

WatchGuard® XCSv

Content Security in virtualisierten Web- und Messaging-Umgebungen

Virtuelle Appliances in einer virtuellen Infrastruktur

- Konkurrenzlose Sicherheit im E-Mail- und Web-Datenverkehr in virtuellen Infrastrukturen
- Einfacher Download, einfache Aktivierung, Bereitstellung und Verwaltung
- Kombination aus Hardware und virtuellen Appliances, Verwaltung über zentrale Plattform
- vSphere für höchste Flexibilität und Verfügbarkeit
- Verschiedene Versionen für Einsatzbereiche vom kleinen Büro bis zum Großunternehmen oder Service Provider

WatchGuard XCS-Lösungen bieten konkurrenzlosen Schutz vor Spam, Malware und Datenverlust. Sie ermöglichen Unternehmen aller Größen den Schutz wichtiger Informationen, ein Höchstmaß an regulatorischer Compliance und die sichere Nutzung des Internets. Viele Unternehmen greifen auf Virtualisierung zurück, um ihre IT-Kosten zu reduzieren und ihre Agilität zu steigern. Im Zuge dieser Entwicklung werden immer häufiger kritische Anwendungen – darunter E-Mail- und Messaging-Infrastrukturen wie Microsoft Exchange sowie weitere Web-Anwendungen – in virtuelle Umgebungen verlagert.

Mit WatchGuard XCSv können die Kostenvorteile der Virtualisierung zur Implementierung einer leistungsstarken und umfassenden Content Security-Gesamtlösung genutzt werden. XCSv vereint alle von der XCS-Serie bekannten Funktionen im Bereich E-Mail- und Web-Sicherheit sowie Data Loss Prevention in einem flexiblen Paket, das Unternehmen aller Größen die optimale Nutzung ihrer Virtualisierungs-Investitionen ermöglicht. Die XCSv-Lösungen von WatchGuard zeichnen sich durch einzigartige Flexibilität bei der Bereitstellung aus. Anwender können Hardware und virtuelle Appliances miteinander kombinieren und über eine gemeinsame zentrale Management-Plattform verwalten.

Mehr Sicherheit durch Integration mit Messaging- und Anwendungsservern – Anwendung in privaten Netzwerken

Zu den am häufigsten in virtuellen Umgebungen implementierten Lösungen zählen Messaging- und Anwendungsserver. Bei Umfragen unter IT-Unternehmen steht Microsoft Exchange regelmäßig weit oben auf der Liste der virtualisierten Dienste. Durch die Bereitstellung von XCSv-Appliances in solchen virtuellen Infrastrukturen können Content Security-Funktionen physischer Server auch für E-Mail- und Webserver genutzt werden. Dies erfolgt innerhalb privater Netzwerke, sodass der gesamte Datenverkehr vom Internet isoliert abläuft. Dieses Konzept bringt dank flexibler Bereitstellungsoptionen und konsolidiertem Management gleichzeitig Kostensenkungen und eine Erhöhung der Sicherheit.

Maßgeschneiderte Sicherheitsfunktionen durch Kombination mehrerer Appliances – mandantenfähiger Schutz

Anbieter von E-Mail-, Cloud- oder Managed Security-Services können auf Standard-Servern in ihren Rechenzentren mehrere Instanzen von XCSv-Appliances für virtualisierte Umgebungen einsetzen. Diese sind vollständig voneinander getrennt, sodass für alle Nutzer individuelle Service Level Agreements (SLAs) möglich sind und Konfigurationsänderungen bei einem Nutzer keine Auswirkungen auf die übrigen haben. Der entscheidende Vorteil: Jede der Instanzen kann individuell entsprechend branchen- und nutzerspezifischen Anforderungen konfiguriert werden. Eine Spamerkennung mit Lernfunktion berücksichtigt die spezifischen Anforderungen und die damit verbundene Terminologie/Fachsprache. Die Steuerung/Verwaltung der XCSv-Appliances erfolgt über eine benutzerfreundliche intuitive Konsole.



	XCSv Small Office	XCSv Medium Office	XCSv Large Office	XCSv Large Office XC
Plattform				
CPU-Kerne	1	2	4	8
Netzwerkschnittstellen	2	3	4	4
Speicher (min.)	2 GB	2 GB	4 GB	8 GB
Festplatte (min.)	64 GB	104 GB	184 GB	280 GB
E-Mail-Nutzer*	100	500	2000	5000
Bedrohungsschutz				
Anti-Spam / Anti-Virus / Anti-Malware				
Blended Threat Prevention				
Reputation Enabled Defense				
Spam-Wörterbücher				
Musterbasierte Nachrichtenfilter				
Nachrichten-Quarantäne				
Analyse eingehender Anhänge				
Web-Sicherheit (optionales Abonnement)				
URL-Filterung**				
Cloud-basierte Web-Reputationsservices**				
Filterung nicht kategorisierter Web-Inhalte**				
Kontrolle der Web-Nutzung**				
Kontrolle von Web-Anwendungen**				
Optimierung des Web-Datenverkehrs**	Web-Caching / Große Datei-Downloads mit schnellem Scanning / Kontrolle von Streaming-Medien / Traffic-Management und Clustering			
Data Loss Prevention				
Musterbasierte Inhaltsregeln				
Verschlüsselung	TLS / Verschlüsselung auf Nachrichtenebene***			
Compliance-Wörterbücher				
Filterung zweifelhafter Inhalte				
Automatisierte Nachrichtenverwaltung				
Zusatzfunktionen	DLP-Assistent / Scanning ausgehender Inhalte und Anhänge / Kontrolle ausgehender Anhänge / Dokument-Fingerabdruck und Datenklassifizierung			
Verwaltung & Berichterstellung	Zentralisiertes Management / Archivierung (Drittanbieter) / Benutzerbasierte Berichterstellung / Messaging-Protokolle / Detaillierte benutzerdefinierbare Richtlinien, einschließlich zeitbasierter Web-Zugriffsrichtlinien und IP-basierter Richtlinien / Detaillierte benutzerdefinierbare Berichte			
Redundanz	Nachrichten-Redundanz / On-Demand-Clustering [†] / Geographische Redundanz / Queue Replication			
Support	LiveSecurity [®] Plus mit 24/7-Support			

*Die tatsächliche Anzahl der unterstützten Nutzer ist abhängig vom Volumen des E-Mail-Verkehrs und den ausgewählten Sicherheitsrichtlinien. **Verfügbar mit einem WatchGuard XCS Web Security-Abonnement für alle XCS-Modelle. ***Verfügbar mit einem WatchGuard XCS SecureMail Email Encryption-Abonnement für alle XCS-Modelle. [†]Nur bei Versionen Large Office und Large Office XC.

WatchGuard ist für Sie da, wenn Sie Hilfe brauchen

Alle XCSv-Appliances beinhalten ein LiveSecurity Plus-Abonnement für technischen Support 24/7.