Vorteile der WatchGuard Firebox

Firewalls, die speziell für die heutigen modernen Netzwerke entwickelt wurden

Im Durchschnitt blockiert eine Firebox jährlich mehr als 1.300 Malware-Angriffe und 250 Netzwerkbedrohungen für WatchGuard-Kunden. Die WatchGuard Firebox bietet erweiterte Firewall-Sicherheit, die IT-Experten dank universell einsatzbarer Sicherheits- und Visualisierungswerkzeuge für die Bedrohungserkennung eine komplette Kontrolle über ihre Netzwerke auf Enterprise-Niveau bietet – unabhängig von dem Budget oder der Komplexität des Unternehmens.

WatchGuard Firewalls können viel mehr als nur den Datenverkehr blockieren. Sie bieten Intrusion Prevention Services, Gateway Antivirus, Anwendungskontrolle, Spam-Blockierung und Web-Filterung sowie die Integration fortschrittlicher Services, um Cloud- und Hybrid-Unternehmen vor ausgefeilter Malware, Ransomware und Datendiebstahl zu schützen.

Die Verwaltung einer Firebox in WatchGuard Cloud erleichtert die Einrichtung und Netzwerkkonfiguration für mehrere Clients und verschiedene Netzwerke. Ihr Team muss sich weniger auf Prozesse konzentrieren und hat daher mehr Zeit dafür, die Rentabilität zu erhöhen und gleichzeitig die Sicherheit zu bieten, die Ihre Kunden erwarten.

Einfache Policy-Verwaltung

Cloudverwaltetes Reporting und Transparenz

Mandantenfähige Verwaltung

Threat Detection and Response

Für hybride Architekturen entwickelt

Hybride Umgebungen sind die neue Norm, in der lokale, Cloud- und Remote-Infrastruktur nahtlos zusammenarbeiten müssen. WatchGuard Firebox Appliances eignen sich für hybride Architekturen besonders gut, da sie eine grundlegende Ebene für den Bau und Betrieb in der heutigen modernen Welt bieten. Firebox Firewalls der nächsten Generation kombinieren leistungsstarke Leistung, intelligente Bedrohungserkennung und umfassende Integrationsfunktionen, die für den Betrieb in der heutigen Welt erforderlich sind.

SSL-Überprüfung und -Schutz

Mittlerweile erfolgen mehr als 80 % des Datenverkehrs Ihrer Kunden über HTTPS. Dadurch entsteht ein riesiger toter Winkel. Bei WatchGuard sehen wir die Analyse von HTTPS-Inhalten nicht als optionales Extra an, sondern als grundlegenden Sicherheitsstandard in jeder WatchGuard Firebox. Darüber hinaus überprüft WatchGuard Firebox als eine der ersten Firewallplattformen TLS 1.3-Verkehr gründlich.

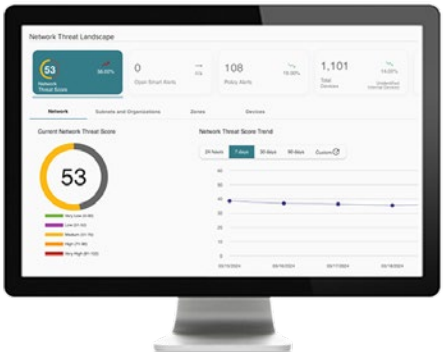
KI-basierter IntelligentAV und Sandbox-basierter APT-Blocker

Erhöhen Sie Ihre Sicherheit mit mehrschichtigem Schutz, der bekannte und unbekannte Bedrohungen abwehrt. IntelligentAV setzt auf maschinelles Lernen, um neue und sich verändernde Schadsoftware zu identifizieren, ohne auf Signaturen angewiesen zu sein. Mithilfe von APT Blocker und Sandboxing werden verdächtige Dateien in einer sicheren, isolierten Umgebung analysiert, um Zero-Day-Angriffe zu erkennen und zu verhindern, bevor sie Schaden anrichten können.

Sicherer Zugriff mit der neuesten VPN-Technologie

Virtuelle private Netzwerke (VPNs) bieten einen sicheren Tunnel von Remotestandorten zurück zu einer Hauptniederlassung. WatchGuard Firebox bietet Branch Office-VPNs (BOVPN) für standortübergreifende Verbindungen mit Remote-/mobilen Büros über IPSec/IKEv2 und SSL-VPN.

Erweiterte Integrationen, um mit fortschrittlicher Malware Schritt zu halten



ThreatSync-Funktionen

Die KI-gestützte, offene Netzwerk-Bedrohungserkennung und -reaktion ist über ThreatSync in die Firebox integriert. Diese Funktion überwacht kontinuierlich das gesamte Netzwerk auf Änderungen und verwendet intelligentes Risiko-Scoring, um Ihnen zu helfen, sich auf das Wesentliche zu konzentrieren. Sie ist in der Total Security Suite enthalten.

Korrelation von Endpoint und Identität

Über Hardware und virtuelle Firewalls hinweg integriert unsere Firebox nahtlos Endpoint- und Identitäts-Sicherheitslösungen, um eine schnellere Reaktion auf Vorfälle und eine effektive Durchsetzung von Richtlinien zu ermöglichen. Diese Mechanismen helfen Unternehmen und Partnern, eine sichere und widerstandsfähige Umgebung zu schaffen, egal ob lokal oder remote.

Sicherheit auf Firewall-Ebene mit FireCloud

Die kombinierte Bereitstellung von Firebox und FireCloud, dem verwalteten, cloudbasierten FWaaS (Firewall-as-a-Service), schafft ein leistungsstarkes hybrides Sicherheits-Setup, das einen einheitlichen und starken Schutz in lokalen, Cloud- und Remote-Umgebungen bietet. Die Integration bietet Wettbewerbsvorteile und unterstützt verschiedene moderne Anwendungsfälle.

> Bei WatchGuard erwerben wir das Total Security-Paket – und das war's. Wir müssen uns um nichts weiter kümmern. Bei einigen Mitbewerbern kauft man sechs oder sieben verschiedene Posten, um dieselbe Leistung zu erhalten wie bei WatchGuard mit einem einzigen Produkt.
>
> **Colin Bridle**
> Direktor, Redinet

THE CHANNEL CO. CRN CHANNEL CHIEFS 2025

SILBER ENTERPRISE NETWORK FIREWALLS SECURITY INSIDER AWARD 2024

canalys GLOBAL CYBERSECURITY CHAMPION 2025

TrustRadius Top Rated 2025

2024 FORTRESS CYBER SECURITY AWARD

GLOBAL INFOSEC AWARDS WINNER CYBER DEFENSE MAGAZINE 2024

Lernen Sie die Firebox Suite kennen

Firebox Tabletop-Modelle

Perfekt für kleine Büros, Zweigstellen und sogar Heimbüros, die erstklassige Sicherheit benötigen

Firebox Rackmount-Modelle

Entwickelt für wachsende Netzwerke, mittelständische Unternehmen und verteilte Unternehmen

Cloudbasierte und virtuelle Firewalls

Speziell für virtuelle Umgebungen entwickelt – mit dem gleichen umfassenden Schutz wie für lokale Netzwerke

Alle Funktionen in einer Gesamtlösung. Keine Zusatzgebühren

Speziell für wachsende moderne Netzwerke entwickelt

Mit unseren Sicherheitspaketen finden Sie schnell die richtigen Funktionen, die Ihr Unternehmen heute – und auch in Zukunft – benötigt.

	WatchGuard	Fortinet	SonicWall	Sophos
Funktionsvergleich	**Total Security Suite**	**Enterprise Protection**	**Advanced Protection**	**Xstream Protection**
Stateful Firewall	✓	✓	✓	✓
VPN	✓			
Access Portal*	✓			✓
SD-WAN	✓	✓	✓	✓
Gateway AntiVirus	✓	✓	✓	✓
Intrusion Prevention Service (IPS)	✓	✓	✓	✓
Anwendungskontrolle	✓	✓	✓	✓
WebBlocker	✓	✓	✓	✓
SpamBlocker	✓	✓	✓	Kostenpflichtiges Add-on
Network Discovery	✓	✓	✓	✓
Reputation Enabled Defense	✓	✓	✓	✓
IntelligentAV**	✓	✓	✓	✓
APT Blocker	✓	✓	✓	✓
DNSWatch	✓	✓	✓	✓
XDR (ThreatSync)	✓	Kostenpflichtiges Add-on		Kostenpflichtiges Add-on
Endpoint Protection (EDR-Core)	✓	Kostenpflichtiges Add-on		Kostenpflichtiges Add-on
Aufbewahrung von Cloud-Protokolldaten	365 Tage		✓	✓
Standard Support (24x7)	✓	✓	✓	✓
Gold-Support	✓			✓

Informationen zu 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 Nordamerika, Lateinamerika und Europa sowie im asiatisch-pazifischen Raum. Weitere Informationen finden Sie unter WatchGuard.de.