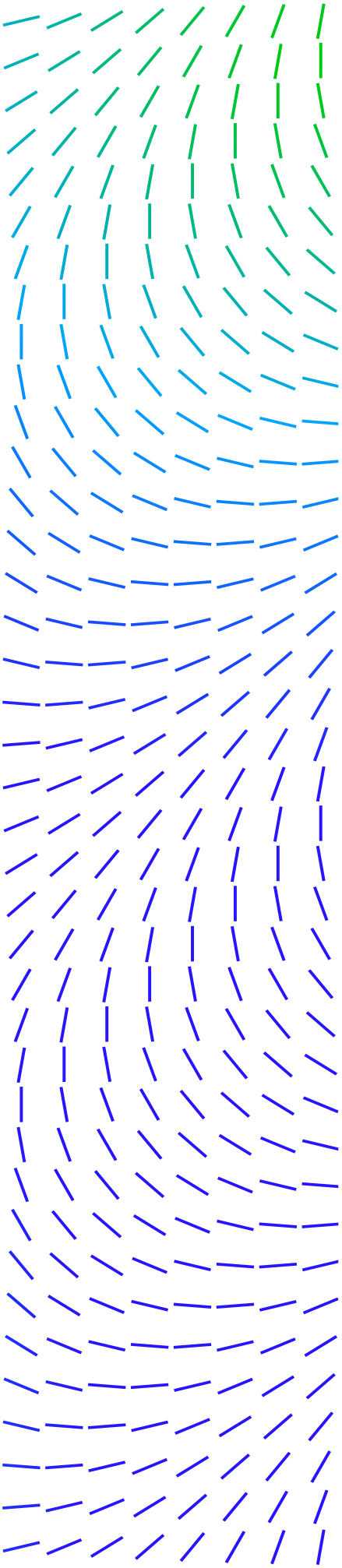
WHITEPAPER



Bei Sicherheitsfragen sollte nichts dem Zufall überlassen werden

3 Wege, wie ein intelligenter, integrierter Ansatz zur Straffung von Sicherheitsabläufen beitragen kann

Trellix

Zusammenfassung

> 75 % der großen Unternehmen werden bis 2025 eine Strategie zur Konsolidierung ihrer Sicherheitspartner anstreben.[1]

Bedrohungen entwickeln sich ständig weiter - und Ihre Sicherheitsmaßnahmen müssen Schritt halten.

Statische und nicht integrierte Tools bieten keinen ausreichenden Schutz. Organisationen wie Ihres benötigen einen neuen Ansatz - nämlich eine neue Art von gebündelten, leistungsfähigen Sicherheitsprodukten.

Vorteile eines intelligenten, integrierten Sicherheitsansatzes:

1. **Mehr Transparenz:**
   Ein klarer Blick auf potenzielle Schwachstellen kann Bedrohungen nicht nur erkennen, sondern auch vorhersagen.
2. **Schnellere Reaktion:**
   Die Konsolidierung von Produkten und leistungsfähige Abwehrmechanismen ermöglichen die Reaktion auf Bedrohungen in Echtzeit.
3. **Effizienz steigern, Kosten optimieren:**
   Die Straffung Ihrer Sicherheitsvorkehrungen und die Erhöhung Ihrer proaktiven Bereitschaft erweitert Ihre Fähigkeit, die Sicherheitslage zu verbessern und den Gewinn zu steigern.

Die Zeit zum Handeln ist jetzt gekommen - und die Antwort zur Steigerung der Effizienz Ihrer Sicherheitsmaßnahmen ist einfach: **Produktintegration und Intelligenz.**

1. Security Vendor Consolidation Trends — Should You Pursue a Consolidation Strategy? Gartner, 2020

Eine neue Ära von Sicherheitsansätzen

In der heutigen, dynamischen Welt tauchen fast täglich neue Bedrohungen auf.

Viele Unternehmen investieren in die Zukunft, indem sie ihre Sicherheit verbessern und dadurch immer einen Schritt voraus bleiben.

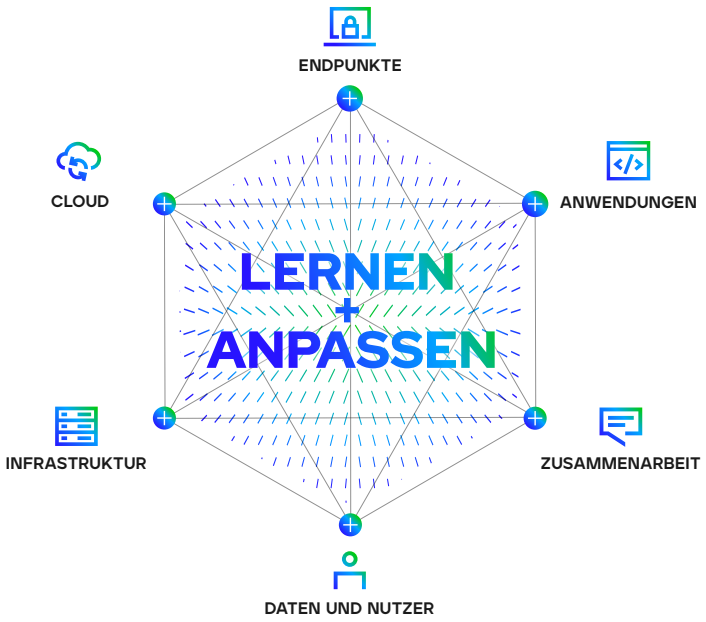
Natürlich ergibt sich eine verbesserte Sicherheit nicht von selbst. Häufig sind damit erhebliche finanzielle Ausgaben verbunden sowie mehr Personal, zusätzliche Komplexität, mehr manuelle Prozesse und vor allem das Risiko nicht richtig implementierter Sicherheitsmaßnahmen.

Gut, dass es inzwischen einen ganzheitlicheren Ansatz gibt.

Mit einem integrierten Ansatz zur Cyber-Sicherheit können Sie Angriffe besser vorhersagen bzw. vermeiden. Doch der gebündelte Einsatz von Sicherheitsprodukten in Form einer einzigen Lösung hat nicht nur mit Schutz zu tun, sondern auch mit der Freisetzung von Effizienzen.

Dieses Whitepaper zeigt drei Möglichkeiten eines intelligenten, integrierten Ansatzes für reibungslose Sicherheitsbemühungen auf.

"LIVING SECURITY" XDR-ECOSYSTEM



1. Mehr Transparenz

45% aller Sicherheitswarnmeldungen stellen sich als falsch heraus.[2]

Sichtbarer Schutz. Unsichtbare Schwachstellen können zu erheblichen Problemen führen. Mangelnde Transparenz kann das Erkennen von Bedrohungen erschweren und die Bedeutung von Warnmeldungen verschleiern. Die Folge sind Fehleinschätzungen bei der Gefahr von Angriffen.

Mit neuen Cyber-Angriffen können Lücken in der Transparenz entstehen – bei Kontaktpunkten mit Lieferanten, Tochtergesellschaften und mehr.

Die vermehrte Nutzung von Cloud-Umgebungen führt ebenfalls zu Schwachstellen. Unternehmen, die wichtige Geschäftsanwendungen in der Cloud ausführen und vertrauliche Daten in der Cloud speichern, sind dem Risiko von Fehleinschätzungen und Datenpannen ausgesetzt.

Ein intelligenter, integrierter Ansatz bei der Sicherheit kann zu mehr Transparenz beitragen und hat folgende Vorteile:

Schnelles Erkennen von Datenschutzverletzungen

In einer Welt, in der jede Minute einer Datenpanne Tausende von Euro an Schaden anrichten kann, ist es entscheidend, dass Sie Pannen möglichst schnell erkennen. Vermehrte Produktintegration führt zu einem schnelleren Aufspüren von Sicherheitsproblemen, damit Sie Bedrohungen erkennen, Risiken einschätzen und die vorliegenden Informationen zur Abwehr von Angriffen verwenden können – in Minuten statt Tagen.

Richtige Interpretation von Warnhinweisen

Ein falscher Alarm kann nicht nur personelle, sondern auch finanzielle Mittel kosten. IT-Mitarbeiter können viele Stunden damit verbringen, ungenauen oder belanglosen Warnhinweisen nachzugehen. Doch mit der richtigen integrierten Lösung können Sie Warnmeldungen automatisch bestätigen und Falschmeldungen ausschließen – und letztendlich wertvolle Zeit und Geld sparen.

Rechtzeitiges Einschätzen von Angreifern

Angreifern einen Schritt voraus zu sein, ist eine ständige Sorge - zumal Übeltäter ihre Identität schnell verschleiern und verbergen können. Doch mit der inhärenten Intelligenz einer leistungsfähigen, integrierten Sicherheitslösung können Sie Bedrohungen so schnell wie nie zuvor erkennen. Gleichzeitig stehen Ihnen damit beste Analysen zur Verfügung, um zukünftiges Angriffsverhalten zu erkennen. Mit maschinellem Lernen und anderen innovativen Eigenschaften können Sie Bedrohungen nach Priorität einschätzen, sie isolieren und entsprechend bekämpfen.

2. The Voice of the Analysts, IDC, 2021

> Es dauert im Durchschnitt 287 Tage, um Datenschutzverletzungen zu erkennen und einzudämmen.[3]

Erhöhung der Bereitschaft vor dem Angriff

Sie werden die Bedrohung durch bösartige Akteure nie ganz eliminieren können. Aber es gibt einen einfachen Weg, sich dagegen zu schützen, indem Sie immer vorbereitet und am Puls globaler Cyber-Sicherheitstrends sind. Mit Taktiken, defensiven Playbooks und empfohlenen Gegenmaßnahmen, die direkt in Ihr Ökosystem integriert sind, sind Sie für die Abwehr von Angriffen gut gerüstet.

2. Schnellere Reaktion

Tagtäglich machen neue große Cyber-Angriffe Schlagzeilen. Doch wir sind an dem entscheidenden Punkt angelangt, an dem auch Laien bewusst ist, dass die Reaktion auf eine Sicherheitspanne ebenso wichtig ist wie der Schutz davor.

Damit auf Vorfälle reagiert bzw. ein Angriff abgewendet werden kann, müssen Unternehmen einen gut funktionierenden Workflow zur obersten Priorität erklären. Der effizienteste und effektivste Prozess besteht aus aussagekräftigen Warnmeldungen, einem ordnungsgemäßen Arbeitsablauf, genauen Analysen und einem reibungslosen Fall-Management.

Die Bündelung von Sicherheitsprodukten – kombiniert mit Fähigkeiten der nächsten Generation wie KI und maschinellem Lernen – kann zu einer schnelleren Reaktion beitragen und weitere Vorteile mit sich bringen:

Integration aller Bestandteile in Sicherheitsbemühungen

Eine schnelle Reaktion ist in der Regel davon abhängig, wie schnell Sicherheitsteams Warnmeldungen interpretieren können. Wenn Warnmeldungen aus mehreren Quellen ohne Kontext oder Korrelation stammen, ist die Quelle der Protokollierung buchstäblich wertlos. Die Konsolidierung von Protokolldateien kann die Reaktionszeit verkürzen. So können Sie sie einfacher und besser interpretieren und sich schnell gegen neue Bedrohungen wappnen.

Intelligente Reaktion

Intelligenz ist ein wesentlicher Bestandteil von leistungsfähigen Sicherheitslösungen. Doch was nützt das, wenn sie nicht direkt in die Betriebsumgebung integriert werden kann? Wenn Sie Ihre intelligenten Lösungen nicht problemlos zur Verteidigung Ihrer Organisation verwenden können, sind diese nutzlos. Wenn Ihre Sicherheitsprodukte jedoch in einer einzigen intelligenten Lösung vereint sind, erhalten Sie Zugriff auf kontextbezogene, relevante Erkenntnisse bezüglich des jeweiligen Sicherheitsproblems und ermöglichen Ihren Teams eine effizientere Untersuchung von Vorfällen.

3. Cost of a Data Breach, IBM, 2021

> Fast zwei Drittel aller Befragten gaben in einer Umfrage an, dass sie jährlich schätzungsweise 25.000 USD einsparen, indem sie einen einzigen XDR-Anbieter nutzen.[4]

Fall-Management

Das Erkennen und Untersuchen von Angriffen bezieht zahlreiche Teammitglieder und Aufgaben ein. Leider sind herkömmliche Projekt-Management und Kommunikationswerkzeuge oft unzureichend, was die Koordination dieser Aktivitäten innerhalb der Sicherheitsteams betrifft. Ein einheitlicher Ansatz bei den Sicherheitsbemühungen erleichtert es Ihren Teams, Aufgaben zuzuweisen und zu verfolgen, Arbeitsabläufe zu verwalten und den Wissensaustausch im Interesse einer schnellen Lösung zu erleichtern.

Erhöhte Mitarbeitereffizienz

Vor dem Hintergrund immer neuer Bedrohungen werden immer mehr Fachkräfte für Cyber-Sicherheit gebraucht, wobei es zunehmend schwieriger wird, qualifizierte Mitarbeiter zu finden. Bereits jetzt sind Sicherheitsteams häufig unterbesetzt, während viele Organisationen sich auf unzureichende Tools verlassen, die zu ineffizienten, fehleranfälligen, manuellen Prozessen führen. Mit einer intelligenten, ganzheitlichen Sicherheitsplattform können Sie repetitive, zeitaufwendige Aufgaben automatisieren, damit Ihr Personal sich besser und effizienter dringenden Problemen zuwenden können.

3. Effizienz steigern – Kosten optimieren

Welchen Wert hat die Sicherheit Ihres Geschäfts für Sie? Dies ist die entscheidende Frage, wenn ein neuer Sicherheitsansatz in Erwägung gezogen wird. Der Schutz Ihrer wertvollsten Assets ist von äußerster Wichtigkeit. Dabei sollten Sie genaue Vorstellungen davon haben, wie viel Sie in die Sicherheit Ihres Unternehmens investieren wollen.

In einem Unternehmen werden oft Preise für Produkte verglichen – selbst wenn diese sich stark voneinander unterscheiden. Wenn es jedoch um die Gesamtbetriebskosten geht, sind ein breiterer Blick und strategische Überlegungen wichtig. Es geht nicht nur darum, welche Anschaffungskosten mit einer Investition verbunden sind, sondern auch um die jeweiligen Betriebskosten.

Ein intelligenter, integrierter Sicherheitsansatz zeichnet sich durch Folgendes aus:

4. Future of Extended Detection and Response (XDR), Cisco, 2021

Klar festgelegte Ausgaben

Hardware und Software. Abonnements und Upgrades. Einführung und Wartung. Die Preise für die einzelnen Komponenten scheinen eindeutig zu sein, sind aber häufig mit versteckten Kosten verbunden – von der Überschneidung mit bestehenden Lösungen bis zu einer mangelnden Integration mit Einzelprodukten. Die Zusammenlegung verschiedenster Endpunkt-, Cloud- und anderer Sicherheitsprodukte ermöglicht es, redundante Produkte leichter zu erkennen, damit Sie entscheiden können, an welcher Stelle Sie Einsparungen vornehmen sollten.

Minimierung von Folgekosten

Cyber-Sicherheit ist ein riskantes Geschäft. Ein Unternehmen, das nicht in der Lage ist, sich vor Angriffen zu schützen, setzt sich größeren Risiken und Verlusten aus. Verlust an Produktivität. Verlust an Ansehen. Und vieles mehr. Die Integration Ihrer Sicherheitsabläufe bietet Ihnen die Möglichkeit, sicher zu bleiben und das Risiko zu überwinden. Mit mehr Transparenz und Kontrolle können Sie Unterbrechungen der Abläufe minimieren und die Wahrscheinlichkeit eines Ereignisses, das sich negativ auf die Meinung Ihrer Kunden auswirkt, verringern.

Bessere Kontrolle von Betriebskosten

Zeit ist Geld. Die Ausgaben für die Einstellung hochqualifizierter Mitarbeiter und deren Einarbeitung sowie die laufenden Kosten für Sicherheitslösungen summieren sich. Die richtige, einheitliche Plattform kann Ihre Betriebskosten auf vielfache Weise niedrig halten. Daneben ergeben sich dadurch breitere Fähigkeiten, weil Sie weniger Zeit mit der Einarbeitung von Mitarbeitern in mehrere Tools verbringen müssen. Dadurch werden Arbeitsabläufe automatisiert, damit sich Ihr Personal um wichtige Dinge kümmern kann, anstatt monotone Aufgaben zu erledigen. Zudem werden die einzelnen Mitarbeiter entsprechend ihrer Kenntnisse eingesetzt, was wiederum Fluktuation vorbeugt.

Der nächste Schritt bei der Entwicklung von Sicherheitsbemühungen

Jedes Unternehmen sollte bestrebt sein, auf intelligente Weise zu expandieren, solider und agiler zu werden.

Dies gelingt zuverlässig, indem alle Sicherheitsprodukte zu einer einzigen, intelligenten Lösung vereint werden. Erst so erwecken Sie Ihre Sicherheitslösungen zum Leben.

Mit der richtigen, integrierten Plattform können Sie von der Kraft künstlicher Intelligenz, maschinellem Lernen und Automation profitieren, um bessere Einblicke zu erhalten und Arbeitsabläufe zu bündeln. Dadurch erhält Ihre Organisation nicht nur die Fähigkeit, effizientere Arbeitsabläufe festzulegen, sondern auch aus Erfahrungen zu lernen und sich neuen und weiterentwickelnden Bedrohungen anzupassen.

Integrierte Sicherheitslösungen ermöglichen zudem einen einheitlicheren Ansatz beim Schutz, indem sowohl hauseigene als auch offene Tools integriert werden, damit Sie je nach Ihren individuellen Bedürfnissen Sicherheitsanpassungen vornehmen können.

Durch eine fest integrierte, intelligente, ganzheitliche Plattform in Ihren Betriebsabläufen können Sie sich auf einen Schutz „von innen" verlassen. So werden Bedrohungen in Echtzeit erkannt, Sie können sofort reagieren und Probleme beseitigen.

Möchten Sie mehr über die Integration Ihrer Sicherheitsprodukte erfahren? Dann besuchen Sie uns noch heute unter trellix.com.

Trellix
6220 American Center Drive
San Jose, CA 95002
www.trellix.com

Über Trellix
Trellix ist ein globales Unternehmen, das die Zukunft der Cybersicherheit neu definiert. Mit der offenen und nativen Plattform Extended Detection and Response (XDR, erweiterte Erkennung und Reaktion) gewinnen Organisationen, die mit den größten Bedrohungen von heute konfrontiert sind, Vertrauen in den Schutz und die Widerstandsfähigkeit ihrer Abläufe. Die Sicherheitsexperten von Trellix beschleunigen zusammen mit einem umfangreichen Partnernetz technologische Neuheiten durch maschinelles Lernen und Automatisierung, um über 40.000 Kunden aus Wirtschaft und Behörden zu unterstützen.