

Day-Zero Defense

Secure Content
Management

Viruses, Worms, Trojans

Vital Security™ Appliance Series NG-5000

For Mid-Range Enterprises

Application-Level
Behavior Blocking

Enterprises
and SMBs

Spyware

Phishing

Active Content
Security

Malicious Mobile Code



finjan
software



Zero-Virus Security for Internet Traffic

Revolutionary security solution on a high performance, scalable and high availability appliance lets enterprises forget about security and focus on business

High-Performance
Appliances

Next Generation Internet Security - Today

Unbeatable Security with "Zero-Virus Infection - Guaranteed" Policy

The Vital Security™ Appliance Series NG-5000 is Finjan's Next Generation Internet Security Offering, comprising an advanced set of robust, hardware-based security solutions for enterprises. Building on a decade of experience as the leading technology innovator in the proactive content security space, this new platform further improves upon Finjan's unmatched security, while enhancing system performance, usability and flexibility through a powerful set of web-based management tools. Finjan's Series NG-5000 gives enterprises the world's best Internet security solution in a high performance, scalable and high availability hardware platform. This total and unbeatable security is backed up with an unprecedented "Zero-Virus Infection - Guaranteed" policy.

Comprehensive Security Offering

Vital Security Appliance Series NG-5000 includes, among others, the following key security components:

- Next Generation Application-Level Behavior Blocking for detection and blocking of unknown attacks
- Vulnerability Anti.dote™ for protection against known software vulnerabilities
- Anti-Spyware for stopping costly spyware attacks at the enterprise gateway before they infiltrate your computers
- Best-of-breed Anti-Virus engines for protection against known viruses
- Best-of-breed URL Filtering engines for full control over your organization's web browsing
- Market-leading Anti-Spam engine* for increased user productivity

Key Highlights

- Patented Next Generation Application-Level Behavior Blocking, Vulnerability Anti.dote, and Anti-Spyware provide Day-Zero defense against unknown malicious code, Spyware, Phishing, viruses, worms, and Trojans
- "Zero-Virus Infection - Guaranteed" policy gives you the peace of mind to focus on business
- High performance solution supports up to 20,000 users
- Scalable and modular architecture enables enterprises to scale up cost-effectively to meet expanding needs without increasing management overhead
- Centralized web-based management and single point of provisioning for reduced TCO
- High Availability features, including Security Load Balancer (optional) and cached configurations and policies, ensure zero downtime
- ICAP standard compliance allows interoperability with third party proxies (e.g., Cisco, NetApp, Blue Coat) and appliances
- Detects malicious content in SSL-encrypted traffic and enforces SSL certificates

* Finjan's next generation email scanner will be available later in 2005

Centralized Web-Based Management for Reduced TCO

The entire system can be managed via one unified management console, minimizing management overhead and provisioning times for large enterprises with multiple and geographically distributed sites. Security policy is set by the system administrator for all appliances, regardless of their physical location, from the central management console. Communication with the remote offices is performed over a secure HTTPS connection.

Flexible Policy Management to Meet Business Needs

Series NG-5000 provides enterprises with optimal granularity in the creation of security policies, based on a highly flexible rule-based engine. Each rule defines a set of criteria and an action to take for each piece of content that matches these criteria. Using an intuitive management console, system administrators can create highly granular policies regarding the content/access allowed or forbidden for any single user or group of users.

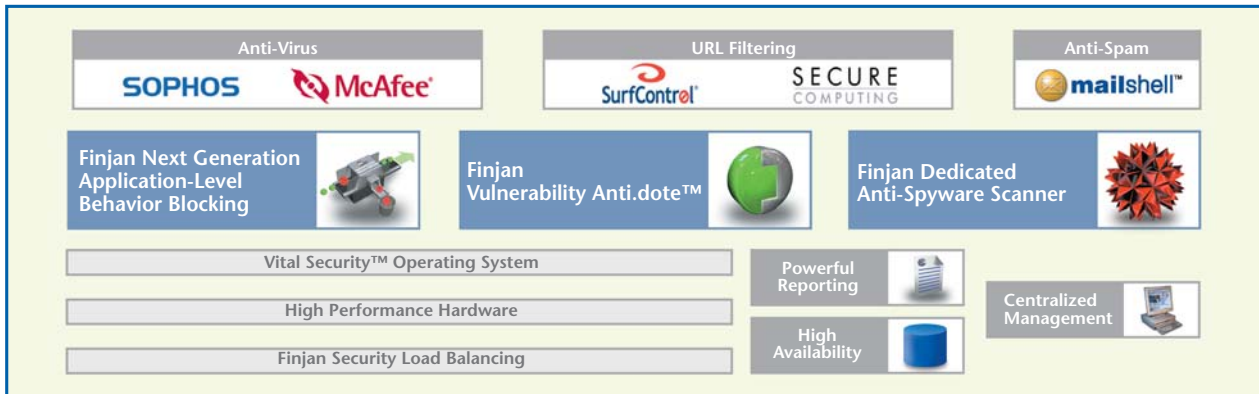
Enhanced Content Management Capabilities Enable Granular Security Policies

Series NG-5000 provides powerful content management capabilities, enabling the creation of granular policies based on customized URL lists, active content lists, file size, direction (incoming/outgoing), time and day, and more. This rule-based approach utilizes powerful synergies between the system's scanning engines and content management capabilities. For example, a rule can be defined to block incoming executable files unless they come from Microsoft Windows Update URLs, or to prevent uploads of Microsoft Office documents to Webmail sites (e.g., YahooMail, Hotmail)

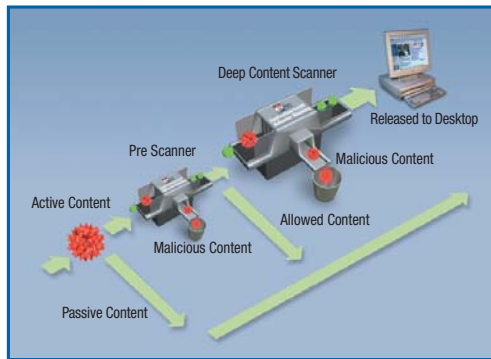
Hardened Vital Security™ Operating System (VSOS)

Series NG-5000 includes its own operating system, based on a hardened, secure version of Linux. VSOS is specially configured and optimized to deliver the highest possible performance. Updates to VSOS are performed as an integral part of the Vital Security automatic update mechanism, eliminating the need for OS patch management.

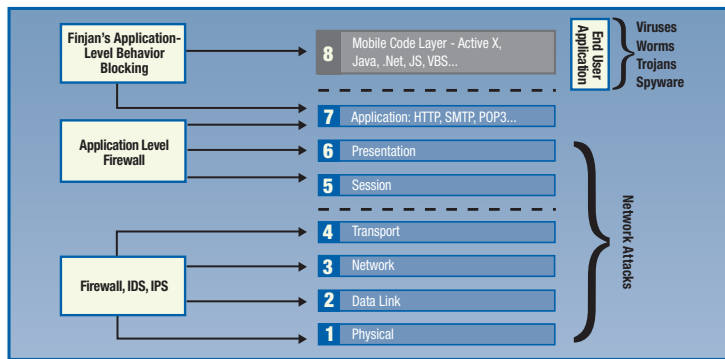




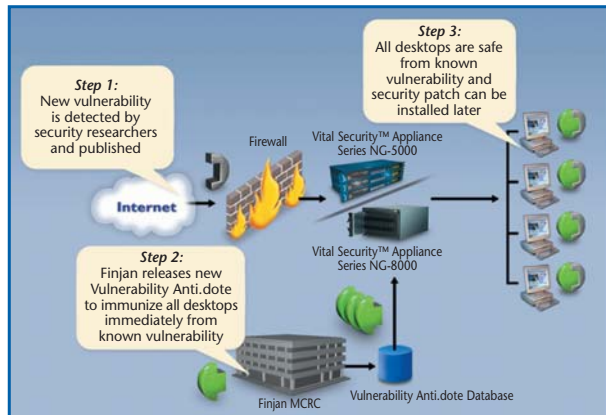
Vital Security™ Appliance Series NG-5000 Solution Architecture



Two-Step Scanning for Enhanced Performance

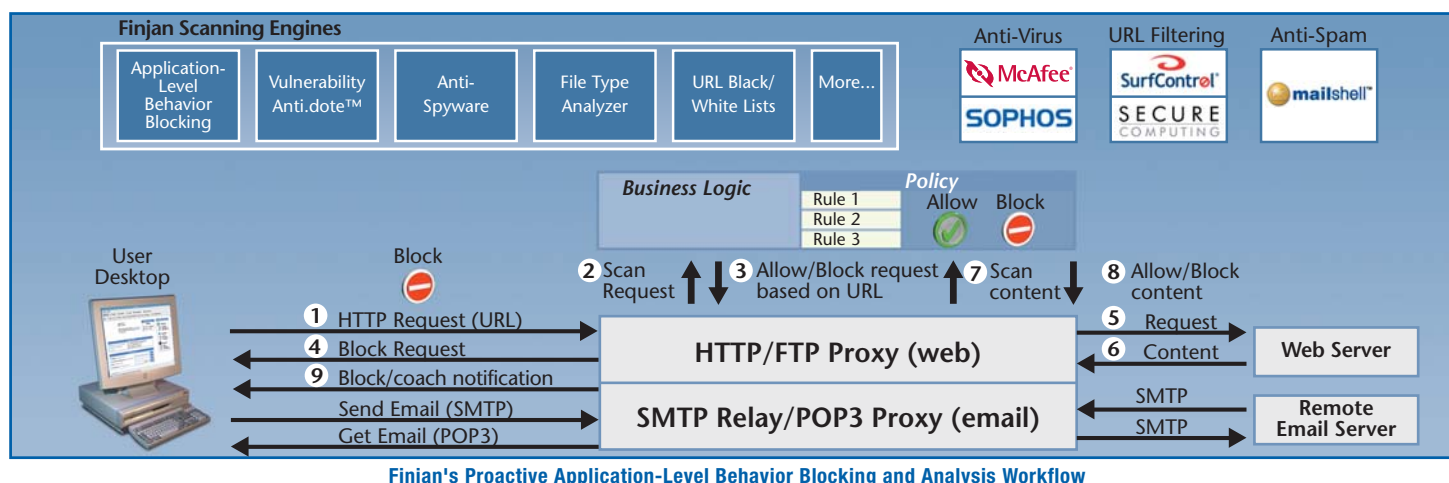


Viruses, Trojans, Worms and Spyware operate at Layers 7 and above (Layer 8). Next Generation Application-Level Behavior Blocking is the only solution that blocks complex attacks at these levels and delivers best defense against unknown Viruses, Worms, Trojans and Spyware.

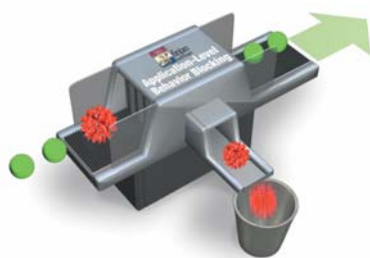


Vulnerability Anti.dote™ Virtual Patching

Zero-Virus Infection - Guaranteed! Policy



Finjan's Next Generation Application-Level Behavior Blocking Keeps You a Step Ahead of the Next Unknown Internet Attack



The Window-of-Vulnerability™ is the period of time from when a new virus outbreak first occurs, until an update or patch is delivered. Because reactive, signature-based solutions depend on database updates for each new virus, they cannot

protect against new, unknown attacks. This leaves enterprises exposed and vulnerable for hours and sometimes days, before anti-virus updates reach the end user. The potential damage to your business - DoS, productivity loss, downtime and recovery costs - is significant. Instead of relying on reactive virus database updates, Finjan's **Series NG-5000** uses patented Next Generation Application-Level Behavior Blocking technology to determine the behavior that a given piece of content will exhibit when loaded into the target application, e.g., a web browser or email program. Complex attacks, such as Spyware, easily elude packet level inspection solutions, e.g., firewall, intrusion detection and intrusion prevention systems, which cannot identify application-level behavior. Finjan's unique Application-Level Behavior Blocking technology is the **ONLY solution** on the market that can stop **known and unknown** threats at the gateway, before they enter your network.

Vulnerability Anti.dote™ - "Virtual Patching" Puts an End to Your Patch Management Headaches



This revolutionary technology protects you against known vulnerabilities without patches, giving you an **optimal balance between powerful proactive 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. It allows an organization to protect itself against browser and operating system vulnerabilities without having to constantly roll out emergency patches, reducing the resources required for patch management.

Intelligent Spyware Prevention at the Gateway

Finjan's dedicated Anti-Spyware solution combines Application-Level Behavior Blocking, URL lists and Active Content profiles to block known and unknown spyware at the gateway. By identifying spyware by its behavior, Finjan provides the **ONLY** gateway based Anti-Spyware solution capable of stopping unknown spyware before it infiltrates your network.

Comprehensive, Best-of-Breed Solution for Round-the-Clock Security

Integrating Finjan's patented Application-Level Behavior Blocking technology with your choice of best-of-breed anti-virus (McAfee®, Sophos®), URL filtering (SurfControl®, Secure Computing®) and anti-spam (Mailshell™) engines, Finjan's layered solution provides enterprise users with superior protection against malicious and inappropriate content.



Cost-Effective, Easy-to-Deploy Appliance

The system is easy to deploy and maintain, supporting simple "appliance on a CD" setup. An auto-update mechanism downloads system software, Finjan security updates and third party anti-virus signatures to appliances across the network from a single point of provisioning. **Series NG-5000** seamlessly integrates with your network and requires only one interaction with the device to be up and running.

X-Ray Mode



X-Ray mode is a unique feature that allows enterprises to test new rules in off-line mode (on live traffic), before actually applying the rule. Rules activated in X-ray mode are transparent to users, but create a log entry. This allows the administrator to ensure that a proposed policy change would not have unforeseen effects on the organization or constrain business operations.

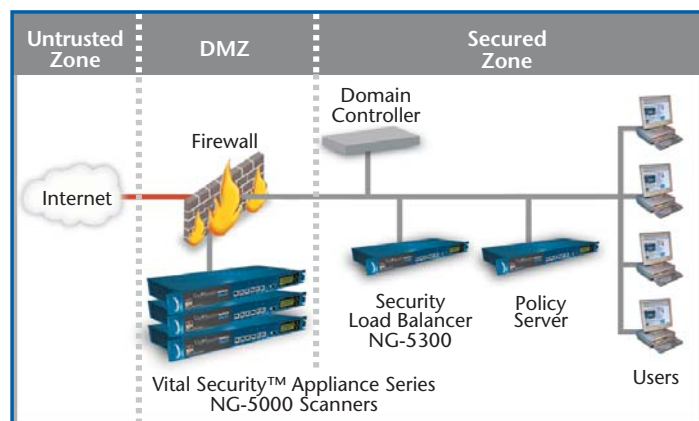
Next Generation Internet Security - Today

Customized Logging and Reporting for Immediate Access to Network Information

An advanced logging and reporting mechanism offers enterprises free choice between over 100 predefined reports or user defined reports that may be generated on known information (e.g., list, actions, transactions, policy, rule, filter, etc). Scanners accumulate transaction information and download to a central logging server. The extensive reporting and logging capabilities provide IT managers with easy access to critical operational information.

High Availability to Ensure Zero Downtime

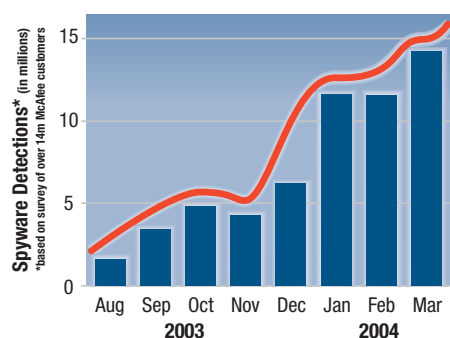
Vital Security Appliance Series NG-5000 includes an optional high availability load sharing mechanism using Finjan's powerful Security Load Balancer (Vital Security Appliance NG-5300). The high availability mechanisms are transparent, providing users with seamless security and allowing your company to conduct business as usual. In the event that a Finjan scanner goes offline for maintenance or other reasons, the Security Load Balancer seamlessly routes traffic to the other online scanners, allowing users to continue business as usual. Even if the Policy Server goes offline, the scanners continue to operate normally using cached configuration and policies, as well as storing logs locally.



High Performance Architecture

Global Customer Support Maximizes Your Security Investment

Finjan offers a range of comprehensive technical support services and plans which further maximize system availability. Finjan's premier Gold Plan, for example, includes unlimited telephone support on a 24x365 basis, dedicated technical support engineer, maintenance releases, product upgrades, and automatic updates.



Spyware Detections

Flexible Licensing for Best Price

Finjan offers a flexible pricing model designed to allow each enterprise to build an integrated package based on its specific needs. This model is based on separately licensable modules, including Application-Level Behavior Blocking, Vulnerability Anti.dote, and Anti-Spyware, as well as the optional Security Load Balancer and third-party anti-virus, URL filtering and anti-spam engines. The licenses include discount mechanisms for multi-year subscriptions and for large quantities of users, to accommodate your company's growth in the simplest possible manner.

Stay a Step Ahead of the Next Spyware, Phishing or Malicious Code Attack

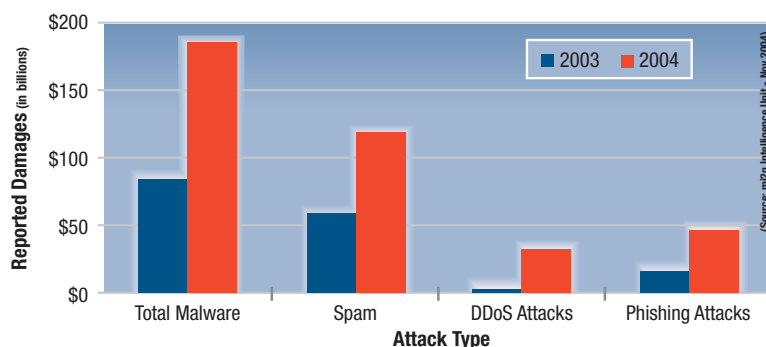
The increasing sophistication and frequency of malware attacks are a growing concern for enterprises. These malicious attacks have a direct impact on businesses' bottom line, resulting in a massive loss of valuable time and resources, reduced productivity and lost revenue.

Reactive, signature-based security solutions, such as anti-virus, firewall and intrusion protection, are only as good as the last known virus. This exposes your organization to dangerous attacks from unknown viruses, as well as new types of malware such as Spyware, Phishing and malicious code.

More likely than not, spyware has already infected your company's computers. It is estimated that close to 90% (US National Cyber Security Alliance) of the world's computers are infected with spyware/adware, resulting in major losses of productivity and often compromising confidential information. Finjan's dedicated Anti-Spyware solution, available with the Series NG-5000, is the ONLY solution capable of combating spyware effectively before it enters your network. Using Finjan's patented Application-Level Behavior Blocking, Series NG-5000 detects malicious and inappropriate behavior of code arriving via the web, hence stopping activities performed by unknown spyware that existing anti-spyware solutions do not yet recognize.

Phishing is one of the fastest growing scams on the Internet, compromising the personal details of millions of users worldwide. Finjan's Series NG-5000 solutions provide superior protection against phishing attacks by identifying the active content that tries to copy the user's personal information and blocking it at the enterprise gateway.

Finjan's security solutions proactively detected and blocked 100% of the viruses in the monthly Sophos top 10 lists in 2004.



Worldwide Economic Damage from Malware

The Best and Most Comprehensive Internet Security in a High Performance, Scalable and High Availability Appliance

Technology	Solution	Benefit
Patented Next Generation Application-Level Behavior Blocking	Proactively protects networks against Internet threats by determining actual code behavior and blocking any action that violates corporate security policies	ONLY solution on market that can identify the "true" behavior of active content and protect against unknown threats
Vulnerability Anti.dote	Identifies and blocks content that tries to exploit known software vulnerabilities	Immunizes all desktops from vulnerabilities without the need for constant patch management
Anti-Spyware Protection	Uses Application-Level Behavior Blocking, Active Content behavior profiles and URL lists to stop spyware at the gateway	ONLY gateway solution that operates at application-level to block unknown and known spyware before it infiltrates your network
Anti-Virus Protection (McAfee, Sophos)	Detects and catches known viruses attempting to enter the network via web or email based on their signatures	Brand-name line of defense against known viruses
URL Filtering and Content Control (SurfControl, Secure Computing)	Filters web traffic based on content category, specific URL and time of day	Full control over web content entering network for improved productivity and network performance
Anti-Spam Protection (Mailshell)*	Detects and blocks incoming email spam messages	Improves productivity and reduces potential for malicious attacks via email, such as rapidly growing phishing attacks
Flexible Policy Management	Rule-based engine with intuitive GUI for creation of security policies	Enables granular security policies per user or group of users
Customized Reporting and Logging	Over 100 standard reports, customizable user-defined reports, and full logging tailored to the needs of enterprises	Empowers organizations to monitor ROI and trends, and to accurately adjust security policies as their company grows
Full ICAP Standard Compliance	Interoperable with third party proxies (e.g., Cisco, NetApp, Blue Coat) and appliances	Increased performance and flexibility in deployment with existing network devices
Integrated support for SSL/HTTPS traffic (with NG-5400)	Detects malicious content in SSL-encrypted traffic and enforces SSL certificates	Protects your users from encrypted threats in webmail and other SSL traffic
High Availability	Optional Security Load Balancer + hot swap mechanism for all critical components based on their signatures	Optimized system performance and continuous operations
High Performance hardware	Up to 5,000 users per appliance	Ensures reliable and efficient operations
Scalability	Add scanner blades as needed to appliance chassis	Enables cost-effective scaling to meet expanding needs
"Hardened" Vital Security Operating System (Linux based)	Ensures that appliance is secure "out of the box", optimized for highest performance, and supports automated updates	Rapid and error-free installation with minimum IT involvement

* Finjan's next generation email scanner will be available later in 2005

Hardware Performance Specifications

Memory	1GB	Fast Ethernet NIC	4
Disk	160GB	Built-in LCD display	1
CPU	Pentium IV 2.8GHz	Maximum users per appliance	5,000
Rack space (1U)	428.6 x 360 x 44 mm (WxDxH) 16.9 x 14.1 x 1.7 inches (WxDxH)	Throughput	20Mbps
Gigabit Ethernet NIC	2	Maximum Cluster Size	10

For Additional Information

For more information, please visit 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 - the Number 1 Name in Security.

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
		
1Box™ Series	Vital Security™ Appliance Series NG-5000	Vital Security™ Appliance Series NG-8000

© 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. Q1/2005.