infinigate
spark your growth

N-ABLE

Endpoint Detection & Response

Warum sich der Invest für MSPs lohnt!

Perfide Cyberbedrohungen – was jetzt?

Schützen Sie sich richtig:

Sie haben sicher gehört, dass das Gesamtvolumen der Angriffe durch Ransomware in 2022 gesunken ist. Aber wussten Sie auch, dass 2022 die Jahre 2018, 2019 und 2020 bei Weitem übertroffen hat und das Angriffsaufkommen sogar größer war als in den Jahren 2019 und 2020 in Summe?*

Allgemein ist zwar ein Rückgang des Ransomware-Gesamtvolumens zu erkennen, allerdings täuscht dieser über Aufwärtstrends in einigen Branchen sowie die Zunahme von zielgerichteten und groß angelegten Cyberangriffen hinweg. „Weniger Bedrohungen“ ist eben nicht gleichzusetzen mit „wenig Bedrohungen“.

Obwohl moderne Cyberangriffe immer häufiger auf KMUs – darunter auch viele MSPs – abzielen, sind diese häufig noch nicht ausreichend auf die perfiden und sich immer schneller anpassenden Angriffe sowie deren Folgen vorbereitet. Eine zuverlässige Früherkennung von Bedrohungen sollte in diesem Sinne elementarer Teil jeder Sicherheitsstrategie sein.
Hier kommt Endpoint Detection and Response (EDR) ins Spiel.

EDR in der aktuellen Cybersecurity-Landschaft

Fortschrittliche Sicherheitslösungen sind die logische Konsequenz für eine sich ständig verändernde Bedrohungslandschaft – so viel ist sicher. Sicher ist aber auch, dass traditionelle Antivirus- und Firewall-Systeme allein nicht mehr ausreichend sind, um die modernen, äußerst komplexen Angriffe abzuwehren. Die ständige Weiterentwicklung von Cyberbedrohungen erfordert eine proaktive Herangehensweise an die IT-Sicherheit. Besonders MSPs stehen vor der Herausforderung, ihre Kunden vor den vielfältigen und hochentwickelten Angriffen zu schützen. EDR ermöglicht es ihnen, die Sicherheitslandschaft zu überwachen, Angriffe in Echtzeit zu erkennen und effektiv darauf zu reagieren. EDR kann alles, was herkömmlicher Virenschutz leistet, und noch einiges mehr.

EDR ist eine Sicherheitstechnologie, die Endpunkte wie PCs, Laptops, Server und mobile Geräte überwacht, um verdächtige Aktivitäten und Angriffe frühzeitig zu erkennen. Integriertes maschinelles Lernen, der Einsatz ausgefeilter KI und automatisierte Gegenmaßnahmen ermöglichen EDR die schnelle Reaktion auf Sicherheitsvorfälle, um Angriffe zu stoppen und Schäden zu minimieren. On top unterstützen entsprechende Lösungen auch bei forensischen Analysen und der Einhaltung von Vorschriften.

Bedrohungslandschaft im Wandel

- Zunahme gezielter Angriffe und Ransomware
- Nutzung von Zero-Day-Exploits und fortschrittlichen Techniken
- Schwer zu erkennende Bedrohungen wie dateilose Malware
- Notwendigkeit einer ganzheitlich ausgelegten Security-Struktur

Moderne Cyberabwehr mit EDR

- Erkennung von Angriffen auf der Grundlage von Verhaltensmustern
- Früherkennung von Bedrohungen in Echtzeit
- Umfassende Sichtbarkeit und Überwachung von Endpunkten
- Notwendigkeit einer ganzheitlich ausgelegten Security-Struktur

Infinigate Deutschland GmbH
Richard-Reitzner-Allee 8
85540 Haar/München

Infinigate N-able MSP Team
+49 511 515151-96
N-able-MSP@infinigate.de

infinigate spark your growth | N-ABLE™

Ein Blick auf die Rentabilität von EDR

Insgesamt ist die Rentabilität ein zentraler Indikator für die Gesundheit und den Erfolg von MSPs. Sie beeinflusst direkt die Fähigkeit des Unternehmens, Wachstum zu realisieren, qualitativ hochwertige Dienstleistungen bereitzustellen und sich in einem dynamischen Marktumfeld zu behaupten. Und genau deshalb ist die Integration von Endpoint Detection and Response ein wichtiger Schritt auf dem Weg zu zukunftsfähiger Cybersicherheit.

6 Gründe, warum sich der Einsatz von EDR-Technologien und Dienstleistungen für Managed Service Provider lohnen

1. Kosteneinsparungen durch Schadensverhinderung

Obwohl die Implementierung von EDR initial Kosten verursacht, überwiegen die langfristigen Vorteile. Bevor fortgeschrittene Bedrohungen zu größeren Sicherheitsverletzungen oder Datenverlusten führen können, werden sie durch EDR erkannt und gestoppt. So können erhebliche Kosten vermieden werden, die mit der Behebung von Sicherheitsvorfällen, der Wiederherstellung von Systemen und dem möglichen Vertrauensverlust der Kunden verbunden sind.

2. Effizienzsteigerung bei der Verwaltung

EDR-Lösungen bieten in der Regel automatisierte Funktionen zur Erkennung und Reaktion auf Bedrohungen. Dies ermöglicht es MSPs, effizienter auf Sicherheitsvorfälle zu reagieren und die Arbeitsbelastung der internen Teams zu reduzieren. Auch eine zentrale Managementplattform, über die sich eine Vielzahl von Endpunkten verschiedener Kunden verwalten lassen, führt zur Prozessoptimierung und erleichtert die Bereitstellung.

Branchenweite Umfragen** und die Erfahrungen von N-able Expertenteams haben gezeigt, dass der Wechsel von manuellen Bedrohungsbehandlungen auf Basis von Antivirus-Lösungen hin zu einer automatisierten Behebung via EDR enorme Auswirkungen auf den Faktor Zeit haben: Statt durchschnittlich 3,5 Stunden wird die Reaktionszeit auf weniger als 30 Minuten verringert.

3. Skalierbarkeit

EDR-Dienste können simpel an wachsende Anforderungen oder Lastspitzen angepasst werden. Dies ermöglicht es MSPs, mehr Kunden und Endpunkte zu unterstützen, ohne dabei die Qualität der Sicherheitsüberwachung und -reaktion zu beeinträchtigen. Egal welche Branche oder Unternehmensgröße – allen Kunden kann ein souveräner Service angeboten werden.

4. Neue Einnahmequellen durch erweiterte Sicherheitsangebote

Die Rentabilität von Endpoint Detection and Response bezieht sich auf das Verhältnis zwischen den Kosten, die für die Implementierung und Bereitstellung der Lösungen aufgebracht werden, und den damit verbundenen finanziellen Nutzen und Gewinnen. Durch die Bereitstellung von umfassenden EDR-Diensten können MSPs neue Einnahmequellen erschließen. Sie können ihren Kunden erweiterte Sicherheitsdienstleistungen anbieten und diese auf wiederkehrender Basis abrechnen, was zu langfristig gesicherten Einnahmen führt.

Beispielsweise können nach einem Angriff detaillierte forensische Untersuchungen durchgeführt werden, um den Ursprung des Angriffs zu finden, sowie die Auswirkungen und Methoden der Angreifer besser zu verstehen. Dies hilft bei der Entwicklung von maßgeschneiderten Gegenmaßnahmen und der Vermeidung ähnlicher Vorfälle in Zukunft.

Infinigate Deutschland GmbH
Richard-Reitzner-Allee 8
85540 Haar/München

Infinigate N-able MSP Team
+49 511 515151-96
N-able-MSP@infinigate.de

infinigate
spark your growth

N-ABLE™

EDR: Warum sich der Invest für MSPs lohnt!

5. Differenzierung vom Wettbewerb

Die Aufnahme einer so leistungsstarken Cybersicherheitslösung wie EDR in das Serviceportfolio ermöglicht es MSPs, sich von ihren Mitbewerbern abzuheben. Dies kann dazu beitragen, neue Kunden zu gewinnen und bestehende Kunden zu binden. Die Bereitstellung von EDR als Teil der Dienstleistung zeigt den Kunden, dass ein MSP bereit ist, moderne Sicherheitsherausforderungen selbstbewusst anzugehen. Dies stärkt zusätzlich das Vertrauen und die Loyalität der Kunden.

6. Neue Einnahmequellen durch erweiterte Sicherheitsangebote

Die Bereitstellung von EDR-Diensten eröffnet MSPs die Möglichkeit, ihren Kunden noch umfassendere Beratungsservices anzubieten. Dies kann zu zusätzlichen Einnahmen führen, da Kunden immer öfter nach externer Expertise und Empfehlungen zur Verbesserung ihrer Sicherheitsstrategie suchen. Umso besser, wenn sie dabei alles aus einer Hand bekommen können. Viele Branchen und Organisationen haben außerdem hohe Compliance-Anforderungen, die eine umfassende Sicherheitsüberwachung und -reaktion auf Endpunkten erfordern. EDR hilft MSPs dabei, diese Anforderungen zu erfüllen und die erforderlichen Standards einzuhalten.

Fazit

Angesichts der stetig wachsenden Cybersicherheitsbedrohungen sollte und wird EDR auch zukünftig eine zentrale Rolle im MSP-Umfeld sowie den Sicherheitsstrategien von Unternehmen spielen. Die Technologie wird stetig fortschrittlicher und intelligenter und wird sich den neuen Bedrohungsszenarien zuverlässig anpassen – und dass ohne großen Mehraufwand für MSPs.

Die Rentabilität von EDR für Managed Service Provider liegt in der Fähigkeit, fortschrittliche Sicherheitsdienste anzubieten, Kosten zu senken, die Kundenzufriedenheit zu steigern und sich im Wettbewerbsumfeld zu differenzieren. Die sorgfältige Auswahl, Implementierung und Nutzung von EDR sind entscheidend, um diese Vorteile zu realisieren und langfristig erfolgreich zu sein. Dabei ist es wichtig, sorgfältig zu planen, wie Dienste in das Gesamtangebot des individuellen MSP-Portfolios integriert werden, um eine nachhaltige Rentabilität zu gewährleisten.

N-able ist der richtige Ansprechpartner, wenn es darum geht, sich mit dem Angebot von Endpoint Detection and Response weiterzuentwickeln.

Über N-able

N-able bietet IT-Serviceanbietern und IT-Abteilungen leistungsstarke Software zur Überwachung, Verwaltung und Absicherung der Systeme, Daten und Netzwerke ihrer Nutzer. 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 Nutzer und beim Ausbau ihrer Services – durch das ständig wachsende flexible Portfolio an Integrationen führender Anbieter. Weitere Informationen zu N-able finden Sie unter: Infinigate - N-able MSP

Weitere Informationen zum Thema

Nehmen Sie direkt Kontakt auf

* SonicWall Cyber Threat Report 2023

** Threat Spotlight: Inefficient incident response (barracuda.com)

Infinigate Deutschland GmbH
Richard-Reitzner-Allee 8
85540 Haar/München

Infinigate N-able MSP Team
+49 511 515151-96
N-able-MSP@infinigate.de

infinigate spark your growth | N-ABLE