



## Umfassende Unified-Threat-Management-Lösung

Firebox® X Core™ UTM Lösungen (Unified Threat Management) bieten die umfassendste Sicherheit in ihrer Klasse und schützen Ihr Netzwerk vor Spyware, Spam, Viren, Trojanern, Webbedrohungen und anderer Malware. Das robuste, mehrschichtige Verteidigungssystem macht nicht nur den Zeit- und Kostenmehraufwand für Mehrfachlösungen hinfällig, sondern bietet auch wesentlich besseren Schutz vor „Blended Threats“ (kombinierten Angriffen). Ein weiteres Plus: die modernen Netzwerkfunktionen werden mit einer intuitiven Benutzeroberfläche verwaltet, die eine schnelle und zuverlässige Konnektivität für die Übertragung von Geschäftsdaten bietet – und das mit einer einzigen Appliance.

### Zuverlässige mehrschichtige Sicherheit

Das Herzstück der Firebox X Core ist eine intelligente mehrschichtige Architektur, die umfassenden Schutz bietet. Durch die Kommunikation zwischen den verschiedenen Ebenen werden die Aufgaben der Sicherheitsfunktionen optimal aufeinander abgestimmt. Dadurch erhalten Sie den Schutz, den Sie brauchen und das ohne jegliche Leistungseinbußen.

### Echter Zero Day Angriffsschutz

Die Sicherheitstechnologie der Firebox X Core schützt das Netzwerk Ihrer Kunden proaktiv gegen Software-Sicherheitslücken, die neue Formen von Angriffen ermöglichen. Durch die auf modernsten Proxy-Technologien basierende Deep Application Inspection, die neue Bedrohungen identifiziert und blockiert, bietet die Firebox X Core automatischen Schutz vor Spyware, Trojanern, Würmern, DoS, DDoS, DNS-Poisoning, Pufferüberläufen und anderen Angriffen.

### Intuitive, zentrale Verwaltung

Der WatchGuard® System Manager (WSM) ermöglicht eine intuitive, zentrale und vor allem benutzerfreundliche Verwaltung aller Firebox X Lösungen, einschließlich Konfigurationsänderungen, der Überwachung von Daten in Echtzeit sowie der Erstellung historischer Berichte – und zwar unabhängig vom Umfang des Gerätenetzwerks und mit signifikanten Zeit- und Kosteneinsparungen.

### Integrierte Sicherheitsfunktionen für umfassenderen Schutz

Stärken Sie Ihren Netzwerkschutz für kritische Bereiche mit den Sicherheitsabonnements für Ihre Firebox X. Die zentrale Verwaltung per WSM sorgt dazu für einen stets aktuellen Schutz.

- **Gateway AV/IPS mit Anti-Spyware**  
Stoppt bekannte Spyware, Trojaner, Viren und Webattacks mit robustem signaturbasierten Schutz am Gateway.
- **spamBlocker mit Viruserkennung:**  
Sichern Sie sich die beste Anti-Spam- und E-Mail-Sicherheitslösung der Branche für die Blockierung von bis zu 100 % aller unerwünschten E-Mails mit Echtzeitschutz gegen Virusangriffe.
- **WebBlocker**  
Steigern Sie die Produktivität und verringern Sie das Sicherheitsrisiko durch Blockieren des Zugriffs auf böartige oder unerwünschte Webinhalte per HTTP und HTTPS.

### Sichere Remote-Konnektivität

Der Schutz von Telearbeitern gestaltet sich mit der Firebox X Core viel einfacher, und zwar unabhängig vom Standort. Mit der größten Vielfalt an Funktionen für den Remote-Zugriff in ihrer Klasse ermöglicht sie die sichere Anbindung an das Firmennetzwerk via:

- IPSec
- SSL VPN
- PPTP

Vom Single-Sign-On bis hin zur gleichzeitigen Authentifizierung mehrerer Benutzer.

### Beratung und Support durch Experten

Mit dem LiveSecurity® Service von WatchGuard steht Ihnen ein globales Team aus Sicherheitsexperten zur Seite, das Ihnen jegliche Unterstützung für eine bessere Verwaltung Ihrer Netzwerksicherheit bietet. Zum Abonnement gehören eine Hardware-Garantie mit Hardware-Vorabaustausch, Software-Updates, umgehender technischer Support, topaktuelle Warnmeldungen vor Sicherheitslücken sowie innovative Fortbildungsressourcen.

### Schutz Ihrer Investitionen

In Anbetracht der Kosten, die bei mehreren Sicherheitslösungen für Implementierung, Verwaltung und spätere Upgrades anfallen, wird klar, warum unsere Firebox X Core UTM-Lösungen einen eindeutigen Mehrwert bieten. Dank des voll integrierten, mehrschichtigen Schutzes einer einzelnen Appliance sparen Sie in jeder Hinsicht Geld, vom Erstkauf bis hin zu den Supportverträgen.

Indem Sie bei wachsenden Bedürfnissen einfach neue Funktionen hinzufügen, sind Sie mit Ihrem Unternehmen sicherheitstechnisch immer auf dem neuesten Stand. Wenn Sie mehr Kapazität benötigen, führen Sie ein Upgrade auf ein höherwertiges Modell durch. Dazu müssen Sie nur einen einfachen Lizenzschlüssel einspielen. Wenn Sie anspruchsvolle Netzwerke betreiben, kommt für Sie vielleicht ein Upgrade von der Fireware® auf die moderne Fireware® Pro Appliance-Software in Frage, die zusätzliche Netzwerkfunktionen wie VLAN, Hochverfügbarkeit und QoS bietet. Und all das, ohne dass Sie neue Hardware kaufen müssen. Keine anderen Sicherheitsprodukte auf dem Markt schützen Ihr Netzwerk auf so vielfältige Weise.

### Unser Engagement für die Umwelt

WatchGuard stellt energiesparende Produkte her, die in wiederverwendbaren Verpackungsmaterialien vertrieben werden. Wir erkennen die internationalen Direktiven zu gefährlichen Substanzen uneingeschränkt an und haben die Nachhaltigkeit zu einem festen Bestandteil unserer weltweit geltenden strategischen Unternehmensgrundsätze gemacht.

- **Umfassender Schutz:**  
macht Ihr Netzwerk immun gegen Bedrohungen
- **Echter Zero Day Angriffsschutz:** stoppt neue Bedrohungen proaktiv
- **Neu! Integriertes SSL VPN**
- **Effizientes Netzwerksicherheitsmanagement:** bietet Zeitersparnis
- **Kontinuierlich aktualisierte Sicherheitsabonnements:** bieten dauerhaften Schutz
- **Integrierte, upgradefähige Funktionen:** bieten ein besseres Preis-Leistungsverhältnis
- **Globales Team aus Sicherheitsexperten:** bietet Unterstützung bei Bedarf



Umweltfreundliche  
Technologie

## Blockieren von Webattacken

Das Internet ist ein überaus wertvolles Werkzeug für viele Geschäftsabläufe, kann sich aber auch als ernsthafte Bedrohung für Ihr Netzwerk erweisen. Durch unbeaufsichtigtes Surfverhalten können absichtlich oder unabsichtlich Schwachstellen entstehen, die von Bots und Spyware ausgenutzt werden und Ihre wichtigen Geschäftsdaten gefährden bzw. zu einem enormen Zeit- und Kostenaufwand im Helpdesk-Bereich führen. Anfällige Netzwerke sind leichte Beute für DNS-Cache-Poisoning (Domain Name Service), Pufferüberläufe und DoS-Attacken (Denial of Service).

### Diese Tools benötigen Sie:

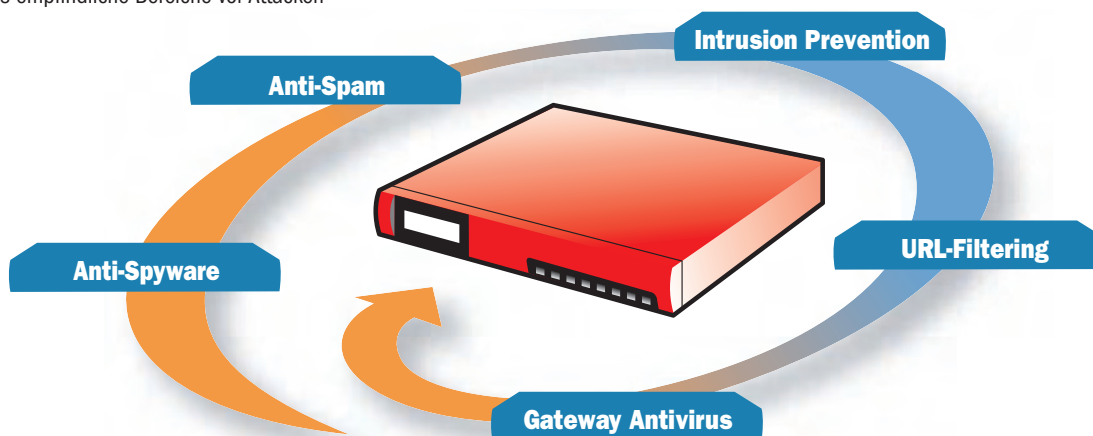
- Eine **Firebox X Core** für echten Zero Day Angriffsschutz
- Gültige Abonnements für **WebBlocker** zur Überwachung von nicht autorisiertem Surfen im Web sowie **Gateway AV/IPS** zur Echtzeit-Blockierung von verdächtigem Internetverkehr und heruntergeladenen Dateien

### Die verschiedenen Sicherheitsfunktionen sind:

- **Echter Zero Day Angriffsschutz:** schützt Ihr Netzwerk mit leistungsstarken, integrierten Anwendungs-Proxy-Technologien vor vielen neuen und unbekanntem Bedrohungen, die durch Sicherheitslücken bei verschiedenen Softwareanwendungen ermöglicht werden

- **Mehrschichtiges Spyware-System:** blockiert den Zugang zu bekannten Spyware-Sites, so genannten „Driveby“-Downloads, durch die Spyware beim Surfen im Internet ins Netzwerk eingeschleust wird, sowie Spyware, die versucht, mit ihrer Host-Site Kontakt aufzunehmen
- **Gateway AV/IPS mit Anti-Spyware:** prüft den Webverkehr auf Viren, Trojaner, Bots und andere Malware und bietet so umfassenden Schutz gegen bekannte Bedrohungen
- **Webserver-Cloaking:** verhindert, dass Hacker Systeminformationen für Angriffe ausnutzen
- **WebBlocker:** Ermöglicht Ihnen, das Surfverhalten Ihrer Angestellten einzugrenzen. Sie schützen damit nicht nur Ihr Netzwerk vor Angriffen, sondern steigern auch noch die Produktivität und verringern das Risiko von Haftungsansprüchen
- **URL-Filterung von HTTPS-Verkehr:** blockiert Schlupflöcher für unerlaubtes Websurfing
- **Intelligente mehrschichtige Sicherheitsarchitektur und DNS-Proxy:** schützen gegen Netzwerkbedrohungen, DoS-Attacken sowie DNS-Cache-Poisoning
- **Integrierte Protokollierung, Berichterstattung und Alarmer:** bieten einen genauen Einblick in die Netzwerkaktivitäten und ermöglichen sofortige Präventiv- oder Abhilfemaßnahmen

Die integrierten Sicherheitsabonnements der Firebox X Core schützen besonders empfindliche Bereiche vor Attacken



## Maßnahmen gegen E-Mail-Bedrohungen

Da Ihr Geschäft vom E-Mail-Verkehr abhängig ist, muss die Kommunikation reibungslos ablaufen, aber ohne dabei die Netzwerksicherheit zu gefährden. Allerdings ist und bleibt E-Mail das am häufigsten verwendete Kommunikationsinstrument für die Verbreitung bössartiger Codes im Netzwerk. Wenn man dann noch die zusätzliche Belastung durch Massen-Spam bedenkt, kann die E-Mail-Umgebung zu einem Ihrer größten Probleme werden.

### Diese Tools benötigen Sie:

- Eine **Firebox X Core** mit echtem Zero Day Angriffsschutz
- Ein **Gateway AV/IPS** Abonnement für das Scannen von E-Mail-Verkehr und die Blockierung bekannter Würmer, Trojaner und anderer Malware
- Ein aktives **spamBlocker**-Abonnement - die beste Lösung der Branche bei der Echtzeit-Differenzierung zwischen legitimer E-Mail-Kommunikation und Spam-Nachrichten. spamBlocker bietet eine leistungsstarke Verteidigungsschicht, die E-Mail-Viren mit fast 100%iger Genauigkeit erkennt und blockiert.

### Die verschiedenen Sicherheitsfunktionen sind:

- **Integrierter Zero Day Angriffsschutz:** für die proaktive Blockierung von Dateitypen, die häufig Malware enthalten, mithilfe leistungsstarker Proxy-Technologien
- **spamBlocker:** nutzt die Spam-Erkennung in Echtzeit, damit Sie jederzeitigen Rundum-Schutz genießen; blockiert unerwünschten E-Mail-Verkehr, und zwar unabhängig von Inhalt, Sprache oder Format
- **Spam- und Antivirus-Quarantäne** zum Schutz Ihres Netzwerks vor Spam und verdächtigen Nachrichten. So haben Administratoren und Endbenutzer genügend Zeit, den Inhalt mit entsprechenden Tools zu prüfen
- **SMTP-Server Cloaking:** verhindert, dass Hacker Systeminformationen für Angriffe ausnutzen
- **Integrierter Gateway AV:** bietet umfassenden Schutz vor Dateien und ihren Anhängen für eine effiziente Blockierung von Viren, Würmern und anderer Malware, bevor diese ins Netzwerk eindringen und Ihre Desktop-Sicherheitsanwendungen deaktivieren können
- **AV-Scanning abgehender E-Mail-Nachrichten:** schützt Ihr Unternehmen davor, selbst Viren, Würmer und Trojaner an Partner, Kunden und andere Empfänger außerhalb des Netzwerks zu verbreiten

**Technische Daten**

	<b>Firebox® X550e</b> WG50550 <b>X550e UTM Bundle</b> WG50553	<b>Firebox® X750e</b> WG50750 <b>X750e UTM Bundle</b> WG50753	<b>Firebox® X1250e</b> WG51250 <b>X1250e UTM Bundle</b> WG51253
<b>Firewall-Durchsatz†</b>	300+ Mbps	750 Mbps	1.5 Gbps
<b>VPN-Durchsatz†</b>	35 Mbps	50 Mbps	100 Mbps
<b>AV-Durchsatz†</b>	50 Mbps	70 Mbps	100 Mbps
<b>Gateway AV/IPS</b> mit Anti-Spyware	Optional	Optional	Optional
<b>URL-Filtering</b> für HTTP und HTTPS	Optional	Optional	Optional
<b>Spam-Blocking</b> mit Viruserkennung	Optional	Optional	Optional
<b>Schnittstellen 10/100</b>	4	8	0
<b>Schnittstellen 10/100/1000</b>	0	0	8
<b>Serielle Ports</b>	1	1	1
<b>VLAN-Unterstützung*</b>	25	25	25
<b>Enthaltene Sicherheitszonen</b>	4	8	8
<b>Gleichzeitige Sitzungen</b>	25.000	75.000	200.000
<b>Unterstützte Knoten</b> (LAN IPs)	Unbegrenzt	Unbegrenzt	Unbegrenzt
<b>VPN-Tunnel für Niederlassungen</b> (inkl./max.)	35/45	100/100	600/600
<b>Mobile VPN-Tunnel – IPSec</b> (inkl./max.)	5/75	50/100	400/400
<b>Mobile VPN-Tunnel – SSL</b> (inkl./max.)	5/75	50/100	400/400
<b>Obergrenze für die lokale Authentifizierungs-DB</b>	250	1.000	5.000
<b>Modell-Upgrades</b>	Ja	Ja	Nein
<b>Fireware® Pro Advanced Appliance-Software</b>	Optional	Optional	Optional

† Durchsatzraten variieren je nach Umgebung und Konfiguration

\*Verfügbar mit einem Upgrade auf die Fireware Pro Appliance-Software

**Funktionen**
**Sicherheitsfunktionen**

- Stateful Packet Firewall
- Deep Application Inspection Firewall
- Anwendungs-Proxies – HTTP, SMTP, FTP, DNS, TCP, POP3
- Spyware-Blocking
- DoS-, DDoS- und progressiver DDoS-Schutz
- Erkennung von Protokollanomalien
- Verhaltensanalyse
- Pattern-Matching
- Fragmented Packet Reassembly-Schutz
- Malformed Packet-Schutz
- Liste statisch und dynamisch blockierter Sites
- Zeitbasierte Regeln
- Instant Messaging und P2P Allow/Deny

**Virtual Private Networks**

- VPN
  - Verschlüsselung (DES, 3DES, AES 128-, 192-, 256-bit)
  - IPSec
    - SHA-1, MD5
    - IKE – Pre-Shared Key, Firebox Zertifikat
    - SSL Thin Client, Web Exchange
- PPTP-Server und -Passthrough
- Dead Peer Detection (RFC 3706)
- Hardware-basierte Verschlüsselung
- Drag-and-Drop-VPN-Tunnel

**Benutzerauthentifizierung**

- Transparente Active Directory Authentifizierung (Single-Sign-on)
- XAUTH
  - RADIUS®, LDAP, Windows® Active Directory
- VASCO
- RSA SecurID®
- Web-basiert
- Lokale Authentifizierung

**IP-Adresszuweisung**

- Statisch
- PPPoE-Client

- DHCP-Server, Client, Relay
- Dynamic DNS-Client

**Hochverfügbarkeit\*\***

- HA Aktiv/Passiv
- Konfigurationssynchronisierung
- Sitzungssynchronisierung
- VPN-Tunnel-Synchronisierung

**WAN-Failover**

- VPN-Failover
- WAN Modi
  - Spill-over\*\*
  - Round Robin
  - Failover
  - ECMP
  - Weighted Round Robin\*\*

**Traffic Shaping\*\***

- Quality of Service
  - 8 Prioritäts-Warteschlangen
  - DiffServe
  - Modified Strict Queuing

**Routing**

- Statisches Routing
- Dynamisches Routing\*\*
  - BGP4, OSPF, RIPv1, v2
- Policy-based Routing\*\*

**Networking\*\***

- Porttrennung
- VLAN
  - Bridging, Tagging, Routed-Modus
- Multi-WAN und Server Load-Balancing
- Unterstützung für VoIP- und Video-Conferencing

**Sicherheitsabonnements**

- spamBlocker
  - Quarantäne für Spam-, Bulk- und verdächtige Mail
  - Viruserkennung
- Gateway AntiVirus/IPS mit Anti-Spyware
- WebBlocker

**Betriebsmodi**

- Transparenter/Drop-in-Modus (Layer 2)
- Routed-Modus (Layer 3)

**Network Address Translation (NAT)**

- Statische NAT (Port-Forwarding)
- Dynamische NAT
- Eins-zu-Eins-NAT
- IPSec NAT Traversal
- Richtlinienbasierte NAT
- Virtuelle IP für das Server Load-Balancing\*\*

**Protokollierung/Berichterstattung**

- Protokollzusammenfassung für mehrere Appliances
- WebTrends®-kompatible Berichte (WELF)
- HTML- und PDF-Berichte
- SQL-Protokolldatenbank
- Verschlüsselter Protokollkanal
- Syslog
- SNMP v2 und v3

**Alarme/Benachrichtigungen**

- SNMP
- E-Mail
- Management System Alert

**Management-Software††**

- WatchGuard System Manager (WSM)

**Zertifizierungen**

- Common Criteria EAL4
- ICSA IPSec und ICSA Firewall
- West Coast Labs Checkmark-Zertifikat

**Support und Wartung**

- 1 Jahr Hardware-Garantie
- 90 -Tage- oder 1-Jahres-Erstabonnement für den LiveSecurity® Service

\*\*Verfügbar mit einem Upgrade auf die Fireware Pro Appliance-Software

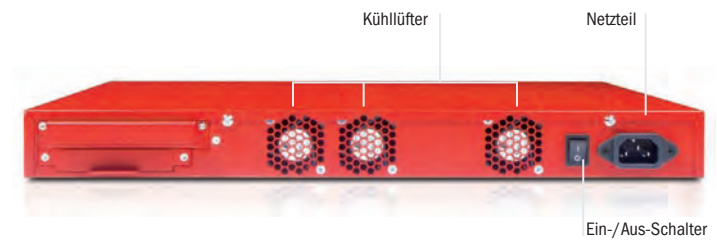
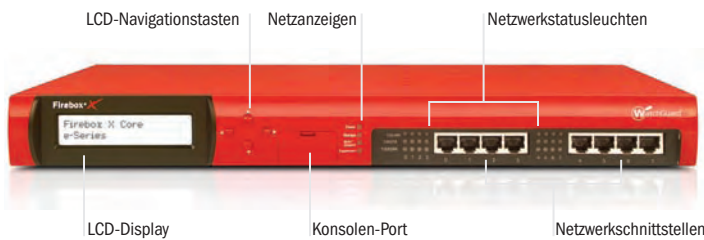
††Die Firebox X 550e umfasst eine Single-Node-WSM-Lizenz. Zur Erstellung von „Drag and Drop“-Tunneln oder zur zentralen Verwaltung mehrerer Firebox X Edge Appliances von einer Firebox X550e aus, sind optionale WSM-Upgrade-Lizenzen erforderlich

**Abmessungen/Leistungswerte**

<b>Abmessungen Appliance</b>	4,5 x 42,6 x 36,2 cm
<b>Abmessungen Verpackung</b>	18,4 x 54,6 x 48,3 cm
<b>Gewicht Appliance</b>	4,39 kg
<b>Gesamtgewicht</b>	6,21 kg
<b>WEEE-Gewicht</b>	4,81 kg
<b>Wechselspannung</b>	100-240 VAC Automumschaltung
<b>Stromverbrauch</b>	USA: 60 Watt Restliche Welt: 860 Kal/min oder 205 BTU/Std.
<b>Rack-fähig</b>	Ja

**Umgebung**

<b>Betriebstemperatur</b>	0 – 45° C
<b>Ruhetemperatur</b>	-40 – 70° C
<b>Betriebsfeuchte</b>	10 – 85 %
<b>Ruhefeuchte</b>	10 – 95 % nicht kondensierend bei 55° C
<b>Nicht periodische Schwingungen (Ruhezustand)</b>	7 – 28 Hz 0,001 bis 0,01 G2 pro Hz
<b>Akustisches Rauschen</b>	54 dB bei 20 – 25° C
<b>Mechanischer Schock (Betrieb)</b>	20 G mit 11 Ms Dauer 1/2 Sinuswelle
<b>WEEE/RoHS-konform</b>	Ja


**Sind Sie bereit für ein Upgrade auf Fireware® Pro?**

Bei wachsenden Netzwerkbedürfnissen können Sie Ihre Firebox X Core von Fireware auf Fireware Pro, die moderne Appliance-Software von WatchGuard für anspruchsvolle Netzwerke aufrüsten. Die neue Version 10 bietet jetzt noch leistungsstärkere Funktionen wie:

- **Traffic Shaping:** Damit geschäftskritische Anwendungen auch die jeweils erforderliche Bandbreite bekommen
- **Dynamisches Routing (BGP, OSPF):** Ermöglicht eine optimale Netzwerkflexibilität, Redundanz und Effizienz durch dynamische Aktualisierung der Routing-Tabellen
- **Hochverfügbarkeit (Aktiv/Passiv):** Bietet Hardwareredundanz für eine Standby-Appliance, plus WAN- und VPN-Failover
- **VLAN-Unterstützung:** Diese Technik, bei der anstatt physikalische logische Netzwerkfigurationen verwendet werden, bietet folgende Vorteile: weniger Hardware-Anforderungen, mehr Kontrolle über verschiedene Typen des Datenverkehrs, bessere Interoperabilität sowie eine einfachere Erstellung von Subnetzen.
- **Multi-WAN:** Ermöglicht die Lastverteilung des abgehenden Datenverkehrs über mehrere ISPs für eine bessere Netzwerkeffizienz
- **Policy Based Routing:** Trägt durch Zuweisung einer Schnittstelle für abgehenden Verkehr je Dienst zur Steigerung der Netzwerkbandbreite und Senkung der Kosten bei
- **Server Load-Balancing:** vereinfacht den Schutz öffentlich zugänglicher e-commerce „Server Farms“
- **SSL VPN:** Steigerung der Anzahl der verfügbaren SSL VPN-Tunnel auf das Maximum für das jeweilige Modell

**Core™ UTM-Bundle – Eine Lösung, eine Lizenz: ein toller Preis.**

Das neue Firebox X Core e-Series UTM-Bundle bietet jetzt umfassenden Schutz in einem praktischen und hochwertigen Paket. Im Einzelnen besteht es aus:

- Firebox X Core e-Series Security Appliance
- WebBlocker\*
- spamBlocker mit Viruserkennung\*
- Gateway AV/IPS mit Anti-Spyware\*
- LiveSecurity® Service\*

Ab der Erstinstallation bietet das Firebox X Core e-Series UTM Bundle ein effizientes und fortlaufendes Sicherheitsmanagement für Ihr Netzwerk. Sie bekommen damit nicht nur die beste UTM Lösung auf dem Markt, sondern realisieren auch noch zusätzliche Einsparungen gegenüber dem Kauf einzelner Komponenten!

\*1-Jahres-Abonnement

**KOSTENLOSE!**
**30-Tage-Demos**

Beim Kauf einer Firebox X Core erhalten Sie kostenlose 30-Tage-Demos für **Gateway AV/IPS**, **spamBlocker**, und **WebBlocker** Weitere Informationen erhalten Sie bei Ihrem Händler.

Weitere Informationen erhalten Sie unter [www.watchguard.com/appliances](http://www.watchguard.com/appliances).

ADRESSE: WatchGuard Technologies, IOM Business Center, Humboldtstr. 12, 85609 Aschheim-Dornach, Germany · WEB: [www.watchguard.de](http://www.watchguard.de)

E-MAIL: [GermanySales@watchguard.com](mailto:GermanySales@watchguard.com) · GERMANY SALES: +49 700 92229333

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. ©2008 WatchGuard Technologies, Inc. Alle Rechte vorbehalten. WatchGuard, das WatchGuard Logo, Firebox, Fireware, LiveSecurity, Peak und Core 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: WGCE66360\_011008

**GepaNet**  
<http://www.gepanet.com>


**GepaNet**

88142 Wasserburg  
Wiesenstraße 12

Tel +49 8382 9479825

Fax +49 8382 9479826

Mail: [info@gepanet.com](mailto:info@gepanet.com)

WEB: [www.gepanet.com](http://www.gepanet.com)