

Total Email Perimeter Defense

ePrism™ Enterprise is an email security solution that provides organizations of any size with comprehensive email perimeter defense. ePrism delivers a unique combination of email security, spam protection, anti-virus and content control in an easy-to-use, high-performance appliance. Designed to be deployed between internal email servers and the Internet, ePrism supports standard email protocols and features a complete set of email filtering and security capabilities specifically designed to protect against the full spectrum of email threats and other policy violations.



Highlights

Stops Viruses and Worms at the Perimeter

ePrism offers Kaspersky Labs Antivirus®, which adds an additional level of defense against all forms of malware. Email is the #1 delivery mechanism for malware and ePrism Enterprise will stop this threat to your business.

New Improved Spam Protection

ePrism Enterprise employs the latest tier-one techniques for eliminating spam. The addition of technologies such as spam dictionaries, IP reputation-based detection, domain keys and anti-phishing to its multiple filtering operation, ensures that ePrism catches spam and reduces false positives better than any other solution.

Content Filtering

ePrism filters content located in message bodies and headers on both inbound and outbound email traffic. New features such as advanced content scanning, expanded filtering options, customized dictionaries and policy integration enable ePrism to protect your organization by filtering confidential emails as well as increasing security and worker productivity.

Threat Prevention

ePrism includes threat prevention capabilities that allow organizations to detect and block incoming threats before they reach their destination. ePrism analyzes mail flow patterns and detects when a host is behaving maliciously, protecting your organization from hackers and DoS attacks.

Features

Spam Protection

ePrism applies multiple tests to email traffic to discover the disposition of messages. These tests use the following technologies: Specific Access Patterns, Pattern-based Message Filtering, Spam Dictionaries, IP Reputation, DNS Block List, Bulk Analysis, Token Analysis, Sender Policy Framework (SPFTM) and DomainKeys™ Authentication. Additional features for spam filtering empower you to define the action taken once a message is tested. These actions include logging, modify subject header, add header, redirection to reject email and BCC. You can manage your quarantine or define trusted senders with a simple click included in the status message from ePrism to the users. You can also define the frequency with which status messages are sent to users.

Virus Protection

Since the most common way to infect a network is through email, virus scanning is an essential component of reliable email protection. ePrism includes Kaspersky Labs Antivirus®, recent winner of the coveted Best Anti Virus Solution award at the annual SC Magazine Global Awards. Automatic hourly updates to this virus-scanning engine ensure that the latest viruses are being identified and eradicated before they reach your host.

Malformed Message Protection

Malformed messages can allow hackers to avoid detection, crash your systems and lock up your mail servers. There are hundreds of malformed messages, but ePrism ensures that only correctly formatted messages are allowed to reach their destination.

Content Filtering and Scanning

- **Advanced Content Scanning** — ePrism’s deep scanning of email attachments ensures that private and confidential files are not sent out. Attachments such as PDFs, Word documents and hundreds of other file types can be scanned for individual words and phrases that are blocked based on your organization’s policies.
- **Expanded Filtering Options** — Several actions allow you to create filter rules that encrypt, quarantine, BCC, notify, redirect or discard messages.
- **Dictionaries** — ePrism offers custom dictionary support for content filtering allowing you to easily match simple words and phrases against message and attachment content.
- **Policy Integration** — Content filtering is integrated with ePrism’s policy engine allowing you to create different sets of filter rules for different users, groups and domains.



High Availability Load Optimization (HALO)

ePrism’s fail-safe clustering architecture for high availability ensures your email is never lost due to individual system failure. ePrism’s HALO provides security, cluster management, load balancing and “stateful failover” queue replication capabilities that guarantee consistency during a crisis. See the HALO for ePrism Enterprise datasheet for a more in-depth discussion of these features.

Hardware Specifications

Model:	M1000	M2000	M3000	M4000
Performance	10,000 MPH	32,500 MPH	65,000 MPH	100,000 MPH*
Dimensions	1.7”(H) x 16.7”(W) x 25.7”(D)		3.5”(H) x 16.7”(W) x 25.7”(D)	
Memory	512MB	1GB	2GB	2GB
LCD	NA	Yes		
Hard Drives	40GB	2 x 80GB ATA	4 x 73GB SCSI	
Form Factor	1U height, rack-mountable		2U height, rack-mountable	
Processor	Intel P4 Celeron 2.0GHz	Intel XEON 2.4GHz	Intel XEON 2.4GHz	2 x Intel XEON 3.2GHz
Power	150 Watts	400 Watts	2 x 400 Watts	
RAID	N/A	RAID 1	RAID 10	
NIC	2 x 10/100 bT	3 x 10/100/1000 bT	4 x 10/100/1000 bT	

Corporate Office
 15333 Avenue of Science
 San Diego, CA 92128



Phone: 858-676-2277 Fax: 858-676-2299
 Toll Free: 800-782-3762 Email: info@edgewave.com