



## Content Security

### With Integrated Support for Finjan SurfinGate for Web

#### Management and Protection Against Malicious Mobile Code

The Internet gives users access to a wide range of content and downloadable software. This content ranges from valuable business-related information and software to potentially damaging executables and malicious mobile code. Today, centralized scanning of Web content at corporate Internet access points is required to stop harmful content at the network perimeter – before it impacts the organization.

However, simply deploying conventional virus scanning alone often does not provide adequate protection against emerging malicious code. An organization is vulnerable from the first time a new virus hits the Internet until the time an Anti-Virus vendor delivers a signature update to stop that virus. Finjan closes this “Window of Vulnerability” left open by anti-virus software while helping to reduce productivity losses and avoid expensive clean-up costs.

“Gartner believes that enterprises should begin to augment and eventually replace signature-based techniques with more-robust approaches. Enterprises that don’t will be swamped by malicious software riding the coming wave of Web services. Finjan Software is a vendor that takes this approach.”  
- Gartner Group

#### Blue Coat Content Security enables organizations to:

- Close the “Window of Vulnerability” by protecting against new viruses that often pass through undetected by conventional virus scanning products
- Increase performance and scalability of malicious mobile code protection by utilizing an optimized appliance with integrated content caching
- Implement comprehensive security policies for active content (Java, JavaScript, Active-X) to Scan, Strip, or Replace potentially dangerous content in real-time
- Simplify installation, management and administration associated with mobile code security
- Obtain comprehensive visibility and reporting on active content and mobile code through integrated reporting software

# Content Security

## With Integrated Support for Finjan

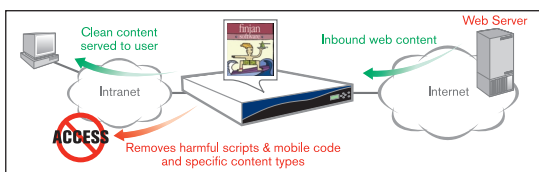
The Web Security Authority.™

### Solution Overview

In order for organizations to safely give users the Internet access they need to do their jobs, it's essential for administrators to be able to create and manage policies governing who can download what types of content. As enterprises move to tighten security against known viruses, new Malicious mobile code viruses such as Sircam, Goner and Code Red, enter the network as embedded executables (e.g. ActiveX, JavaScript, or Visual Basic Scripts). Unfortunately, signature-based virus scanning products are not designed to effectively secure against malicious mobile code viruses.

Unlike other content security products operating on general-purpose platforms, the Blue Coat appliance platform is built specifically to manage, secure and accelerate Web content. The foundations of the Web Security Appliance are a patented proxy caching technology and a Policy Processing Engine™ - a powerful combination for achieving optimal performance and enforcing granular security policy for malicious code protection.

*Blue Coat Systems security appliances in conjunction with integrated Finjan SurfinGate™ provides a policy-based approach to real-time, malicious code protection*



Blue Coat Systems and Finjan have partnered to close the Window of Vulnerability. Leveraging the Internet Content Adaptation Protocol (ICAP), the integrated solution provides administrators the flexibility to scan all active content, or only specific content based on the mime type, web site, protocol, requesting user, file type and more, depending on the needs of organization. For example, administrators may choose to have data deemed safe, like images from trusted sources, not vectored to the Finjan server for scanning. Other Active X controls requested from any unknown sites could always be sent to the Finjan server for inspection prior to forwarding to the user.

Finjan has developed the Vital Security™ software that inspects active content entering an organization. Based on proactive behavioral analysis, the combined Blue Coat/Finjan

solution defends against new and unknown viruses, Trojan horses, worms and other malicious code attacks. The flexible policy architecture, allows system managers to defend against attack while allowing known, safe active content to be passed to users.

### Key Features:

**Policy Processing Engine** – Patent-pending system enables sophisticated security policies based on any combination of individual users, groups of users, time of day, location, protocol, user agent, content type and much more.

**Proactive Behavior Inspection** – SurfinGate performs real-time content inspection of ActiveX, Java, VBScript and JavaScript. On any given Web page (including personal web based email), code behavior that violates the defined security policy is denied access to the network, while all other content on the page is allowed to reach the user, enabling greater productivity.

**Visual Policy Manager** – Enables point-and-click configuration of security policies. Administrators can set policies based on user or group information, content type, URL categorization, time of day, location, subnet, user domain and other factors.

**Optimized Appliance** – Delivers powerful, scalable content security that can be easily expanded to perform other security services such as HTTP virus scanning and content filtering.

**ICAP Support** – Allows standards-based integration of SurfinGate Web with the Blue Coat security appliance platform enabling best-of-breed content security.

**Send To MCRC** – Administrators can send blocked active content details to Finjan's Malicious Content Research Center (MCRC) for analysis.

**Comprehensive Logging and Reporting** – Provides complete visibility and reporting to network and security administrators detailing information and all events managed and monitored by the Blue Coat appliances.