anzahl der Mitarbeiter eher klein

- Sie sammelt und speichert nur begrenzte Datenmengen, und die gesamte Finanzabwicklung wird ausgelagert und außerhalb des Standorts durchgeführt
- Sie hat eine begrenzte Anzahl strategischer Partnerschaften
- Die Auswirkungen eines Cyberangriffs wären geringer und das Unternehmen würde wahrscheinlich überleben, wenn es zu einer Kompromittierung käme

Obwohl diese Art von Kunden als kleiner und weniger anfällig für Risiken gilt, sind kleinere Unternehmen in Wirklichkeit dreimal so häufig das Ziel von Angreifern wie größere Unternehmen, da sich die Angreifer dessen bewusst sind, dass gerade kleinere Unternehmen nicht die notwendigen Investitionen in ihre Cybersicherheit tätigen. Zudem versäumen es viele MSPs, diese kleineren Unternehmen dazu zu verpflichten, sich für ein Cybersicherheitspaket anzumelden. Stattdessen bieten sie diesen Unternehmen weiterhin ein Break/Fix- oder A-la-carte-Supportmodell an. Obwohl sie also aus Sicht der Risikosegmentierung als weniger risikoreich eingestuft werden können, sollten sie dennoch von ihrem MSP ein Mindestmaß an Schutzmaßnahmen erhalten. Aus diesem Grund wurde das Essential Security Program entwickelt.

Im Essential Security Program enthaltene Dienste und Funktionen

Das Essential Security Program wurde gemäß dem NIST Cybersecurity Framework entwickelt und umfasst die sechs unten aufgeführten Schlüsselfunktionen.



IDENTIFIZIEREN: Bestandserkennung für Netzwerktransparenz

- Vierteljährliche Bewertung des Sicherheitsrisikos
- Bestandserkennung (mithilfe einer **RMM-Plattform wie N-central oder N-sight**)
- 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
- Grundlegende Gefahrensensibilisierung der Mitarbeiter durch Schulungen
- Endpoint Detection & Response (**einsetzbares N-able-Produkt: SentinelOne EDR Complete)**

ERKENNEN: Abweichende Aktivitäten

- Endpoint Detection & Response (**einsetzbares N-able-Produkt: SentinelOne EDR Complete)**

REAGIEREN: Auf erkannte Bedrohungen

- Entweder unter Verwendung des EDR-Reaktionsprotokolls des MSP oder des **„Vigilance Service“ von SentinelOne** gemäß SLA/MSA (**einsetzbares N-able-Produkt: SentinelOne EDR Complete**)

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**)
- Endpoint Detection & Response (**einsetzbares N-able-Produkt: SentinelOne EDR Complete**)

BERICHTEN: Treuhänderische Verantwortung und Rechenschaftspflicht

- Monatlicher Bericht
- Lebenszyklusplanung für Bestände
- Halbjährliche Übersicht für die Geschäftsführung

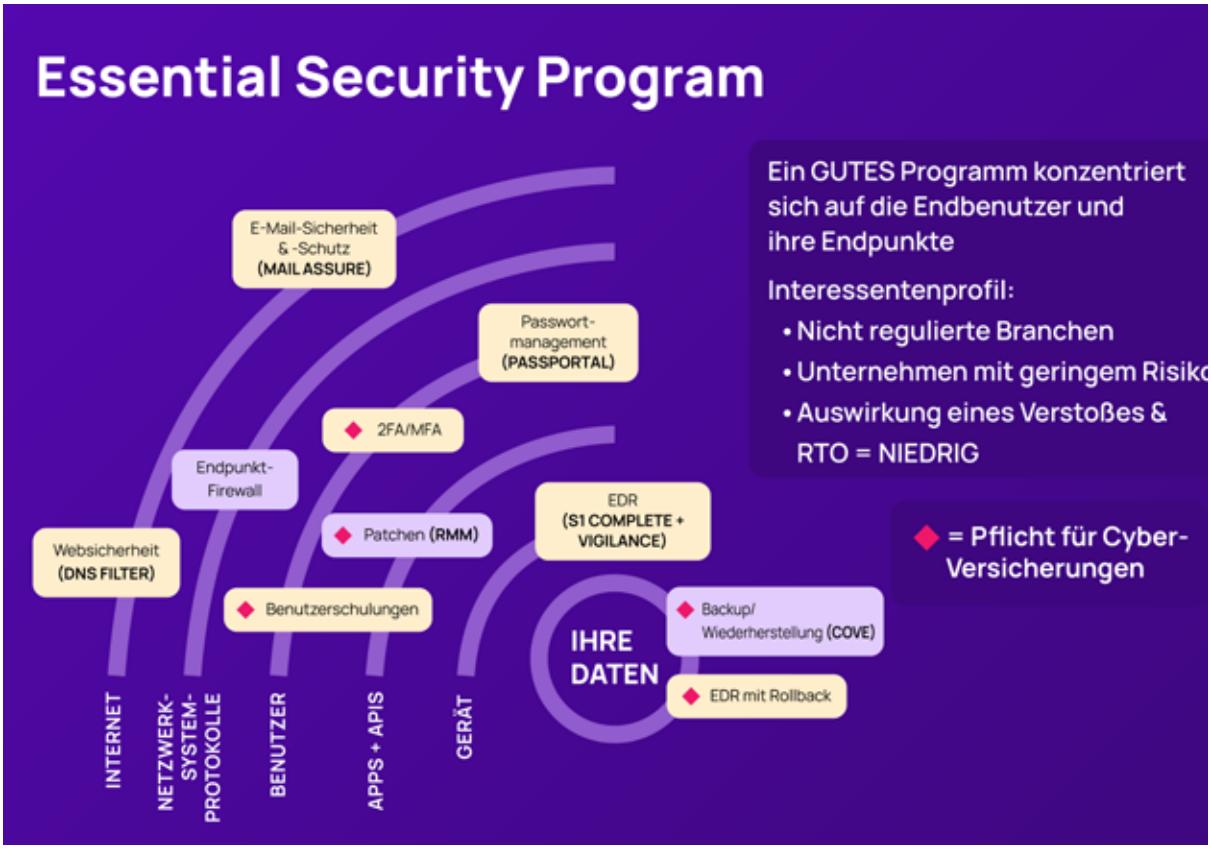
Support-Dienstleistungen:

- Der einzige enthaltene Support wird vom SentinelOne Vigilance-Team bereitgestellt, wenn eine Bedrohung am Endpunkt erkannt wird, sowie eine begrenzte Zeit für den MSP, um die Empfehlungen des SentinelOne Vigilance-Teams umzusetzen
- Es werden Wiederherstellungsdienste bereitgestellt, um kompromittierte Geräte und Daten mithilfe vorhandener Backups wiederherzustellen. Es gibt jedoch kein festgelegtes SLA und diese Wiederherstellung erfolgt nach bestem Bemühen.

Nicht inbegriffen:

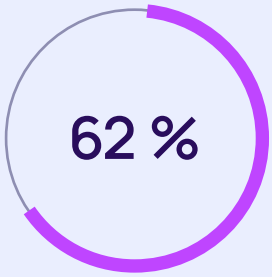
- Helpdesk-Anrufe sind nicht im Leistungsumfang enthalten und werden nach Zeit- und Materialaufwand abgerechnet
- Sämtliche reaktive Unterstützung per E-Mail, Chat sowie Anrufe im Notfall sind nicht im Leistungsumfang enthalten und werden nach Zeit- und Materialaufwand abgerechnet
- Support-Anrufe bezüglich der Unterstützung beim Lieferantenmanagement sind nicht im Leistungsumfang enthalten und werden nach Zeit- und Materialaufwand abgerechnet
- Alles, was nach einem Cyberangriff als „Reaktion auf Vorfälle“ gilt und über die automatischen Reaktionen des SentinelOne Vigilance-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 Essentials Security Program

Ab 120 USD/Monat



(62 % Bruttomarge)*

*Nur Beispiel: Bruttomarge nicht garantiert.

Die monatlichen Preise beginnen bei 120 USD pro Benutzer* und beinhalten:

- Kosten für Ihren RMM-Agenten (N-central, N-sight oder RMM-Toolkit Ihrer Wahl)
- Kosten für SentinelOne EDR „Complete“ EDR-Agent + Vigilance SOC-Service
- Kosten für Cove Data Protection Desktop – „Dokumente“
- Kosten für Cove Data Protection Server
- Kosten für Cove Data Protection für Microsoft 365
- Kosten für den N-able Mail Assure-Agenten
- Kosten für den N-able DNS Filtering-Agenten
- Kosten für die N-able Passportal „Site“-Lizenz
- Arbeitskosten für die Vorbereitung und Durchführung der halbjährlichen Übersichtsbesprechung mit der Geschäftsführung
- Arbeitskosten für die Vorbereitung und Durchführung von Basisschulungen (2 Stunden/Jahr inbegriffen – vorausgesetzt, die Schulung wird vom MSP durchgeführt)
- Arbeitskosten für die Vorbereitung und Durchführung der vierteljährlichen Risikobewertung
- Arbeitskosten für regelmäßige Backups, einschließlich Fehlerbehebung und einfache Datei-/Ordnerwiederherstellungen
- Eine geringe Anzahl an Arbeitsstunden seitens des MSP ist mit inbegriffen, um die Empfehlungen des SentinelOne Vigilance Teams umzusetzen, wenn eine Bedrohung am Endpunkt erkannt wird
- Wiederherstellungsdienste für kompromittierte Geräte und Daten unter Verwendung vorhandener Backups, jedoch ohne festgelegtes SLA. Die Wiederherstellung erfolgt nach bestem Ermessen auf „best effort“ Basis.

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 zur Risikobewertung fehlen und für den Endpreis berücksichtigt werden müssen
- Unvollständige Kostenkalkulation, da das Essential Program keine reaktiven oder Notfallarbeiten außerhalb des Budgets für den SentinelOne Vigilance Service umfasst

Nicht inbegriffen:

- Helpdesk-Anrufe sind nicht im Leistungsumfang enthalten und werden nach Zeit- und Materialaufwand abgerechnet oder von einem bestimmten Stundenkontingent abgezogen
- Sämtliche reaktive Unterstützung per Email, Chat sowie Anrufe im Notfall sind nicht im Leistungsumfang enthalten und werden nach Zeit- und Materialaufwand abgerechnet oder von einem bestimmten Stundenkontingent abgezogen
- Support-Anrufe bezüglich der Unterstützung beim Lieferantenmanagement sind nicht im Leistungsumfang enthalten und werden nach Zeit- und Materialaufwand abgerechnet oder von einem bestimmten Stundenkontingent abgezogen
- Alles, was nach einem Cyberangriff als „Reaktion auf Vorfälle“ gilt und über die automatischen Reaktionen des SentinelOne Vigilance-Teams hinausgeht, ist nicht im Leistungsumfang enthalten und wird nach Zeit- und Materialaufwand abgerechnet oder von einem bestimmten Stundenkontingent abgezogen

N-ABLE
OFFICE HOURS

Fragen zur Programmentwicklung und Preisgestaltung können Sie stellen, indem Sie sich für die monatlichen Sprechstunden der Head Nerds anmelden

Jetzt anmelden

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

---