

## BENEFIT

### High Performance Message Processing

Provides carrier-grade scale and performance for L7 transparent content security delivered in a hardened, multi-threaded Linux appliance form factor.

### Integration and Deployment

Integrated edge security solution allows scanning of all email, web, and file transfer protocols within a carrier-grade security appliance.

### Built for Performance

Capable of supporting carrier-grade data throughput with fully redundant hardware and software systems.

### Seamless Network Integration

Simply integrates into existing network with minimal topology changes.

### Easy System Administration

Customers can enable automatic integration with external reporting solutions. Cloudmark Edge provides granular reporting and the ability view detailed logs of scanning activity.

### Flexible Policy Control

Cloudmark Edge provides flexible application of policy control for various user groups, including ability to configure policy exclusions based on source and destination IP, file size, text keyword content, and destination URL.

### Visibility and Insight

Delivers granular visibility into traffic and abuse patterns, enables control of abuse vectors in the network.

## CARRIER-GRADE PROTECTION FOR SOPHISTICATED WEB-BASED AND EMAIL-BASED ATTACKS

Fixed line and mobile broadband operators are facing greater challenges than ever in securing their networks against the propagation of sophisticated email spam, malware and web-based attacks. Customers using 3G and 4G connected laptops, netbooks and tablets are just as vulnerable to malware infection as PCs connected to fixed line networks. Once compromised, these computers are often indoctrinated into existing global botnets and leveraged to send spam to destinations on the internet using the available data network. Without protection, spam and malware laden traffic is sent to the internet and reported to commercial security vendors and Real-time Blackhole Lists (RBLs), likely resulting in large amounts of an operator's IP range being listed on these various RBLs. Once this occurs, valid subscribers are unable to send emails from these IP ranges or they may be limited in their ability to access web based services. This can result in increased customer care calls, customer churn, and poor brand reputation. Cloudmark Edge protects the network by transparently preventing spam and malware delivery from local broadband networks to the internet for early detection and blocking of infected systems before they can impact the service for other broadband subscribers

## REAL-TIME THREAT RESPONSE

Cloudmark Edge intercepts email, web requests, and file transfers at the network layer, scans traffic at multi-gigabit speeds at the application-layer, and blocks infected content or threats, thus allowing only filtered content to enter or leave the network. With its combination of best-in-class content filters, URL reputation, intelligent throttles and protocol filters along with Cloudmark's global threat network of over 1.8 billion protected users, Cloudmark Edge delivers the industry's most comprehensive zero-hour protection against outbound messaging attacks.

## CLOUDMARK EDGE ANTI-VIRUS BLADE

Extending its coverage beyond messaging security, Cloudmark Edge stops sophisticated and emerging web-based threats before they reach vulnerable endpoints with a fast, accurate gateway anti-virus engine.

The platform protects against malicious code attacks from unknown or compromised sites. Operators can help stop data thieves, key loggers, and viruses from sending information out of their networks through unsuspecting subscribers by disallowing them to contact known malicious sites.

## UNMATCHED PERFORMANCE AND ACCURACY FOR THE BEST PROTECTION

Cloudmark Edge is purpose-built for industry-leading performance and unparalleled accuracy leveraging proven security-scanning technology Cloudmark Authority®. Cloudmark Authority® delivers a high-performance, scalable and easy-to-manage email security solution. Integration of multiple security blades for spam and virus filtering, anti-phishing, malicious content detection, and web filtering ensures organizations have the highest level of perimeter defense against security threats. Unlike pure Bayesian rules based systems that are susceptible to significant delays

## SYSTEM REQUIREMENTS

### Performance

Inline Throughput: 1Gbps to 4Gbps  
 Emails per hour: 3,600,000+  
 HTTP pages per hour: 11,500,000  
 Users: Over 50,000 (all services)

### Hardware

CPU: 2 x Six Core Intel® Xeon®  
 2.4GHz  
 RAM: 16GB  
 Compact Flash: 4GB  
 Network Ports: 4GbECopper + 2GbE  
 SL w/LAN Bypass  
 Power Supply: 460W ATX 1 +  
 1 Redundant Power, AC / DC  
 90~264VAC full range 4A~8A @  
 47~63Hz

### Physical / Operational

Form Factor: 2U Rack mount  
 Height: 16.7"  
 Width: 23.62"  
 Depth: 3.5"  
 Weight: 55.11lbs  
 Operating Temperatures: 0°C to 40°C  
 Storage Temperatures: -20°C to 80°C  
 Relative Humidity: 5% to 90%  
 Power Consumption: 349.4 W  
 MTBF: 86,587 hours  
 Certifications: CE, FCC, RoHS, PSE

(from hours to days) in updating signatures for emerging threats, Cloudmark's automated threat network delivers automated fingerprint updates every 30 seconds.

## ADDITIONAL PROTECTION BLADES AVAILABLE

The modular Cloudmark Edge security solution within a carrier-grade security appliance, designed for simplicity, capable of integrating in most networks with minimal changes. In addition to Cloudmark Authority for SMTP stream scanning, the following optional protection blades are available that allow scanning of web content, URL's, and file transfer protocols:

- **Cloudmark Edge Anti-Virus Blade** - Combats propagation of Web-based threats, Viruses/Malware, and Code Injection Attacks. It enables mobile operators to stop sophisticated and emerging threats by scanning bi-directional web and FTP traffic before the content has a chance to infect vulnerable endpoints
- **Cloudmark Edge Content Filter Blade** - Delivers Email and Web Usage Controls. It enables mobile operators to understand, filter, and monitor Internet usage while maximizing network availability. Operators can reduce legal liability and preserve bandwidth for subscribers, exceeding SLAs. Includes categorization of over 30 million websites into more than 90 content categories that can each be assigned to user population polices. Protection can also include real-time keyword, URL, and regular expression-based filters with Time of Day support.

## DEPLOYMENT POINTS:

- Web/Network Gateway
- Transparent Proxy
- ICAP Server
- Inline, Stealth Mode (Bridge)
- Offline Proxy
- WCCP Server

## INDUSTRY AFFILIATIONS



For more information  
 visit us at [www.cloudmark.com](http://www.cloudmark.com)

