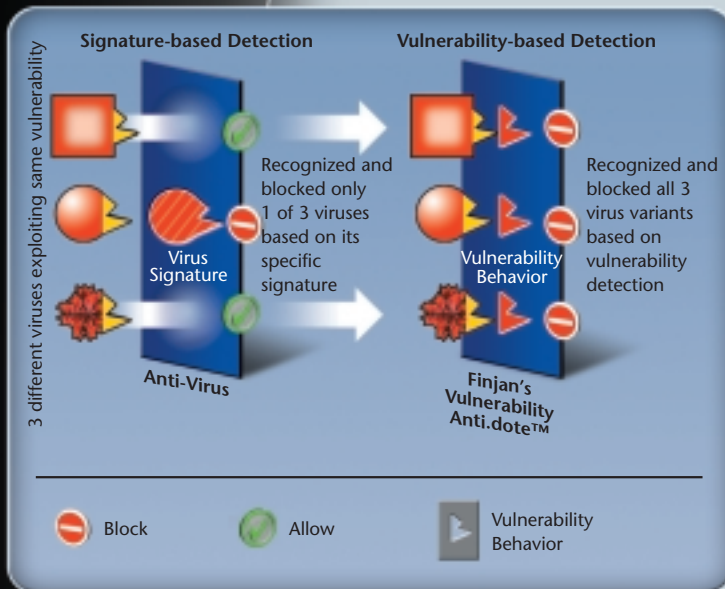


## Vulnerability Anti.dote™

“Virtual Patching” to End Businesses' Patch Management Headaches



### Proactive Protection Against Known Vulnerabilities

The new generation of sophisticated malware, including Spyware, viruses, worms, Trojans and blended threats, exploit vulnerabilities (i.e., software flaws, security holes) in standard software to deliver payloads that cause major damage to enterprises' business operations. Carnegie Mellon University's CERT Coordination Center states that the number of vulnerabilities each year has been doubling since 1998. **Gartner reports that over 90% of the security exploits are carried out through vulnerabilities for which there are known patches (Lynda McGhie, Secure Business Quarterly).**

Remember the Memail worm that wreaked havoc worldwide in August 2003? It was exploiting an Internet Explorer vulnerability, published in August 2002, for which Microsoft released a patch in April 2003. Memail attacked four months after the patch's release and a full 12 months after proof-of-concept!

The explanation for this phenomenon is simple: organizations cannot patch their systems at the rate that new vulnerabilities are discovered. This opens the classic Window-of-Vulnerability™ that leaves enterprises exposed to malware attacks for intolerably long periods of time, resulting in significant financial and Denial of Service losses.

### Vulnerability Anti.dote™ Enables "Virtual Patching" Automatically

Finjan's breakthrough **Vulnerability Anti.dote™** offers 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. This enables you 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.

### Key Highlights

- Protects you before the next virus/exploit outbreak, based on known vulnerabilities in any mainstream software system (e.g., Microsoft, Netscape)
- Frees you of the need to worry about frequent patches
- Utilizes extensive database of known and newly discovered vulnerabilities, constantly updated by Finjan's Malicious Code Research Center (MCRC) - a group of world-class security experts dedicated to keeping Finjan's customers steps ahead of the hacker community
- Virtually eliminates false positives for optimal transparency and user productivity
- Breakthrough technology blocks any potential attack based on the known vulnerability as well as its variants
- Automatic update mechanism ("virtual patches") for new vulnerabilities, including "hot updates" from Finjan as required
- Optimal balance between proactive behavior-based security and minimal management costs

### How Vulnerability Anti.dote™ Works

**Vulnerability Anti.dote** security scanning utilizes a multi-layered rule-based engine that can "understand" HTML, scripts and other programmatical components that make up 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 and email 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 scanners detect any attempt to exploit one or more vulnerabilities and block such content from entering your network. These rules enable the scanners to identify a wide range of possible attacks that will inevitably try to exploit a given vulnerability.



finjan software

## Ease of Management

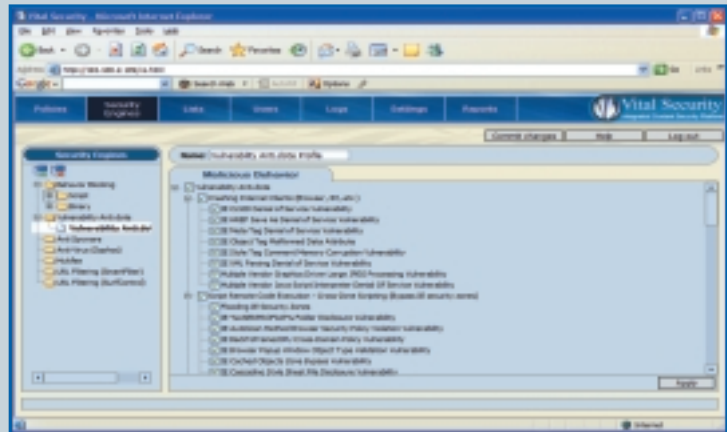
Vulnerabilities are logically arranged into categories, for ease of management. **Vulnerability Anti.dote** is managed using the unified, web-based Vital Security™ management console.

## Complete Protection Against the Most Dangerous Types of Malware Attacks

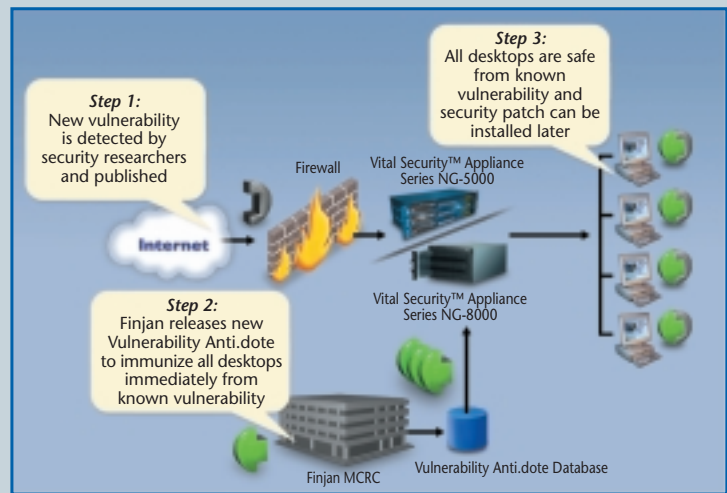
**Vulnerability Anti.dote** provides Day-Zero protection against known vulnerabilities in mainstream operating systems and applications that could be exploited by unknown viruses, spyware and other dangerous forms of malware. **Vulnerability Anti.dote** proactively protects against spoofing attacks, phishing attacks, denial of service attacks, silent "drive-by" installations of spyware, and remote code execution attacks, among others.

## Ongoing Research of New Vulnerabilities

Finjan's renowned MCRC team specializes in the discovery and analysis of new vulnerabilities, i.e., any security hole, bug, maligned feature or combination of operations that can constitute a malicious attack. In the second half of 2004 alone, Finjan reported dozens of high risk vulnerabilities to Microsoft and other software vendors. MCRC analyzes the vulnerabilities and creates the rules that feed Finjan's Vital Security™ scanners, enabling the identification of active content that may try to exploit a given vulnerability, keeping Finjan's customers a step ahead the next Internet attack and vulnerability exploit.



Management of Vulnerability Anti.dote™ Categories



Virtual Patching - How It Works

# Finjan - the Number 1 Name in Security.

### For Additional Information

For more information, please visit [www.finjan.com](http://www.finjan.com) or contact our regional offices:

#### San Jose, USA

2025 Gateway Place, Suite 180 San Jose, CA 95110, USA  
Toll Free: 1 888 FINJAN 8 (1 888 346 5268)  
Tel: +1 408 452 9700 Fax: +1 408 452 9701

#### New York, USA

420 Lexington Avenue, 24th Floor, Suite 2400,  
New York, NY 10017, USA  
Toll Free: 1 888 FINJAN 8 (1 888 346 5268)  
Tel: +1 408 452 9700 Fax: +1 408 452 9701

#### United Kingdom

4th Floor, Westmead House, Westmead  
Farnborough, GU14 7LP, UK  
Tel: +44 (0)1252 511118 Fax: +44 (0)1252 510888

#### Germany

Haidgraben 2, 85521 Ottobrunn, Munich, Germany  
Tel: +49 (0)89 673 5970 Fax: +49 (0)89 673 597 50

#### Asia Pacific

2 Karikal Lane, Singapore 427086  
Tel: +65 67415289 Fax: +65 68421327

#### Israel

Hamachshev St. 1, New Industrial Area, Netanya,  
42504, Israel  
Tel: +972 (0)9 864 8200 Fax: +972 (0)9 865 9441

## Finjan's Family of Next Generation Internet Security Solutions for Businesses of All Sizes

Small & Medium-Sized Business Solutions	Mid-Range Enterprise Solutions	Large Enterprise Solutions
		
<b>1Box™ Series</b>	<b>Vital Security™ Appliance Series NG-5000</b>	<b>Vital Security™ Appliance Series NG-8000</b>

© Copyright 2005. Finjan Software group of companies. All rights reserved.

All text and figures included in this publication are the exclusive property of Finjan Software 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 Software. Information in this document is subject to change without notice and does not present a commitment or representation on the part of Finjan Software. The Finjan Software technology and/or products and/or software described and/or referenced to in this material are protected by registered and/or pending patents including U.S. Patents No. 6092194, 6154844, 6167520, 6480962, 6209103, 6298446, 6353892 and 6804780. Finjan, Finjan logo, Vital Security, Internet 1Box, SSL 1Box, Documents 1Box, Vulnerability Anti.dote and Window-of-Vulnerability are trademarks or registered trademarks of Finjan Software, Inc., and/or its subsidiaries. SurfControl is a registered trademark of SurfControl plc. Sophos is a registered trademark of Sophos plc. Mailshell is a trademark of Mailshell Inc. Microsoft and Microsoft Office are registered trademarks of Microsoft Corporation. All other trademarks are the trademarks of their respective owners. 01/2005.