BESUCHEN SIE UNSER ENDPOINT PORTAL

WWW.BOC.DE/ENDPOINT

WatchGuard Endpoint Security

THREATSYNC - BESSERE THREAT DETECTION AND RESPONSE MIT XDR

WatchGuardONE® | PLATINUM PARTNER

b.o.c. IT-SECURITY

WATCHGUARD THREATSYNC

Frühere Erkennung und schnellere Reaktion auf Bedrohungen mit XDR

Ausgeklügelte Bedrohungen können überall und jederzeit auftreten und Ihr Unternehmen lähmen, bevor Sie die Anzeichen für eine Sicherheitsverletzung erkennen. Unternehmen haben Schwierigkeiten, mit einer schnell wachsenden und immer komplexer werdenden Bedrohungslandschaft Schritt zu halten. In der heutigen hybriden Welt arbeiten IT-Sicherheitsteams in mehr Umgebungen und unterstützen mehr Benutzer und Geräte als je zuvor.

Jeder dieser Angriffsvektoren birgt eine Reihe von Risiken und Schwachstellen, die spezielle Sicherheitslösungen erfordern. Eine unausgereifte Sammlung von Sicherheitsprodukten kann diese Sicherheitsherausforderungen nicht in großem Umfang bewältigen. Zudem fehlen Unternehmen die Zeit und qualifizierte Cybersicherheitsressourcen, um viele unterschiedliche Sicherheitstools zu verwalten oder das erforderliche Maß an manueller Visualisierung, Überwachung und Abwehr von Bedrohungen zu bewältigen.

Heutige Sicherheitsexperten benötigen eine einheitliche Sicherheitslösung, um neue Bedrohungen zu identifizieren, einzudämmen und schneller auf sie zu reagieren.

Extended Detection and Response (XDR) ist die Antwort. WatchGuard ThreatSync stattet Unternehmen mit dieser XDR-Funktionen aus, um Erkennungen zu zentralisieren und die Reaktion auf Bedrohungen über eine einzige Oberfläche zu orchestrieren.

Die Lösung vereinfacht die Cybersicherheit und verbessert gleichzeitig die Visualisierung und automatisiert eine schnellere Reaktion auf Bedrohungen im gesamten Unternehmen, wodurch Risiken und Kosten reduziert werden und eine höhere Genauigkeit erreicht wird.

ENDPOINT SECURITY

BESSERE VISUALISIERUNG

von Netzwerk- und Endpointaktivitäten zur Erkennung von Bedrohungen, die ansonsten unerkannt bleiben könnten.

UMFASSENDE SICHERHEIT

durch die Vereinheitlichung von Daten und Warnungen auf einer zentralen Plattform, auf der mit verschiedenen Lösungen ein gemeinsamer Ansatz zur Priorisierung und Reaktion auf Bedrohungen verfolgt werden kann.

ENTLASTUNG DES SICHERHEITSTEAMS

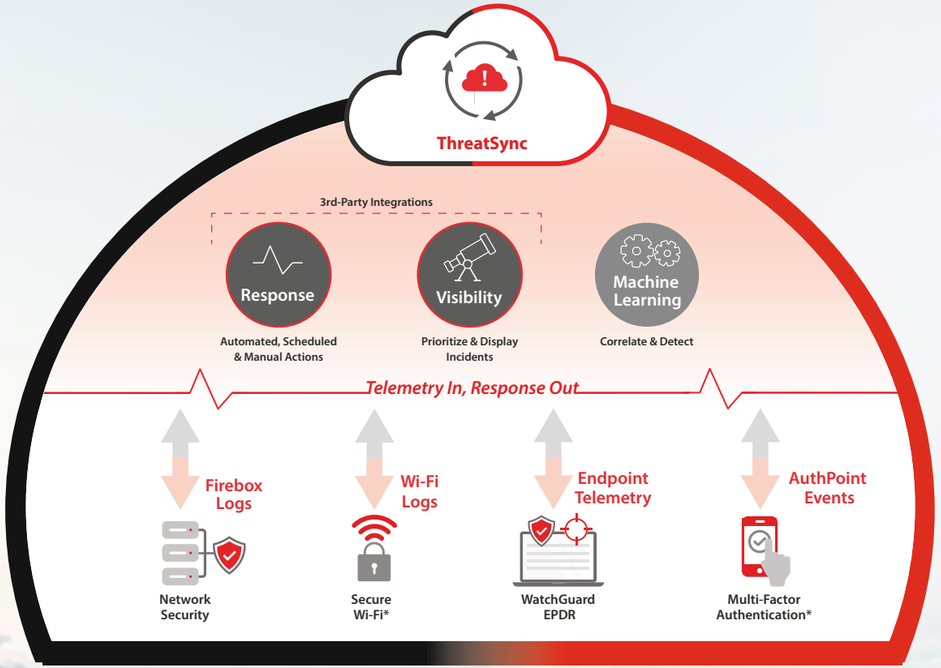
durch die Automatisierung der Bedrohungserkennung, des Reaktionsprozesses und durch mehr Zeit und Ressourcen für Sicherheitsteams.

OPTIMIERUNG DES REAKTIONSPROZESSES

durch die Bereitstellung koordinierter und automatisierter Reaktionen auf erkannte Bedrohungen.

KEINE ZUSÄTZLICHEN KOSTEN FÜR DEN ZUGRIFF AUF XDR

XDR ist ein zentrales Element der modernen Cybersicherheit, das für jedes Unternehmen zugänglich sein sollte. WatchGuard bietet ThreatSync daher in der Total Security Suite ohne zusätzliche Kosten an. Mit WatchGuard ThreatSync erhalten Sicherheitsexperten wieder die Kontrolle über ihre Sicherheitsstruktur. ThreatSync ist geeignet für jedes Unternehmen - unabhängig von Budget, Größe oder Komplexität.



* Secure Wi-Fi und AuthPoint werden demnächst in ThreatSync integriert.

Plattformübergreifende Erkennung von Bedrohungen

Die Lösung bietet erweiterte Erkennungsfunktionen, indem sie Gefährdungsindikatoren (IoCs) aus allen WatchGuard-Sicherheitsprodukten nutzt und entsprechend korreliert. Diese domänenübergreifende Kombination aus Kontext und Korrelation ermöglicht es ThreatSync, potenziell schädliche Aktivitäten in Bezug auf bestimmte Umgebungen, Benutzer und Geräte zu erkennen und zu bewerten, um die mittlere Zeit bis zur Erkennung (MTTD) zu reduzieren, die Genauigkeit zu verbessern und letztendlich eine schnellere Beseitigung der Bedrohung zu ermöglichen.

Einheitliche Sicherheitsorchestrierung und Reaktion auf Bedrohungen

Wenn Sicherheits- und IT-Administratoren einen ganzheitlichen Überblick über ihre Bedrohungslandschaft haben, können sie Bedrohungen schnell und zuverlässig nach ihrem Schweregrad einstufen und entsprechend reagieren. ThreatSync ermöglicht es IT-Sicherheitsadministratoren, mit intelligenter Alarmbewertung, automatisierten Abhilfemaßnahmen und Optionen für manuelle Eingriffe effizienter zu arbeiten. Dieser Grad der Orchestrierung von Bedrohungsreaktionen erweitert sowohl den Umfang als auch die Genauigkeit für Sicherheitsteams.

Einfache Bereitstellung und einfaches Management

WatchGuard ThreatSync macht die Einführung eines XDR-Ansatzes mit seinen intuitiven cloudbasierten Verwaltungs- und Automatisierungsfunktionen für einen Markt einfach, bei dem Zeit und Leistung eine wichtige Rolle spielen. Als leistungsstarke XDR-Ebene im Rahmen der Unified Security Platform®-Architektur von WatchGuard integriert ThreatSync produktübergreifende Intelligenz, um die Kosten und den Verwaltungsaufwand beim Einsatz von mehreren Punktlösungen zur Erkennung und Reaktion auf Bedrohungen zu reduzieren.

» XDR ist ein zentrales Element der modernen Cybersicherheit, das jedem Unternehmen zugänglich sein sollte. WatchGuard stellt ThreatSync als produktübergreifende Funktion, ohne zusätzliche Kosten in der Total Security Suite zur Verfügung. «

WATCHGUARD THREATSYNC

Unsicherheit mit einheitlicher Transparenz überwinden

Ihre Bedrohungserkennung ist zu ungenau? ThreatSync erhöht die Genauigkeit und beschleunigt die Erkennung, indem es die Bedrohungsdaten des gesamten Sicherheits-Stacks von WatchGuard automatisch in einer einzigen Oberfläche zusammenführt. Verschaffen Sie sich ein vollständiges Bild der Bedrohungen und des Kontextes von übergreifenden Erkennungen von einer einzigen Oberfläche aus, ohne dass die Benutzer mehrere Konsolen erlernen und verwenden müssen.

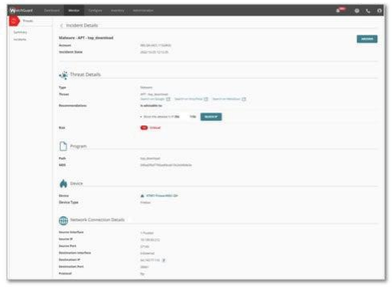
Schenken Sie Ihrem IT-Team Zeit – mit der Priorisierung von Vorfällen

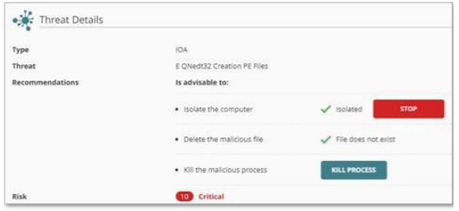
Allzu häufig investieren Cybersicherheitsteams viel Zeit in die Priorisierung von Risiken, Vorfällen und Bedrohungen – in der Erwartung, dass sie diese schnell verstehen werden. Erhalten Sie Bewertungen und erkennen Sie bösartige Szenarien, die den Kontext für die Priorisierung von Vorfällen liefern. So können IT- und SEC-Teams die Risikostufe der Bedrohung nachvollziehen und wissen genau, wo sie ansetzen müssen, um schneller die richtigen Entscheidungen zu treffen.

WICHTIGE FUNKTIONEN

Frühzeitige Erkennung für besseren Schutz

Die manuelle Zusammenstellung von Sicherheitsdaten aus verschiedenen Quellen entfällt, wodurch der Aufwand für die Suche nach Bedrohungen reduziert wird. Erkennen Sie Bedrohungen mit ThreatSync früher – einem Tool, das ein einheitliches Benutzererlebnis bietet, indem es Aktivitäten korreliert, die anhand domänenübergreifender Daten überwacht werden. Dies verringert die durchschnittliche Erkennungszeit und beseitigt die Hindernisse, die das Sicherheitsteam ausbremsen. Je früher Sie die Bedrohung erkennen, desto schneller können Sie reagieren.





Schnelleres Reagieren auf Bedrohungen

Im Bereich der Sicherheit ist die Chance, erfolgreich auf eine Sicherheitsverletzung zu reagieren, eine Frage des Wissens und der Zeit. Sobald die Sicherheitsexperten über die benötigten Informationen verfügen, ist es einfach, schnell zu reagieren. Verknüpfen Sie mit ThreatSync die im gesamten Ökosystem verteilten Erkennungen miteinander und geben Sie Ihrem Team die Möglichkeit, mehrere Reaktionsmaßnahmen festzulegen und zu automatisieren, damit sich Bedrohungen nicht auf das gesamte Unternehmen ausbreiten können.

WATCHGUARD SECURITY SERVICES

Jede WatchGuard Firebox kommt ab Werk immer mit einer Lizenz für 1, 3 oder 5 Jahre - in den Stufen "Standard Support", "Basic Security Suite" oder "Total Security Suite".

Fireboxen mit **Standard Support** stellen nur die Basis-Funktionalität als Firewall und VPN Endpunkt zur Verfügung.

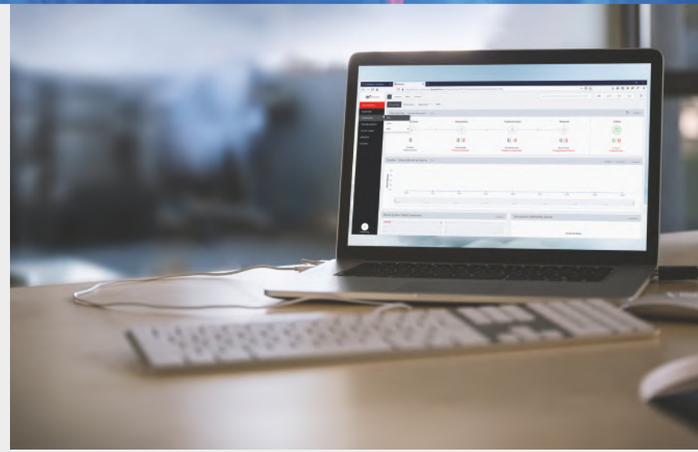
Den eigentlichen Nutzen als Network Security Appliance entfaltet eine WatchGuard Firebox erst, wenn die Lizenzierungsstufen **Basic Security Suite** oder **Total Security Suite** gewählt werden.

	Standard Support	Basic Security Suite	Total Security Suite
Stateful Firewall	✔	✔	✔
VPN	✔	✔	✔
SD WAN	✔	✔	✔
Access Portal [1]	✔	✔	✔
Intrusion Prevention Service (IPS)		✔	✔
Application Control		✔	✔
WebBlocker		✔	✔
spamBlocker		✔	✔
Gateway Antivirus		✔	✔
Reputation Enabled Defense (RED) + Botnet Detection		✔	✔
Network Discovery		✔	✔
APT Blocker			✔
ThreatSync (XDR)			✔
EDR Core			✔
DNSWatch			✔
IntelligentAV [2]			✔
WatchGuard Cloud Visibility Datenaufbewahrung		1 Tag	**30 Tage**
Hersteller-Support	Standard (24x7)	Standard (24x7)	**Gold (24x7)** [3]

[1] nicht erhältlich auf Firebox T20/T20-W, T25/T25-W, T35-R. Total Security Suite erforderlich für M270, M370, M470, M570, M670, FireboxV und Firebox Cloud
[2] nicht erhältlich auf Firebox T20/T20-W, T25/T25-W, T35-R oder älteren Firebox Modellen
[3] verkürzte Reaktionszeit

WATCHGUARD CLOUD

DEMO UMGEBUNG: ThreatSync in der WatchGuard Cloud **live** erleben



Erfahren Sie bei dieser Online-Tour, wie einfach es ist, WatchGuard AuthPoint, Endpoint Security, Firebox und WLAN zu verwalten und lernen dabei auch die Funktionen von ThreatSync kennen.

Besuchen Sie dazu einfach www.boc.de/watchguard-cloud-demo und starten Sie die Demo, um die WatchGuard Cloud kennenzulernen.

In dem Demokonto befinden sich Beispieldaten, die einem typischen Administratorkonto entsprechen. Nach der Anmeldung können Sie eigenständig durch die WatchGuard Cloud navigieren, um sich u.a. Folgendes anzusehen:

- Firebox-Richtlinienmanagement und VPN-Bereitstellung
- Einfache MFA-Konfiguration für die verschiedenen Firebox-Authentifizierungsoptionen
- Dashboards und Berichte zur Netzwerksicherheit
- Dashboards zur Endpoint Security, einschließlich Zero-Trust und Threat Hunting Services
- Berichte zu Authentifizierung und Benutzeraktivität
- Konfigurationsseiten für WatchGuard Firebox und AuthPoint
- Lizenzdetails und vieles mehr

DREI BEISPIELE FÜR ANWENDUNGSSZENARIEN

1

Rüsten Sie ausgehend von einem kostenlosen oder auf private Nutzung ausgerichteten Endpoint-AV-Produkt auf.

Manchmal setzen kleinere Unternehmen oder solche, die nur wenige Geräte außerhalb des Netzwerkperimeters haben, auf ein reduziertes Risikoprofil und schieben Investitionen in die Sicherheit auf. Aber die Welt verändert sich. Da Unternehmen immer mehr Risiken ausgesetzt sind und strengere Vorschriften zur Datensicherheit und zum Datenschutz erfüllen müssen, gehen sie zu einer Business-Lösung wie dem Produkt WatchGuard EPP über. WatchGuard EPP ist mit starker signaturbasierter Prävention, einschließlich Signaturen von Malware aus unserer Installationsbasis, sowie Verhaltensanalyse und Filterung von Webinhalten eine kluge Wahl, die zukunftssicher ist, da die Plattform mit dem Geschäftswachstum Schritt hält.

☆ Empfohlene Lösung

WatchGuard EPP oder WatchGuard EPDR

2

Fügen Sie als geplante Sicherheitsinvestition die EDR-Funktion zu einer vorhandenen AV-Lösung hinzu.

Diese Unternehmen sind sich der Sicherheitsrisiken am Endpoint bewusst und haben ein AV-Produkt eingeführt. Doch sie wissen, dass sie eine EDR-Lösung benötigen, um Hackern einen Schritt voraus zu sein. Es besteht keine Notwendigkeit, auf eine Verlängerung des AV-Vertrags zu warten. Unsere WatchGuard EDR-Lösung ergänzt eine vorhandene AV-Bereitstellung, so dass Kunden schnell von unserem fortschrittlichen, differenzierten Ansatz profitieren können.

☆ Empfohlene Lösung

WatchGuard EDR

3

Wiederherstellung nach einem Angriff oder nach der Erkennung von verborgener Malware auf Endpoints oder in Unternehmensnetzwerken, wenn die Malware von einem Endpoint stammt.

Unternehmen in dieser Position haben zwei Gewissheiten – erstens, dass sie für Cyberkriminelle von Interesse sind, und zweitens, dass ihr derzeitiges Schutzniveau nicht angemessen ist. Da sich der erweiterte Schutz von WatchGuard EPDR mit dem Zero Trust Application Service und dem Threat Hunting Service weiterentwickelt hat, ist die Anzahl der auf Malware basierenden Angriffe, die das Support-Team untersucht/bearbeitet hat, auf nahezu null gesunken – WatchGuard-Endpoint-Kunden erleben diese Angriffe also gar nicht mehr. In Kombination mit den Visualisierungs- und Management-Tools zur Steigerung der Produktivität eines überlasteten IT-Teams ist der Service dafür gerüstet, wiederholte Angriffe und teure Behebungsmaßnahmen zu verhindern.

☆ Empfohlene Lösung

WatchGuard EPDR

ENDPOINT PORTAL

Auf unserem Endpoint Security Portal **www.boc.de/endpoint** finden Sie hilfreiche Informationen und Lösungen rund um das Thema Endpoint Sicherheit.

b.o.c. IT-SECURITY

BOC IT-Security GmbH
Essener Straße 2-24
46047 Oberhausen
T: +49 208 8596 440
E: info@boc.de

IMPRESSUM
Herausgeber: BOC IT-Security GmbH
Grafik & Layout: Nina Wiegand
Bild- und Textnachweise: WatchGuard Technologies Inc., BOC IT-Security GmbH, envato
Keine Gewährleistung für Druckfehler oder Irrtümer. Stand: März 2023