

WatchGuard XCS™ 170, 370, 570

Empfohlen für kleine bis mittlere Unternehmen mit bis zu 1.000 Benutzern.

WatchGuard® XCS-Appliances (Extensible Content Security) bieten zuverlässige Sicherheit und Datenschutz für eingehende und abgehende E-Mails. Die leistungsstarken und dennoch einfach zu verwaltenden XCS-Appliances kombinieren mehrere Schutzschichten in einer Plattform, um eine vereinfachte Verwaltung und solide E-Mail-Sicherheit zu gewährleisten.


Wieso Sie die XCS-Lösung kaufen sollten

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

- einen tiefgehenden Schutz des Netzwerks vor E-Mails, die Bedrohungen enthalten
- umfassenden Schutz vor Spam-Nachrichten
- vollständige Transparenz und Kontrolle des abgehenden E-Mail-Verkehrs zur Vermeidung von Datenverlust
- notwendige Werkzeuge und Informationen zum Nachweis der Einhaltung der Vorschriften
- eine kosteneffektive Möglichkeit, um unerwünschte E-Mails am Rande des Netzwerks zu blockieren und die Bandbreite optimal zu nutzen

„Wir konnten von **enormen Kosteneinsparungen** und **erheblich höheren Sicherheitsstandards** profitieren.“

Börje Justrel
Leiter der IT-Abteilung
Riksarkivet

 Umweltfreundliche Technologie



Entlasten Sie Ihre E-Mail-Server durch die Blockierung von Spam-Nachrichten und E-Mail-Bedrohungen

XCS-Appliances gewährleisten die Sicherheit beim E-Mail-Verkehr und sorgen dafür, dass keine vertraulichen Informationen nach außen durchsickern und keine unbeabsichtigten Datenlecks bzw. Fälle von Datendiebstahl auftreten. Es handelt sich um eine ideale Lösung für alle Unternehmen, die eine solide und erschwingliche Anti-Spam- und E-Mail-Sicherheitslösung mit Funktionen zur Vermeidung von Datenverlust benötigen.

TIEFGEHENDER SCHUTZ

- **Blockiert über 98 % der unerwünschten E-Mails** am Rande des Netzwerks mit 99,9 %iger Genauigkeit und unter Verwendung der branchenführenden Cloud-basierten Echtzeit-Reputationsservices von WatchGuard.
- **Untersucht Absenderdaten 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.
- **Stellt Spam-Nachrichten und verdächtige E-Mails unter Quarantäne** durch die Weiterleitung an einen lokalen Quarantäneserver und ermöglicht Endbenutzern die Verwaltung ihrer in Quarantäne befindlichen Nachrichten, Sicherheitslisten und Blockierungslisten über eine einfach zu bedienende, webbasierte Oberfläche.
- **Das dynamische On-Demand Clustering** ermöglicht Ihnen, die Konfigurationseinstellungen und Nachrichten-Warteschlangen auf mehrere Systeme zu kopieren, um somit die Redundanz und Skalierbarkeit für einen unterbrechungsfreien Betrieb zu erhöhen.
- **Beinhaltet eine redundante Verarbeitung des E-Mail-Verkehrs**, um den Verlust von Nachrichten auszuschließen und eine hohe E-Mail-Sicherheit aufrechtzuerhalten.

SCHUTZ VOR VIREN, SPYWARE UND SCHADPROGRAMMEN

- **Schließt die Lücke der Anfälligkeit** zwischen dem Beginn des Angriffs und der Entwicklung und Distribution der Scan-Filter-Updates für einen „Zero-Hour“-Bedrohungsausbruchschutz.
- **Scannt eingehende E-Mails auf schädliche Inhalte** in Kombination mit anderen Bedrohungen für eine erweiterte Inhaltsfilterung und optimierten Schutz vor Schadprogrammen.
- **Blockiert Dateianhänge**, die bekanntermaßen schädlich sind, vor dem Eindringen in Ihr Netzwerk.

SCHUTZ VOR DATENVERLUST FÜR SICHEREN DATENSCHUTZ UND EINHALTUNG DER VORSCHRIFTEN

- **Automatische Blockierung, Quarantänisierung, Weiterleitung**, Sendung von blinden Kopien, Verschlüsselung oder Zulassung von Nachrichten auf der Grundlage von benutzerkonfigurierbaren Richtlinien mit leistungsstarken Funktionen für transparente Problembeseitigung, um einen Datenverlust zu verhindern.
- **Vordefinierte Compliance-Wörterbücher** für GLB, HIPAA, PCI und andere Vorschriften sind je nach den Richtlinienanforderungen für Echtzeitschutz vor Datenverlust und spezifischen Branchenvorschriften anpassbar.
- **Klassifizierung von empfindlichen Dateien** durch Datenauffindungs- und -klassifizierungsprofile. Dabei wird dem System gezeigt, was zu beachten ist und welche Maßnahmen zu ergreifen sind, wenn solche Daten in abgehenden Nachrichten entdeckt werden.
- **Anwendung einer einzigen Richtlinie für mehrere Protokolle** dank einer zentralisierten Datenverlustrichtlinienverwaltung, zum Schutz vor Datenverlust und Richtlinienverstößen.

E-MAIL-VERSCHLÜSSELUNG

- **Die reibungslose E-Mail-Verschlüsselung** schützt vertrauliche Nachrichten für die Versendung an jeden beliebigen Empfänger. Sie ist für alle XCS-Appliances als einfach hinzuzufügendes, optionales Sicherheitsabonnement erhältlich und benötigt keinen eigenen Server. Somit fallen Kosten, die bei den meisten anderen Verschlüsselungstechnologien aufkommen, weg.

ZENTRALISIERTE VERWALTUNG UND BERICHTERSTELLUNG

- **Durch die kinderleichte Verwaltung** können Sie den E-Mail-Verkehr durch eine einzige Richtlinie kontrollieren. Somit verbringen Sie weniger Zeit mit der Sicherung Ihres Netzwerks und können sich IT-Projekten mit einem höheren Geschäftswert widmen.
- **Beseitigung der E-Mail-Sicherheitslücken und Reduzierung des Verwaltungsaufwands** durch die Bereitstellung eines ganzheitlichen Überblicks über eingehende und abgehende E-Mails in Ihrem Netzwerk.
- **Einfache Verwaltung der benutzerdefinierten Berichte mit nur einem Mausklick.** Es sind verschiedene Dateiformate verfügbar. Einhaltung der Prüfungsanforderungen durch einfach zu exportierende oder lokal gespeicherte zeit-, funktions- und gruppenbasierte Berichte.

	XCS 170	XCS 370	XCS 570
Durchsatz			
Nachrichten pro Stunde	12.000	24.000	48.000
Chassis/Prozessor			
Formfaktor	1U, für Rack-Montage geeignet	1U, für Rack-Montage geeignet	1U, für Rack-Montage geeignet
Abmessungen	4,32 cm x 42,67 cm x 35,56 cm	4,32 cm x 42,67 cm x 35,56 cm	4,32 cm x 42,67 cm x 35,56 cm
Gewicht	7,7 kg	7,7 kg	7,7 kg
CPU	Intel Celeron Prozessor	Intel Dual Celeron Prozessor	Intel Dual Celeron Prozessor
Leistung	Festes 200-W-Universalnetzteil, 100/240 V	Festes 200-W-Universalnetzteil, 100/240 V	Festes 200-W-Universalnetzteil, 100/240 V
Lagerung			
Arbeitsspeicher	2 GB (2 x 1 GB) DDR2 667 MHz	2 GB (2 x 1 GB) DDR2 667 MHz	4 GB (2 x 2 GB) DDR2 667 MHz
HDD	160 GB SATA, 7.200 U/Min	160 GB SATA, 7.200 U/Min	160 GB SATA, 7.200 U/Min
Konnektivität			
Ethernet	2 Intel Gigabit Ethernet	2 Intel Gigabit Ethernet	3 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	5 % bis 95 % nicht kondensierend	5 % 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

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

Die XCS 170- und -370-Appliances beinhalten das Standard-Abonnement des LiveSecurity Service. Die XCS 570-Appliances beinhalten LiveSecurity Plus,* das anstatt einer 12-Stunden-Unterstützung an fünf Tagen einen Rund-um-die-Uhr-Support über die gesamte Woche bietet.

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

* LiveSecurity Plus ist ebenfalls als Upgrade für die Modelle XCS 170 und 370 verfügbar.

Weitere Informationen zu den WatchGuard XCS-Lösungen erhalten Sie auf [visit www.watchguard.com/xcs](http://www.watchguard.com/xcs).

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

XCS verwendet WatchGuard ReputationAuthority™ zur Identifizierung von böswilligen 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

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, welches 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 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. Um zu gewährleisten, dass empfindliche Daten, die Ihr Netzwerk verlassen, bis sie vom Empfänger entschlüsselt werden unlesbar bleiben, kann das E-Mail-Verschlüsselungs-Abonnement ganz einfach in die Data Loss Prevention Funktion Ihrer XCS-Appliance integriert werden.

Beseitigung von Sicherheitslücken für eine umfassende E-Mail-Sicherheit

XCS ermöglicht IT-Administratoren, Richtlinien für den gesamten E-Mail-Verkehr zu erstellen, zu verwalten und umzusetzen. Die ausführliche Berichterstattung liefert einen umfassenden Überblick über den eingehenden und abgehenden E-Mail-Verkehr Ihres Netzwerks.

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: WGCE66667_040710