

- **Robuste, proaktive Netzwerksicherheit**
- **Schutz vor neuen und unbekanntem Bedrohungen**
- **Keine Ausfallzeiten durch Sicherheitslücken**
- **Weitaus bessere Sicherheit als rein signaturbasierte Lösung**

## Das leistungsstärkste Element Ihrer Netzwerkverteidigung

Mit den Funktionen der ILS-Architektur (Intelligent Layered Security) seiner UTM-Appliances (Unified Threat Management) für die Firebox X bietet WatchGuard® echten Sofortschutz für Ihr Netzwerk vor neuen und unbekanntem Angriffen – und das ganz ohne Signaturen.

### Das Prinzip der Zero-Day-Protection

Das Zauberwort in der Branche heißt „Zero-Day“. Doch obwohl alle von Zero-Day-Protection reden, gibt es teilweise erhebliche Unterschiede zwischen den einzelnen Lösungen für den Angriffsschutz.

- Bei Zero-Day-Bedrohungen handelt es sich um neue und unbekanntem Angriffen, für die es noch keine Patches oder Signaturen gibt.
- Zero-Day-Protection schützt daher vor Angriffen, bevor Sicherheitslücken überhaupt festgestellt und entsprechende Hackerangriffe entwickelt und lanciert werden.

### Echter Zero-Day-Angriffsschutz – ein fester Bestandteil der Firebox® X Architektur

Die ILS-Architektur der Firebox X kombiniert wichtige Sicherheitsfunktionen für den Schutz gegen bestimmte Angriffskategorien und verschiedene Varianten, noch bevor diese bekannt werden. Dazu gehören u. a.:

- **Erkennung von Protokollanomalien:** – Bössartiger Datenverkehr, der nicht den bestehenden Protokollstandards entspricht, wird blockiert.
- **Pattern Matching:** Nach vollständiger Inspektion des gesamten Pakets werden risikoreiche Dateien wie .exe und Skripting-Dateien, Viren, Spyware und Trojaner identifiziert und aus dem System entfernt.
- **Verhaltensanalyse:** – Hosts, die ein verdächtiges Verhalten zeigen, wie DoS, DDoS und Port- und Adress-Scans, werden identifiziert und der Verkehr von diesen Hosts wird gestoppt.

### Die Vorteile von Signaturen für Sicherheitslösungen

Manche Anbieter versprechen zwar Lösungen mit Zero-Day-Angriffsschutz, in Wahrheit aber arbeiten diese Lösungen lediglich mit einer einfachen signaturbasierten Filterung.

Sie versehen neue Angriffen mit einer Art elektronischem Fingerabdruck bzw. einer „Signatur“, um diese später wiedererkennen zu können. Das hat mit Zero-Day-Angriffsschutz nichts zu tun. Signaturen gehören zu den passiven Lösungen, d. h. ohne entsprechende regelmäßige Updates können sie nicht vollständig gegen neue und unbekanntem Angriffen schützen.

Die signaturbasierte Filterung bietet grundlegenden Schutz gegen Spyware, Viren, Würmer, Trojaner und Blended Threats durch die Identifizierung bekannter, bössartiger Codes in wichtigen Geschäftsdaten und Dateien. Diese Methode stellt allerdings nur einen Teil einer umfassenden UTM-Lösung dar.

*Von den zwischen 2003 und 2006 aufgetretenen gefährlichsten Viren sowie deren Varianten wurden 22 von 30 standardmäßig von einer Firebox® blockiert. So waren unsere Kunden bis zur Entwicklung entsprechender Signaturen jederzeit geschützt.\**

### Zeiten mit Sicherheitslücken

Signaturbasierte Lösungen blockieren nur die Angriffen, die bereits identifiziert wurden. Neue Bedrohungen bleiben daher so lange für Ihr Netzwerk gefährlich, bis eine neue Signatur bzw. ein neues Patch entwickelt wurde und angewendet wird.

Angesichts der Geschwindigkeit und Zerstörungskraft solcher Angriffen können selbst wenige Minuten ohne Schutz schon verheerende Folgen haben. Meist dauert es Stunden, Tage oder sogar Wochen, bis entsprechende Schutzmaßnahmen entwickelt sind. Und genau diese Zeiten mit Sicherheitslücken, in denen Ihr Netzwerk verwundbar ist, ist der Albtraum aller IT-Systemadministratoren.

### Robuster Allzeitschutz

Das Herzstück unserer Firebox X Sicherheitslösungen ist Zero-Day-Angriffsschutz, damit Sie auch vor dem Bekanntwerden neuer Angriffen jederzeit geschützt sind. Entscheiden auch Sie sich für maximale Sicherheit. Informationen erhalten Sie unter [www.watchguard.com](http://www.watchguard.com)

\*Basierend auf den am häufigsten verwendeten Verbreitungsmethoden (SMTP)

## WatchGuard bietet echten Zero-Day-Angriffsschutz



Zero-Day-Protection bedeutet, dass Sie sind während der Zeitspanne mit Sicherheitslücke gegen neue und unbekanntem Bedrohungen geschützt sind.



Stronger Security, Simply Done™

- **Voll integrierter vielseitiger Schutz**
- **Die umfassendste Sicherheitslösung ihrer Klasse**
- **Mit integriertem Zero-Day-Angriffsschutz**
- **Leistungsstarke Sicherheitsdienste für noch größeren Schutz in gefährdeten Bereichen**
- **Funktionsumfang inkl. Unified Threat Management, Überwachung und Protokollierung**

## Leistungsstarke Sicherheitsfunktionen mit echtem Zero-Day-Angriffsschutz

Die UTM-Lösungen für die Firebox® X von WatchGuard bieten die umfassendste Sicherheit ihrer Klasse – für voll integrierten, vielschichtigen Schutz gegen Netzwerkbedrohungen, wie:

- ✓ **Spyware**
- ✓ **Viren**
- ✓ **SQL-Injektionen**
- ✓ **Trojaner**
- ✓ **Spam**
- ✓ **Pufferüberläufe**
- ✓ **Würmer**
- ✓ **Blended Threats**
- ✓ **DoS/DDoS-Attacken**
- ✓ **Bots**
- ✓ **Internetattacken**
- ✓ **Richtlinienverletzungen**

### Was ist Unified Threat Management?

Unified Threat Management (UTM) ist ein neuer Trend auf dem Markt für Netzwerksicherheit. UTM-Appliances haben sich von traditionellen Firewall und VPN Appliances zu Lösungen mit vielfältigen Funktionen entwickelt, zu denen URL-Filterung, Spam-Blocking, Spyware-Schutz, Intrusion Prevention und Gateway-Antivirus zählen sowie integrierte Verwaltungs-, Überwachungs- und Protokollierungsfunktionen. Alle diese Aufgaben wurden vorher von mehreren Systemen übernommen.

### Integrierter Zero-Day-Angriffsschutz als wichtige Grundlage

In jedem Fall benötigen Sie leistungsstarke Sicherheitsfunktionen wie die Intelligent Layered Security der Firebox X, die echten Zero-Day-Angriffsschutz gegen neue und unbekannte Bedrohungen bietet, und zwar noch bevor Schwachstellen entdeckt und entsprechende Attacken entwickelt und lanciert werden. Viele Anbieter liefern lediglich einen passiven, signatur-basierten Schutz, bei dem der Kunde bis zum Bekanntwerden der Bedrohung und der Entwicklung und Implementierung der neuen Signatur ungeschützt ist.

### Verzahnte, leistungsstarke Verteidigungsschichten

Im Gegensatz zu vielen anderen UTM-Appliances auf dem Markt ermöglicht die Intelligent Layered Security der Firebox X das Zusammenwirken von Sicherheitsschichten und damit eine höhere Sicherheit. Dank koordinierter Softwarefunktionen wird jede Komponente effizient in die gesamte Sicherheitsstruktur integriert. Wenn also z. B. der Intrusion Prevention Service einen Angriff identifiziert, werden die notwendigen Informationen für Gegenmaßnahmen sofort an die Firewall weitergeleitet.

Durch die Kommunikation zwischen den verschiedenen Ebenen werden die Aufgaben der Sicherheitsfunktionen optimal aufeinander abgestimmt. Dadurch erhalten Sie genau den Schutz, den Sie brauchen, und das ohne jegliche Leistungseinbußen.

### Leistungsstarke Sicherheitsdienste für effektiven Schutz

Dank der Flexibilität unserer Lösungen können Sie jederzeit beliebige der neuesten WatchGuard Sicherheitsdienste hinzufügen und so einen noch besseren Schutz für wichtige Bereiche gewährleisten. Dabei gestaltet sich die Verwaltung

über eine einzelne integrierte Managementkonsole kinderleicht. Zu diesen Sicherheitsdiensten gehören:

- **spamBlocker:** Der beste Dienst der Branche für die Echtzeit-Unterscheidung zwischen legitimer Kommunikation und Spam-Attacken, der mit der Eliminierung von 97 % aller unerwünschten E-Mails eine unglaublich hohe Erfolgsquote bietet.
- **Gateway AV/IPS:** Robuster, signaturbasierter Schutz am Gateway gegen bekannte Viren, Spyware, Trojaner und Internetattacken.
- **WebBlocker:** Erhöht den Schutz und verringert das Sicherheitsrisiko durch Blockierung des Zugriffs auf bösartige Internetinhalte und Verwaltung des Internetsurfverhaltens Ihrer Benutzer.

### Das Prinzip der integrierten Verwaltung

Ganz gleich, ob Sie IT-Profi oder Anfänger sind, die integrierte Verwaltung, interaktive Echtzeit-Überwachung und Protokollfunktionen unserer UTM-Lösungen bieten höchste Benutzerfreundlichkeit beim Konfigurieren und Verwalten Ihrer Sicherheit.

- Verwaltung mehrerer Appliances von einem zentralen Standort aus
- Einfache Erstellung und globale Implementierung kohärenter Sicherheitsrichtlinien
- Zuverlässige interaktive Überwachung und Protokollierung in Echtzeit
- Installation/Verwaltung aller modernen Sicherheitsfunktionen und -dienste über eine einzige intuitive Benutzeroberfläche, einschließlich Sicherheitsdienste

### Wichtige Aspekte: Skalierbarkeit und Kostenvorteile

Der Betrieb von mehreren Security Appliances und der dazugehörigen Softwareprogrammen verursacht Zusatzkosten für Ihr EDV-Gesamtbudget. Bei anderen UTM-Lösungen fallen eventuelle zusätzliche Ausgaben für Benutzerlizenzen sowie die zentrale Protokollierung und Berichterstellung an. Nicht so bei den Lösungen von WatchGuard. Und dank einer einzigen Benutzeroberfläche gestaltet sich die Verwaltung auch noch kinderleicht. Jede der integrierten und zentral verwalteten Sicherheitsfunktionen bietet netzwerkweiten Schutz für alle hinter der Firebox X konfigurierten Benutzer.

Die einzige Grenze für Sie ist die Kapazität Ihres Datenverkehrs. Aber sobald Sie diese erreicht haben, müssen Sie lediglich per Lizenzschlüssel das anschließende Modell aktivieren und schon können Sie mehr Daten mit einem höheren Durchsatz übertragen. Müheloser und kostengünstiger können Sie Ihre Investitionen in die Netzwerksicherheit nicht schützen.

ADRESSE: WatchGuard Technologies Schellerdamm 16 21079 Hamburg Germany · WEB: [www.watchguard.com](http://www.watchguard.com)

E-MAIL: [germany@watchguard.com](mailto:germany@watchguard.com) · GERMANY SALES: +49 40 689876 10 · FAX: +49 40 689876 76

Für die Richtigkeit/Aktualität der hierin enthaltenen Informationen (die jederzeit geändert werden können) wird weder eine ausdrückliche noch eine konkludente Garantie übernommen. Zukünftige Produkte oder Funktionen werden zum gegebenen Zeitpunkt zur Verfügung gestellt.  
© 2006 WatchGuard Technologies, Inc. Alle Rechte vorbehalten. WatchGuard, das WatchGuard Logo, Firebox, Firewall, LiveSecurity und Stronger Security, Simply Done sind in den USA und/oder anderen Ländern entweder Markenzeichen oder eingetragene Markenzeichen von WatchGuard Technologies, Inc. Alle anderen Markenzeichen oder Markennamen sind Eigentum ihrer jeweiligen Besitzer. Teilnr. WGCE66355\_0506