

We secure the world's largest networks.

Content & Mail Security

In the beginning, anti-virus software ran on the desktop. In time, the management of thousands of desktops overwhelmed the IT staff and anti-virus software moved to gateway-based systems running on or next to the corporate mail server. But the advent of the Web enabled the bypassing of the gateway completely. Any employee receiving e-mail at a personal account such as bob@my-provider.com never gets scanned on the way in. But to put traditional server gear in the data path at the network ingress point causes as many problems as it solves:

- The equipment is not designed for high performance and can't keep up with the scanning requirements. Users will not accept delays in their web surfing or network experience.
- The equipment is not highly available. A failure causes rupture of the entire network behind it.
- Networking engineers don't like to put servers in the data path.
- The gear is yet another appliance that has to be managed and added to an already-growing stack of disparate equipment, which increases management complexity and costs.

Fast, Highly Available, Easily Managed

The requirements of entrance facility content scanning are thus:

- High performance
- High availability
- Reduced management

Best-in-class Solutions from Crossbeam

To achieve the requirements of next generation content security, Crossbeam has incorporated the world's best content protection software – Trend Micro InterScan VirusWall and Aladdin eSafe OPSEC-compliant anti-virus– into its X-Series and C-Series security services switches. These integrated solutions eliminate the need for multiple servers and multiple load balancers, switches and separate High Availability software required to make competitive solutions scale.

The next two sections describe the delivery of content security protection on specific Crossbeam platforms. Because both Trend Micro and Aladdin eSafe operate in the same way from a network perspective, the operational description below applies to each solution.

X-Series Content and Anti-Virus Solution

For large data centers, the Crossbeam X40 provides scalable scanning and virus cleaning performance, single and dual box high availability and the ability to integrate with other best-in-class security solutions, especially firewall and VPN (for example, one could “decontaminate” decrypted streams emerging from a VPN tunnel before sending them to their final destinations).

The content security engine runs on up to ten X40 Application Processing Modules (APM). Performance scales linearly as APMs are added to the system. The front-end Network Processing Modules (NPM) perform an initial flow classification and load balancing function, distributing only traffic that NEEDS to be scanned. For example, an enterprise might wish only to perform HTTP email scanning at the perimeter and let the corporate gateway continue to perform anti-virus scanning. In this case, the NPMs would only direct HTTP traffic through the APMs dedicated to handling that function. SMTP traffic, on the other hand, would either pass through with no scanning or receive standard firewall policy application if a firewall was also loaded. Of course, both SMTP and FTP traffic could also be scanned at the perimeter if the security policy called for it.

Besides making use of single or dual Pentium class processors, the APMs offer additional local working storage in the form of hard drives and up to 4G of RAM per APM. These expansion capabilities are more important for content scanning because a large compressed file may need to be decompressed before being scanned – with any degradation in performance.

From a security standpoint, the NPMs are unaddressable and do not report any fingerprinting information nor do they respond to port scans. Initial packet verification occurs at this level and frees the content processing system for more intensive work. Up to 4096 VLANs are supported, meaning that the X40 integrates easily into any network environment. Interface options on each NPM are 1GE+8FE (10/100) or 2GEs.

Administration of the system is performed through an entirely separate switched control plane. Gigabit logging ports on this same out-of-band network also ensure that data traffic is not affected by management traffic. Sixteen administrative levels are supported along with GUI and command-line configuration options.

C-Series Content and Anti-Virus Solution

Crossbeam offers the Crossbeam C30 content security solution. This turnkey system delivers price/performance excellence for medium or large enterprises.

The C30 integrates functionality from Trend Micro in a slim two-rack-unit (2RU) form factor with sixteen 10/100 interfaces, two gigabit Ethernet interfaces and five additional function slots for acceleration of encryption functions and other security related processing tasks. The high density of network interfaces provides for granular application of scanning policies based on the network from which a traffic stream originates. In addition, the system is designed to run content scanning in parallel with firewall functionality at high speeds, yielding a high return on investment since additional appliances are not needed.

Failover is dual box in an active-active deployment via VRRP and, like the X40, management is performed via a separate management network. The C30 also delivers all the advantages of performance, high availability and multi-function security in a price/performance leading compact package.

Which Content Security Engine to Choose?

Crossbeam typically selects its security engine partners based on customer feedback. We support both Trend Micro and Aladdin eSafe, having tested the products extensively. In each case, Crossbeam platforms have become the highest performance appliances for the respective applications.

Both applications come pre-installed on Crossbeam platforms. Below are the key features of these products.

Aladdin is a leader in digital security, providing the eSafe product line for integrated content security. eSafe is a comprehensive gateway-based, fully-integrated content security solution that addresses all content security layers:

- Real-time protection for all Internet born traffic - SMTP, POP3 (with secure mail relay), HTTP, and FTP
- Proactive anti-virus and malicious code protection engine that is ICSA and Checkmark certified
- Exploit and worm protection against new vulnerabilities as well as protect various hacking attacks
- Advanced Anti-spam module utilizing multiple spam control methods including real-time black lists (RBL), DNS lookup, header verification and keyword filtering to keep spam to a minimum
- URL filtering module to keep out unwanted web content
- Web application filtering such as instant messengers, P2P and file sharing, remote access, spyware and adware

eSafe provides a rich feature set to allow flexible implementation for any type of organization – SMB, Mid size, Large and xSP (ISPs and any type of service provider)

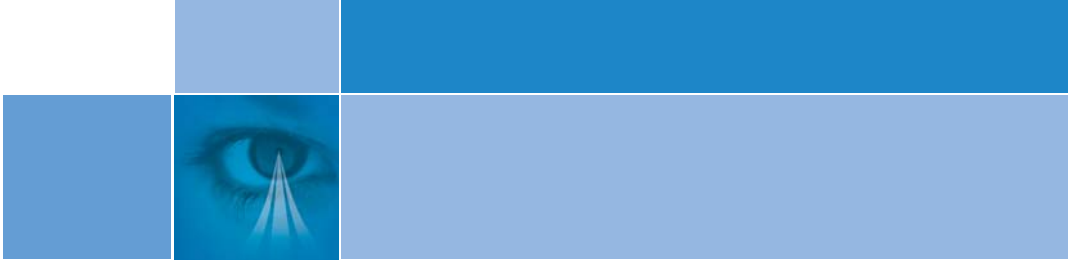
- High performance with innovative NitroInspection™ packet collector engine for inline deployment, scalable up to hundreds of megabit of traffic on Crossbeam X-series platforms with built-in load balancing and failover mechanism
- Seamless integration with major firewalls, including Check Point firewall for a complete regional office / SMB deployment of firewall and content security on Crossbeam C-series
- Strong security oriented development with numerous proactive techniques to protect against future unknown threats
- Fully integrated management console, automated signature and engine updates, and value-added services such as 24 x 7 premium support and security configuration gap analysis
- Special focus on the xSP market with a tier structure to enable offering different service levels and value-added services to fit the business model

Trend Micro is the worldwide market share leader in anti-virus gateways.

- Real-time Protection at the Gateway: InterScan VirusWall™ provides real-time detection and cleanup of viruses and malicious code at the gateway for SMTP, HTTP, and FTP Internet traffic.
- Multiple Response Options to Virus Outbreaks
- InterScan VirusWall can be configured to respond to virus detection and security violation incidents in several ways, alone or in combination:

- Alert the system administrator
- Isolate the infected file for later cleaning or other action
- Delete the infected file
- Permit the user to download the file under certain strictly controlled conditions

- Automatic Virus Pattern File Updates: Frequent updates of virus pattern files are available from the Trend Micro Web site, and can be scheduled for automatic download and installation. Emergency pattern files are made available on an "as needed" basis.
- Flexible Configuration and Management: InterScan VirusWall can be configured locally via a Windows interface or remotely using a Web browser. Windows GUI and ISAPI/CGI Web browser configuration interfaces offer administrators flexible management options.
- Compatibility with major firewalls and third-party products
- Centralized Management: InterScan VirusWall integrates with Trend Micro Control Manager™ for centralized configuration and management of Trend Micro products and services.



About Crossbeam Systems

Crossbeam Systems, Inc., is a leading global developer of total security solutions required for safer, simpler networks. Crossbeam enables companies to consolidate their security infrastructures while preserving their security policies, resulting in significant savings in capital and operational expenses. Crossbeam's patent-pending architecture integrates best-in-class security engines such as firewall, virtual private networks, intrusion detection, and content security into high-performance, highly available, self-healing security services switches. The company has tailored solutions for global enterprises, carrier networks, and medium-sized businesses. More information is available at www.crossbeamsystems.com.



www.crossbeamsystems.com

Corporate Headquarters
200 Baker Avenue
Concord, MA 01742 USA
p: [+1] 978-318-7500
f: [+1] 978-287-4210

European Headquarters
E. Space, Bat C.
45 allée des Ormes
06250 Mougins – France
p: [+33] (0)4 92 28 89 89
f: [+33] (0)4 92 28 72 60

Asia Pacific Headquarters
80 Raffles Place
Levels 36 UOB Plaza 1
Singapore 048624
p: [+65] 6248 4684
f: [+65] 6248 4988