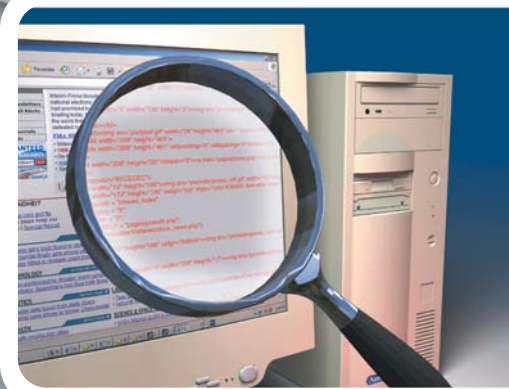


Anti-Spyware Solution

Proactive Spyware Prevention at the Gateway



Cybercrime is booming and money is the driving force behind the growth of targeted attacks against corporate networks that steal business data that can be sold on to other criminals.

Cybercriminals use the web as a highly effective attack vector for a wide range of illegitimate and malicious activities, including identity theft through keylogging, financial fraud, espionage, and intelligence gathering.

Security vendor reported that 51% of the malicious sites found in the second half of 2007 were legitimate sites that were compromised by attackers. They also point out that these sites pose a significant risk to companies who rely on website reputation to protect their users.



Percentage of top 50 threats that expose confidential information

Spyware has evolved from an online nuisance to a dire web threat.

Cybercriminals use Spyware programs to hijack users' sensitive personal information at will for profit.

Spyware distributors use evasive techniques to avoid detection. Spyware presents a problem for corporations.

If their employees' machines are not sufficiently protected, Spyware attacks can result in employee login information being compromised, allowing access to the employee's network account and thus accessing confidential and business information.

Solution Highlights

- Proactive real-time content inspection solution that detects and blocks both unknown and known Spyware
- Comprehensive solution, including Anti-Spyware, Anti-virus and URL filtering
- Centralized web-based management and single point of provisioning for reduced TCO
- Wizard-driven security policy decision-making system, with a single-click rules refinement enhancement, to easily set up and manage security policies
- Powerful reporting and logging capabilities empower enterprises to monitor ROI and trends, and to adjust security policies as their business evolves
- Support of Cisco WCCPv2 and ICAP standards ensures interoperability with various networking and caching systems
- Integrated dashboard provides instant information on the system's performance and risk level, using an extensive set of graphs and views
- Supports compliance with regulatory initiatives such as SOX (COBIT) DS5, PCI DSS 1.1, GLB Act, HIPAA, and FISMA

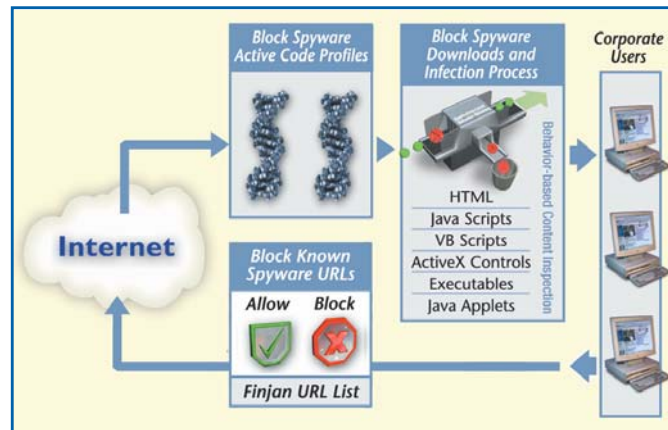
Stops Spyware In Real-Time at the Gateway

Active real-time content inspection protects the networks and vital information assets of organizations around-the-clock.

Finjan's Secure Web Gateway products utilize active real-time content inspection to understand the intended criminal behavior of web content. Each and every piece of incoming and outgoing web content in HTTP/HTTPS/FTP is analyzed in real time regardless of its originating URL and without signature matching. It therefore detects and blocks Spyware (also when hiding in SSL traffic) from entering corporate networks. It thus prevents malicious web content from entering the corporate network, thus protecting enterprises from Spyware that may result in severe business damage.

How Finjan Protects Your Business Assets from Spyware

- Blocks downloads, silent installations and automatic launch of Spyware (including drive-by downloads) performed during web browsing
- Blocks malicious content matching Finjan's extensive list of known Spyware behavior profiles
- Prohibits access to and downloads from known Spyware sites based on Finjan's URL blacklists
- Detects and blocks Spyware that tries to access local information, files, user details, registry and other local resources to prevent collection of personal information
- Detects installed Spyware (on previously infected machines) trying to access the Internet and blocks it from sending back "spied" information to its home site using integrated URL blacklist functionality
- Detects and blocks Spyware that tries to exploit known vulnerabilities
- Detects Spyware attacks that use SSL-encrypted content which are invisible to most standard gateway scanning applications
- Protects against Spyware attacks that use invalid, revoked or otherwise problematic certificates by enforcing your organization's certificate policies at the gateway



Proactive, Multi-Layered Spyware Protection

Finjan's comprehensive and fully integrated Vital Security™ Web Appliances leverage patented active real-time Security technology to achieve the highest level of protection against incoming and outgoing Spyware.

This solution protects your organization without compromising productivity or performance. Finjan's solution lets you avoid the potentially devastating damage and costs resulting from Spyware, including theft of intellectual property, confidential information or violations of customer privacy.

For Additional Information

For more information, please visit www.finjan.com or contact our regional offices:

USA

Toll Free: 1 888 FINJAN 8 (1 888 346 5268)
Tel: +1 408 452 9700
Email: salesna@finjan.com

United Kingdom

Tel: +44 (0)1252 511118
Email: salesuk@finjan.com

Germany

Tel: +49 (0)89 673 5970
Email: salesce@finjan.com

The Netherlands

Tel: +31 (0)33 454 3555
Email: salesne@finjan.com

Asia Pacific

Tel: +972 (0)9 864 8200
Email: salesapac@finjan.com

Israel

Tel: +972 (0)9 864 8200
Email: salesis@finjan.com

Finjan - Securing Your Web

Finjan Secure Web Gateway Appliances for Enterprises



© Copyright 1996 - 2009. Finjan Inc. and its affiliates and subsidiaries. All rights reserved.

All text and figures included in this publication are the exclusive property of Finjan and are for your personal and non-commercial use. You may not modify, copy, distribute, transmit, display, perform, reproduce, publish, license, create derivative works from, transfer, use or sell any part of its content in any way without the express permission in writing from Finjan. Information in this document is subject to change without notice and does not present a commitment or representation on the part of Finjan. The Finjan technology and/or products and/or software described and/or referenced to in this material are protected by registered and/or pending patents including European Patent EP 0 965 094 B1 and U.S. Patents No. 6092194, 6154844, 6167520, 6480962, 6209103, 6298446, 6353892, 6804780, 6922693, 6944822, 6993662, 6965968, 7058822, 7076469, 7155743, 7155744, 7418731 and may be protected by other U.S. Patents, foreign patents, or pending applications.

Finjan, Finjan logo, Vital Security, Vulnerability Anti.dot, Window-of-Vulnerability, RUSafe and SecureBrowsing are trademarks or registered trademarks of Finjan Inc., and/or its affiliates and subsidiaries. Sophos is a registered trademark of Sophos plc. McAfee is a registered trademark of McAfee Inc. IBM Proventia Web Filter technology is a registered trademark of IBM Internet Security Systems. Kaspersky is a registered trademark of Kaspersky Lab. SurfControl and Websense are registered trademarks of Websense, Inc. Microsoft and Microsoft Office are registered trademarks of Microsoft Corporation. All other trademarks are the trademarks of their respective owners. Q1 2009.