WatchGuard

Datasheet

WatchGuard® XCSv

Content Security for Web and Messaging Virtualization

Run virtual appliances on your virtual infrastructure

- Industry-leading email and web content security for the virtual infrastructure
- Easy to download, enable, deploy, and manage
- Mix hardware with virtual appliances and manage all from centralized platform
- Leverages vSphere flexibility and availability
- Includes editions sized to meet the requirements of businesses ranging from small office to large business and service provider.

The best-in-class anti-spam, anti-malware, and data loss prevention available in WatchGuard XCS have enabled organizations of all sizes to protect their valuable information, attain high levels of regulatory compliance, and safely define their relationship to the Internet. As many of these organizations have taken advantage of virtualization to reduce IT costs and increase agility, they have identified key applications to move to virtualized environments – and among the most frequent and most strategic choices are email and messaging infrastructure (including Microsoft Exchange) and web application platforms.

With WatchGuard XCSv, the cost-effectiveness and efficiency of virtualization can be leveraged to implement powerful content security. XCSv delivers all of the email security, web security, and data loss prevention capabilities of XCS in flexible packaging that lets organizations of all sizes take advantage of their investment in virtualization. WatchGuard's XCSv offers unmatched deployment flexibility. You can choose to deploy a mix of hardware and virtual appliances, managed from a common centralized management platform.

Integrate with messaging and application servers for stronger protection – private-network deployment

Among the most popular applications that organizations have chosen to implement within their virtual environments are messaging and web application servers; surveys of IT organizations consistently place Microsoft Exchange at or near the top of the list of virtualized services. Deploying XCSv virtual appliances within the same virtualized infrastructure allows content security on the same physical servers to be connected to the email and web servers using private networks, insulating all traffic from the public Internet. Combined with the flexibility of virtualized deployment and consolidated management, this approach yields cost savings while increasing security.

Consolidate multiple security appliances for custom security – multi-tenant protection

Service providers – email hosting, cloud, or managed security services – can deploy multiple instances of XCSv in virtualized environments on shared industry standard servers within their datacenters. These virtual content security appliances are isolated from each other, so service level agreements (SLAs) can be guaranteed to each tenant, and a configuration change to one doesn't affect the others. Most important, each of these instances can be configured independently for the industry-specific and user-specific needs of the customer, including the ability to learn spam detection information that takes into account those needs and the associated vocabulary. And yet the XCSv virtual appliances can all be managed by the provider using a single intuitive console.

	XCSv Small Office	XCSv Medium Office	XCSv Large Office	XCSv Large Office XC
Platform				
CPU cores	1	2	4	8
Network interfaces	2	3	4	4
Memory (min.)	2 GB	2 GB	4 GB	8 GB
Disk (min.)	64 GB	104 GB	184 GB	280 GB
Email users*	100	500	2000	5000
Threat Protection				
Anti-Spam / Anti-Virus / Anti-Malware	✓	✓	✓	✓
Blended Threat Prevention	✓	✓	✓	✓
Reputation Enabled Defense	✓	✓	✓	✓
Spam Dictionaries	✓	✓	✓	✓
Pattern-based Message Filters	✓	✓	✓	✓
Message Quarantine	✓	✓	✓	✓
Inbound Attachment Control	✓	✓	✓	✓
Web Security (subscription-based)				
URL Filtering**	✓	✓	✓	✓
Cloud-based Web Reputation Services**	✓	✓	✓	✓
Uncategorized Web Content Filtering**	✓	✓	✓	✓
Acceptable Web Usage**	✓	✓	✓	✓
Web Application Control**	✓	✓	✓	✓
Web Traffic Enhancements**	Web caching / large file downloads with rapid scan / streaming media control / traffic management and clustering			
Data Loss Prevention				
Pattern-based Content Rules	✓	✓	✓	✓
Encryption	TLS / Message-level encryption***			
Compliance Dictionaries	✓	✓	✓	✓
Objectionable-Content Filtering	✓	✓	✓	✓
Transparent Remediation	✓	✓	✓	✓
Additional Capabilities	DLP Wizard / Outbound content and attachment scanning / outbound attachment control / document fingerprinting and data classification			
Management & Reporting	Centralized management / archiving (third party) / user-based reporting / messaging logs / customizable granular policies, including time-based web access policies and IP-based policies / customizable granular reports			
Redundancy	Message-level redundancy / on-demand clustering / geographical redundancy / queue replication			
Support	LiveSecurity® Plus with 24/7 technical support			

* Actual number of users supported is dependent on email traffic and security policies configured. **Available for all XCS models with a WatchGuard XCS Web Security Subscription. ***Available for all XCS models with a WatchGuard XCS SecureMail Email Encryption Subscription.

WatchGuard Is There When You Need Assistance

All editions of XCSv come with a subscription to LiveSecurity Plus for technical support 24 hours a day, 7 days a week.

U.S. SALES 1.800.734.9905 INTERNATIONAL SALES +1.206.613.0895 www.watchguard.com