



Behavior-Based Security

**The Key to Staying a Step Ahead
of the Next Unknown Attack**

Finjan White Paper

September 2006

THIS DOCUMENT INCLUDES PROPRIETARY INFORMATION OF FINJAN INC. AND/OR ITS
AFFILIATES AND MAY NOT BE USED, CIRCULATED OR QUOTED EXCEPT IN ACCORDANCE WITH
EXPLICIT WRITTEN AUTHORIZATION FROM FINJAN

© Copyright 1996 - 2006. Finjan Inc. and its affiliates and subsidiaries ("Finjan"). 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, 7058822 and may be protected by other U.S. Patents, foreign patents, or pending applications.

Finjan, Finjan logo, Vital Security, Vulnerability Anti.dote and Window-of-Vulnerability are trademarks or registered trademarks of Finjan. 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.

For additional information, please visit www.finjan.com or contact one of our regional offices:

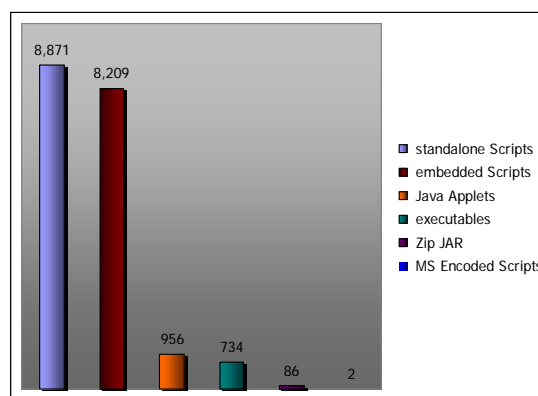
<p>USA 2025 Gateway Place Suite 180 San Jose, CA 95110, USA Toll Free: 1 888 FINJAN 8 Tel: +1 408 452 9700 Fax: +1 408 452 9701 salesna@finjan.com</p>	<p>Europe 4th Floor, Westmead House, Westmead, Farnborough, GU14 7LP, UK Tel: +44 (0)1252 511118 Fax: +44 (0)1252 510888 salesuk@finjan.com</p>
<p>Chrysler Building 405 Lexington Avenue, 35th Floor New York, NY 10174, USA Tel: +1 212 681 4410 Fax: +1 212 681 4411 salesna@finjan.com</p>	<p>Haidgraben 2, 85521 Ottobrun, Germany Tel: +49 (0)89 673 5970 Fax: +49 (0)89 673 597 50 salesce@finjan.com</p>
<p>Israel/APAC Hamachshev St. 1, New Industrial Area Netanya, Israel 42504 Tel: +972 (0)9 864 8200 Fax: +972 (0)9 865 9441 salesint@finjan.com</p>	

Email: info@finjan.com
 Internet: www.finjan.com

Executive Summary

Traditional Internet security solutions, such as anti-virus, firewall, intrusion detection, intrusion prevention and heuristic-based systems, are incapable of preventing today's highly sophisticated attacks. New, ultra-fast malicious code can infect your network and systems within seconds – undetected by packet-level Intrusion Detection and Intrusion Prevention systems and long before a signature-based anti-virus solution can be updated or a software patch can be installed. Based on the results of the FBI 2005 Computer Crime Survey, US companies lost an estimated \$67 billion in 2005 due to computer crimes (e.g., viruses, Spyware, PC theft and other computer crimes). This is despite the fact that virtually all of the organizations surveyed use anti-virus software (98.2%) and firewalls (90.7%). For purposes of comparison, losses due to telecommunication fraud in the US are about \$1 billion a year (FBI Computer Crime Survey). Also, the overall cost to Americans of identity fraud reached \$52.6 billion in 2004 (Javelin Strategy & Research).

Today's sophisticated web-based threats, such as Spyware and malicious code, are primarily driven by Active Content, e.g., Java applets, VB Scripts, JavaScripts and executables. This can clearly be seen in the graph below, which shows the number and types of content that violated a telecommunication company's security policy, based on a security audit conducted by Finjan in Q2/2005.



Sophisticated malware applications do not leave "fingerprints" at the network or data layers that are sufficient to distinctively identify them. Moreover, modern hackers are well aware of traditional security systems such as firewalls, anti-virus and Intrusion Prevention/Detection products, and are crafting their malicious code to "outsmart" such systems.

In order to differentiate legitimate business applications using Active Content, such as web conferencing, e-commerce, and webmail, from malware using these same Active Content elements, security solutions must analyze behavior at the level where the Active Content resides and operates.

Finjan's breakthrough **behavior-based security technology** is the ultimate solution for enterprises' content security needs. This patented technology inspects the application-level traffic (i.e., the Active Content objects) that might carry the malicious mobile code which can infect the computers, and analyzes the behavior of the code itself - **before** it even arrives and begins to run on the target computer.

Finjan's behavior-based security 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.** Taking Internet security to previously inconceivable levels, this is the **ONLY** solution to effectively and proactively combat new and unknown attacks driven by Active Content.

Contents

Introduction.....	1
What is Active Content?	1
Where Does Active Content Operate?	2
The Window-of-Vulnerability™	3
How Finjan’s Behavior-Based Technology Works.....	4
Behavior-Based Security as a Metaphor	6
Behavioral Rules	7
Synergies with Vital Security™ Components	7
Benefits to the Enterprise	8
Core Behavior-Based Technology	8
Deploying Behavior Based Technology within Vital Security™ Solutions.....	8
Advantages over Packet Level and Other Types of “Proactive” Solutions.....	8
Anti-Virus	9
Firewall	9
Intrusion Detection and Intrusion Prevention Systems.....	9
Heuristic Technologies Are Prone to False-Positives	10
What Do the Industry Experts Say?.....	10
Conclusion	11
About Finjan.....	11

Introduction

In today's highly networked business environment, enterprises and organizations are increasingly dependent on the Internet for access to information, email, e-commerce and the like. While web-based applications increase productivity and are essential for everyday business activities, the underlying technologies enabling these applications can be exploited for malicious purposes. As a result, businesses realize that they must take proactive measures to protect their network systems from malicious and/or inappropriate content.



In light of the increasingly sophisticated nature of malware attacks, enterprises require highly intelligent security solutions that are capable of analyzing the behavior of Active Content in order to block malicious or inappropriate content before it enters their networks and infects their computers. At the same time, this high level of proactive security must be achieved without compromising the productivity of the enterprise's users.

Finjan delivers proactive web security solutions, based on its patented behavior-based technology, that protect companies from new, unknown attacks driven by Active Content. Finjan's solutions allow enterprises and organizations to take full advantage of the web as a business tool, increasing business productivity without security worries.

What is Active Content?

Active Content refers to software components that are embedded in an electronic document which can carry out or trigger actions automatically (and dynamically), often without the user's knowledge or consent. Active Content is delivered to the user's computer while browsing the web, enabling web sites to provide increased functionality, such as interacting dynamically with visitors, delivering animation and interactive applications, and much more. Of course, Active Content can be delivered also via email, file transfers, instant messaging and other means of communication. Active Content is sometimes referred to also as "mobile code."

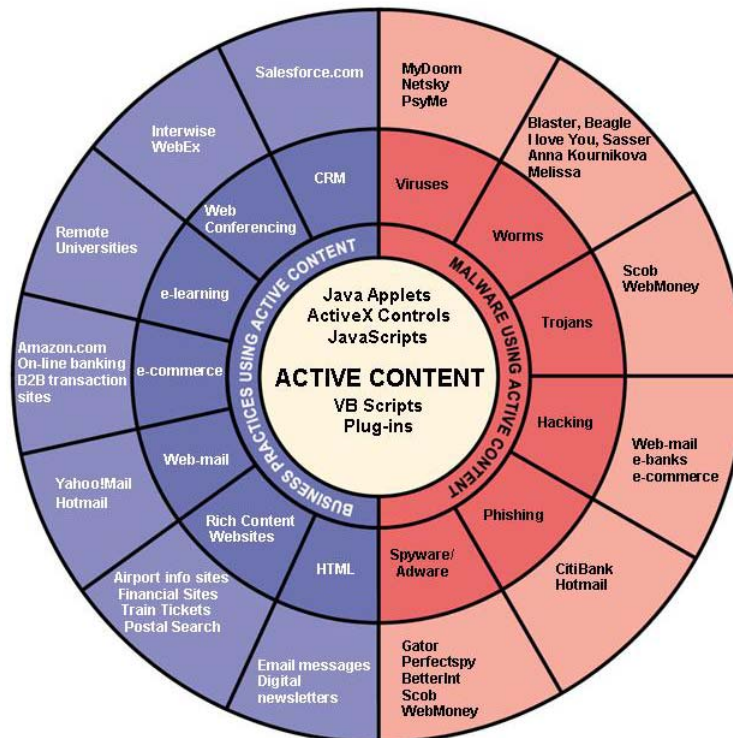
Active Content technologies include:

- Java Scripts: a common type of web script (examples of other types are VBScript, ECMAScript, and JScript), which are used by Web programmers
- Java applets, ActiveX controls: programs that reside on the computer or can be downloaded from the web into the browser (either as independent (standalone) files or as an embedded part of an HTML web page)
- Macros, spreadsheet formulas, or other interpretable or executable code contained in proprietary desktop-application formatted files
- Executable files

In most cases, Active Content serves legitimate purposes, being used in common business applications such as web conferencing, e-learning, e-commerce, webmail and others. However, at the same time, Active Content technology may be exploited to carry malicious mobile code, which is downloaded and executed on a local system without the explicit

knowledge or consent of the user. This dichotomy creates a difficult security challenge for enterprises and organizations.

The figure below illustrates how Active Content can be used for both business (left side) and malware (right side) purposes.



The Active Content Security Challenge

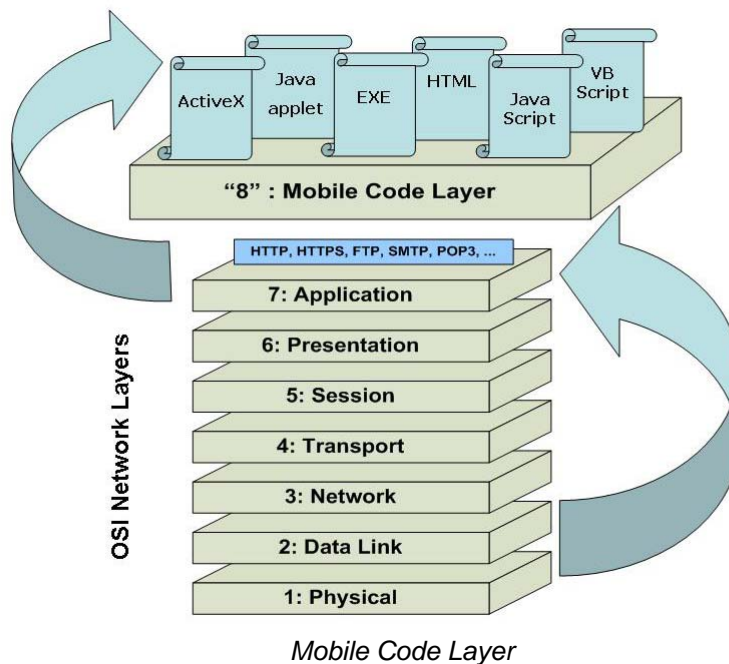
Attacks by Active Content using malicious code are growing exponentially and account for the vast majority of today's malware. These attacks have a direct impact on businesses' bottom lines, as they result in a massive loss of valuable time and resources, reduced productivity and lost revenue. In addition, Active Content can expose or even lead to theft of confidential or competitive information.

Where Does Active Content Operate?

From the perspective of the OSI network-layers model, we can observe that Active Content, such as Java applets, Active X controls, JavaScripts, VB Scripts and executable files, operate at a layer above the Application Layer (Layer 7), which we refer to as the "**Mobile Code Layer**" – this layer can be conceptualized as a "**Virtual Layer 8**". The Active Content objects serve as the enablers of higher level applications such as web conferencing or CRM, that use HTTP (layer 7) for transport, and the browser as a platform for operation.

In order to differentiate the legitimate business Active Content from malware using these same Active Content elements, security solutions must analyze behavior at the "mobile code layer". Sophisticated Active Content-driven malware, such as Spyware or certain worms, do

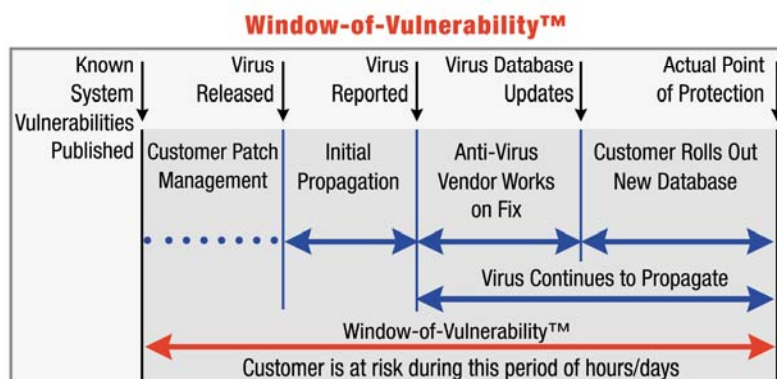
not leave “fingerprints” at the network or data layers that are sufficient to distinctively identify them.



Finjan's behavior-based solution operates **above** the Application Layer (Layer 7) of the OSI network model. Viruses, Trojans, worms and Spyware operate at Layers 7 and above (Layer 8).

The Window-of-Vulnerability™

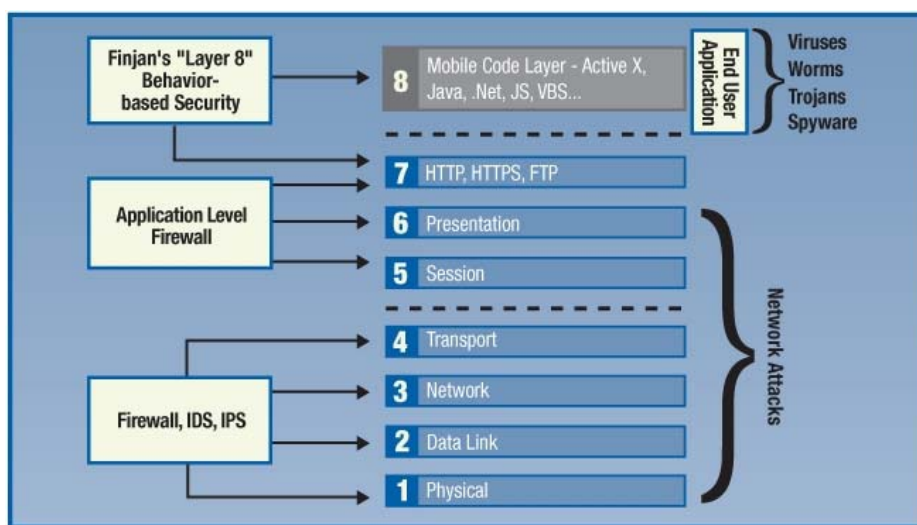
The Window-of-Vulnerability™ is the time span from the moment a new vulnerability is published or a malware attack is launched, until protection is delivered to combat the virus, either via a signature update or a software patch, and deployed across the corporate network. New, ultra-fast malicious code can infect your network and PCs within seconds – undetected by packet-level Intrusion Detection and Intrusion Prevention systems and long before a traditional signature-based anti-virus solution can be updated or a software patch can be installed, resulting in costly damages. Even once the patch is issued, studies show that about one-half of enterprise systems remain unpatched for a period of between 21-60 days. Enterprises require intelligent, proactive solutions that close this Window-of-Vulnerability™, while reducing the need for frequent patches and their associated costs.



Instead of relying on reactive virus database updates, Finjan's patented behavior-based technology closes your Window-of-Vulnerability™ by blocking malicious and inappropriate content the first time it strikes. Deployed at the gateway, it protects your business in real time, preventing attacks from reaching local computers. It is the only technology that can truly provide zero-hour protection. Finjan's best-in-class technology saves your business time and money, and lets you avoid the IT headaches associated with security incidents.

How Finjan's Behavior-Based Technology Works

Finjan's breakthrough and patented behavior-based technology inspects the application-level traffic (the Mobile Code Layer) that might carry the malicious mobile code which can infect the computers, and analyzes the behavior of the code itself - **before** it even arrives and begins to run on the target computer. Finjan's behavior analysis and blocking technology identifies the combinations of operations, parameters, script manipulations and other exploitation techniques, and can determine that a piece of mobile code is trying to exploit one or more types of vulnerabilities. Then, in accordance with each organization's specific security policy, Finjan's system decides whether to pass, block or neutralize the content. Powered by this technology, **Finjan offers the ONLY solution to effectively combat malicious code in Active Content.**



Viruses, worms, Trojans and Spyware operate at Layers 7 and above

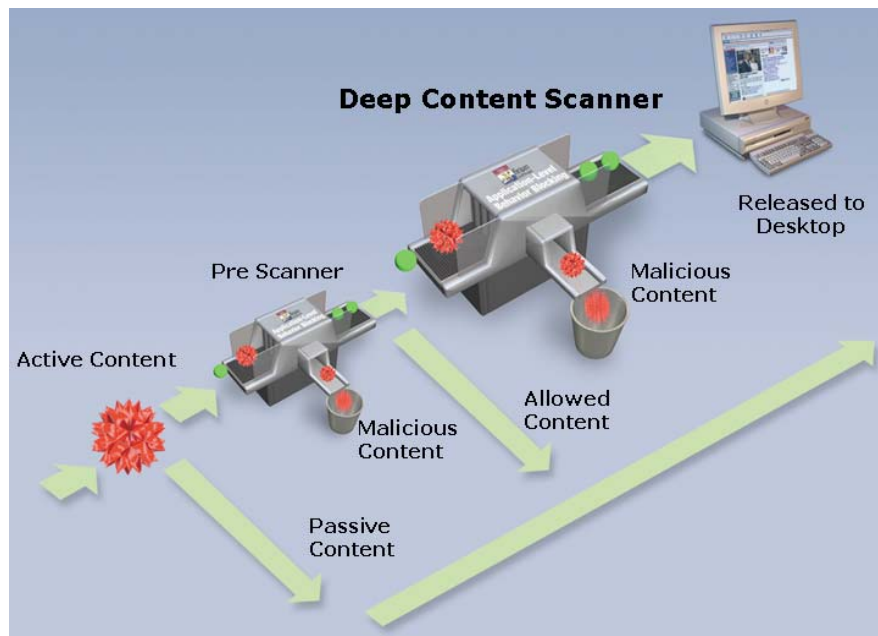
When the web content is processed by Finjan's behavior-based scanning engine, the analysis progresses along the following logical steps:

- **True content type detection** is used to identify multiple types of content. The type detection algorithms can identify file type variations, spoofed file types, archived executables, encoded script files and more.
- **Detect and decode obfuscated codes**, a technique often used to "bypass" security scanners
- **Break up HTML code into components** (HTML commands, text sections, style sheets, URI, scripts, external object activation, etc.)
- **Each Active Code component is scanned** in-context by a sub-engine specialized at analyzing that type (Java, ActiveX, Scripts, HTML, CSS and so on)
- **Build a behavior profile** that encompasses the combined operational behavior of the active code components
- **Compare the behavior profile** against a comprehensive list of security profiles, and if it violates any of them, it is blocked

By employing this holistic analysis approach, the behavior-based security engine can understand the programmatic connections among the various bits and pieces of code. Each individual piece of code can be quite benign, and easily slip through network-level scanning devices, as well as signature-based scanning technologies. Only by deep scanning of the combined operations in a way that resembles a compiler working with a runtime interpreter, can the engine detect the true malicious behavior that the code will perform when it reaches the user's desktop.

Based on these principles of operation, Finjan's scanning engine is not affected by programmatic variances, such as changing names of objects and variables in the scripts, cross-calls between scripts, and alternating calling sequences.

To further accelerate the scanning process, Finjan's engines keep a unique mathematically-computed key that identifies each active code object, and cache the behavior profile of the active code object indexed by that key. Therefore when the same piece of active code will be examined by the scanners again, its cached behavior profile will be used. These cached behavior profiles are called *Active Content Lists (ACL)*, and Finjan manages and distributes updates of Malware ACLs to the multiple installations of the Vital Security™ solutions worldwide. ACLs are also used as one of the building blocks of Finjan's *Anti-Spyware* engine.



Two-Step Scanning Approach for Highest Performance

When deployed on a customer's site, an administrator or security officer can use Active Content Lists to white-list particular Active Code objects which are known to the company and proven to be safe; for example, a stock-ticker and financial information Java Applet that communicates information in and out of the user's PC and pops up message windows, can be identified by its unique key and behavior profile, and can be placed on the "white" Active Content List.

Behavior-Based Security as a Metaphor

The following metaphor illustrates the concept behind our patented Behavior Based technology. A bank uses three separate and accepted techniques to detect possible robbers:

- Metal detector
- Fingerprints
- Facial recognition (based on FBI's most wanted list)

An unknown robber (with no previous criminal record) without a gun or knife passes the bank's security inspection and is allowed into the bank. He approaches the teller and quietly uses the power of hypnosis to convince the teller to hand over all the money in his drawer.

There is no way that the bank's security can stop this robbery before it actually happens.

Finjan's security, on the other hand, is based on an in-depth psychological interrogation of each person before he/she enters the bank, in addition to the above measures. This analysis looks for psychological elements that would point to possible criminal tendencies and helps to build a full behavioral profile. Based on our extensive experience in this area, we know the right questions to ask and how to interpret the answers in such a way that allows us to

discover the robber's hidden intentions. Finjan's behavior analysis would have prevented this robbery by stopping the robber at the bank's entrance.

Similarly, Finjan's patented behavior-based technology utilizes our experience in identifying malicious behavior in Active Content that can proactively block new malware attacks before anti-virus vendors even know that this malware exists.

Behavioral Rules

The rules that drive the operation of the behavior-based security engine are not signatures. Rules at various levels define Active Content program and language tokens, semantic patterns of Active Code, permitted combinations of operations, parameters and programming techniques. These rules are created by security experts from Finjan's Malicious Code Research Center (MCRC) group, and fed into the behavior-based security and Vulnerability Anti.dote™ scanning engines, enabling the identification of Active Content that may try to exploit a given vulnerability. Vulnerability Anti.dote is a unique technology that protects computers against known vulnerabilities without the need for software patches. Finjan's Malicious Code Research Center (MCRC) is a leader in the detection of dangerous vulnerabilities that could be exploited for malicious attacks, keeping our customers steps ahead of the hacker community and unauthorized users.

Synergies with Vital Security™ Components

Finjan's Vital Security™ Appliances leverage synergies between the behavior-based engine and other security engines (such as Anti-Virus, URL Filtering, HTTP headers filters and more) to provide the best and most comprehensive content security solution. These synergies are implemented in Finjan's rule-based security policies system, which is used to define flexible sets of rules that describe expected cases and conditions on the content, and how the system should react in each case. Using these rules, each organization can create highly granular policies regarding the content/access allowed or forbidden for any single user or group of users, based on their particular responsibility and access rights.

The following are examples of how rules can utilize synergies between Finjan's various security engines:

- Block ActiveX and Java Applets from entertainment sites
- Prevent uploads of MS Office documents to webmail sites
- Block IM conversations if the word "confidential" is used
- Warn users before visiting a site on the "Restricted" list
- Allow downloads of executable files signed by Microsoft
- Identify cases when some sites or URLs get blocked for violating the generic Active Content Security profile, and then hours or days later the user can discover that the same URL gets blocked by the AV engine (that already names it and assigns a version to it).

Finjan has encountered numerous such cases while reviewing customer log files – which means that Finjan users were proactively protected even before the exploit had even started to spread.

Benefits to the Enterprise

Core Behavior-Based Technology

- The ability to prevent new and previously unknown viruses, Spyware, malicious code and complex attacks, leading to a significant increase in ROI from your security investment
- Reduction in 'false positives' that may occur if relying on heuristics based techniques, leading to a reduced cost of solution management
- Minimized overblocking enables users to leverage the full power of Internet as a business tool
- Increased knowledge and awareness of the content (and associated behavior) entering your organization, leading to more educated security policy definition and risk analysis
- Deep code analysis to reveal malicious combinations of individually innocent functions
- Scanners use cached behavior profiles (Active Content Lists) for accelerated performance
- Expose malware that tries to extract private information and publish it to the Internet, or other forms of trying to access private and unprivileged information (HIPAA and Sarbanes-Oxley compliance)

Deploying Behavior Based Technology within Vital Security™ Solutions

- Advanced and rich categorization of Active Content actions
- Finjan provides a comprehensive list that includes actions on the 'File Access' level, 'Processes' level, 'Registry' level, 'Network Access' level, 'Windows' level, etc. In each category Finjan offers a long list of actions.
- Flexibility to create rules with connections between all types of filters
- Granular security policies enable any rule to be attributed to any user or group of users
- True content type detector – Can identify multiple types of content, regardless of variations and spoofed types; archived executables; encoded script files and more
- Ability to scan encrypted content that travels over HTTPS and so it passes through all the known gateway solutions

Advantages over Packet Level and Other Types of “Proactive” Solutions

Many companies today claim that their products deliver “proactive” security. However, this does not refer to the behavior of the content. It refers to the patterns and tell-tale signs exhibited by the network traffic that are monitored by these products. Packet inspection products, for example, cannot “understand” how a given web page will behave when loaded into a browser, because they never “see” the web page as a whole and analyze it -- they only see individual packets. For this reason, packet level solutions have difficulty in identifying complex attacks, such as spyware and phishing. Only at the application level (e.g., browser) is it possible to understand the full context of the eventual execution environment and determine accurately what the real behavior is going to be.

Anti-Virus

Anti-virus solutions are reactive in nature and, as such, are powerless against new unknown attacks, which are driven by Active Content and may utilize multiple technologies, stages and angles of attack. The traditional anti-virus solutions block known viruses and worms by comparing content against signature databases, which need to be updated each time a new virus is discovered. Given the prolific speed at which viruses spread today, companies know they have very limited protection from new attacks until their anti-virus vendor receives the new attack sample, creates a new patch (or signature), and delivers that patch to the antivirus product's database. The paradox is that while the anti-virus vendor is updating its signature database, the virus writers are busy working on the next new virus for which a signature does not exist. This endless loop always has the same result - the end user is exposed to dangerous attacks.

Firewall

Firewalls traditionally operate at Layers 2, 3 and 4 of the OSI model and effectively isolate corporate networks from the Internet as well as hide IP addresses and protect ports from the outside world. While firewalls may still be very useful for intrusion prevention and remote access control, they are no longer efficient for preventing today's malicious code. This is because today's complex threats, such as Spyware and Phishing, enter the network via port 80 (HTTP) and port 443 (HTTPS) which are left open in the firewall. In most organizations, these ports cannot be closed without severely hampering the productivity of the users. Firewalls can either block or allow a certain port, but cannot inspect the content allowed to pass through. Email transportation also opens the door to many threats, and the combination of web and email transportation is highly exploited by various types of threats, such as Phishing. The ineffectiveness of firewalls against such threats is evidenced by the rapid increase in worm penetration (such as MyDoom and Sasser), despite the extremely wide deployment of firewalls (99% of respondents to 2005 E-Crime Watch™ Survey).

Intrusion Detection and Intrusion Prevention Systems

Intrusion Detection System (IDS) products are designed to detect situations when the network has **already been infected**, by identifying patterns of network traffic behavior (of one computer or a group of computers) that may indicate the spread of a worm or other anomalies. When this happens, they perform "damage control" by cutting off the network traffic, isolating a group of computers and alerting the administrator, resulting in decreased user experience.

In contrast, Finjan's scanning technologies scan the application-level traffic (Mobile Code Layer) that might carry the malicious mobile code which can infect the computers, and analyze the behavior of the code itself **-before it begins to run on the target computer.** Finjan's behavior-based technology can determine that a mobile code is trying to exploit one or more of types of vulnerabilities, which indicates that this code will attempt malicious operations if allowed to reach the end user's PC. In this manner, Finjan's behavior-based solution protects against multiple possible variations and combinations of exploit attempts even before the first worm or virus is created that will try to exploit software vulnerabilities.

Intrusion Prevention Systems (IPS) and similar "smart packet filtering" solutions usually operate at Layers 2 through 4 of the OSI networking model, and attempt to identify communication patterns (e.g., rate of transmission) of packets coming into the network, rather than analyzing the code entering the network. The problem is that powerful, sophisticated attacks cannot be identified at the single-packet level - such attacks are made up of high-

level scripting and HTML operations within the context of whole web pages, so any pattern identified in a single packet cannot determine if this packet is a part of a code that will try to exploit the target PC.

Only by intelligently analyzing the whole content at the Mobile Code layer (Virtual Layer 8) can the full scope of such attacks be identified. Finjan's behavior-based solution does not scan for a specific pattern, but rather runs the whole HTML page with the embedded scripts and objects through a Behavior Based engine. It can identify correlations between various parts of the multi-packet content to point out an attempted attack.

Heuristic Technologies Are Prone to False-Positives

Heuristic-based technologies detect infections by scrutinizing a program's overall structure, its computer instructions and other data contained in the file. The heuristic scanner then makes an assessment of the likelihood that the program is malicious based on the logic's apparent intent. Anti-virus engines often use heuristics to identify variations of known viruses. However, since these schemes don't actually observe full execution of the scanned software, they often fail to detect new infections; there are simply too many ways to obfuscate malicious code, and often the only way to know content is malicious is to watch it run in real-time. This accounts for the high rate of false-positives when using such heuristic-based systems.

In contrast, Finjan's behavior-based engine identifies "concrete" behavior and as such is able to minimize overblocking. It is well-equipped to detect and identify the true behavior of obfuscated code which might be used for malicious purposes. Finjan reduces false-positives, reducing the cost of solution management.

What Do the Industry Experts Say?

Industry players are in agreement regarding the need for behavior blocking:

- "This [2005 FBI] computer security survey eclipses any other that I have ever seen. After reading it, everyone should realize the importance of establishing a proactive information security program." - Kevin Mitnick, Mitnick Security Consulting
- "You can really think of this as taking the notion of **secure-by-default** to the next level. The system will truly know what actions are allowed for operating-system components and the applications that are running", Bill Gates, Chairman & Chief Security Architect, Microsoft – at RSA Conference 2004 on behavior-based security solutions.
- "**Reactive, signature-based protection is becoming less effective.** The time from software patch to exploit is dropping below the time needed for companies to install the patch. Even if you start when the patch is released, most IT departments will take 30 days to test and patch a system and hackers are faster than that now. Therefore we need more proactive security", "...**behavior-blocking looks promising**", Robert Clyde, Symantec CTO, Vnunet.com
- "If the AV Industry were getting started today, **we would not** choose the approach that we currently pursue....The pot of gold at the end of the rainbow AV detection is **day-zero detection**: to be able **to detect and prevent** an item of malware or other undesired attacks (rather than move it post infection). In order to achieve this, **reactive action will have to become a thing of the past, making way for generic**

and behavior-based blocking,” Paul Gartside, McAfee Inc. – Virus Bulletin
Comment, September 2004 Issue.

Conclusion

The use of Active Content technologies, such as Java applets, ActiveX controls, JavaScripts and executable files, for malware purposes presents a complex security challenge. This is due to the fact that Active Content is commonly used for regular business practices such as CRM, ERP, web conferencing, e-commerce and webmail, which means that it is not feasible or productive to simply block all Active Content. Moreover, traditional security solutions, such as anti-virus and intrusion detection and prevention systems, are reactive in nature and, as such, are powerless against unknown and complex attacks, which may utilize multiple technologies, stages and angles of attack.

Utilizing its breakthrough and patented behavior-based technology, Finjan offers the ONLY proactive content security solution that effectively combats and protects against new, unknown attacks driven by Active Content. Finjan offers the world's most comprehensive security solution, integrating its patented behavior-based technology, Vulnerability Anti.dot and Anti-Spyware engines with industry-leading Anti-Virus and URL Filtering engines. Finjan's solutions deliver the most effective shield against web-borne threats, freeing businesses to harness the web for maximum commercial results while minimizing the risks associated with malware attacks.

About Finjan

Finjan is a global provider of best-of-breed web security solutions for businesses and organizations, protecting millions of users from known and unknown threats. Finjan uses its patented behavior-based security technologies to determine actual code behavior and block any action that violates an organization's predefined security policy, therefore surpassing the levels of defense offered by reactive and signature-based anti-virus and intrusion detection solutions. This superior technology enables Finjan to proactively repel all types of web-borne attacks, securing businesses against known, unknown and emerging threats. Finjan's security solutions have received industry awards and recognition from leading analysts and publications including IDC, Butler Group, SC Magazine, PCPro, ITWeek, and Information Security. For more information about Finjan and its proactive protection solutions against threats driven by mobile malicious code, please visit: www.finjan.com.