



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. Dieses 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

Der integrierte Zero Day Angriffsschutz der Firebox X Core schützt das Netzwerk proaktiv gegen Software-Sicherheitslücken, die neue Formen von Angriffen ermöglichen. Die auf modernsten Proxy-Technologien basierende Deep Application Inspection identifiziert und blockiert neue und unbekannte Bedrohungen. So sind Sie automatisch vor Spyware, Trojanern, Würmern, DoS, DDoS, DNS-Poisoning, Pufferüberläufen und anderen Angriffen geschützt.

Intuitive, zentrale Verwaltung

Der WatchGuard® System Manager (WSM) ist die intuitive Benutzeroberfläche, mit der alle Funktionen der Firebox X Core zentral verwaltet werden. Für IT-Administratoren bietet er leistungsstarke Tools zur Echtzeitüberwachung und -protokollierung sowie völlige Transparenz von Sicherheit, Netzwerk und Benutzeraktivitäten – und das ohne versteckte Kosten oder zusätzliche Investitionen. Und da Sie alle Aspekte Ihrer Sicherheitslösung(en) mit nur einer Benutzeroberfläche verwalten können, sparen Sie dazu noch Zeit und Geld.

Integrierte Sicherheitsfunktionen für umfassenderen Schutz

Alle im Abonnement erhältlichen Sicherheitsdienste lassen sich mit dem Zero Day Angriffsschutz der Firebox X Core integrieren und bieten so eine unschlagbare Kombination. Diese zusätzlichen Sicherheitsschichten sind voll integriert und alle Abonnements gelten pro Appliance und nicht pro Benutzer, so dass die Kosten nicht eskalieren. Alle Abonnements erledigt der WSM mit seinen Echtzeitansichten aller Dienstaktivitäten, wodurch ein stets aktueller Schutz gewährleistet wird.

■ Gateway AV/IPS mit Anti-Spyware

Stoppt bekannte Spyware, Trojaner, Viren und Webattacken mit robustem signaturbasierten Schutz am Gateway.

■ spamBlocker mit Quarantänefunktion

Holen Sie sich den besten Anti-Spam-Dienst der Branche für die Blockierung von bis zu 97 % aller unerwünschten E-Mails, mit vollständiger Quarantänefunktion.

■ WebBlocker

Regeln Sie das Surfverhalten Ihrer Mitarbeiter am Arbeitsplatz und schützen Sie Ihr Netzwerk vor schädlichen Webinhalten.

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 Firewall® auf die moderne Firewall® Pro Appliance-Software in Frage, die zusätzliche Netzwerkfunktionen wie VLAN, Hochverfügbarkeit, dynamisches Routing 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 verpflichtet sich zur Herstellung von energiesparenden Produkten, die in wiederverwendbaren Verpackungsmaterialien vertrieben werden. Wir erkennen die EU-Direktive über gefährliche 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
- **Effizientes Netzwerksicherheitsmanagement:** bietet Zeitersparnis
- **Kontinuierlich aktualisierte Sicherheitsdienste (im Abonnement):** bieten dauerhaften Schutz
- **Integrierte, upgradefähige Funktionen:** bieten ein besseres Preis-Leistungsverhältnis
- **Globales Team aus Sicherheitsexperten:** bietet Unterstützung bei Bedarf
- **RoHS/WEEE-konform**



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 Server), Pufferüberläufe und DoS-Attacken (Denial of Service).

Diese Tools benötigen Sie:

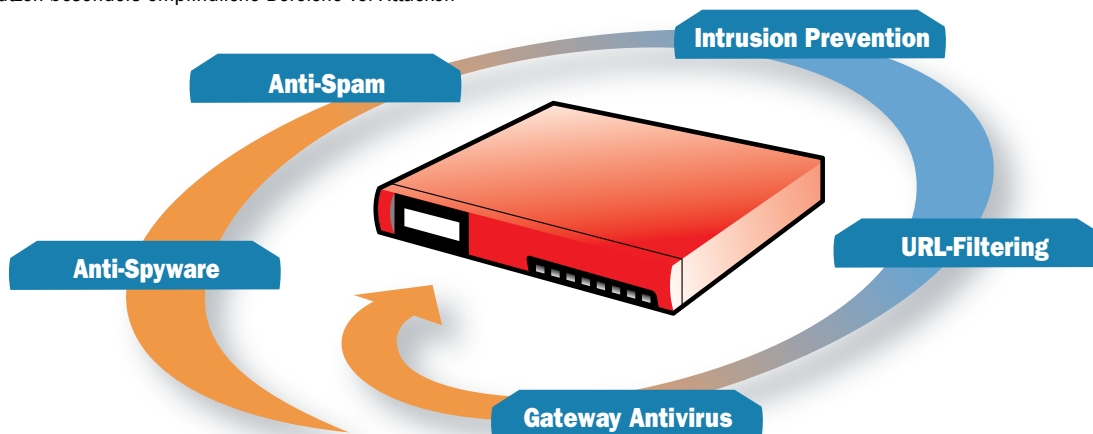
- Eine **Firebox X Core** für echten Zero Day Angriffsschutz
- Gültige Abonnements für **WebBlocker** zur Überwachung von nicht autorisiertem Surfen im Web sowie **Gateway AV/IPS** zur Echtzeit-Blockierung von verdächtigem Internetverkehr und heruntergeladenen Dateien

Die verschiedenen Sicherheitsfunktionen sind:

- **Zero Day Angriffsschutz:** schützt Ihr Netzwerk mit leistungsstarken, integrierten 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 Antivirus:** 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
- **URL-filtering** 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
- **Intelligente mehrschichtige Sicherheitsarchitektur und DNS-Proxy:** schützen gegen Netzwerkbedrohungen, DoS-Attacken sowie DNS-Cache-Poisoning
- **Robuste IPS-Funktionen:** steuern die Verwendung von Instant Messaging (IM) und Peer-to-Peer (P2P) Anwendungen, zwei der am häufigsten verwendeten Kanäle für die Verbreitung von Spyware
- **Integrierte Protokollierung, Berichterstattung und Alarmer:** bieten einen genauen Einblick in die Netzwerkaktivitäten und ermöglichen sofortige Präventiv- oder Abhilfemaßnahmen

Die integrierten Sicherheitsdienste (im Abonnement) 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, dem besten Dienst der Branche bei der Echtzeit-Differenzierung zwischen legitimer E-Mail-Kommunikation und Spam-Nachrichten

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 bis zu 97 % des unerwünschten E-Mail-Verkehrs, und zwar unabhängig von Inhalt, Sprache oder Format
- **Quarantänefunktion** zur Trennung von Spam und verdächtigen Nachrichten von geschäftskritischen, „sauberen“ Mails. So haben Administrator und Endbenutzer genügend Zeit, den Inhalt 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

	Firebox® X550e WG50550 X550e UTM Bundle WG50553	Firebox® X750e WG50750 X750e UTM Bundle WG50753	Firebox® X1250e WG51250 X1250e UTM Bundle WG51253
Firewall-Durchsatz†	300+ Mbps	300+ Mbps	300+ Mbps
VPN-Durchsatz†	35 Mbps	50 Mbps	100 Mbps
AV-Durchsatz†	50 Mbps	70 Mbps	100 Mbps
Gateway AV/IPS mit Anti-Spyware	Optional	Optional	Optional
URL Filtering	Optional	Optional	Optional
Spam-Blocking	Optional	Optional	Optional
Schnittstellen 10/100	4	8	0
Schnittstellen 10/100/1000	0	0	8
Enthaltene Sicherheitszonen	4	8	8
Gleichzeitige Sitzungen	25.000	75.000	200.000
Unterstützte Knoten (LAN IPs)	Unbegrenzt	Unbegrenzt	Unbegrenzt
Serielle Ports	1	1	1
VLAN*	25	25	25
VPN-Tunnel für Niederlassungen (inkl./max.)	35/45	100/100	600/600
VPN-Tunnel für mobile Benutzer (inkl./max.)	5/75	50/100	400/400
Obergrenze für die lokale Authentifizierungs-DB	250	1.000	5.000
Modell-Upgrades	Ja	Ja	Nein
Fireware® Pro Advanced Appliance-Software	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
- Spyware-Blocking
- Anwendungs-Proxies – HTTP, SMTP, FTP, DNS, TCP, POP3
- DoS- und DDoS-Schutz
- Progressiver DDoS-Schutz
- Erkennung von Protokollanomalien
- Verhaltensanalyse
- Pattern-Matching
- Fragmented Packet Reassembly-Schutz
- Malformed Packet-Schutz
- Liste statisch blockierter Sites
- Liste 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
- PPTP-Server
- PPTP-Passthrough
- Dead Peer Detection (RFC 3706)
- Hardware-basierte Verschlüsselung
- Drag-and-Drop-VPN-Tunnel

Benutzerauthentifizierung

- XAUTH
 - RADIUS®, LDAP, Windows® Active Directory
- RSA SecurID®
- Web-basiert
- Lokale Authentifizierung

IP-Adresszuweisung

- Porttrennung
- Statisch
- PPPoE-Client
- DHCP-Server
- DHCP-Client

- DHCP-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
- RIPv1, v2
- Dynamisches Routing*
 - BGP4, OSPF
 - RIPv1, v2
- Policy-based Routing*

Networking

- VLAN*
 - Bridging, Tagging, Routed-Modus
- Server Load-Balancing*

Abonnements für Sicherheitsdienste

- spamBlocker
 - Quarantäne für Spam-, Bulk- und verdächtige Mail
- Gateway AntiVirus/IPS mit Anti-Spyware
 - Unbegrenztes AV-Datei-Scanning
- 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-Berichte
- XML-Protokollformat
- Verschlüsselter Protokollkanal
- Syslog
- SNMP

Alarme/Benachrichtigungen

- SNMP
- E-Mail
- Management System Alert

Management-Software

- WatchGuard System Manager (WSM)

Zertifizierungen

- Common Criteria EAL4
- ICSA IPsec
- ICSA Firewall
- West Coast Labs Checkmark-Zertifikat
 - Firewall Level 1, VPN, Web Filtering, Intrusion Prevention, Anti-Spam

Support und Wartung

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

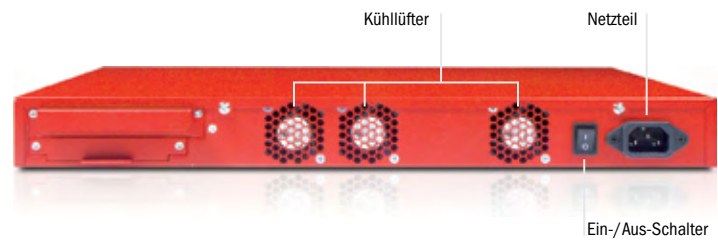
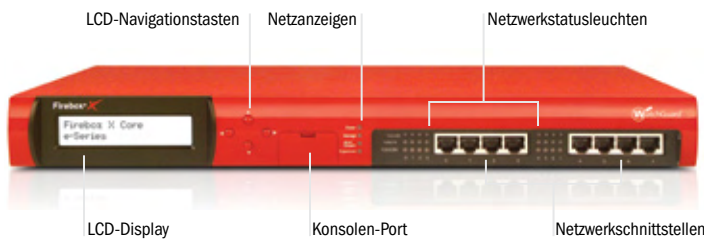
* Verfügbar mit einem Upgrade auf die Fireware Pro Appliance-Software

Abmessungen/Leistungswerte

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

Umgebung

Betriebstemperatur	0 – 45° C
Ruhetemperatur	-40 – 70° C
Betriebsfeuchte	10 – 85 %
Ruhefeuchte	10 – 95 % nicht kondensierend bei 55° C
Nicht periodische Schwingungen (Ruhezustand)	7 – 28 Hz 0,001 bis 0,01 G2 pro Hz
Akustisches Rauschen	54 dB bei 20 – 25° C
Mechanischer Schock (Betrieb)	20 G mit 11 Ms Dauer 1/2 Sinuswelle
WEEE/RoHS-konform	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 9.1 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**: Diese Technik, bei der anstatt physikalische logische Netzwerkconfigurationen 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“

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

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

- Firebox X Core e-Series X550e, X750e oder X1250e Security Appliance
- WebBlocker*
- spamBlocker*
- 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 zur Firebox X Core erhalten Sie unter www.watchguard.com/appliances.

ADRESSE: Watchguard Technologies, IOM Business Center, Humboldtstr. 12, 85609 Aschheim-Dornach, Germany · WEB: www.watchguard.de

E-MAIL: 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. ©2007 WatchGuard Technologies, Inc. Alle Rechte vorbehalten. WatchGuard, das WatchGuard Logo, Firebox, Fireware, LiveSecurity, Peak, Core 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.: WGCE66360_090607



IPSec

Firewall

Firewall Level 1

VPN

Web Filtering

Intrusion Prevention

Anti-Spam