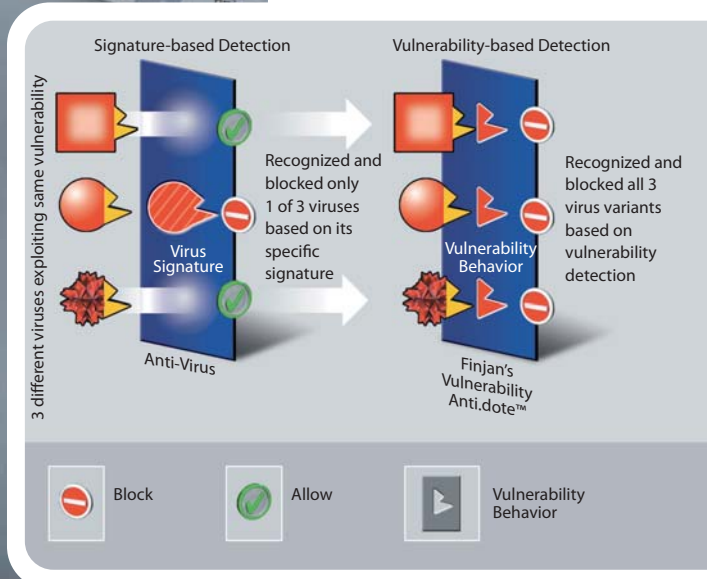


Vulnerability Anti.dote™



Vulnerability-based vs. Signature-based Detection

Zero-Hour Protection Against Known Vulnerabilities

The latest generation of sophisticated malware, including Crimeware, Web 2.0 attacks, Spyware, Trojans and blended threats, exploit vulnerabilities (such as software flaws and security holes) in standard software to deliver payloads that cause major damage to organizations and enterprises.

Enterprise vendors need time to develop a patch, which creates a Window-of-Vulnerability™ (the time between the exploit and availability of the patch against it).

According to Symantec, the window of exposure was 55 days during the first half of 2007. This was based on an average exploit development time of 5 days and an average patch development time of 61 days. The enterprise window of exposure during the second half of 2006 was 47 days.

This leaves organizations and enterprises vulnerable to cybercriminals out to steal their valuable personal, financial and business data.

With the multitude of operating systems, service packs, applications and security settings each organization has to maintain, IT managers are under constant pressure to patch their systems at the same rate that new vulnerabilities are discovered. To address this need, Finjan provides them with its Vulnerability Anti.dote solution. It is an integral part of Finjan's Vital Security™ Web Appliances.

Vulnerability Anti.dote™

Vulnerability Anti.dote provides an optimal balance between powerful proactive security and minimal patch management overhead. Based on Finjan's extensive knowledge of new software vulnerabilities, Finjan's security experts at its Malicious Code Research Center (MCRC specializes in research, analysis and detection of web threats) create behavioral rules that enable the Vulnerability Anti.dote scanning engines to identify and block content that tries to exploit one or more vulnerabilities. This enables you to immunize all your desktops from vulnerabilities without having to constantly issue emergency patches. It therefore reduces the resources required for patch management. It also allows you to benefit from Finjan's early discovery of new software vulnerabilities.

Solution Highlights

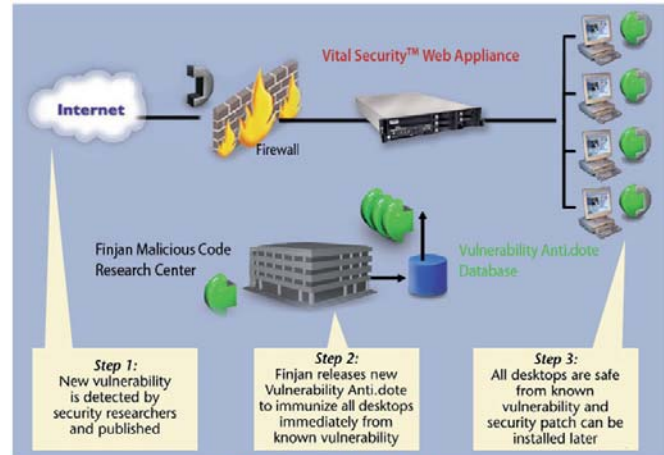
- Protects your company from the next virus/exploit outbreak
- Blocks any attack trying to exploit the known vulnerabilities as well as their variants
- Utilizes extensive databases of known and newly discovered vulnerabilities, which is constantly updated by Finjan's Malicious Code Research Center (MCRC)
- No need to worry about frequent patches
- Automatic update mechanism for new vulnerabilities, including "hot updates" pushed out by Finjan as required
- Optimal balance between proactive behavior-based security and minimal management costs

How It Works

Vulnerability Anti.dote utilizes a multi-layered rule-based engine that can "understand" HTML, scripts and other program components that compose HTTP-based content, at a level similar to compiler analysis. Finjan's MCRC experts create detailed rules that capture the essence of the various possible vulnerabilities in browser applications, Windows operating system and services, and other applications that can be accessed by Active Content such as FTP, Windows Media Player, etc. Based on these behavioral rules, Finjan's web scanners detect any attempt to exploit one or more vulnerabilities and block such content from entering your network.

Vulnerability Anti.dote technology represents an optimal balance between powerful proactive web security and minimal patch management overhead. Based on Finjan's knowledge of new software vulnerabilities, Finjan's security experts create behavioral rules that enable the Vulnerability Anti.dote scanning engines to identify and block content that tries to exploit one or more vulnerabilities.

New rules are included in Finjan's security updates which are installed transparently in all of Finjan's deployed appliances. This enables an organization to immunize all desktops from vulnerabilities without having to constantly roll out emergency patches, reducing the resources required for patch management. It also allows you to benefit from Finjan's early discovery of new software vulnerabilities.



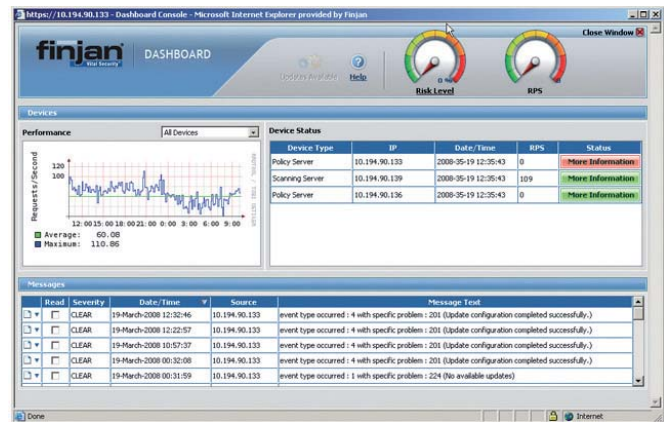
Virtual Patching - How It Works

Ongoing Research of New Vulnerabilities

Finjan's renowned MCRC team specializes in the discovery and analysis of new vulnerabilities or combinations of operations that can constitute a malicious attack. Each year Finjan reports dozens of high risk vulnerabilities to leading software vendors around the world. MCRC analyzes the vulnerabilities and creates the rules that feed Finjan's Vital Security Web Appliances, enabling the identification of any inbound or outbound web content that may try to exploit a given vulnerability.

Ease of Management

Vulnerabilities are logically arranged into categories, for ease of management. Vulnerability Anti.dote is managed using the unified, web-based Vital Security™ management console.



Management of Vulnerability Anti.dote™ Rules

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



NG-8100



NG-6100



NG-5100

© 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.dote, 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.