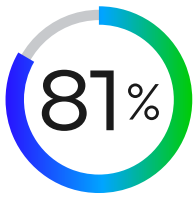
Trellix

KURZVORSTELLUNG

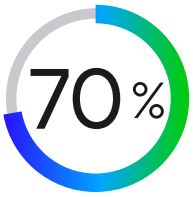
Stärken Sie Ihre Sicherheit mit Trellix

Wie eine sich ständig anpassende XDR-Lösung Ihrem Unternehmen lebendige Sicherheit geben kann

Stand der Sicherheit: Statistik



Laut einer Umfrage fällt es 81 % der CISOs schwer, Angriffe unter Kontrolle zu halten.[1]



70 % der IT-Sicherheitsverantwortlichen berichten von einer Verdoppelung der Sicherheitsmeldungen in den letzten fünf Jahren.[2]

35 % der Sicherheitsanalysten ignorieren Meldungen, wenn sie der schieren Menge nicht Herr werden können.[3]

Für die Identifizierung und Eindämmung von Datenkompromittierungen benötigen Unternehmen durchschnittlich 287 Tage.[4]

Im Durchschnitt dauert die Reaktion auf einen weltweiten Vorfall 20,9 Stunden.[5]

Die Welt von heute ist voller dynamischer Bedrohungen, die jeden Tag komplexer werden.

Das stellt Unternehmen vor enorme Herausforderungen. Ein statischer Sicherheitsansatz mit isolierten Lösungen führt dazu, dass viele Firmen nicht in der Lage sind, die sich ständig ändernden Bedrohungen abzuwehren.

Um mit dynamischen Angriffen Schritt zu halten und sich viele Sorgen zu ersparen, benötigen Unternehmen eine Lösung, mit der sie an zentraler Stelle einen vollständigen Überblick erhalten und Sicherheitsprobleme schnell beheben können.

XDR steht für Extended Detection and Response (erweiterte Erkennung und Reaktion):

- **Extended** bezieht sich darauf, dass die Lösung mehrere Sicherheitsvektoren abdeckt – einschließlich Endgeräte, Netzwerk, Cloud und E-Mail – und Sicherheitsprodukte von Dritten integriert.
- **Detection** ist die Fähigkeit, Bedrohungen bei allen Vektoren im Moment ihres Auftretens zu erkennen.
- **Response** bietet Unternehmen die Möglichkeit, sich besser vorzubereiten, um auf Angriffe effektiv und in Echtzeit reagieren zu können.

Mit einer intelligenten, anpassbaren XDR-Lösung macht die Sicherheit Ihres Unternehmens einen großen Schritt nach vorn.

1. State of Cybersecurity Resilience 2021, Accenture, 2021 | 2. 2020 State of SecOps and Automation, Dimensional Research, 2020 | 3. The Voice of the Analysts, IDC, 2021 | 4. Cost of a Data Breach, IBM, 2021. | 5. Voice of SecOps, Deep Instinct, 2021

Warum derzeitige Sicherheitslösungen gegen neue Bedrohungen machtlos sind

Angesichts immer raffinierterer Bedrohungen ist es kein Wunder, dass so viele Unternehmen gegenüber Angriffen anfällig sind. Dies liegt in erster Linie daran, dass sie nicht über adäquate Sicherheitslösungen verfügen.

1. Zu starke Konzentration auf die Bekämpfung der letzten statt der nächsten Bedrohung

Auch wenn viele Unternehmen recht gut für heutige Bedrohungen gewappnet sind, stellen die Bedrohungen von morgen das größere Problem dar. Allerdings fehlt es häufig an Fachwissen und Personal, sodass sie Angriffe nicht sofort erkennen und beheben können.

Ein noch größeres Problem sind fehlende zukunftsorientierte Tools, mit denen zukünftige Bedrohungen abgewehrt werden können. Mit maschinellem Lernen und künstlicher Intelligenz erhalten sie die nötigen Einblicke, um schwerwiegende Angriffe zu identifizieren, fundierte Entscheidungen zu treffen und Probleme zu beheben.

2. Zu starke Abhängigkeit von fehleranfälligen manuellen Prozessen statt Automatisierung

Selbst mit der richtigen Lösung sind viele IT-Abteilungen bei der Verwaltung der Sicherheitsinfrastruktur auf manuelle Prozesse angewiesen. Dies führt zu einer ganzen Reihe von Problemen und insbesondere zu Ineffizienz. Wenn ein IT-Mitarbeiter eine Meldung zu einer Bedrohung erhält, muss diese Meldung verlässlich sein. Andernfalls würden wertvolle Zeit und Ressourcen für die Prüfung von Problemen verwendet, die letztendlich gar keine sind.

3. Fehlende Abdeckung aller Vektoren und Angriffspunkte

Viele Unternehmen verlassen sich nach wie vor auf intern entwickelte Sicherheitslösungen. Dabei kosten diese letztendlich mehr als vorgefertigte Produkte. Weil das Sicherheitsteam weder die ganze Bandbreite an Bedrohungsvektoren abdecken, noch dynamisch reagieren kann, sind diese internen Lösungen meist problembehaftet, weniger effizient und mit mehr Aufwand verbunden als etablierte, bewährte Lösungen.

So definiert Trellix Sicherheit neu

Trellix ist Vorreiter bei der XDR-Revolution und bietet einen völlig neuen Ansatz in puncto Erkennung, Reaktion und Behebung: eine zentrale, lebendige Sicherheitslösung. Die Vorteile des innovativen XDR-Ökosystems:

- Sofortige Datenanalyse, Prognose und Prävention von Angriffen mit einer Lösung, die ständig dazulernt und sich anpasst
- Möglichkeit der Schaffung von offenen Partnerschaften und nativen Verbindungen zur automatischen Abstimmung von Sicherheitsrichtlinien
- Unterstützung durch integrierte Tools und Expertenwissen, um die Komplexität zu reduzieren und die Effizienz zu steigern

Der neue, einheitliche Ansatz für XDR

Trellix XDR lässt sich nahtlos in Ihr breites Portfolio an Sicherheitsprodukten für Endgeräte, E-Mail, Netzwerk, Cloud sowie weitere Bereiche integrieren. Außerdem lässt sich die Lösung einfach mit Sicherheitsanwendungen von Drittanbietern verknüpfen. Durch diese Konnektivität erhält Ihr Unternehmen intelligente Bedrohungserkennung, Analysefunktionen sowie automatisierte Reaktionen.

Unser einheitlicher Ansatz bietet folgende Vorteile:

Vektorübergreifende Erkennung raffinierter Angriffe

Trellix XDR ermöglicht die zuverlässige Erkennung von Sicherheitsvorfällen. Sie erhalten Erkenntnisse basierend auf Telemetriedaten aus mehreren Vektoren und Assets in Ihrem gesamten Unternehmen und können diese zur Abwehr von umfangreichen Angriffen einsetzen.

Wechsel von Angriffserkennung zur Bedrohungsprävention

Trellix XDR blockiert Angriffe, die über E-Mails, das Netzwerk und Endgeräte in Ihr Unternehmen gelangen. Mit dieser intelligenten, adaptiven Lösung können Sie aufkommende Bedrohungen vorhersehen und vermeiden, Ursachen erkennen und in Echtzeit reagieren.

Integration einer Sicherheitslösung der nächsten Generation in Ihre Abläufe

Trellix XDR bietet Workflows für geführte Untersuchungen. Da Ihre Abläufe mehr Daten und Analysen nutzen, können Sie Prozesse automatisieren und Ihre größten Sicherheitsprobleme priorisieren.

KURZVORSTELLUNG

Lebendige Sicherheit für Ihr Unternehmen – mit Trellix

Zukunftsorientierte Unternehmen müssen bereits heute gut geschützt sein. Das bedeutet, dass Ihre Teams in der Lage sein müssen, proaktiv zu handeln, statt nur zu reagieren. So können Sie geschäftliche Chancen wahrnehmen und sind für Bedrohungen gewappnet.

Trellix XDR verbindet innovative Technologie mit Fachwissen, um Folgendes zu ermöglichen:

- Schaffen Sie eine widerstandsfähigere digitale Welt, da Sie mit neuen globalen Bedrohungen stets Schritt halten können.
- Nutzen Sie Wissen über die Bedrohungen von heute, um Angriffe von morgen abzuwehren, indem Sie scheinbare Einzelvorfälle aus verschiedenen Tools zu nützlichen Erkenntnissen korrelieren.
- Handeln Sie zukunftsorientiert, indem Sie die Risiken für Ihr Unternehmen mit automatisierter Erkennung und Behebung von Bedrohungen reduzieren.

Sind Sie bereit, Ihrem Unternehmen mit XDR eine lebendige Sicherheit zu geben? Überzeugen Sie sich selbst auf trellix.com oder sprechen Sie mit einem unserer XDR-Experten darüber, wie Sie mit Trellix Ihr Unternehmen stärker wachsen lassen können.

Trellix