

Eine Appliance. Ein Paket. Totale Sicherheit.

Wir bei WatchGuard halten alles möglichst einfach – und das betrifft weit mehr als den Aufbau und die Lizenzierung unserer Produkte. Unsere Dienste sind sozusagen Konfektionsware. In diesem Sinne haben wir zwei Lizenzpakete entwickelt, um unseren Kunden die Entscheidung zu erleichtern. Sowohl die Total Security Suite als auch die Basic Security Suite sind für die Modelle Firebox T und M sowie die Firebox Cloud und die virtuelle Plattform FireboxV verfügbar.

- Die **Basic Security Suite** beinhaltet alle gängigen Network Security-Dienste für UTM-Appliances: IPS, GAV, URL-Filterung, Application Control, Spam Abwehr, Reputation-Suchdienst sowie zentralisiertes Management und Netzwerkvisualisierungsfunktionen, ergänzt um unseren Support, der standardmäßig rund um die Uhr verfügbar ist.
- Die **Total Security Suite** verfügt neben sämtlichen Diensten der Basic Security Suite über Advanced Persistent Threat Abwehr, Schutz vor Datenverlust, erweiterte Netzwerkvisualisierungsfunktionen und Mechanismen zur Abwehr von Bedrohungen direkt aus Dimension, unserer Netzwerkvisualisierungsplattform. Abgerundet wird die Suite durch erweiterten Gold-Support rund um die Uhr.

Funktionen und Dienste	TOTAL SECURITY SUITE	Basic Security Suite
Intrusion Prevention Service (IPS)	✓	✓
App Control	✓	✓
WebBlocker	✓	✓
spamBlocker	✓	✓
Gateway Antivirus	✓	✓
Reputation Enabled Defense (RED)	✓	✓
Network Discovery	✓	✓
APT Blocker	✓	
Data Loss Protection (DLP)	✓	
Threat Detection and Response	✓	
DNSWatch	✓	
Access Portal*	✓	
IntelligentAV*	✓	
Dimension Command	✓	
WatchGuard Cloud Visibility Datenaufbewahrung	30 Tage	1 Tag
Support	Gold (24x7)	Standard (24x7)

*Verfügbar für die letzte Generation der M-Serie Appliances

*Threat Detection and Response ist im Rahmen unserer Total Security Suite erhältlich. Host Sensor-Lizenzen variieren je nach eingesetzter Appliance. Der Host Sensor ist auch im Rahmen einer Ergänzungsoption (Add-on) erhältlich.

Einstieg

WatchGuard verfügt über ein Netzwerk an Vertriebspartnern und Service Providern, das branchenweit seinesgleichen sucht. Für den Einstieg empfehlen wir einen Besuch unserer Webseite. Dort finden Sie den passenden Partner für Ihr Unternehmen. Selbstverständlich können Sie uns auch direkt ansprechen. Wir beantworten gerne alle Fragen und vermitteln Ihnen den Kontakt zu dem Partner, der Ihren Anforderungen optimal gerecht wird.

- Durchsuchen Sie unser Partner-Netzwerk: findpartner.watchguard.com
- Sprechen Sie mit einem WatchGuard-Sicherheitsexperten: <http://www.watchguard.com/de/wgrd-international/contact-us>
- Weitere Informationen zum Kauf: www.watchguard.com/totalsecurity

Informationen zu WatchGuard

WatchGuard® Technologies, Inc. gehört zu den führenden Anbietern im Bereich Netzwerksicherheit, sicheres WLAN, Multifaktor-Authentifizierung und Network Intelligence. Beinahe 10.000 Vertriebspartner und Dienstleister im Bereich Sicherheit verlassen sich auf die prämierten Produkte und Dienste des Unternehmens, um mehr als 80.000 Kunden zu schützen. Die Philosophie von WatchGuard ist es, Sicherheit auf Enterprise-Niveau für Unternehmen jeder Größenordnung und Art zu realisieren. Das macht WatchGuard insbesondere für kleine und mittlere sowie dezentral aufgestellte Unternehmen zum idealen Anbieter. 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.

Mit diesem Dokument werden keine ausdrücklichen oder implizierten Gewährleistungen gegeben. Alle hier aufgeführten technischen Daten können sich ändern. Informationen zu zukünftigen Produkten, Ausstattungsmerkmalen und Funktionen werden zu gegebener Zeit zur Verfügung gestellt. ©2019 WatchGuard Technologies, Inc. Alle Rechte vorbehalten. WatchGuard, das WatchGuard-Logo, DNSWatch, IntelligentAV, Firebox und WatchGuard Dimension sind Marken bzw. eingetragene Marken von WatchGuard Technologies, Inc. in den USA und/oder anderen Ländern. Alle weiteren Markennamen sind das Eigentum ihrer jeweiligen Inhaber. Teilnr. WGC66926_052219

WatchGuard Total Security

Umfassender Netzwerkschutz aus einer Hand

Totale Sicherheit

Eine Stateful Packet Firewall ist unerlässlich, aber längst nicht mehr genug. In der Realität benötigt jedes Netzwerk ein ganzes Arsenal an Sicherheitsfunktionen, um sich vor Spyware und Viren, bössartigen Anwendungen, Datenverlust, Ransomware, Botnets, APT (Advanced Persistent Threats) und Zero-Day-Schadprogrammen schützen zu können. Eine Network Security-Lösung, die diesen Namen wirklich verdient, deckt dabei sämtliche Aspekte der Abwehr, Erkennung, Zuordnung und Bekämpfung von aufkommenden Bedrohungslagen ab. Die prämierte Plattform für Network Security von WatchGuard bietet nicht nur die branchenweit umfassendsten Sicherheitskontrollen, sondern ist auch seit jeher Vorreiter bei der Erkennung und Abwehr neuer Bedrohungen, insbesondere hoch entwickelter Schadsoftware (Advanced Malware) und Ransomware.

Total simpel

Neben den Sicherheitsscanmodulen spielen jedoch noch weitere Faktoren eine Rolle. Wir bei WatchGuard sind der festen Überzeugung, dass Technologie vor allem einfach sein muss, wenn sie erfolgreich sein soll. Deshalb sind all unsere Produkte nicht nur einfach zu konfigurieren und bereitzustellen. Bei der Entwicklung liegt das Hauptaugenmerk auf dem zentralen Management, das die Richtlinien- und Netzwerkverwaltung strafft und vereinfacht. Das Thema Sicherheit ist komplex genug, die Verwaltung muss es nicht auch noch sein.

Total stark

Jedes Unternehmen, gleich welcher Größenordnung, muss beim Thema Security auf die Leistung achten. Denn langsame Sicherheitsscans können ein Netzwerk schnell in die Knie zwingen. Nicht selten müssen Unternehmen in solchen Fällen den Schutz verringern, um die erforderliche Leistung aufrechtzuerhalten. Mit WatchGuard müssen sie diese faulen Kompromisse nicht mehr eingehen. Die Plattform von WatchGuard, auf der alle Scanvorgänge dank Multicore-Verarbeitung gleichzeitig erfolgen, liefert den schnellsten Durchsatz, wenn es darauf ankommt – ohne Abstriche bei der Sicherheit. Auf unserer Plattform können alle Scanmodule gleichzeitig ausgeführt werden. Das Ergebnis: maximaler Schutz bei enorm hohem Datendurchsatz.

Totale Visualisierung

Durch die leistungsstarken Lösungen zur Visualisierung der Netzwerksicherheit von WatchGuard – WatchGuard Cloud Visibility und WatchGuard Dimension – werden sämtliche Daten aller Geräte im Netzwerk zusammengetragen und optisch ansprechend aufbereitet. Mithilfe dieser Visualisierungslösungen können Sie Verhaltenstrends ermitteln, potenzielle Netzwerkbedrohungen lokalisieren, eine unangemessene Nutzung unterbinden und haben somit Ihr Netzwerk jederzeit vollständig unter Kontrolle.

Sicherheit auf Enterprise-Niveau



Simple



Hervorragende Leistung



Bedrohungserkennung



Zukunftssicher



WatchGuard Security Services

WatchGuard bietet das umfassendste Paket an Netzwerksicherheitsdiensten. Zu den klassischen Komponenten IPS, GAV, Application Control, Spamblocking und Webfilterung kommen erweiterte Dienste zum Schutz vor Advanced Malware, Ransomware und dem Verlust sensibler Daten. Abgerundet wird das Angebot von WatchGuard durch ein Komplettpaket mit Diensten zur Netzwerkvisualisierung und -verwaltung.

„Die wichtigsten Vorteile für uns haben sich durch den Wechsel von einer normalen Stateful Firewall zu einer vollumfänglichen Layer-7-Sicherheitsplattform ergeben. Dadurch gelang die Einbindung von IPS/IDS, Anwendungsfilterung, Malware-Erkennung, Gateway AV, Webfilterung und aller anderen Sicherheitsfunktionen von WatchGuard. In dieser einen Einheit sind bereits so viele Sicherheitsfunktionen enthalten, dass deren Einzelanschaffung bereits aus finanziellen Gründen nicht sinnvoll gewesen wäre.“
 ~ Peter Thomas, IT Manager, Roland UK

GRUNDLEGENDE SICHERHEITSDIENSTE

Intrusion Prevention Service (IPS)
Dieser Dienst überwacht mithilfe laufend aktualisierter Signaturen den Datenverkehr in allen gängigen Protokollen und bietet Echtzeit-Schutz vor Netzwerkbedrohungen.

Reputation Enabled Defense (RED)
Ein cloudbasierter Reputations-Suchdienst, der Benutzer vor böartigen Websites und Botnets schützt und dabei den Overhead bei der Webverarbeitung erheblich verbessert.

Network Discovery
Ein abonnementbasierter Dienst, der eine visuelle Topologie sämtlicher Knoten in Ihrem Netzwerk generiert. So können Sie umgehend riskante Bereiche erkennen.

WebBlocker-URL-Filterung
Blockiert böartige Websites automatisch; durch Einsatz granularer Content-Filter-Tools können unangemessene Inhalte blockiert und die Produktivität gesteigert werden.

Application Control
Mit diesem Feature können Sie den Zugriff auf Anwendungen in Abhängigkeit von Abteilung, Position im Unternehmen und Tageszeit gewähren, verweigern oder einschränken. Anschließend verfolgen Sie in Echtzeit, was von wem aufgerufen wurde.

Gateway Antivirus (GAV)
Laufend aktualisierte Signaturen identifizieren und blockieren bekannte Spyware, Viren, Trojaner und mehr – einschließlich neuer Varianten bekannter Viren.

spamBlocker
Spam-Erkennung in Echtzeit ... Unser spamBlocker ist so schnell und effektiv, dass er täglich bis zu vier Milliarden Nachrichten überprüfen kann.

ERWEITERTE SICHERHEITSDIENSTE

APT Blocker – erweiterter Schutz vor Schadsoftware
Durch Einsatz einer prämierten Sandbox der nächsten Generation werden selbst raffinierteste Attacken erkannt und gestoppt, einschließlich Ransomware und Zero-Day-Angriffen.

Data Loss Prevention (DLP)
Verhindert versehentlichen oder böswillig herbeigeführten Datenverlust, indem Texte und gängige Dateiformate auf vertrauliche Inhalte analysiert werden. Dabei werden Versuche, sensible Informationen aus dem Netzwerk herauszuschleusen, sofort erkannt.

Access Portal
Bietet einen zentralen Zugangspunkt für in der Cloud gehostete Anwendungen und einen sicheren, clientlosen Zugriff auf interne Ressourcen über RDP und SSH.

Dimension Command
IP-Experten erhalten Zugriff auf eine Vielzahl von Netzwerksteuerelementen. Dazu gehören z. B. Konfigurationsänderungen per einfachem Klick mit Zugriff auf einzelne Appliances über eine Weboberfläche und VPN-Managementtools.

Threat Detection and Response
Setzen Sie Sicherheitsereignisse im Netzwerk und am Endpunkt in Bedrohungsanalysen in Beziehung. Dadurch können potenzielle Angriffe noch früher erkannt, priorisiert und bewertet werden. Sofortmaßnahmen zur Abwehr erfolgen ohne Verzögerung.

DNSWatch™
Verringert Infektionen durch Schadsoftware, indem böartige DNS-Anforderungen blockiert und Benutzer zu Informationen umgeleitet werden, die ihnen Best Practices in puncto Sicherheit vermitteln und betonen, wie wichtig deren Einhaltung ist.

IntelligentAV™
IntelligentAV ist eine signaturlose Anti-Malware-Lösung, die künstliche Intelligenz zur automatischen Erkennung von Schadsoftware einsetzt. Durch Nutzung umfassender statistischer Analysen kann aktuelle und Zero-Day-Schadsoftware in Sekundenschnelle klassifiziert werden.

Ein einheitlicher Ansatz bei der Netzwerksicherheit

Kleine und mittelständische Unternehmen sowie dezentral aufgestellte Organisationen fallen trotz vorhandener Sicherheitsstrukturen immer wieder ausgefeilten Angriffen zum Opfer – mit erheblichen Beeinträchtigungen für den operativen Betrieb. Einzelmaßnahmen oder eine begrenzte Anzahl an Sicherheitstechnologien reichen meist nicht aus. Je mehr Angriffsphasen Sie abdecken können, umso effizienter wird Ihre Abwehr – selbst dann, wenn neue Bedrohungen eine bestehende Verteidigungslinie überwinden.

Mit der Total Security Suite profitieren Unternehmen jeder Größe von einer Lösung auf Enterprise-Niveau, die dank umfassender Funktionalität zur Prävention, Erkennung, Korrelation und Abwehr maximale Netzwerksicherheit garantiert – vom Perimeter bis zum Endgerät. Das cloudbasierte Modul ThreatSync zur Korrelation und Bewertung von Bedrohungen erfasst Netzwerkeignissdaten von verschiedenen Sicherheitsdiensten der Firebox – einschließlich APT Blocker, Reputation Enabled Defense, Gateway AntiVirus und WebBlocker. Durch den Abgleich mit den vom WatchGuard Host Sensor erkannten Bedrohungsaktivitäten sowie intelligenten Analysen auf Enterprise-Niveau ergibt sich eine einzigartige Übersicht zur gesamten Netzwerkumgebung inklusive umfassender Bewertungen zum Schweregrad einzelner Bedrohungen.

Und das Beste ist: Alle diese Sicherheitsvorteile sind über unser großes MSSP-Partnernetzwerk im Rahmen eines Komplettpakets erhältlich, das sowohl die Lizenz als auch die Appliance umfasst.



Die Macht der Visualisierung

WatchGuard Cloud Visibility und WatchGuard Dimension (lokal) sind leistungsstarke Lösungen zur Realisierung von Netzwerksicherheit durch Visualisierung. Sie sind standardmäßig Teil der Netzwerksicherheitsplattform von WatchGuard. Mit diesem Angebot aus Werkzeugen für Big Data-Visualisierung und -Reporting lassen sich wichtige Bedrohungen für die Netzwerksicherheit sowie Probleme und Trends zeitnah identifizieren und analysieren. Auf diese Weise können Sie schneller entsprechende Sicherheitsrichtlinien für das gesamte Netzwerk festlegen. Jede Lösung umfasst mehr als 100 Dashboards und Berichte, mit denen Sie schnell allgemeine Trends und Anomalien sehen und dann detaillierte Informationen anzeigen können.

