

Day-Zero Defense

Secure Content  
Management

Viruses, Worms, Trojans

# Vital Security™ Appliance NG-1100

for Small and Medium-sized Businesses

Application-Level  
Behavior Blocking

Enterprises  
and SMBs

Spyware

Phishing

Active Content  
Security

Malicious Mobile Code



finjan  
software



## Zero-Virus Security for Web Traffic

Revolutionary security appliance proactively protects SMBs against the next unknown Internet attack

High-Performance  
Appliances

# Next Generation Internet Security - Today

## Unbeatable Security with “Zero-Virus Infection - Guaranteed” Policy



Vital Security™ Appliance NG-1100 is Finjan's Next Generation web security platform for small and medium-sized businesses (SMBs). 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 unbeatable security, while enhancing system performance, usability and flexibility through a powerful set of web-based management tools. NG-1100 gives SMBs the world's best and most comprehensive web security solution in an all-in-one, easy to install and “self-managing” appliance. This total and unbeatable security is backed up with an unprecedented “Zero-Virus Infection - Guaranteed” policy.

## Comprehensive Security Offering

NG-1100 is designed to allow each SMB to build an integrated solution based on its specific needs. The following licensable modules are available:

- **Next Generation Application-Level Behavior Blocking** for detection and blocking of unknown attacks
- **Vulnerability Anti.dote™** for protection against known software vulnerabilities through “virtual patching”
- **Anti-Spyware** for stopping costly spyware attacks at the gateway before they infiltrate your computers
- Integrated best-of-breed **Anti-Virus** engines (McAfee®, Sophos®) for protection against known viruses
- Integrated best-of-breed **URL Filtering** engines (SurfControl®, Secure Computing®) for full control over your organization's web browsing

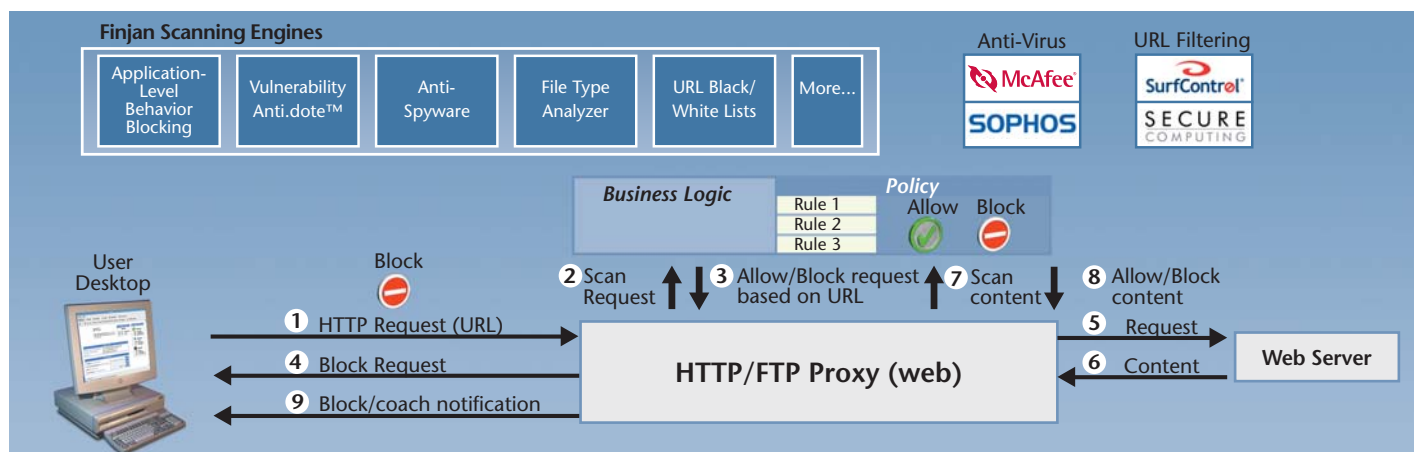
## Key Highlights

- Patented **Next Generation Application-Level Behavior Blocking, Vulnerability Anti.dote, Anti-Spyware and Anti-Virus** provide Day-Zero defense against unknown malicious code, Spyware, Phishing, viruses, worms, and Trojans
- **All-in-one, cost-effective solution**, including Anti-Virus and URL Filtering, eliminates need for integration efforts
- “**Zero-Virus Infection - Guaranteed**” policy gives you the peace of mind to focus on business
- **Easy deployment and automatic updates** reduce total cost of ownership
- **Seamless integration** with your existing network systems
- **Centralized web-based management** reduces overhead and accelerates provisioning
- **ICAP standard compliance** allows interoperability with third party proxies (e.g., Cisco, NetApp, Blue Coat) and appliances
- **Integrates with Finjan's SSL solution** to protect against malicious content in SSL-encrypted traffic

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

Traditional security solutions, such as anti-virus, firewall and intrusion detection/prevention, are only as good as the last known virus. This exposes your business to dangerous attacks from unknown viruses, as well as new types of malware such as spyware, Phishing and malicious code.

Finjan's NG-1100 uses patented Next Generation Application-Level Behavior Blocking to determine the behavior that a given piece of content will exhibit when loaded into the target application, e.g., web browser. It is the only technology on the market that can stop both **known and unknown** threats at the gateway, before they enter your network. Finjan's best-in-class technology saves your business time and money, and lets you avoid the IT headaches associated with security incidents.

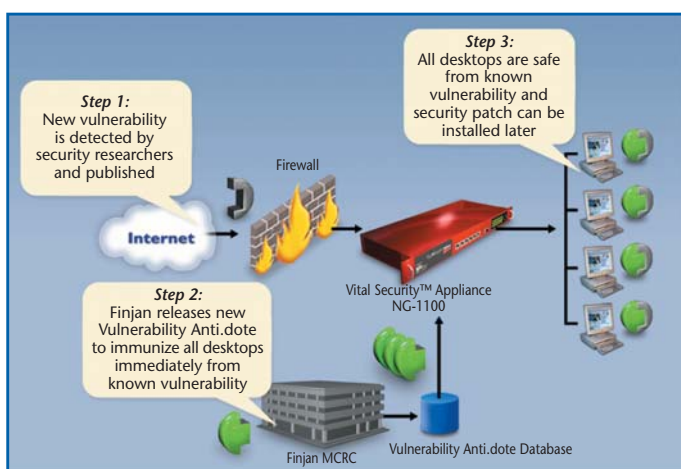


Finjan's Proactive Application-Level Behavior Blocking and Analysis Workflow

# Industry-First Zero-Virus Infection Guarantee

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

This revolutionary technology protects you against known vulnerabilities without frequent patches, giving you an optimal balance between powerful proactive web security and minimal patch management overhead. Based on 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.



Virtual Patching - How It Works

## Intelligent Spyware Prevention at the Gateway



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 Anti-Spyware solution, available as part of the NG-1100, identifies known and unknown spyware by behavior and blocks it at the gateway. It also detects spyware already on your computer, blocks it from "calling home" and provides identification details for cleanup.

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

Integrating Finjan's patented Application-Level Behavior Blocking technology, Vulnerability Anti.dote and Anti-Spyware with your choice of best-of-breed Anti-Virus (McAfee, Sophos) and URL Filtering (SurfControl, Secure Computing) engines, Finjan's layered solution provides SMB users with superior protection against malicious and inappropriate content.



## Flexible Policy Management to Meet Dynamic Business Needs

NG-1100 provides SMBs with optimal granularity in the creation of security policies, based on a highly flexible rule-based engine. 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.

## Hardened Vital Security™ Operating System (VSOS)

NG-1100 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.

## Centralized Web-Based Management

The entire system, including the integrated third party Anti-Virus and URL Filtering engines, is managed via one unified web-based management console, minimizing overhead and provisioning times. The centralized Vital Security™ management console features a web-based GUI with intuitive icons, navigation trees and extensive on-line help for maximum usability.

## 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 from a single point of provisioning. NG-1100 seamlessly integrates with your network and requires only one interaction with the device to be up and running.

## Customized Logging and Reporting for Immediate Access to Network Information

An advanced logging and reporting mechanism offers SMBs 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). The extensive reporting and logging capabilities provide IT managers with easy access to critical operational information.

## The Best and Most Comprehensive Web Security in a Cost-Effective Appliance

Technology	Solution	Benefit
Patented Next Generation Application-Level Behavior Blocking	Proactively protects networks against Internet threats by monitoring actual code behavior and blocking any action that violates corporate security policies	<b>ONLY</b> 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	<b>Virtual patching immunizes all desktops from vulnerabilities without the need for constant patch management</b>
Anti-Spyware Protection	Uses Application-Level Behavior Blocking, Active Content behavior profiles and URL lists to stop spyware at the gateway	<b>ONLY</b> gateway based solution that operates at the application-level to block both unknown and known spyware before it infiltrates your network
Anti-Virus Protection (McAfee, Sophos)	Detects and blocks known viruses attempting to enter the network via web	<b>Brand-name</b> line of defense and catalog of known viruses that were blocked
URL Filtering and Content Control (SurfControl, Secure Computing)	Filters web traffic based on content category, specific URL and time of day	<b>Full control over web content entering network for improved productivity and network performance</b>
"All-in-one" solution	Integrates Finjan's Application-Level Behavior Blocking, Vulnerability Anti.dote and Anti-Spyware with your choice of best-of-breed Anti-Virus and URL Filtering engines	<b>Reduces businesses' total cost of ownership and eliminates need for integration efforts</b>
Full ICAP standard compliance	Interoperable with third party proxies (e.g., Cisco, NetApp, Blue Coat) and appliances	<b>Increased performance and flexibility in deployment with existing network devices</b>
"Hardened" Vital Security Operating System (Linux based)	Ensures that appliance is secure "out of the box", optimized for higher performance; and supports automated updates	<b>Rapid and error-free installation with minimum IT involvement</b>

## Hardware Performance Specifications

Memory	1GB
Hard Drive	40GB
CPU	Pentium IV 2.4GHz
Flash Card	64 MB
Rack space (1U)	428.6 x 360 x 44 mm (WxDxH) 16.9 x 14.1 x 1.7 inches (WxDxH)
Gigabit Ethernet NIC	2
Fast Ethernet NIC	4
Built-in LCD display	1
Maximum users per appliance	250
Throughput	20Mbps
Maximum Cluster Size	10



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 and Vital Security™ Appliance NG-1100</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. Q2/2005.