

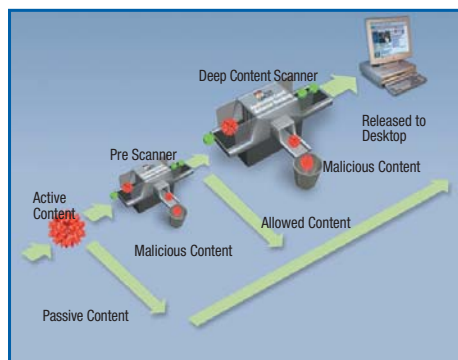
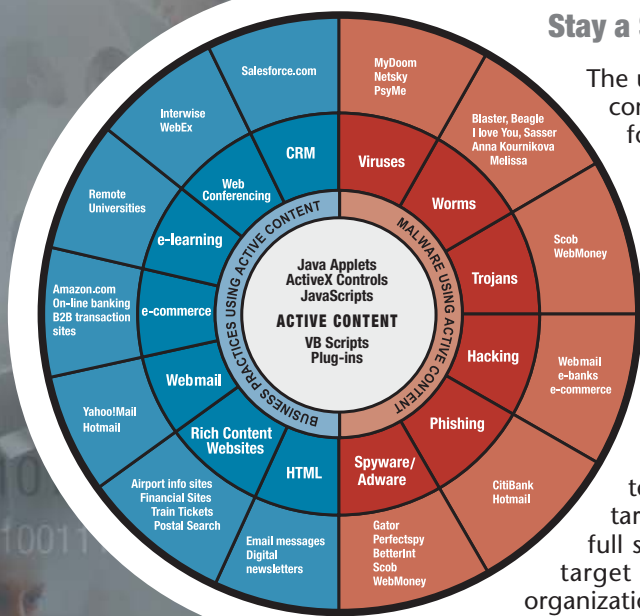
## Proactive Behavior-Based Web Security

### Stay a Step Ahead of the Next Unknown Attack

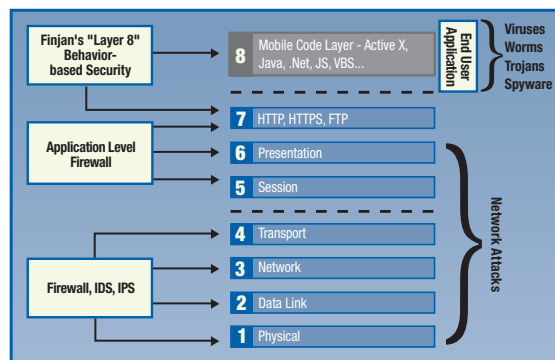
The ubiquity of Active Content technologies, such as JavaScripts, ActiveX controls, VB Scripts and Java applets, presents a difficult security challenge for enterprises. In most cases, Active Content is used for legitimate business applications such as web conferencing, e-commerce, and webmail. However, Active Content technology may also be exploited to download and execute malicious mobile code on a local system without the user's explicit knowledge or consent.

With Finjan's breakthrough and patented behavior-based technology, it's never been easier to protect your organization from **new and unknown** threats driven by Active Content, such as Spyware, Phishing, Trojans and malicious code.

Finjan's behavior-based content inspection identifies the combinations of operations, parameters, script manipulations and other exploitation techniques for a given piece of content **before** it begins to run on the target computer. By working at the application level, it determines the full set of behaviors that the content will exhibit when loaded into the target application, e.g., web browser. Then, in accordance with each organization's specific security policy, Finjan's system decides whether to pass, block or neutralize the content.



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.

### Solution Highlights

- Detects complex attacks driven by Active Content that easily elude packet level inspection solutions, e.g., firewall, intrusion detection and intrusion prevention systems
- Minimizes over-blocking so that users can leverage the web as a business tool
- Deep code analysis and true type detection reveal malicious combinations of individually innocent functions
- Near "real-time code interpretation" and cached behavior profiles for best performance
- Saves your business time and money, letting you conduct business as usual without the IT headaches associated with security incidents
- Flexible behavior-based security engine can be customized to block specific types of malicious threats, such as Spyware
- ONLY proactive web security solution that effectively combats and protects against new, unknown attacks driven by Active Content

## Keeps You a Step Ahead of the Next Unknown Attack

Enterprises realize that reactive, signature-based security solutions, e.g., Anti-Virus, are not sufficient to combat today's complex threats using myriad propagation techniques. Since these solutions require time to create and deliver a signature update to their databases, they cannot offer immediate protection against new, unknown attacks. This leaves enterprises exposed and vulnerable for hours and even days to new attacks, which can spread through corporate networks in a matter of minutes. The potential damage to your business from Spyware and other web-based threats – information and identity theft, compromised intellectual property, productivity loss, downtime and recovery costs – is significant.

Finjan's unique behavior-based technology is the **ONLY** solution that can stop **known and unknown** web threats at the gateway, **before** they enter your network.

## Breakthrough in Security and Performance

Finjan has implemented a revolutionary two-step scanning approach, consisting of pre-scanning and deep content scanning. This enables Finjan to achieve close to "real time code interpretation" for pinpoint detection of unknown viruses, Spyware and other types of malicious content. When active code is scanned, a behavior profile is generated for that code and cached. The next time the same active code enters the system, its profile can be used without having to rescan it, saving resources and boosting performance.

## Advantages over Packet-Level and Other Types of "Proactive" Solutions

Many products claiming to be "proactive" actually monitor the patterns and tell-tale signs exhibited by the network traffic, rather than the content's behavior. Packet inspection products (e.g., intrusion detection and intrusion prevention systems) have difficulty in identifying complex attacks, such as Spyware and Phishing, that do not leave identifiable "fingerprints" at the network or data layers.

- **Heuristics** are used to identify variations of known viruses based on "telltale" signs, but are not intelligent enough to decipher obfuscated code and are prone to false-positives.
- **Firewalls** are no longer sufficient for preventing today's malicious code, because complex threats enter the network via port 80 (HTTP) and port 443 (HTTPS) which are typically left open in the firewall.
- **Intrusion Detection System** products are designed to detect situations when the network has already been infected and, at best, can help to control the damage.
- **Intrusion Prevention Systems** usually attempt to identify communication patterns (e.g., rate of transmission) of packets coming into the network, rather than analyzing application-level behavior.

Only at the application level is it possible to understand the full context of the execution environment and accurately determine the real behavior of a given piece of content once loaded into the browser. **Finjan's behavior-based solution is unique in its ability to determine whether Active Content complies with your company's security policy – securing your web and letting you conduct business as usual.**

## Finjan - Securing Your Web

### For Additional Information

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

#### San Jose, USA

Toll Free: 1 888 FINJAN 8 (1 888 346 5268)  
Tel: +1 408 452 9700  
Email: [salesna@finjan.com](mailto:salesna@finjan.com)

#### New York

Tel: +1 212 681 4410  
Email: [salesna@finjan.com](mailto:salesna@finjan.com)

#### United Kingdom

Tel: +44 (0)1252 511118  
Email: [salesuk@finjan.com](mailto:salesuk@finjan.com)

#### Germany

Tel: +49 (0)89 673 5970  
Email: [salesce@finjan.com](mailto:salesce@finjan.com)

#### Asia Pacific

Tel: +972 (0)9 864 8200  
Email: [salesapac@finjan.com](mailto:salesapac@finjan.com)

#### Israel

Tel: +972 (0)9 864 8200  
Email: [salesis@finjan.com](mailto:salesis@finjan.com)



*Finjan's Family of Best-of-Breed Web Security Appliances*

© Copyright 1996 - 2006. 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 U.S. Patents No. 6092194, 6154844, 6167520, 6480962, 6209103, 6298446, 6353892, 6804780, 6922693, 6944822, 6993662, 6965968 and 7058822 and may be protected by other U.S. Patents, foreign patents, or pending applications.

Finjan, Finjan logo, Vital Security, Vulnerability Anti.dot and Window-of-Vulnerability 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. Kaspersky is a registered trademark of Kaspersky Lab. SurfControl is a registered trademark of SurfControl plc. Microsoft and Microsoft Office are registered trademarks of Microsoft Corporation.

All other trademarks are the trademarks of their respective owners. Q3 2006.