Vital Security™

Integrated Content Security Platform

for Web

Features & Capabilities

- Traditional anti-virus provides the first line of defense against signature based, known viruses.
- Behavior Scanning and Analysis Inspection provides an additional, proactive, layer of defense against new, unknown viruses.
- Content Filtering guards against manual and automatic downloads of documents based on document extension and MIME type.
- Web Filtering and Content Control allows administrators to create an Internet access policy, filter access to Web sites based on URL categorization and receive automatic updates to the database transparently.
- User Detection enforces security policies on real logged in users and not only on fixed IP addresses.
- Centralized management and reporting provides over 100 standard reports and custom reports.
- Customizable features allow administrators to configure according to their unique organizational needs.

A Comprehensive Layered Defense Against Internet

In today's e-business environment, it has become increasingly more important for enterprises to provide access to information via the Internet, while at the same time effectively manage and protect mission critical systems and information resources. Vital Security for Web's unique proactive defense detects Active Content and mobile malicious code, such as ActiveX and Java, as well as embedded and stand-alone VBScript and JavaScript. Vital Security for Web performs content inspection using multiple content specific scanners. These scanners create a security profile for each Active Content, identifying potential hostile attacks or suspicious commands. Using security policies, administrators can block mobile malicious code that intends to perform hostile attacks and stop new viruses, worms, Trojan horses and spyware even before the anti-virus signature database is updated. This unique feature, integrated with anti-virus engines, can detect and log viruses and worms from their introduction through their entire lifecycle, resulting in a zero Window of Vulnerability.

Behavior Analysis Inspection

While firewalls protect against packet level attacks, Web traffic and other application level activity can bring hostile active content into a network undetected. Similarly, traditional anti-virus software can be effective against known viruses and worms, but they are unable to effectively protect organizations against new, unknown viruses and active content in real-time. Vital Security for Web does not depend upon reactive anti-virus signature database updates alone. These updates can take hours, if not days. Instead, Vital Security for Web uses its patented real-time proactive content scanning and profiling technology to provide day-zero defenses against new, unknown and targeted attacks by mobile malicious code and Active Content. Vital Security for Web represents the most effective way to combat Trojan horses, worms and malicious ActiveX, Java, VBScript and JavaScript programs.

Vital Security for Web identifies and analyzes downloaded content as it enters the network. All characteristics of the content are contextually examined for security violations in real-time. Any content that violates the corporate security policies is logged and blocked at the gateway, while end-users are notified with an onscreen alert. Examples of security policy violations include attempts to delete or create files, open network connections or modify the user's registry settings.

Traditional Anti-Virus

Vital Security for Web offers an optional integrated anti-virus scanner to detect traditional, known viruses. An integrated log captures all known viruses attempting to enter the network and administrators can customize policies to suit their needs. Signature database updates are automatic and transparent.

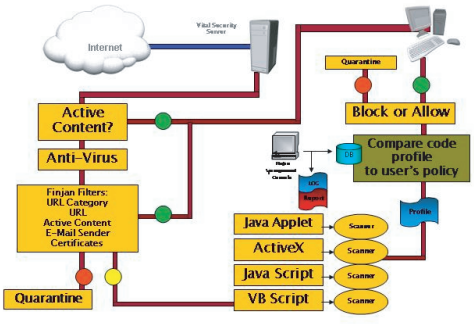
Unique Proactive Defense

Vital Security for Web protects the Internet gateway from new, unknown attacks, long before any anti-virus software signatures can be updated. Active Content is scanned for potential hostile attacks or suspicious commands at the gateway. Granular policies and strict security configurations can stop new viruses, worms, Trojan horses or spyware from ever infectng your network, resulting in a zero Window of Vulnerability.

Web Filtering and Content

Another option is integrated Web filtering, allowing organizations to have full control over Web traffic and Web content that enters into their network based on content category, specific URL and time of day. Administrators also have the ability to create Internet access policies for both users and groups. Since Web sites are constantly changing and new sites are regularly born, Vital Security for Web automatically updates its database of sites and URL categories transparently in the background.

Vital Security for Web
Active Content Inspection



Vital Security *for Web*

System Requirements

Vital Security Server on Solaris

- Sun v120/E250/E420/E450
- Solaris 8 (fully patched)
- Oracle v7.3.4.
- 1 GB free disk space is required for VS Server
- 300 MB of free disk space is required for Oracle Server (an additional 70 MB is required during installation)
- 1 GB RAM

Vital Security Server on Windows

- Windows 2000 Server or Advanced Server, SP2 or above
- Pentium IV 2.4 GHz processor and above
- 1 GB of free disk space during installation
- 1 GB RAM

Vital Security Console

- Windows NT 4.0 SP6a, 2000 SP2, 98 SE or ME
- Microsoft Internet Explorer 5 and above
- Pentium IV 1.6GHz processor and above
- 50 MB of free disk space during installation and 15 MB of free disk space at the end of the installation
- 256 MB RAM (512 recommended)

Certificate Server and Oracle Client

- Windows 2000 Server or Advanced Server, SP2 or above
- Pentium IV 1.6GHz processor and above
- Oracle Client v7.3.4.
- 256 MB RAM (512 MB RAM recommended)
- 20 MB of free disk space is required for certificate Server, and 30 MB for Oracle Client

**Finjan Software was awarded EAL3 certification from the SAIC for Vital Security 5.6 for Web.*

Content Filtering

Vital Security for Web can be configured to allow or block other active content entering the network. It can detect executables, plug-ins and unscannable objects such as password protected zip files. It can also be configured to allow or block the simple download of documents or documents automatically launched by the browser. Security policies on downloads are enforced based on document extension and MIME type.

Management and Reporting

Vital Security for Web's management and reporting capabilities provide administrators with high level and detailed views of their network security. Enterprise-wide reports such as mobile malicious content received, viruses stopped and top 10 Web sites blocked, empower IT managers with the information they need to accurately adjust their security policies as their company grows and changes. Some of the features include:

- Granular Policy Management: Multiple security policies can be created for different users, groups or departments.
- Exception Handling: Enables administrators to "white list" approved content according to URL, specific active content or a specific digital certificate, without the need to compromise on the security levels for unknown and untrusted content.
- Content Filtering: Blocks manual and automatic downloads of active content documents based on document extension and MIME type.
- Integrated Logging: All mobile code security violations, viruses detected and cleaned, and Web access violations are listed in a centralized log allowing the security administrator to track new and unknown attacks.
- Enhanced Logging: Every HTTP request, security policy violation, resource misused, performance and throughput, etc., can be logged, allowing detailed analysis of usage attacks, Web traffic, Web content and security policy violations patterns.
- Management Reports: More than 100 standard reports are provided by Vital Security for Web. Dynamic custom reports can also be created using the built in report generator.

Integrated Solution Reduces Cost of Ownership

Vital Security for Web is an integrated, best-of-breed secure content management solution, providing:

Single Point of Management: Integrated components with one management console provide administrators with all of the information required to stop potential attacks from ever entering the network.

Single Vendor: Significant total cost of ownership savings can result from purchasing a complete solution from a single vendor.

Integrated Components: Costs for purchasing an integrated solution can be as much as 40% less than purchasing individual, stand-alone, software.

Other Features

- X-Ray Mode: Operate in a pass through mode designed to provide a clear view of active content activity prior to implementation, enabling the fine-tuning of security policies.
- ICAP Support: Vital Security for Web fully supports ICAP 1.0 so existing ICAP environments don't need to change organizational topology in order to install and configure Vital Security for Web.
- Single Point of Management: Graphical management console manages multiple distributed servers from a single location, providing an enterprise-ready and scalable solution.
- LDAP/NTLM User Authentication: Policies are enforced on real logged-in users, not only on fixed IP addresses, to detect every HTTP request and the user behind the request.
- Digital Certificate Filtering: Allows administrators the ability to detect, filter and assign policy for digitally signed content.
- High Availability: Local Vital Security for Web databases can operate independently from the central database allowing Vital Security for Web to remain active even if the primary database server is offline. Vital Security for Web has the option to operate in load balancing mode.
- Malicious Code Research Center (MCRC): Administrators can send blocked active content details to Finjan's Malicious Code Research Center for analysis and advice by our expert security engineers.

For more information

on products, services or support, contact a local Finjan sales representative at www.finjan.com