

WatchGuard XCS™ 770, 970, 1170



XCS-Appliances garantieren Sicherheit und Datenschutz für eingehenden und abgehenden Netzwerkverkehr

Empfohlen für mittlere bis große Unternehmen, Regierungsbehörden und ISPs inklusive Global-2000- und Fortune-500-Organisationen

Die WatchGuard® **XCS-Appliances (Extensible Content Security)** bieten zuverlässige Sicherheit und Datenschutz für eingehende und abgehende E-Mails. In Kombination mit einem Websicherheitsabonnement erhalten Sie umfassende Kontrolle über E-Mail- und Webverkehr für einen leistungsstarken, einheitlichen Schutz.

Wieso Sie die XCS-Lösung kaufen sollten

Eine XCS-E-Mail- und Web-Sicherheitslösung bietet Ihrem Unternehmen:

- effiziente und umfassende Inhaltssicherheit und Schutz vor Bedrohungen über mehrere Protokolle hinweg
- vollständige Transparenz und Kontrolle des gesamten E-Mail- und Webverkehrs
- notwendige Tools und Informationen zum Nachweis der Einhaltung der Vorschriften
- erhebliche Verringerung von Kosten und Verwaltungsaufwand im Vergleich zu Lösungen mit mehreren Einzelprodukten

All das führt zu einem zuverlässigen Schutz, der Industrievorschriften entspricht, geringe Betriebskosten erfordert und Ihnen mehr Zeit gibt, sich auf andere IT-Prioritäten zu konzentrieren.

Dank der XCS-Plattform
 „...**hat sich unser E-Mail-Volumen erheblich reduziert**,
 und es gab viel weniger schädliche
E-Mail-basierte Angriffe.“

Stan Prothero
 Netzwerkdienstleister
 Puget Sound Blood Center

 Umweltfreundliche Technologie

SPAMSCHUTZ

- **Die ReputationAuthority**, eine der wichtigsten „cloud-basierten“ Komponenten von XCS, blockiert bis zu 98 % unerwünschter E-Mails vor dem Eintreffen, sorgt so für eine erhebliche Optimierung der Bandbreite und hält Bedrohungen vom Eintritt in Ihr Netzwerk ab.
- **Die Anti-Spam Engine** überprüft Absenderinformationen und -inhalte wie Bilder, Anhänge und enthaltene URLs. Führt eine automatische Kontextanalyse des E-Mail-Verkehrs sowie eine kategorisierende und gewichtete Auswertung für einen hocheffizienten, intelligenten Schutz durch.
- **Quarantäne für Spam und verdächtige E-Mails** leitet unerwünschten Spam zu einem lokalen Quarantäneserver und ermöglicht Endbenutzern die Verwaltung ihrer in Quarantäne befindlichen Nachrichten, Sicherheitslisten und Blockierungslisten über eine einfach zu bedienende, webbasierte Oberfläche.

SCHUTZ VOR VIREN, SPYWARE UND SCHADPROGRAMMEN

- **Zero-Hour-Bedrohungserkennung** schließt die Lücke der Anfälligkeit zwischen dem Beginn eines Angriffs und der Entwicklung und Distribution von Scan-Filter-Updates.
- **Umfangreiches Filtern von Inhalten und Schutz vor Schadprogrammen** scannt eingehende E-Mails auf schädliche Inhalte in Kombination mit weiteren Bedrohungen (Blended Threats).

SCHUTZ VOR DATENVERLUST FÜR SICHEREN DATENSCHUTZ UND EINHALTUNG DER VORSCHRIFTEN

- **Automatisierte Weiterverarbeitung** von Nachrichten sorgen für Blockierung, Quarantänisierung, Weiterleitung, Sendung von Blindkopien, Verschlüsselung oder Zulassung von Nachrichten auf der Grundlage von benutzerkonfigurierbaren Richtlinien zum Schutz vor Datenverlusten.
- **Vordefinierte Compliance-Wörterbücher** für GLB, HIPAA, PCI und andere Vorschriften sind je nach den Richtlinienanforderungen für Echtzeitschutz vor Datenverlust und spezifische Branchenvorschriften anpassbar.
- **Integrierte E-Mail-Verschlüsselung**, erhältlich als Add-On-Funktion für die XCS-Plattform, schützt vertrauliche Nachrichten für die Versendung an jeden beliebigen Empfänger, ohne dass ein eigener Server benötigt wird. Somit fallen Kosten, die bei den meisten anderen Verschlüsselungstechnologien aufkommen, weg.
- **Elektronische Datenauffindungs- und -klassifizierungsprofile** ermöglichen die Klassifizierung von empfindlichen Dateien. Dabei wird dem System gezeigt, wonach gesucht werden soll und welche Maßnahmen zu ergreifen sind, wenn solche Daten in abgehenden Nachrichten entdeckt werden.
- **Zentralisierte Data Loss Prevention:** Anwendung einer einzigen Richtlinie für mehrere Protokolle, um die Daten während der Übertragung vor Datenverlust und Richtlinienverstößen zu schützen.

VERLÄSSLICHE, PERMANENTE E-MAIL-ÜBERWACHUNG

- **Das dynamische On-Demand Clustering** ermöglicht es Ihnen, die Konfigurationseinstellungen und Nachrichten-Warteschlangen innerhalb weniger Minuten auf mehrere Systeme zu kopieren, um somit die Redundanz und Skalierbarkeit für einen unterbrechungsfreien Betrieb zu erhöhen.
- **Redundante Speicherung des E-Mail-Verkehrs** schließt den Verlust von Nachrichten aus und garantiert, dass die E-Mail-Sicherheit immer eingeschaltet ist und funktioniert.

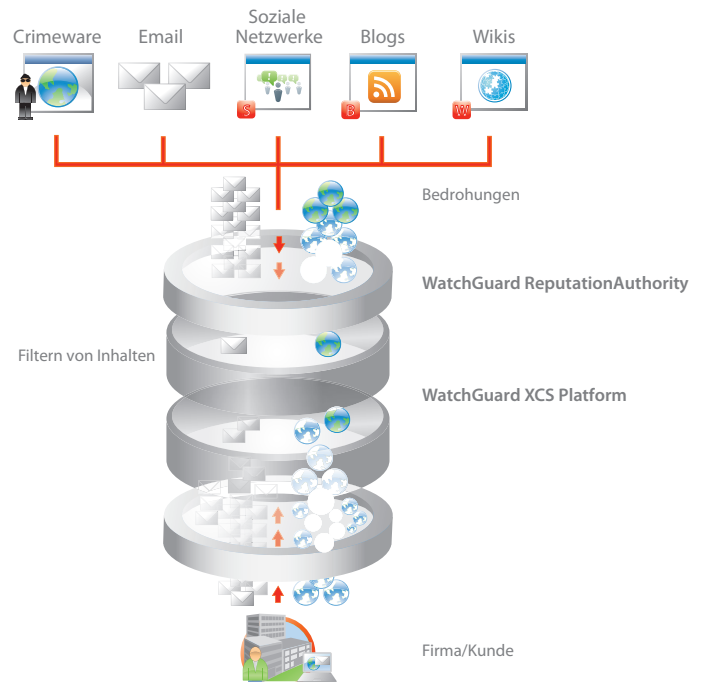
WEITEN SIE DIESEN SCHUTZ GANZ EINFACH AUCH AUF IHREN WEBVERKEHR AUS – MIT EINEM WEBSICHERHEITS-ABONNEMENT

- **Anhand der Steuerung der akzeptierten Benutzer und Anwendungen** können Sie den Zugang zum Internet und zu bestimmten Anwendungen zentral verwalten und mit Hilfe detaillierter Richtlinien für einzelne Benutzer und Benutzergruppen beschränken. Zeit- und IP-basierte Richtlinien liefern dabei eine bessere und flexiblere Kontrolle. Weniger Web-Verbindlichkeiten und mögliche Bedrohungen.
- **Die URL-Filterung und -Kategorisierung** analysiert und blockiert basierend auf Inhalten und Richtlinien dynamisch den Zugang zu Websites. Bietet unmittelbaren und exakten Netzwerkschutz vor schädlichen und unangemessenen Websites.
- **Cloud-basierte URL-Überwachung in Echtzeit** analysiert jede einzelne URL schon bevor die Verbindung zustande kommt, um das Risikoniveau zu bestimmen. Gefährliche URLs und URLs, die Bedrohungen enthalten, werden blockiert, ehe Sie in Ihr Netzwerk eindringen können – für ein schnelleres und sichereres Surfen im Web.
- **Optimierung des Web-Traffics** mit Web-Caching, erweitertem HTTP-Scanning, großen Downloads und Unterstützung von Streaming-Medien bewirken eine geringere Auslastung der Bandbreite sowie eine geringere Serverlast und Latenz für den Webverkehr.
- **Tools zur Verwaltung der Berichterstellung** bieten einen ganzheitlichen Überblick über Ihre Websicherheit. Umfasst nutzerbasierte Berichterstellung und eine Online-Instrumententafel zur Überwachung der Webnutzung und -bedrohungen.

	XCS 770	XCS 970	XCS 1170
	Mittleres Unternehmen	Großes Unternehmen	Fortune-500- / Global-2000- Unternehmen
Durchsatz			
Nachrichten/ Stunde	75k	100k	150k
Chassis/Prozessor			
Formfaktor	1U kurz, für Rack-Montage geeignet	1U tief, für Rack-Montage geeignet	1U tief, für Rack-Montage geeignet
Abmessungen	4,32 cm x 42,67 cm x 35,56 cm	4,32 cm x 43,69 cm x 65,02 cm	4,32 cm x 43,69 cm x 65,02 cm
Gewicht	7,7 kg	19 kg	19 kg
CPU	Intel Xeon Quad-Core Prozessor	Intel Xeon Quad-Core Prozessor	2 Intel Xeon Quad-Core Prozessoren
Leistung	Festes 200-W-Universalnetzteil, 100/240 V	Zwei redundante Hot-Plug-650-W-Universalnetzteile, 100/240 V	Zwei redundante Hot-Plug-650-W-Universalnetzteile, 100/240 V
Lagerung			
RAID	-	RAID 1	RAID 10
Arbeitsspeicher	4 GB (2 x 2 GB) DDR2 667 MHz	4 GB (2 x 2 GB) DDR3 1.066 MHz	4 GB (2 x 2 GB) DDR3 1.066 MHz
HDD	160 GB SATA, 7.200/Min	2 x 160 GB SATA-II, 7.200/Min	4 x 146 GB SAS, 15.000/Min
Konnektivität			
Ethernet	3 Intel Gigabit Ethernet	4 Intel Gigabit Ethernet	4 Intel Gigabit Ethernet
Serielle Schnittstelle	1 RS-232 (DB-9)	1 RS-232 (DB-9)	1 RS-232 (DB-9)
Temperatur			
Betrieb	0 °C bis 45 °C	0 °C bis 45 °C	0 °C bis 45 °C
Lagerung	-40 °C bis 70 °C	-40 °C bis 70 °C	-40 °C bis 70 °C
Relative Feuchtigkeit			
Betrieb	10 % bis 85 % nicht kondensierend	10 % bis 85 % nicht kondensierend	10 % bis 85 % nicht kondensierend
Lagerung	5 % bis 95 % nicht kondensierend	10 % bis 95 % nicht kondensierend	10 % bis 95 % nicht kondensierend
Höhe			
Betrieb	0 – 3.000 m	0 – 3.000 m	0 – 3.000 m
Lagerung	0 – 4.570 m	0 – 4.570 m	0 – 4.570 m

Blockierung von 98 % des unerwünschten E-Mail-Verkehrs am Rande des Netzwerks

XCS verwendet WatchGuard ReputationAuthority™ zur Identifizierung von schädlichen Absendern und blockt 98 % der Bedrohungen auf Basis des Echtzeitverhaltens ab. Das System geht über die einfache Absenderreputation hinaus und bietet einen umfassenden Überblick über das Verhalten der IP-Adresse in Echtzeit. Durch die Verknüpfung und Analyse von Daten aus mehreren Protokollen wird sichergestellt, dass schädlicher und unerwünschter E-Mail-Verkehr nicht in das Netzwerk eindringen kann.



Tiefgehende Inhaltsfilterung (Defense-in-Depth)

Eingehender und abgehender E-Mail-Verkehr wird mehreren tiefgehenden Überprüfungen unterzogen. Inhalte, Bilder und Absenderinformationen werden gründlich analysiert und untersucht, um eine kontextbasierte, gewichtete Auswertung zu erstellen, die anzeigt, wer der Absender ist, was genau in der Nachricht enthalten und wie sie aufgebaut ist und wohin sie den Empfänger weiterleitet. Dadurch ergibt sich ein bestimmtes Bedrohungsverdachtsniveau, das sicherstellt, dass nur sichere Kommunikation in Ihr Netzwerk vordringen kann.

Data Loss Prevention in Echtzeit

XCS liefert eine Echtzeit-Lösung, die Daten nach benutzerdefinierten Richtlinien während der Übertragung über mehrere Protokolle hinweg blockiert, unter Quarantäne stellt, zulässt, verschlüsselt oder weiterleitet. XCS bietet eine umfassende Risikoverwaltung und Richtlinienumsetzung und beseitigt somit den Bedarf an mehreren Einzelprodukten bei gleichzeitiger Sicherstellung von Datenschutz und Einhaltung der Vorschriften.

Beseitigung von Sicherheitslücken für umfassende Sicherheit

Mit XCS können IT-Administratoren auf ein und derselben Oberfläche Richtlinien über mehrere Protokolle hinweg erstellen, verwalten und umzusetzen. Die ausführliche Berichterstattung liefert einen umfassenden Überblick über den ein- und ausgehenden E-Mail- und Webverkehr Ihres Netzwerks.

Zentralisierte Verwaltung und Berichterstellung

Durch die kinderleichte Verwaltung können Sie den ein- und ausgehenden Datenverkehr durch eine einzige Richtlinie über mehrere Protokolle hinweg kontrollieren. So verbringen Sie weniger Zeit mit der Sicherung Ihres Netzwerks und können sich IT-Projekten mit einem höheren Geschäftswert widmen.

Ein ganzheitlicher Überblick über den ein- und ausgehenden Datenverkehr in Ihrem Netzwerk über mehrere Protokolle hinweg ermöglicht Ihnen die Schließung von Sicherheitslücken und einen im Vergleich zu Einzelproduktlösungen geringeren Verwaltungsaufwand.

Integrierte Systemberichte können mit nur einem Mausklick verwaltet werden – benutzerdefinierte Berichte in festgelegten Intervallen und in verschiedenen Dateiformaten sind verfügbar. Einhaltung der Prüfungsanforderungen durch einfach zu exportierende oder lokal gespeicherte zeit-, funktions- und gruppenbasierte Berichte.

Beratung und Support durch Experten

Jede XCS-Appliance beinhaltet ein Abonnement* für den LiveSecurity Service, ein umfassendes Support- und Wartungsprogramm mit den folgenden Leistungen:

- **Hardware-Garantie** mit erweitertem Hardware-Austausch
- **Technischer Support** mit einer angestrebten Reaktionszeit von 4 Stunden
- **Software-Updates**
- **Warnmeldungen**

Weitere Informationen erhalten Sie auf www.watchguard.com/livesecurity.

*1-, 2- und 3-Jahres-Abonnements erhältlich

Adresse: Max-Planck-Str. 4, 85609 Aschheim, Germany • Web: www.watchguard.de • Telefon: +49 (700) 92229333

In diesem Dokument werden keine ausdrücklichen oder konkludenten Garantien gegeben. Sämtliche hier aufgeführten technischen Daten können jederzeit geändert werden. Informationen zu zukünftigen Produkten, Merkmalen und Funktionen werden zum gegebenen Zeitpunkt zur Verfügung gestellt. ©2010 WatchGuard Technologies, Inc. Alle Rechte vorbehalten. WatchGuard, das WatchGuard-Logo, WatchGuard ReputationAuthority und LiveSecurity sind Marken oder eingetragene Marken von WatchGuard Technologies, Inc. in den USA und/oder anderen Ländern. Alle anderen Markennamen sind Eigentum ihrer jeweiligen Inhaber. Teilen: WGC66665_052710