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, bösartigen 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

Ob in der Führungsetage oder in der Zweigniederlassung: Wichtige Entscheidungen hinsichtlich der IT-Sicherheit müssen meistens schnell getroffen werden – bevor irgendein Schaden entsteht. In diesem Zusammenhang sollte man nicht nur wissen, was im Netzwerk vor sich geht. Es gilt zudem, den Überblick über alle Endgeräte innerhalb und außerhalb der Firewall zu behalten. Der Begriff „Visualisierung“ geht hier weit über die reine Informationsdarstellung hinaus. Maximale Kontrolle ist erst möglich, wenn Daten in verständliche Übersichten umgewandelt werden, mit denen Sie wirklich etwas anfangen können. Durch den WatchGuard Host Sensor, der Ihnen im Rahmen von Threat Detection and Response zur Verfügung steht, werden sicherheitsrelevante Vorkommnisse am Endgerät kontinuierlich überwacht – für die lückenlose Erkennung und Abwehr aller Bedrohungen. Durch das preisgekrönte Visualisierungswerkzeug WatchGuard Dimension werden sämtliche Daten aller Geräte im Netzwerk zusammengetragen und optisch ansprechend aufbereitet. Dank Dimension können Sie Verhaltenstrends ermitteln, potenzielle Netzwerkbedrohungen lokalisieren, eine unangemessene Nutzung unterbinden und haben somit Ihr Netzwerk jederzeit vollständig unter Kontrolle.

Sicherheit auf Enterprise-Niveau

Simpel

Hervorragende Leistung

Bedrohungserkennung

Zukunftssicher

WatchGuard Sicherheitsdienste

WatchGuard hat das umfassendste Paket an Network Security-Diensten im Programm. Zu den klassischen Komponenten IPS, GAV, Application Control, Spamblocking und Webfilterung kommen erweiterte Dienste für den Schutz vor Advanced Malware, Ransomware und dem Verlust sensibler Daten. Abgerundet wird das Angebot von WatchGuard durch ein Komplettpaket von Diensten für die Netzwerkvisualisierung und -verwaltung.

GRUNDLEGENDE SICHERHEITSDIENSTE

INTRUSION PREVENTION SERVICE (IPS)

Mithilfe laufend aktualisierter Signaturen für die Überwachung des Datenverkehrs in allen gängigen Protokollen liefert IPS echtzeitbasierten Schutz vor Netzwerkbedrohungen, darunter Spyware, SQL-Injections, standortübergreifende Scripting-Angriffe und Pufferüberläufe.

REPUTATION ENABLED DEFENSE SERVICE (RED)

Ein leistungsstarker, cloud-basierter Reputations-Dienst, der Internetnutzer vor bösartigen Websites und Botnetzen schützt und dabei den Overhead bei der Webverarbeitung erheblich verbessert.

NETWORK DISCOVERY

Ein abonnementbasierter Dienst für Firebox-Appliances, der eine visuelle Topologie sämtlicher Knoten in Ihrem Netzwerk generiert. So können Sie umgehend riskante Bereiche erkennen.

GATEWAY ANTIVIRUS (GAV)

Unsere Signaturen werden permanent aktualisiert und helfen Ihnen, bekannte Spyware, Viren, Trojaner, Würmer, Rogueware und Blended Threats zu ermitteln und zu sperren – einschließlich neuer Varianten bekannter Viren. Gleichzeitig verfolgt die heuristische Analyse verdächtiger Datenpakete und Aktionen, um zu verhindern, dass unbekannte Viren eindringen.

WEBBLOCKER-URL-FILTERUNG

WebBlocker blockiert automatisch bekannte bösartige Websites. Darüber hinaus können Sie mithilfe der differenzierten Inhalts- und URL-Filterungstools von WebBlocker unangemessene Inhalte sperren, die Netzwerkbandbreite beibehalten und die Produktivität Ihrer Mitarbeiter steigern.

APPLICATION CONTROL

Mit diesem praktischen Feature können Sie für Benutzer je nach Abteilung, Position im Unternehmen und Tageszeit den Zugriff auf Anwendungen gewähren, verweigern oder begrenzen. Anschließend verfolgen Sie in Echtzeit, was in Ihrem Netzwerk von wem aufgerufen wurde.

SPAMBLOCKER

Spam wird in Echtzeit erkannt, bevor er massenhaft um sich greifen kann. Dabei ist spamBlocker ultraschnell – und äußerst effektiv: Tagtäglich werden bis zu vier Milliarden Nachrichten überprüft.

ERWEITERTE SICHERHEITSDIENSTE

APT BLOCKER – ERWEITERTER SCHUTZ VOR SCHADSOFTWARE

Dank Einsatz einer prämierten Sandbox der nächsten Generation erkennt und stoppt APT Blocker selbst raffinierteste Attacken, einschließlich Ransomware, Zero-Day-Angriffe und andere hochentwickelte Malware.

DATA LOSS PREVENTION (DLP)

Dieser Dienst verhindert versehentlichen oder böswillig herbeigeführten Datenverlust, indem Texte und gängige Dateiarten in Bezug auf vertrauliche Inhalte analysiert werden. Dabei werden Versuche, sensible Informationen aus dem Netzwerk herauszuschleusen, sofort erkannt.

DIMENSION COMMAND

Dimension wandelt Daten aus sämtlichen Appliances in Ihrem Netzwerk in verwertbare Netzwerk- und Bedrohungsdaten um. Mit Dimension Command können Sie dann geeignete Maßnahmen ergreifen, um diese Bedrohungen umgehend zu entschärfen – über eine zentrale Konsole.

THREAT DETECTION AND RESPONSE

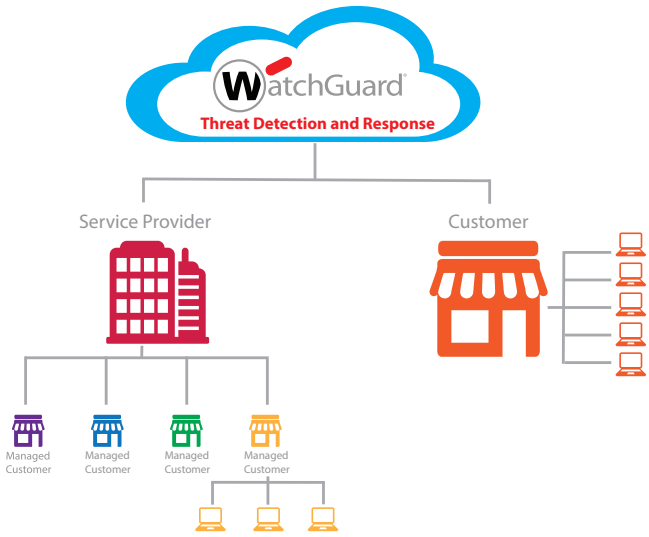
Setzen Sie Security-Events im Netzwerk und am Endpunkt mit detaillierten Analysen zur Bedrohungslage auf Enterprise-Niveau in Verbindung. Dadurch lassen sich potenzielle Angriffe noch früher erkennen und priorisieren. Sofortmaßnahmen zur Abwehr können rechtzeitig eingeleitet werden. Sorgen Sie für mehr Transparenz, indem Sie Ihr bisheriges Sicherheitsmodell um zusätzliche Funktionen zur Korrelation erweitern – zur noch besseren Erkennung und Abwehr von Gefahren.

Ein einheitlicher Ansatz bei der Sicherheit

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 und die geschäftliche Kontinuität. Einzelmaßnahmen oder ein begrenztes Subset 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.

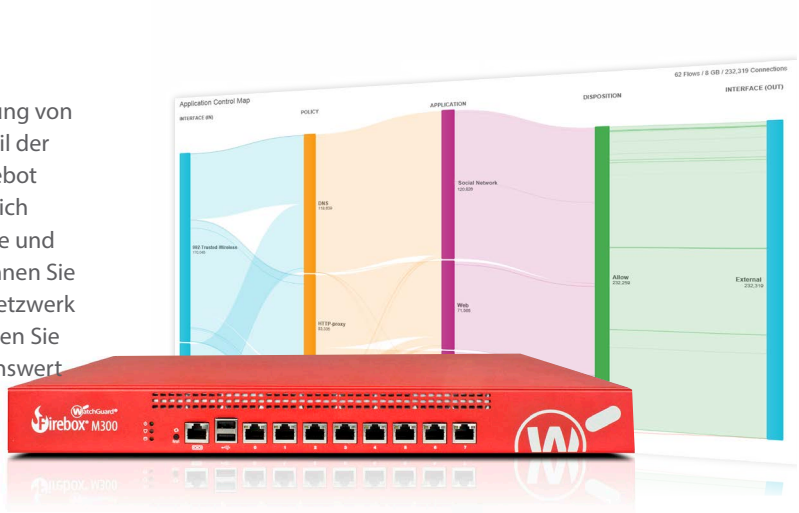
Mit der Total Security Suite profitieren Unternehmen jeder Größe von einer Lösung auf Enterprise-Niveau, die dank umfassender Funktionalität zur Prävention, Erkennung, Korrelation und Abwehr maximale Netzwerksicherheit garantiert – vom Perimeter bis zum Endgerät. Das Cloud-basierte Modul ThreatSync zur Korrelation und Bewertung von Bedrohungen erfasst alle Ereignisdaten der verschiedenen Sicherheitsdienste der Firebox – einschließlich APT Blocker, Reputation Enabled Defense, Gateway AntiVirus und WebBlocker. Durch den Abgleich mit den vom WatchGuard Host Sensor erkannten Bedrohungsaktivitäten sowie detaillierten Analysen zur aktuellen Gefahrenlage 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 Dimension ist eine cloudfähige Lösung zur Realisierung von Netzwerksicherheit durch Visualisierung. Sie ist standardmäßig Teil der Plattform für Network Security von WatchGuard. Mit diesem Angebot aus Big Data-Visualisierungs- und Reporting-Werkzeugen 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. Durch die Aktivierung von Dimension Command erhalten Sie Zugriff auf diverse Netzwerksteuerelemente. Besonders erwähnenswert sind hierbei Konfigurationsänderungen pereinfachem Klick, die Wiederherstellung vorheriger Konfigurationen, direkter Zugriff auf einzelne Appliances über eine Weboberfläche und VPN-Managementtools. Wissen ist Macht. Und Durchblick schafft Wissen.



> 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

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.

Product	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)	✓	
Dimension Command	✓	
Threat Detection & Response	✓	
Support	Gold (24x7)	Standard (24x7)

*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 mit GepaNet über einen Vertriebspartnern und Service Providern, der branchenweit seinesgleichen sucht. Für den Einstieg empfehlen wir einen Besuch unserer Webseite. Dort finden Sie die passenden Dienstleistungen für Ihr Unternehmen. Selbstverständlich können Sie uns auch direkt ansprechen. Wir beantworten gerne alle Fragen und vermitteln Ihnen den Kontakt zu dem Mitarbeiter, der Ihren Anforderungen optimal gerecht wird.

- Durchsuchen Sie unser Security Netzwerk: **http://www.gepanet.com/netz-sicherheit.htm**
- Sprechen Sie mit einem WatchGuard-Sicherheitsexperten: **http://www.gepanet.com/kontakt.htm**
- Weitere Informationen zum Kauf: **http://www.gepanet.com/watchguard_preisliste.htm**

Informationen zu WatchGuard

Weltweit wurden nahezu eine Million integrierter multifunktionaler Threat Management Appliances von WatchGuard installiert. Die roten Gehäuse stellen so etwas wie ein Markenzeichen unserer Produkte dar. Sie sind aufgrund ihrer Architektur die intelligentesten, schnellsten und effektivsten Sicherheitsgaranten auf dem Markt – selbst wenn alle Scanmodule mit maximaler Leistung laufen. Die Zentrale von WatchGuard befindet sich in Seattle, Washington. Das Unternehmen betreibt Niederlassungen in ganz Nordamerika, Europa, dem asiatisch-pazifischen Raum und Lateinamerika. Weitere Informationen finden Sie auf unserer Website unter **http://www.gepanet.com/watchguard.htm**. Im InfoSec-Blog **Secplicity** wird einfach und nachvollziehbar beschrieben, wie Sie den neuesten Bedrohungen am besten begegnen. Hier ist der Link: **www.watchguard.com/secplicity**.