Zukunftssichere Endpoint-Sicherheit in 2025

KI, Automatisierung und Compliance in Aktion

Cybersicherheit leicht gemacht

Inhalts-verzeichnis

01 Fazit

02 Einleitung

03 Warum sich der Endpoint-Schutz im Jahr 2025 weiterentwickeln muss

04 Die Rolle von KI in der modernen Endpoint-Sicherheit

05 Strategie in die Tat umsetzen

01 Fazit

Der Endpoint-Schutz im Jahr 2025 und darüber hinaus erfordert mehr als nur ein Antivirenprogramm. Es erfordert KI-gesteuerte Abwehrmechanismen, Automatisierung und Compliance-Bereitschaft, um den immer fortschrittlicheren Bedrohungen einen Schritt voraus zu sein.

Dieses eBook untersucht, wie sich moderne Sicherheitsstrategien für Endpoints entwickeln, um Folgendes zu gewährleisten:

- Stoppen unbekannter und ausweichender Bedrohungen mithilfe von KI und Zero Trust-Prinzipien, bevor sie ausgeführt werden
- Korrelieren von Signalen und Automatisieren von Reaktionen, über die gesamte Angriffskette hinweg und in Echtzeit
- Abwehren fortschrittlicher Techniken wie LOTL-Angriffe (Living-off-the-Land) und dateilose Malware
- Anpassung an Compliance-Standards wie NIS 2 und DORA sowie an Anforderungen von Cyberversicherungen
- Erweiterung des Schutzes über den Endpoint hinaus mit Korrelation auf XDR-Ebene und verwalteter Erkennung und Reaktion

Indem Unternehmen diese Trends verstehen und proaktive Lösungen einführen, können sie Risiken reduzieren, die Zeiten verkürzen, in denen das Unternehmen Angriffen ausgesetzt ist, und eine stärkere Cyberresilienz aufbauen.

02 Einleitung

Die Cybersicherheitslandschaft entwickelt sich rasant. Bedrohungen sind ausgefeilter, Angriffe sind zielgerichteter und die Fehlermarge schrumpft. In dieser neuen Realität reicht traditionelle Endpoint-Sicherheit nicht mehr aus. Unternehmen müssen über die Erkennung hinausgehen – sie benötigen intelligenten, automatisierten Schutz, der wirkt, bevor Angreifer Schaden anrichten können.

Die effektivsten Strategien für den Endpoint-Schutz kombinieren heute künstliche Intelligenz, Echtzeit-Automatisierung und integrierte Compliance-Tools.

Diese Technologien helfen Unternehmen, sich effektiver zu verteidigen und gleichzeitig Aufwand, Komplexität und Betriebsrisiken zu reduzieren.

03 Warum sich der Endpoint-Schutz im Jahr 2025 weiterentwickeln muss

Unternehmen stehen mehr denn je unter Druck. Remote-Arbeit hat die Angriffsfläche erweitert. Cyberkriminelle nutzen KI, um herkömmliche Abwehrmechanismen zu umgehen.

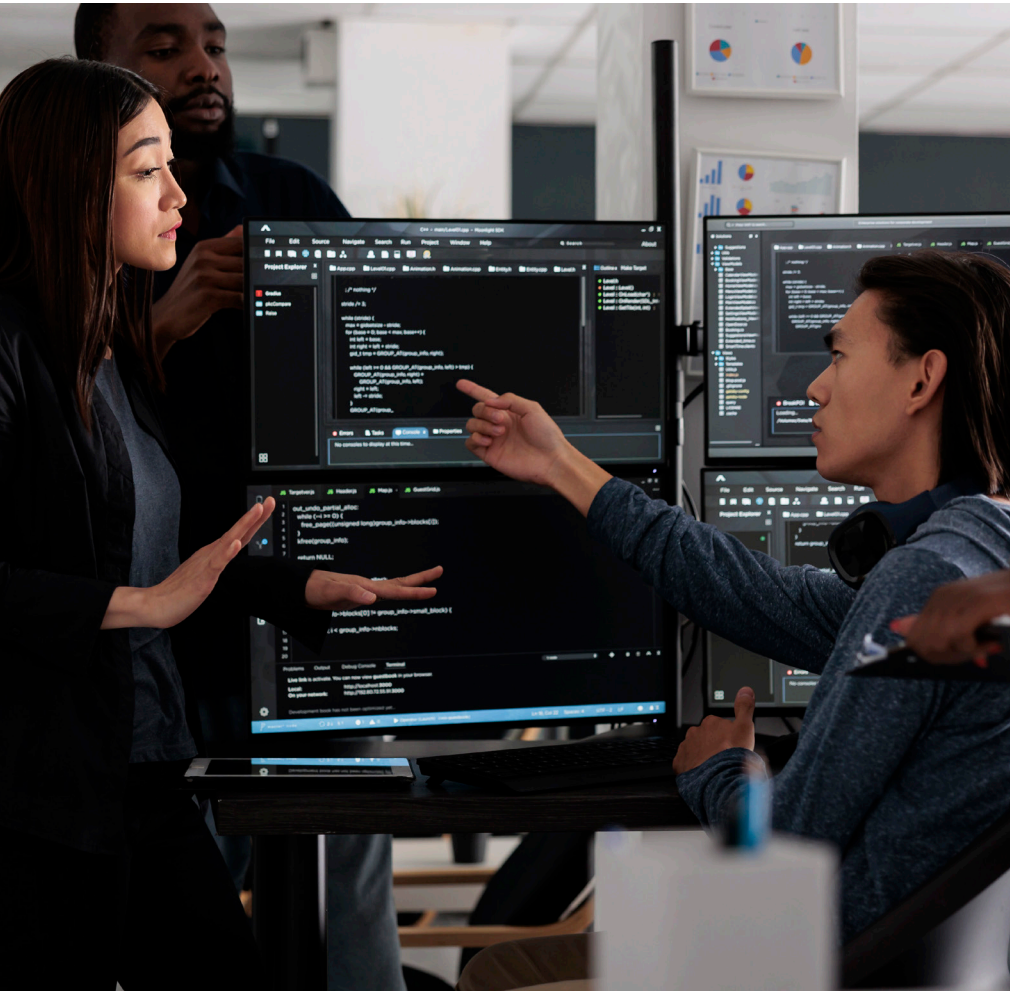
Compliance-Anforderungen werden immer strenger und komplexer. Und interne Ressourcen sind ausgelastet.

Diese Kombination aus Risiko und Komplexität spricht eindeutig für die Modernisierung der Endpoint-Sicherheit. Im Jahr 2025 muss eine zukunftsfähige Lösung Folgendes leisten:

- Das Ausführen unbekannter Bedrohungen verhindern
- Kontinuierliche Überwachung auf abnormales Verhalten
- Automatisierung der Erkennung und Priorisierung von Sicherheitsvorfällen
- Anpassung an sich ändernde Compliance-Rahmenbedingungen
- Nahtlose Integration in bestehende Umgebungen

Eine zukunftsfähige Endpoint-Sicherheitslösung sollte an all diesen Fronten liefern – mit leichten Agenten, schneller Bereitstellung und Kompatibilität mit bestehenden Antivirenumgebungen. Viele Lösungen enthalten jedoch keine KI-gesteuerten Präventionsmechanismen, Echtzeit-Verhaltensanalyse und die automatisierte Reaktion als Standardfunktionen.

Compliance-Anforderungen werden immer strenger und komplexer. Und interne Ressourcen sind ausgelastet.



Fünf Bedrohungen, die Ihr traditionelles Antivirenprogramm nicht stoppen kann (im Gegensatz zu KI-gestützten Endpoint Detection and Response (EDR)-Lösungen)

Traditionelle Antivirenlösungen wurden für eine andere Ära entwickelt. Obwohl sie immer noch eine Rolle beim grundlegenden Schutz spielen, können sie einfach nicht mit den fortschrittlichen Bedrohungen mithalten, mit denen Unternehmen heute konfrontiert sind. Im Folgenden finden Sie fünf Arten von Angriffen, für die eine moderne, KI-gestützte EDR-Lösung entwickelt wurde:

1 **RDP-Brute-Force- und Credential-basierte Angriffe:** Herkömmliche Antivirenlösungen überwachen weder das Verbindungsverhalten noch den Missbrauch von Konten. EDR-Lösungen mit KI erkennen ungewöhnliche Zugriffsversuche und blockieren seitliche Bewegungen frühzeitig.

2 **Unbekannte oder polymorphe Malware:** Herkömmliche Antivirenlösungen stützen sich auf bekannte Signaturen. KI-gestützte EDR klassifiziert unbekannte Bedrohungen in Echtzeit – auch wenn sie zuvor noch nie gesehen wurden.

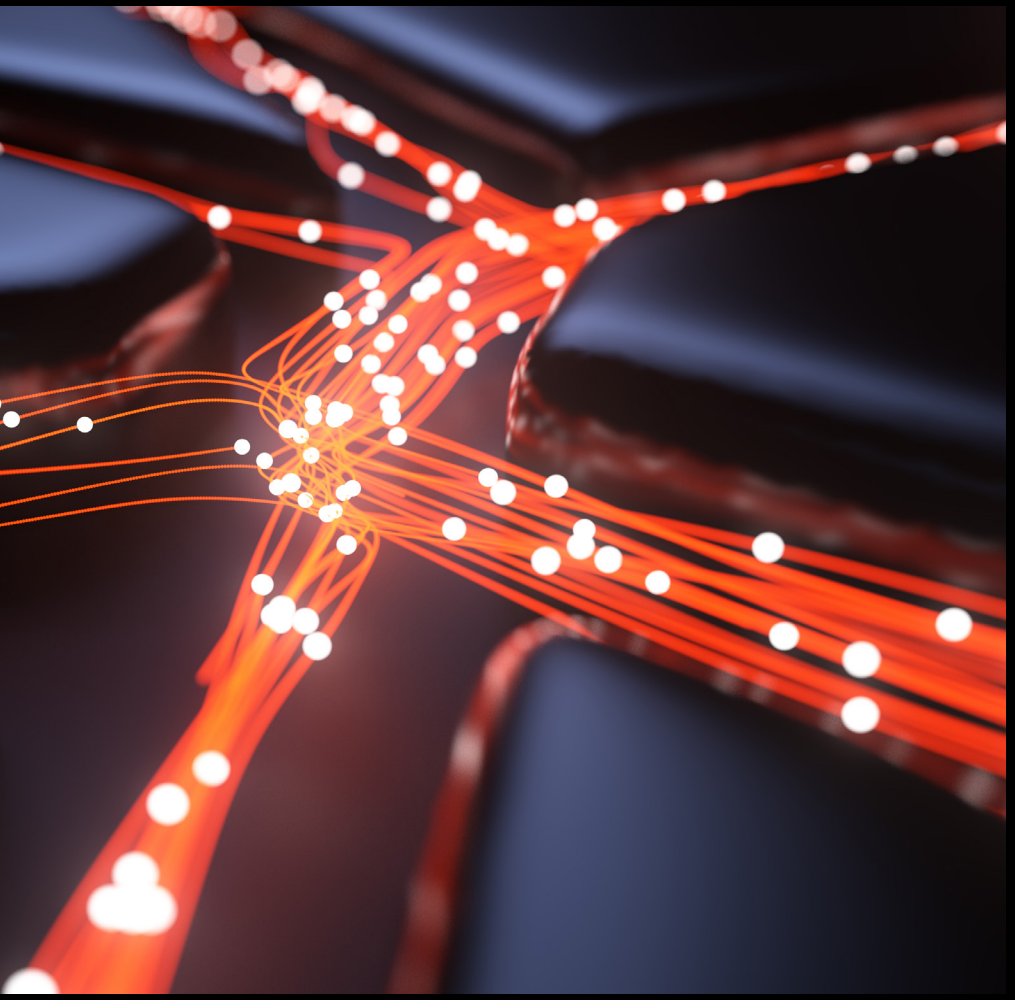
3 **Living-off-the-Land-Binärdateien (LOLbins)[1]:** Diese Techniken verwenden legitime, signierte System-Binärdateien (wie PowerShell, WMIC oder Rundll32), die Angreifer missbrauchen, um böswillige Aktionen auszuführen, ohne dabei neue Dateien abzulegen. EDR identifiziert und stoppt verdächtiges Verhalten, auch wenn keine Malware vorhanden ist.

4 **Dateiloses Skripting und PowerShell-Missbrauch:** Bei skriptbasierten Angriffen werden keine ausführbaren Dateien abgelegt, und sie sind daher für Antivirenlösungen nicht erkennbar. Die KI-gesteuerte Erkennung identifiziert böswillige Absichten in Skripten basierend auf dem Verhalten.

5 **Erweiterte Schwachstellen-Exploits:** EDR erkennt Ausbeutungsmuster entlang der Kill Chain, selbst wenn ein Patch fehlt, und bietet so Eindämmung in Echtzeit.

Diese Bedrohungen werden immer häufiger und sind darauf ausgelegt, traditionelle Kontrollen zu umgehen. Aus diesem Grund muss sich der moderne Endpoint-Schutz über die statische Erkennung hinaus entwickeln – KI-gestützte EDR ist daher inzwischen unerlässlich.

1. LOLBins und LotL sind verwandt, aber nicht identisch. LotL ist eine umfassende Taktik, die vertrauenswürdige, native Tools (Skripte, Admin-Tools, geplante Aufgaben usw.) verwendet, um der Erkennung zu entgehen. LOLBins sind eine Untergruppe legitimer System-Binärdateien (z. B. PowerShell, WMIC), die missbraucht werden, um schädliche Aktionen auszuführen, ohne neue Dateien hinzuzufügen.



04 Die Rolle von KI in der modernen Endpoint-Sicherheit

KI ist zu einem grundlegenden Element effektiver Cybersicherheit geworden. Im Jahr 2025 ist KI in der Cybersicherheit nicht mehr optional, sondern sie wird eine wesentliche Rolle spielen. KI ermöglicht schnellere Bedrohungserkennung, intelligentere Entscheidungen und eine nahezu sofortige Reaktion.

> Sicherheitsanbieter mit ausgereiften KI-Modellen haben über Jahre adaptive Erkennungsfunktionen entwickelt, die sich mit der Bedrohungslandschaft weiterentwickeln und zum Schutz von Anwendern und Systemen in Echtzeit beitragen.

Moderne Endpoint-Lösungen, die auf KI basieren, erwecken dies zum Leben, indem sie Schutz vor verschiedenen Bedrohungen bieten, einschließlich heimlicher Taktiken wie LotL-Angriffe. Diese Lösungen bieten Folgendes:

- **KI-gesteuerte Verhaltenserkennung und -klassifizierung**
- **Kontextbezogene Analyse von Anwendungen und Prozessen**
- **Autonome Prävention unbekannter Bedrohungen**
- **Sichtbarkeit der Angriffsflächen in Echtzeit**

Visualisierung und Risikobewusstsein

Was Sie nicht sehen, können Sie nicht schützen. Aus diesem Grund umfassen führende EDR-Lösungen integrierte Telemetrie- und Risiko-Dashboards, um Echtzeit-Transparenz in Endpoint-Umgebungen zu ermöglichen. Komplementäre Tools wie Patch-Management und Verschlüsselung helfen, die Angriffsfläche zu reduzieren, und unterstützen sowohl regulatorische als auch versicherungsbezogene Anforderungen.

Automatisierter Zero Trust-Schutz

Die erste Verteidigungslinie ist Vertrauen – oder besser gesagt: das Fehlen von Vertrauen. Ein modernes Zero Trust-Modell sollte alle unbekannten Anwendungen standardmäßig blockieren, bis sie als sicher eingestuft werden. Dieser proaktive Ansatz stoppt Bedrohungen, bevor sie ausgeführt werden, und schließt die Tür vor Malware, die von herkömmlichen Antiviren-Tools übersehen wird.

Im Gegensatz zu reaktiven Systemen, die auf Signaturen oder Eingriffe von Analysten warten, kann eine echte KI-gesteuerte Sicherheitsplattform die überwiegende Mehrheit der Anwendungen in Echtzeit autonom klassifizieren. Die wenigen verbleibenden Anwendungen werden zur Expertenanalyse eskaliert. Auf diese Weise wird ein kontinuierliches Gleichgewicht zwischen Geschwindigkeit und Genauigkeit bei der Verhinderung unbekannter Bedrohungen gewährleistet.

Intelligente Korrelation und automatisierte Reaktion

Proaktiver Schutz hört nicht auf der Anwendungsebene auf. Moderne Angriffe beinhalten oft subtile, heimliche Verhaltensweisen, die sich im Laufe der Zeit entfalten. Aus diesem Grund überwachen moderne Endpoint Detection and Response (EDR)-Lösungen kontinuierlich die Geräteaktivität, erkennen ungewöhnliches Verhalten und korrelieren mehrere Signale und Indikatoren für Angriffe zu bestätigten Vorfällen – automatisch und in Echtzeit. Dies ermöglicht eine frühere Erkennung, eine schnellere Untersuchung und eine präzise Abhilfe, wodurch die Exposition und die Alarmmüdigkeit von Sicherheitsteams verringert werden.

Endpoint-Sicherheit und Compliance

Die Erfüllung regulatorischer Anforderungen ist ein wachsendes Anliegen für Organisationen jeder Größe. Unabhängig davon, ob Sie sich auf NIS 2, DORA, HIPAA oder Cyberversicherungsschutz vorbereiten, unterstützen moderne Endpoint-Plattformen diese Ziele, indem sie sich an den sich entwickelnden Vorschriften orientieren und die Erfassung von Nachweisen für Audits vereinfachen.

Mit automatisierter Risikobewertung, Policy-Durchsetzung und detaillierter Berichterstattung können Sie ohne zusätzlichen Verwaltungsaufwand die Erfüllung Ihrer Sorgfaltspflicht nachweisen und Ihre Compliance stärken.

Cyberversicherungs-bereitschaft

Da Cyberversicherungen in vielen Branchen zu einer Voraussetzung für die Geschäftstätigkeit werden, fordern Versicherer höhere Sicherheitsstandards. Erweiterte Endpoint-Plattformen helfen Unternehmen, diese Anforderungen zu erfüllen, indem sie Folgendes bieten:

- Aktive Eindämmung von Bedrohungen und Echtzeit-Validierung von Vorfällen
- Dokumentation der automatisierten Prävention und Reaktion
- Risikobasierte Telemetrie, abgestimmt auf die Bewertungskriterien der Versicherer

Diese Funktionen machen es einfacher, die Voraussetzungen zu erfüllen, und stärken die Bereitschaft zur Cyberversicherung.

Einfach, effizient, skalierbar

Die führenden Endpoint-Sicherheitslösungen sind auf Einfachheit und Skalierbarkeit ausgelegt. Sie arbeiten plattformübergreifend, lassen sich in bestehende IT-Umgebungen integrieren und werden von zentralen Konsolen aus verwaltet, die auf Benutzerfreundlichkeit ausgelegt sind. Dies führt zu einer geringeren Komplexität und besseren Ergebnissen.

05 Strategie in die Tat umsetzen

In diesem E-Book haben wir die entscheidenden Funktionen skizziert, die eine moderne Strategie für den Endpoint-Schutz ausmachen – viele der Funktionen gehen über das hinaus, was herkömmliche Antiviren- und sogar viele EDR-Plattformen heute bieten.

> Von der KI-gesteuerten Erkennung und Zero Trust-Ausführungskontrolle bis hin zur automatisierten Korrelation von Living-off-the-Land-Angriffen, Visualisierung von Schwachstellen und integrierter Compliance-Unterstützung sind dies nicht einfach nur Funktionen, sondern sie entsprechen auch den aktuellen Anforderungen.

WatchGuard EPDR vereint all diese Funktionen in einer einzigen, leichten Lösung. Sie kombiniert KI-gestützte Verhaltenserkennung mit einem Zero-Trust Application Service, der maschinelles Lernen nutzt, um unbekannte Anwendungen zu klassifizieren und zu blockieren, bevor sie automatisch ausgeführt werden können.

Unsere KI-gesteuerten Engines analysieren riesige Mengen an Telemetriedaten in Echtzeit. Sie erkennen Anomalien, klassifizieren neue Bedrohungen und automatisieren Reaktionen ohne menschliches Eingreifen. In Kombination mit menschlichem Fachwissen aus unserem Threat Hunting Service und Security Operations Center sorgt dieses proaktive und hybride Modell für Geschwindigkeit und Genauigkeit und reduziert das Risiko neuer Bedrohungen, ohne Ihre aktuelle Infrastruktur zu stören oder bestehende Lösungen zu ersetzen.

WatchGuard MDR bietet eine von Experten gesteuerte Überwachung und Reaktion, während ThreatSync Transparenz auf XDR-Ebene und eine automatisierte Bedrohungskorrelation über Endpoints, Netzwerke, Identitäten und Cloud-Umgebungen hinweg ermöglicht.

Mit modularen Add-ons wie Patch-Management und vollständiger Festplattenverschlüsselung können Sie Ihre Angriffsfläche reduzieren, sich an Compliance-Standards ausrichten und den Schutz vor Data Loss oder unbefugtem Zugriff stärken.

Erweiterung der Cybersicherheit auf Angriffsflächen

Der Endpoint-Schutz ist nur ein Teil des Cybersicherheitspuzzles. In den heutigen vernetzten Umgebungen sind Unternehmen mit Bedrohungen konfrontiert, die sich seitlich bewegen – von Endpoints über Identitäten bis hin zu Netzwerken und der Cloud. Angreifer nutzen häufig legitime Tools und Systemfunktionen bei diesen Living-off-the-Land-Techniken, wodurch es schwieriger wird, Bedrohungen zu erkennen und zu stoppen. Ein isolierter Ansatz wird diese Herausforderung nicht meistern.

ThreatSync

ThreatSync ermöglicht die Korrelation auf XDR-Ebene zwischen Endpoints, Netzwerken und Cloud-Diensten und verwandelt isolierte Ereignisse in kohärente Incident-Zeitpläne, Bedrohungsvalidierung und umsetzbare Anleitungen – insbesondere in Umgebungen ohne interne Cybersicherheitsteams.

Zusammen bieten diese Lösungen eine kohärente, skalierbare Verteidigungsstrategie – Bedrohungen werden proaktiv identifiziert, korreliert und beantwortet, egal, wo sie auftreten.

MDR

WatchGuard MDR bietet eine professionelle SOC-Unterstützung, die eine kontinuierliche Überwachung umfasst.

WatchGuard bietet einen einheitlichen Ansatz zur Erkennung von und Reaktion auf Bedrohungen über mehrere Angriffsflächen hinweg, durch ThreatSync und WatchGuard MDR.

WatchGuard®

Nachgewiesene Leistung und Anerkennung in der Branche

Bei der Auswahl einer Endpoint-Sicherheitslösung ist eine unabhängige Bewertung wichtig. Der Ansatz von WatchGuard ist innovativ, getestet und vertrauenswürdig.

Im Jahr 2024 erhielt WatchGuard Endpoint-Sicherheit Bestnoten in mehreren unabhängigen Bewertungen:

- PassMark Software hat WatchGuard mit einer führenden Bewertung in Bezug auf Leistung, Schutzgenauigkeit und Ressourceneffizienz ausgezeichnet.
- MITRE ATT&CK-Auswertungen bestätigten einen Schutz von 100 % vor Malware-Beispielen, dank starker Erkennung über alle Stufen der Angriffskette hinweg.
- Branchenanalysten und globale Auszeichnungen würdigten WatchGuard als einen Top-Anbieter für Endpoint-Sicherheit, der in Sachen Benutzerfreundlichkeit, Automatisierung und Bedrohungsabwehr punktet.

Diese Anerkennung unterstreicht die Erfahrung, die unsere Kunden jeden Tag machen: Endpoint-Schutz, der intelligent, effektiv und auf die heutige Cyberlandschaft ausgelegt ist.

PASSMARK™ SOFTWARE

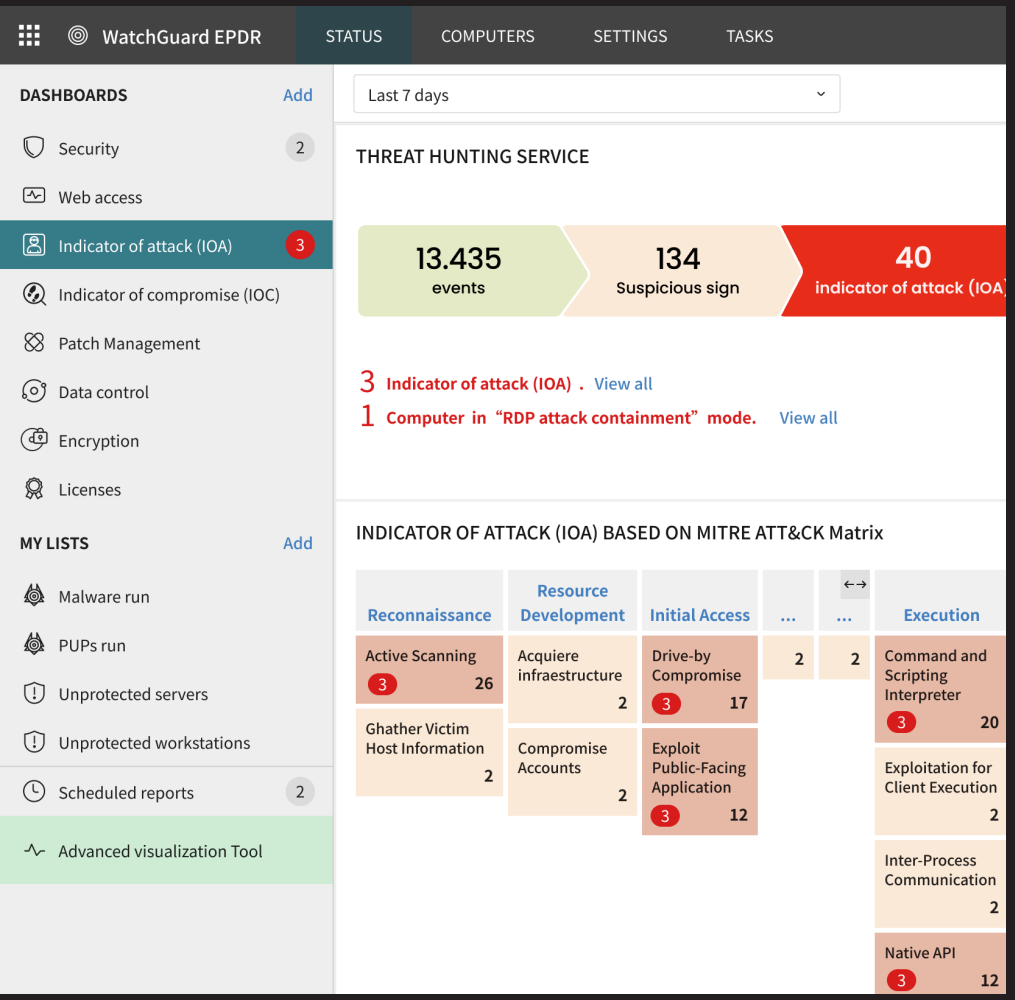
MITRE | ATT&CK® Evaluations

canalys GLOBAL CYBERSECURITY CHAMPION 2025

EXCELLENCE IN CUSTOMER SERVICE AWARD 2024

THE CHANNEL CO. CRN PARTNER PROGRAM GUIDE WINNER 2025

2024 VISIONARY SPOTLIGHT AWARDS



Machen Sie sich noch heute bereit für die Zukunft.

Cybersicherheit ist nicht mehr nur eine technische Notwendigkeit – sie ist ein strategischer Imperativ. In einer Welt, in der Bedrohungen unsichtbar, automatisiert und unerbittlich sind, reicht der Schutz Ihrer Endpoints nicht aus. Sie müssen den Bedrohungen zuvor kommen.

Mit WatchGuard EPDR blockieren Sie nicht nur Bedrohungen – Sie verhindern das Unbekannte, automatisieren das Komplexe und verwandeln Chaos in Kontrolle.

Mit MDR und ThreatSync erweitern Sie diese intelligente Lösung auf Ihre gesamte Angriffsfläche.

Und mit unserer Unified Security Platform vereinfachen Sie Ihre Betriebsabläufe, ohne Kompromisse in Sachen Schutz zu machen.

Es ist an der Zeit, Patchwork-Lösungen hinter sich zu lassen.

Es ist Zeit für eine wirklich proaktive Verteidigung.

Bereit für den nächsten Schritt?

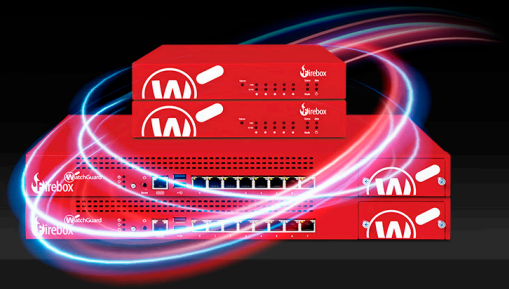
Sehen Sie WatchGuard EPDR in Aktion.

Fordern Sie Ihre kostenlose Testversion an, und schützen Sie noch heute die Zukunft Ihres Unternehmens:

Jetzt loslegen

WatchGuard

WatchGuard-Portfolio



Netzwerksicherheit

Netzwerksicherheitslösungen von WatchGuard sind von Grund auf so konzipiert, dass sie einfach zu implementieren, verwenden und verwalten sind – und darüber hinaus ein Höchstmaß an Sicherheit bieten. Unsere einzigartige Herangehensweise an die Netzwerksicherheit bedeutet, jedem Unternehmen, unabhängig von seiner Größe oder seinem technischen Fachwissen, die bestmögliche Sicherheit auf Enterprise-Niveau zur Verfügung zu stellen.

Identitätssicherheit

Die AuthPoint Identity Security-Lösungen von WatchGuard bieten erstklassige Multifaktor-Authentifizierung (MFA) und Zero-Trust-Risikorichtlinien für maximalen Online-Schutz. Nutzen Sie außerdem unsere Dark Web-Überwachungsdienste, um die Risiken weit verbreiteter Angriffe auf die Anmeldeinformationen von Mitarbeitern zu minimieren. AuthPoint widmet sich der Bereitstellung der ultimativen Benutzererfahrung und bietet Online- und Offline-Authentifizierungsmethoden sowie ein Webanwendungsportal für einen einfachen Single Sign-On-Zugriff.

Sicheres WLAN

Die sicheren WLAN-Lösungen von WatchGuard sind eine richtungsweisende Neuerung für den Markt von heute: Sie schaffen eine sichere, geschützte WLAN-Umgebung, eliminieren den Verwaltungsaufwand und ermöglichen beträchtliche Kostensenkungen. Die Kombination aus leistungsstarken Verwaltungs- und Analysemöglichkeiten und einer tiefgehenden Visualisierung sichert Unternehmen die entscheidenden Wettbewerbsvorteile für den geschäftlichen Erfolg.

Endpoint Security

WatchGuard Endpoint Security ist ein cloudnatives, fortschrittliches Endpoint-Sicherheitsportfolio, das Unternehmen jeder Art vor gegenwärtigen und zukünftigen Cyber-Angriffen schützt. Die auf künstlicher Intelligenz basierende Flagship-Lösung WatchGuard EPDR verbessert unmittelbar die Sicherheitslage von Unternehmen. Sie kombiniert die Funktionen Endpoint-Schutz (EPP) und Detection and Response (EDR) mit Zero Trust Application und Threat Hunting Services.

Über WatchGuard

WatchGuard® Technologies, Inc. gehört zu den führenden Anbietern im Bereich Cybersicherheit. WatchGuards Unified Security Platform®-Ansatz ist speziell auf Managed Service Provider ausgelegt, damit sie erstklassige Sicherheit bieten können, die die Skalierbarkeit und Schnelligkeit ihres Unternehmens erhöht und gleichzeitig die betriebliche Effizienz verbessert. Über 17.000 Vertriebspartner und Dienstleister im Bereich Sicherheit verlassen sich auf die prämierten Produkte und Services des Unternehmens, die die Bereiche Network Security and Intelligence fortschrittlicher Endpoint-Schutz, Multifaktor-Authentifizierung sowie sicheres WLAN umfassen, und sorgen somit für den Schutz von mehr als 250.000 Kunden. Gemeinsam bieten diese Bereiche die fünf entscheidenden Elemente einer Sicherheitsplattform: umfassende Sicherheit, kollektive Intelligenz, Transparenz und Kontrolle, operative Ausrichtung und Automatisierung. Neben der Zentrale in Seattle im US-Bundesstaat Washington unterhält das Unternehmen Niederlassungen in ganz Nordamerika, Lateinamerika und Europa sowie im asiatisch-pazifischen Raum. Weitere Informationen finden Sie unter WatchGuard.com.

DEUTSCHLAND, ÖSTERREICH, SCHWEIZ +49 700 92229333 **INTERNATIONALER VERTRIEB:** +1 206 613 0895 **WEB** www.watchguard.com

Mit diesem Dokument werden keine ausdrücklichen oder stillschweigenden Gewährleistungen gegeben. Alle hier aufgeführten technischen Daten können sich ändern. Informationen zu zukünftigen Produkten, Ausstattungsmerkmalen und Funktionen werden zu gegebener Zeit zur Verfügung gestellt. ©2025 WatchGuard Technologies, Inc. Alle Rechte vorbehalten. WatchGuard, das WatchGuard-Logo, Firebox, ThreatSync, Unified Security Platform und AuthPoint sind eingetragene Marken von WatchGuard Technologies, Inc. in den USA und/oder anderen Ländern. Alle weiteren Markennamen sind das Eigentum ihrer jeweiligen Inhaber. Teilenr. WGCE67830_080425