

Feature Brief

Übersicht über die Funktionen der Firebox Security Suites

Wählen Sie die richtige Sicherheitssuite für Ihre Anforderungen

Die Firebox Security Suites von WatchGuard wurden entwickelt, um Unternehmen dabei zu unterstützen, ihre Sicherheitslage im Zuge sich wandelnder Anforderungen zu stärken. Ganz gleich, ob Sie grundlegenden Netzwerkschutz, fortschrittliche Bedrohungsprävention oder umfassende Erkennungs- und Reaktionsfunktionen benötigen – Firebox bietet eine auf Ihre Bedürfnisse zugeschnittene Security Suite.

BASIC
Grundlegende Sicherheit

Basic Security Suite (BSS)
Bietet die wesentlichen Schutzfunktionen, die man von einer modernen UTM-Firewall erwartet

PRIME
Erweiterter Schutz

Prime Security Suite (PSS)
Erweitert Firebox um fortschrittlichen Schutz, verbesserte Transparenz und umfassendere Einblicke in den Betrieb.

TOTAL
Umfassende Security Suite

Total Security Suite (TSS)
Bietet das umfassendste Sicherheitsangebot von WatchGuard und vereint Funktionen zur Prävention, Erkennung, Untersuchung und Reaktion.

In Security Suite enthalten	Basic Security	Prime Security	Total Security
Stateful Firewall	✓	✓	✓
VPN	✓	✓	✓
SD-WAN	✓	✓	✓
Access Portal	✓	✓	✓
Intrusion Prevention Service (IPS)	✓	✓	✓
Application Control	✓	✓	✓
WebBlocker	✓	✓	✓
spamBlocker	✓	✓	✓
Gateway AntiVirus	✓	✓	✓
Blockierung der Geolokalisierung	✓	✓	✓
Botnet Detection	✓	✓	✓
Tor Exit Node Blocking	✓	✓	✓
Network Discovery	✓	✓	✓
APT Blocker		✓	✓
DNSWatch		✓	✓
Schatten-KI		✓	✓
Netzwerkverwaltung		✓	✓
IntelligentAV			✓
ThreatSync (XDR)			✓
EDR Core			✓
WatchGuard Cloud			
Aufbewahrung von Protokolldaten	45 Tage	90 Tage	**365 Tage**
Aufbewahrung von Berichtsdaten	1 Tag	7 Tage	**30 Tage**
Support	Standard (24 x 7)	Standard (24 x 7)	**Gold (24 x 7)**

Total Security Suite

Was ist das

Die Total Security Suite ist das umfassendste Firebox-Sicherheitsangebot von WatchGuard. Sie vereint fortschrittliche Bedrohungsprävention, Endgeräteschutz, XDR und Reaktionsfunktionen mit erweiterter Datenaufbewahrung und Premium-Support.

Unternehmen profitieren über die WatchGuard Cloud von einer einheitlichen Sicherheitserfahrung und gehen dabei über die herkömmliche Netzwerksicherheit hinaus, hin zu umfassenderen Erkennungs- und Reaktionsworkflows.

Für wen ist sie gedacht

Die Total Security Suite ist ideal für Unternehmen, die:

- umfassenden Sicherheitsschutz benötigen
- Funktionen zur Erkennung und Reaktion auf Bedrohungen benötigen
- Endgeräteschutz in ihre Sicherheitsstrategie integrieren möchten
- Compliance- oder Audit-Anforderungen erfüllen müssen
- eine verlängerte Aufbewahrungsdauer für Sicherheitsdaten benötigen
- eine einheitliche Sicherheitsplattform bevorzugen

Kundennutzen	
Mehr Bedrohungen erkennen	Gehen Sie über die reine Prävention hinaus – mit XDR- und Endpoint-Schutzfunktionen, die darauf ausgelegt sind, verdächtige Aktivitäten in der gesamten Umgebung zu erkennen.
Reaktionsfähigkeit verbessern	Ermitteln Sie Bedrohungen aus der WatchGuard Cloud und ergreifen Sie entsprechende Maßnahmen – alles über eine zentrale Verwaltungsoberfläche.
Risiken minimieren	Kombinieren Sie Netzwerksicherheit, Endgeräteschutz und fortschrittliche Malware-Prävention zu einer einheitlichen Sicherheitsarchitektur.
Unterstützung des Sicherheitsbetriebs	Sichern Sie sich Transparenz, Kundenbindung und erstklassigen Support, die für ausgereifte Sicherheitsprogramme erforderlich sind.
Sicherheit vereinfachen	Verwalten Sie mehrere Schutzebenen über eine einzige Plattform statt über einzelne Sicherheitsprodukte.

Prime Security Suite

Was ist das

Die Prime Security Suite ist eine Suite von Sicherheitsdiensten, die Firebox um Cloud-Sandboxing, DNS-Filterung, Transparenz durch Schatten-KI und umfassendere Einblicke in den Betrieb erweitert.

Sie richtet sich an Unternehmen, die sich einen stärkeren Schutz und mehr Transparenz wünschen, ohne dabei auf eine einfache Bereitstellung und Verwaltung verzichten zu müssen.

Für wen ist sie gedacht

Die Prime Security Suite eignet sich ideal für Unternehmen, die:

- mehr als nur den grundlegenden UTM-Schutz benötigen
- Schutz vor komplexen und unbekannten Bedrohungen wünschen
- Sicherheit auf DNS-Ebene benötigen
- Einblick in die Nutzung generativer KI wünschen
- Topologie-Mapping und Transparenz der Infrastruktur benötigen
- längere Aufbewahrungsfristen für Untersuchungen und Berichterstellung benötigen
- erweiterten Schutz ohne eine vollständige Security-Operations-Plattform wünschen

Kundennutzen	
Erweiterte Bedrohungen abwehren	Mithilfe von Cloud-Sandboxing lassen sich schwer zu erkennende und bisher unbekannte Schadprogramme identifizieren, bevor sie den Nutzern Schaden zufügen.
DNS-Sicherheit verbessern	Durch DNS-Filterung lassen sich Verbindungen zu bösartigen Zielen unterbinden, bevor Sitzungen aufgebaut werden.
Sichtbarkeit erhöhen	Verstehen Sie die Nutzung von KI-Anwendungen und gewinnen Sie umfassendere Einblicke in die Netzwerkinfrastruktur und deren Zustand.
Betriebsabläufe verbessern	Netzwerküberwachung, Topologie-Kartierung und Berichterstellung helfen den Teams dabei, Probleme schneller zu erkennen und zu beheben.
Mehr Sicherheitskontext beibehalten	Eine Protokollaufbewahrungsdauer von 90 Tagen bietet einen besseren Überblick über vergangene Ereignisse und erleichtert so die Fehlerbehebung und Untersuchungen.

Basic Security Suite

Was ist das

Die Basic Security Suite bietet die wesentlichen Netzwerksicherheitsdienste, die man von einer modernen UTM-Firewall erwartet. Sie vereint zentrale Funktionen zur Bedrohungsabwehr, Anwendungskontrolle, Webfilterung und Transparenz in einem einzigen Firebox-Sicherheitspaket.

Für wen ist sie gedacht

Die Basic Security Suite eignet sich ideal für Unternehmen, die:

- wesentliche Firewall-Sicherheitsdienste benötigen
- Schutz vor gängigen Netzwerkbedrohungen wünschen
- Kontrolle über die Anwendungs- und Webnutzung benötigen
- Einblick in die Geräte im Netzwerk benötigen
- ein einfaches Modell für die Sicherheitsbereitstellung wünschen
- grundlegende Anforderungen an die Aufbewahrungsfristen haben

Kundennutzen	
Grundlegende Gefahrenprävention	Schützen Sie Benutzer und Netzwerke vor gängiger Malware, bösartigen Websites, unerwünschten Anwendungen und bekannten Angriffstechniken.
Netzwerkaktivität überwachen	Verwalten Sie die Anwendungsnutzung und den Webzugriff, um die Sicherheit, die Produktivität und die Durchsetzung von Richtlinien zu verbessern.
Netzwerkgeräte erkennen	Ermitteln Sie die mit dem Netzwerk verbundenen Systeme und verbessern Sie den Überblick über die Umgebung.
Sicherheitsmanagement vereinfachen	Verwalten Sie Sicherheitsdienste über die WatchGuard Cloud mit einer zentralisierten Verwaltungsoberfläche.
Sicherheitsgrundlage schaffen	Richten Sie die zentralen Kontrollmaßnahmen ein, die zur Unterstützung eines modernen Cybersicherheitsprogramms erforderlich sind.

Informationen zu WatchGuard

WatchGuard® Technologies, Inc. gehört zu den führenden Anbietern im Bereich Cybersicherheit. Unser Unified Security Platform®-Ansatz ist speziell auf Managed Service Provider ausgelegt, damit sie erstklassige Sicherheit bieten können, die die Skalierbarkeit und Schnelligkeit des 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 über 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.