

Real time content inspection

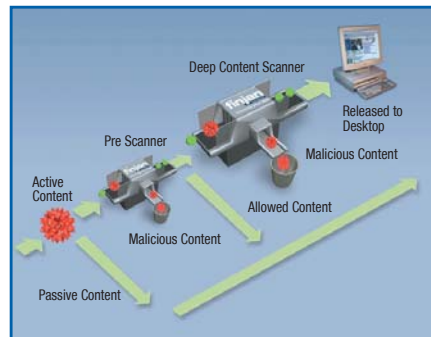
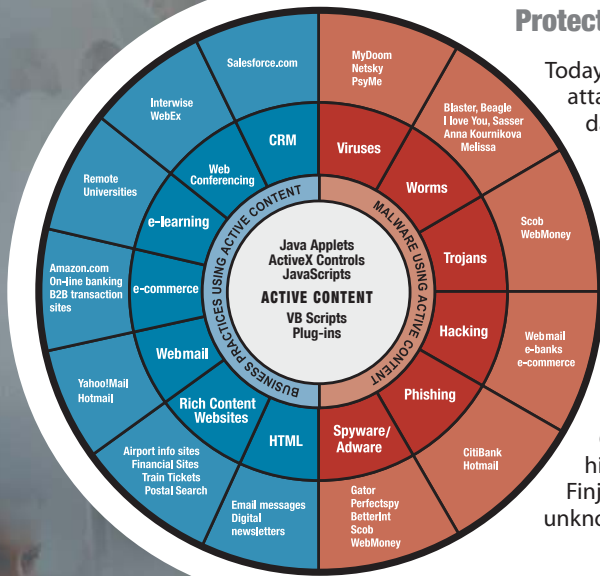
Protects Against the New Cybercrime Wave

Today's cybercriminals are motivated by financial gain, and their main vector of attack has become the Web. They understand too well that signature and database reliant solutions are not designed to protect against obfuscated malicious codes served on compromised legitimate sites, Web 2.0 -based attacks, and other dynamic attack vectors that use the Web.

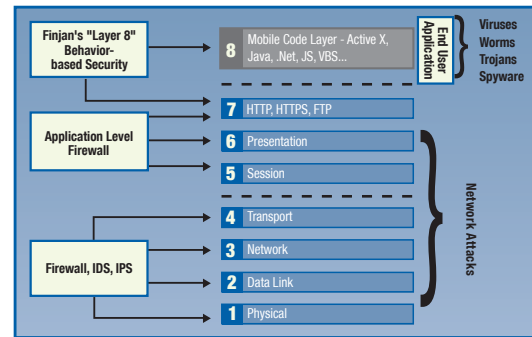
These sophisticated Web-based attacks are specifically designed to hit the "blind spots" of traditional security systems that rely on signatures or databases (such as anti-virus, URL filtering and reputation based security).

Finjan's patented active real-time content inspection technology scans each and every piece of incoming and outgoing Web content, including HTTP/HTTPS content, analyzes it in real time regardless of its originating URL and without signature matching. It therefore detects and blocks Crimeware, targeted attacks and other malicious web content, also when hiding in SSL traffic, from entering corporate networks.

Finjan's active real-time code analysis approach is highly effective in handling unknown, dynamic and rich Web as well as traditional threats.



Two-Step Scanning for Enhanced Performance



Viruses, Trojans, Worms and Spyware operate at Layers 7 and above (Layer 8). Finjan offers the only solution that blocks complex attacks at these levels and delivers best defense against unknown Viruses, Worms, Trojans and Spyware.

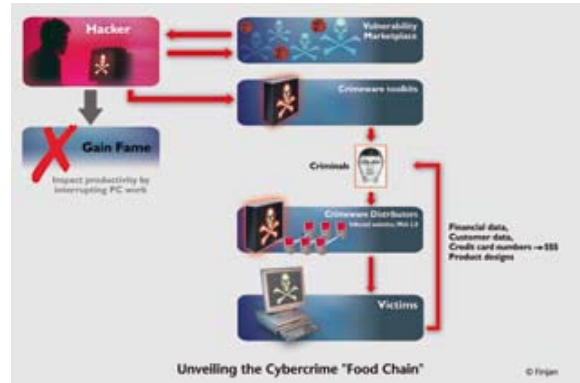
Finjan's Solution Highlights

- Detects and prevents Crimeware and Web 2.0 attacks despite the advanced propagation techniques and anti-forensic methods (code obfuscating, evasive attacks, random files names and URLs) being used
- Analyzes each and every piece of incoming and outgoing Web content in real time, regardless of its originating URL and without signature-matching
- Deep code analysis and true type detection reveal malicious combinations of individually innocent functions. Inspects all inbound and outbound content including HTTP/HTTPS content
- Transparent handling of Web traffic reduces transmission costs and downloading time
- Wizard-driven security policy decision-making system with a single-click rules refinement enhancement
- Integrated dashboard provides instant information on the system's performance and its risk level, using an extensive set of graphs and views for quick and accurate insight
- Supporting Cisco WCCPv2 to ensure interoperability with various Cisco systems
- External reporting and logging system provides a flexible and scalable data analysis platform for internal use, audits, and compliance requirements
- Assistance in complying with regulations such as SOX, HIPAA, FISMA, GLBA and PCI DSS
- For increased Web 2.0 and productivity control, URL filtering engines from IBM Proventia Web filtering and Websense are available as an extra option

The Business Impact of Crimeware

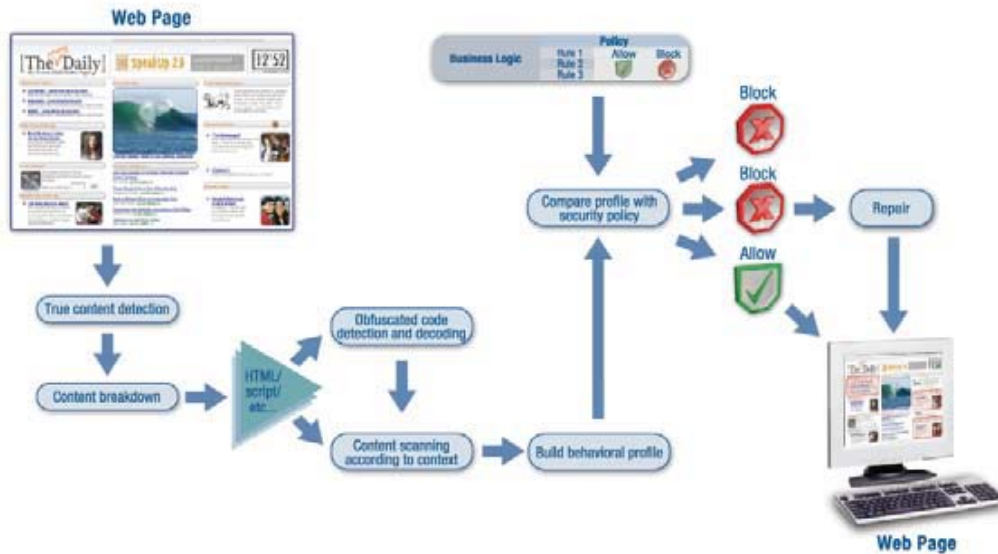
Enterprises and organizations are becoming more and more dependent on the Web for online business applications, access to information, and communication with the public. This offers cybercriminals lots of opportunities to invisibly inject and propagate malicious code. Enterprises, corporations, organizations and governmental agencies alike realize that they need to adopt a security strategy that protects their network systems and data from malicious content.

Today's cybercriminals use sophisticated Web-based attacks specifically designed to hit the "blind spots" of traditional security systems that rely on signatures or databases (such as anti-virus, URL filtering and reputation based security). Professional hackers use sophisticated Crimeware to evade signature- and database-reliant security tools. More and more enterprises realize that active real-time content inspection is needed to face today's sophisticated web threats.



Finjan's Active Real-Time Content Inspection

Finjan's Vital Security™ with active real-time content inspection technology achieves the highest rate of malicious code prevention. Finjan's secure web gateway solution analyzes each and every piece of incoming and outgoing Web content in real-time, regardless of its original source, and understands its potential effects before it executes itself. By understanding the true intent of Web content, Finjan's active real-time content inspection technology detects and prevents Crimeware despite the propagation techniques and anti-forensics methods in use. This prevents any malicious Web content from entering or exiting the corporate network, thus protecting enterprises from Crimeware that may result in severe business damage.



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, 63533892, 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.