



Vital Security™ SDK

Leverage Finjan's Breakthrough Security Technologies to Empower Content Management Applications

Finjan White Paper

February 2006

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

Contents

Introduction.....	1
The Evolving Security Challenge.....	2
Window-of-Vulnerability™	2
Web-Based Threats.....	3
The Spyware Threat.....	3
Vital Security™ SDK – Functional Description	4
Patented Behavior-Based Security	4
Vulnerability Anti.dote™ Scanning Engine	6
Anti-Spyware Engine	9
Research-Driven Security Policy.....	10
Additional SDK Features and Benefits	11
Advantages over Packet Level and Other Types of Security Solutions	11
Anti-Virus.....	11
Firewall.....	12
Intrusion Detection and Intrusion Prevention Systems.....	12
Heuristic Technologies Are Prone to False-Positives	13
Conclusion	13
About Finjan.....	14

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 technologies and applications, such as Instant Messaging and web conferencing, increase productivity and have become essential for everyday business activities, the underlying technologies enabling these applications can be exploited for malicious purposes. In fact, web threats are getting more sophisticated and dangerous, as developers of malicious code are constantly seeking new ways to exploit business and personal computing systems for financial gain.

Thus, organizations require content management and security solutions that will enable them to take advantage of new web-based technologies to drive business, without compromising their network security and valuable business assets.

Finjan is a global provider of best-of-breed, proactive web security solutions for businesses and organizations. Finjan's web security solutions utilize patented **behavior-based technology** to proactively repel all types of threats arriving via the web, such as *Spyware*, *Phishing*, *Trojans* and *other malicious code*, securing businesses against unknown and emerging threats, as well as known malware.

Finjan has packaged its patented next generation security technologies and proven content scanning capabilities into a Software Development Kit (SDK), which is now being made available to content management system vendors. The **Vital Security™ SDK** allows 3rd party gateway vendors, such as vendors of email gateways or caching servers, to incorporate the world's best content security functionality in their enterprise applications. The host application uses a simple Application Programming Interface (API) to invoke Finjan's state-of-the-art scanning engines, which proactively detect and block malicious content and code that attempt to exploit vulnerabilities and compromise users' computers, data, networks or any other system resource. The SDK blocks malicious elements that have been identified within the examined content, in accordance with Finjan's best-in-class default security policy.

The **Vital Security™ SDK** is designed to integrate with the following systems:

- **Any** Content Management System, such as email gateways, web caching devices, web servers, messaging servers, load balancers, network redirectors, and application switches, that deals with content and also needs to provide application security.
- Security devices, such as Firewalls, Intrusion Prevention Systems (IPS), URL Filters, and Anti-Virus gateways that want to add advanced proactive capabilities to their existing functionality

How Gateway Vendors Benefit from the Vital Security™ SDK

- Lets you offer your customers the highest available level of Internet security, based on Finjan's proven and patented, industry-leading technologies and security expertise
- Allows you to differentiate your company's offering by integrating proactive content security
- Delivers unmatched proactive Internet security technology, incorporating comprehensive security features, with minimal integration efforts

- Extensive logging and reporting capabilities enable your customers to monitor ROI and securely optimize their use of the Internet
- Simple-to-use API supported with low-risk C++ API, which requires minimal integration effort
- Thread safe SDK lets you run multiple threads for using the SDK in parallel for separate pieces of content
- Access to Finjan's Malicious Code Research Center (MCRC) security experts and 24 x 7 support staff availability

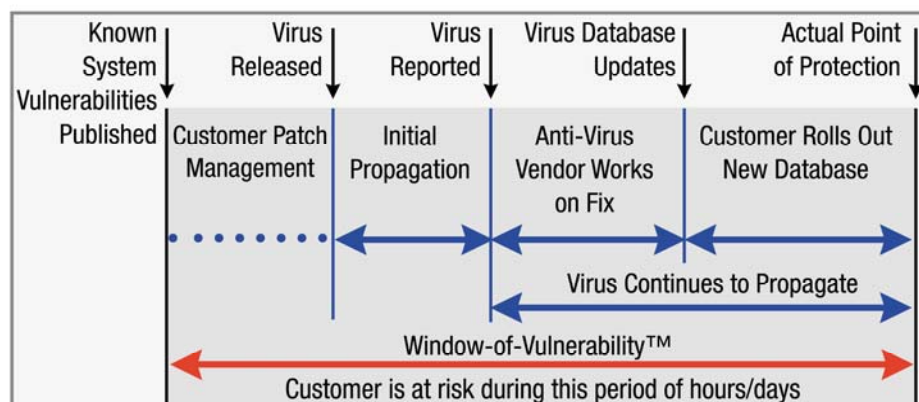
Provide your customers with the best protection against unknown malware threats, including Spyware, Phishing, Pharming, viruses, worms and Trojans, by easily integrating Finjan's Vital Security™ SDK into your product.

The Evolving Security Challenge

The increasing sophistication and frequency of malicious Internet-borne attacks (malware) 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. In addition, some types of malware, such as Spyware, can expose or even lead to theft of confidential data, intellectual property and sensitive business information. The overall damage inflicted by malware (viruses, worms, Trojans) in 2004 was estimated at \$169 billion annually worldwide (mi2g Intelligence Unit). As a result, enterprises realize that they must take proactive measures to protect their network systems from malicious and/or inappropriate content.

Window-of-Vulnerability™

The **Window-of-Vulnerability™** is the time from when either a new vulnerability is published or an Internet attack is launched (exploiting an unknown vulnerability) until protection is delivered, either via a signature update or a software patch, and deployed across the corporate network. During the Window-of-Vulnerability, new ultra-fast malicious code can infect your network and PC system within seconds, 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 solutions that close this Window-of-Vulnerability, while reducing the need for frequent patches and their associated costs. By integrating the **Vital Security™ SDK**, you can intelligently analyze the behavior of the content downloaded through your gateway solution, and close the Window-of-Vulnerability™ for your customers.



Web-Based Threats

Web-based threats, driven by Active Content (e.g., Java applets, Java Scripts, ActiveX and VB Scripts), present a serious security challenge for businesses. Since these technologies are an integral part of legitimate business applications, they cannot simply be blocked “across-the-board.” In order to be effective, security solutions need to perform intelligent behavioral analysis at the application level. Firewall and other network-level security solutions are not appropriate to combat web threats, since it is not feasible to block the HTTP port. 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. Furthermore, an attack can be easily changed to bypass an IPS product and still be malicious. For this reason, packet level solutions have difficulty in identifying complex attacks, such as Spyware and Phishing.

Hackers are familiar with the workings of traditional security systems such as firewalls, anti-virus and Intrusion Prevention/Detection products, and are crafting malicious code and targeted attacks to “outsmart” such systems. Driven by business interests, web-based attacks will become more targeted and hence more difficult to detect and prevent by traditional means. Due to their complexity, along with the new focus of attackers, web threats can inflict severe damage to organizations and even compromise their confidential information, often without the user being aware that his/her computer has been infected. It should be noted that web-based attacks that may also use email (i.e., HTML) as an infection vector.

The Spyware Threat

Spyware is a serious threat to your company, both due to the potential damage and risks it poses, and to the fact that your computers may already be infected without you even knowing it. Sophos Labs predicts that quantity of Spyware will increase in 2006 and the threat from Spyware and Adware will continue to grow during 2006. This means that if your company does not have effective Spyware protection, your corporate systems and data may already be exposed to extensive security, privacy, legal and productivity risks.

Consider the following facts:

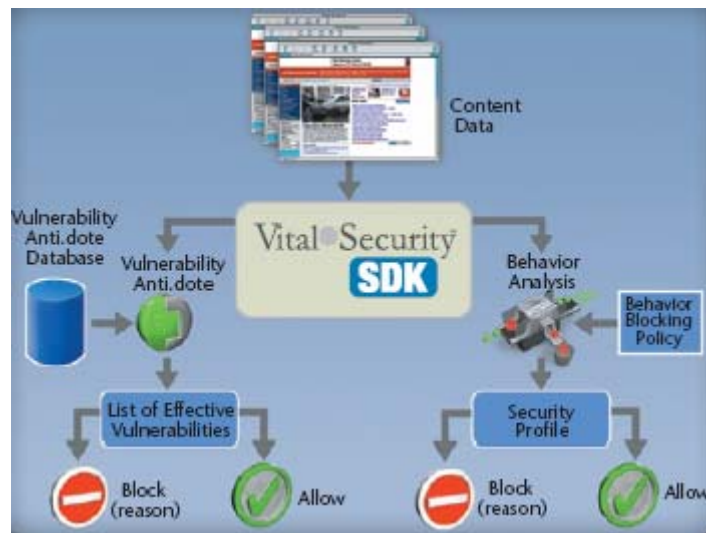
- Sophos reports that the number of keylogging Trojans has tripled in the first six months of 2005 compared to the first half of 2004.
- IDC estimates that more than 75% of all corporate machines are infected with various forms of Spyware (Source IDC's 2005 Enterprise Security Survey).
- McAfee AVERT research center has reported a 12 percent increase in the number of new potentially unwanted programs (PUP) created in Q2 2005 as compared to Q1 2005.
- The number of new malware threats (i.e., Spyware, virus, worm, and Trojan horse) rose by 48% between January-November 2005 (Sophos Security Threat Management Report 2005). The quantity of reported Spyware as a percentage of total malware rose from 54.2% in January 2005 to 66.4% in November 2005.
- As indicated in the chart below, over 79% of companies surveyed had been affected by Spyware and almost 84% had been affected by a virus attack at least one time within the last 12 months (2005 FBI Computer Crime Survey). These facts speak even louder given the fact that 98.2% of the surveyed companies were protected by Anti-virus software and 90.7% of the companies were protected by Firewall.

Fueled by large financial rewards and driven by advertisers and organized crime, Spyware is expected to continue to grow at a rapid pace.

Vital Security™ SDK – Functional Description

The **Vital Security™ SDK** incorporates the same proactive, behavior-based technologies that are implemented in Finjan’s market-leading gateway appliances. The SDK is comprised of the following scanning engines, each of which may be licensed separately:

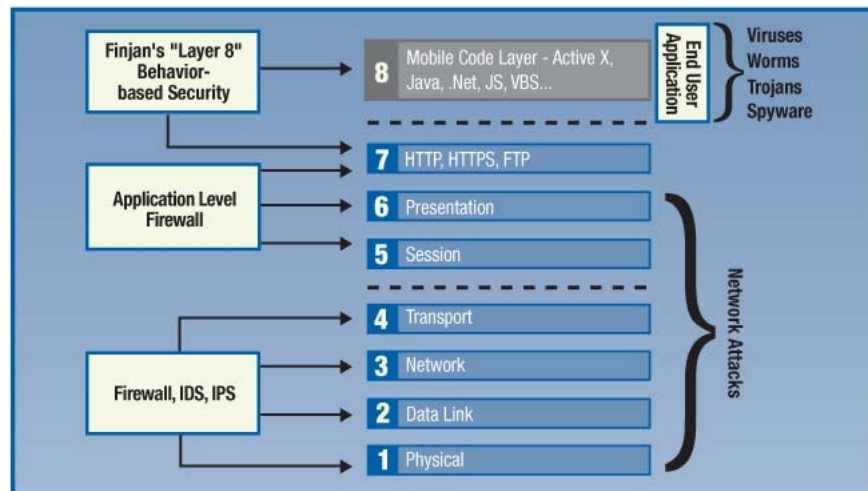
- **Behavior-based security engine** for detection and blocking of unknown attacks
- **Vulnerability Anti.dote™ engine** for protection against known software vulnerabilities
- **Anti-Spyware engine** for stopping known and unknown Spyware at the gateway



Vital Security™ SDK Functional Workflow

Patented Behavior-Based Security

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.**



Stopping Complex Attacks at the Mobile Code Layer

As illustrated in the diagram above, viruses, worms, Trojans 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.

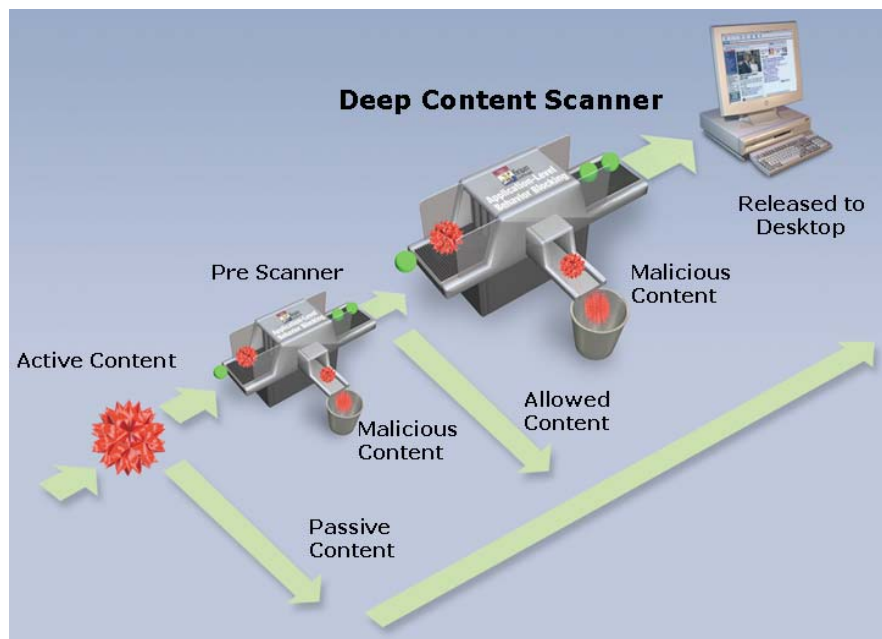
When the web content is processed by Finjan's behavior-based scanning engine, the analysis progresses along the following logical steps:

- **True content type detection** is used to identify multiple types of content, by analyzing the binary or textual elements in conjunction with extension and MIME type information. The type detection algorithms can identify file type variations, spoofed file types, packed 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™ scanning engines worldwide. ACLs are also used as one of the building blocks of Finjan's **Anti-Spyware engine**.



Two-Step Scanning Approach for Highest Performance

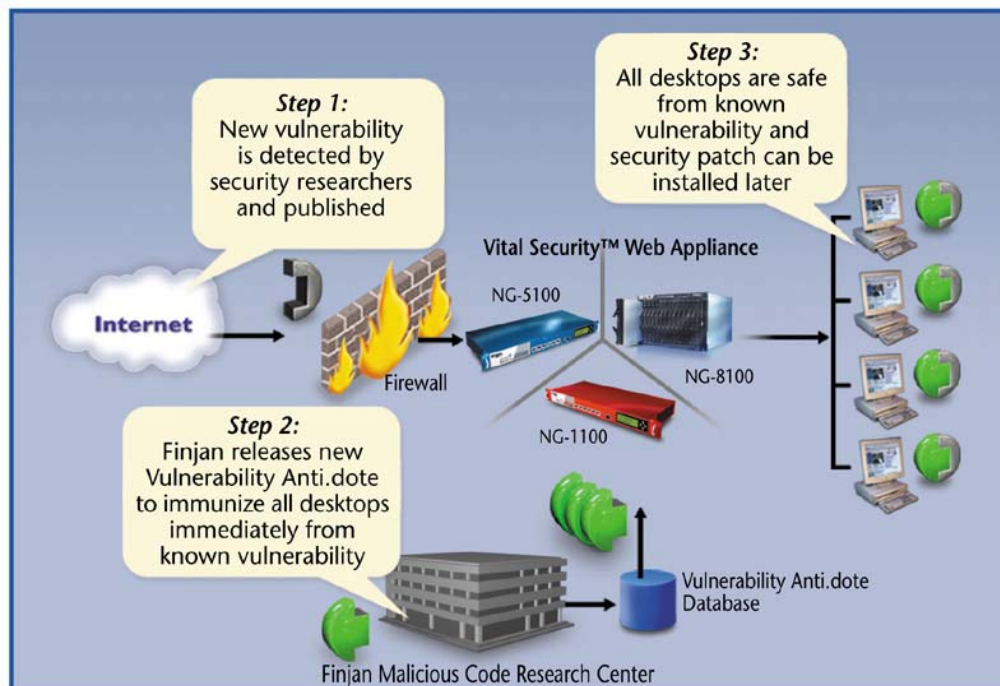
Vulnerability Anti.dote™ Scanning Engine

Finjan's breakthrough **Vulnerability Anti.dote™** technology represents an optimal balance between powerful proactive web security and minimal security and patch management overhead.

Finjan's dedicated team of Malicious Code Research Center (MCRC) experts specialize in the discovery and analysis of new vulnerabilities, i.e., any bug, security hole, maligned feature or combination of operations that can constitute a malicious attack. Based on Finjan's extensive database of published vulnerabilities, as well as unpublished vulnerabilities discovered by MCRC researchers (and disclosed by Finjan only to the vendors of the relevant products), Finjan creates behavioral rules that enable the **Vulnerability Anti.dote™** scanners to identify and block content that tries to exploit one or more vulnerabilities.

Finjan has built and is constantly maintaining a database that contains samples and technical details of numerous vulnerabilities. The sources of this database are publicly known vulnerabilities and attacks, internal research conducted at the MCRC labs in Finjan and collaboration with security vendors and security researchers. For each vulnerability, the database determines several key elements, including:

- Core elements of the vulnerability
- A description of the damage or malicious operation made available by the vulnerability
- Systems exposed to this vulnerability (Operating System, service pack, patch etc.)
- Whether or not the attack may be neutralized, and if it can be - how



Vulnerability Anti.dote™ Workflow

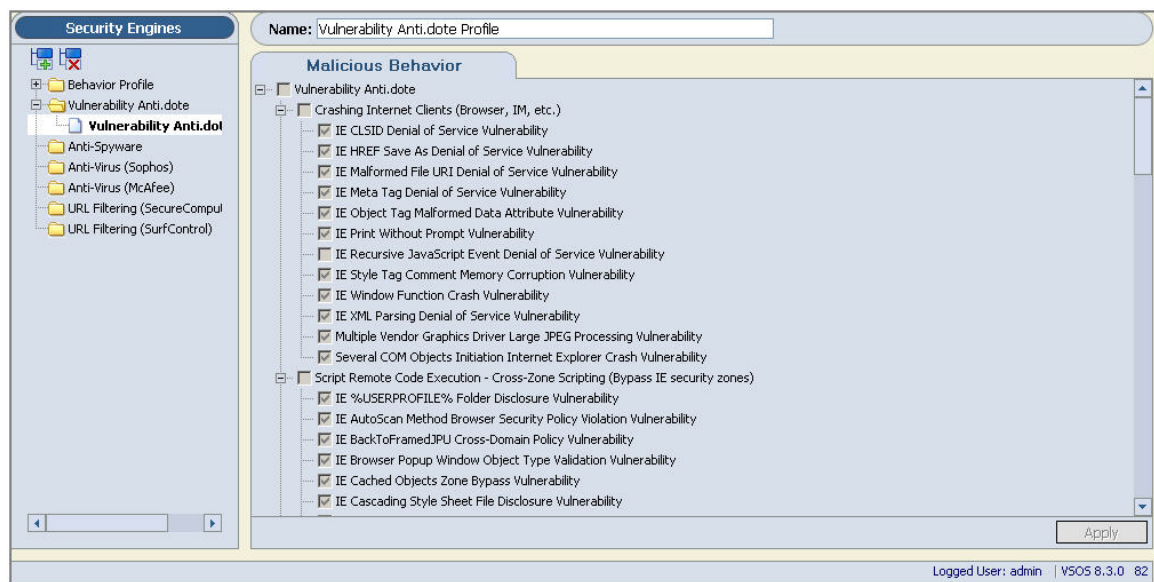
Vulnerability Anti.dote™ security scanning utilizes multi-layered rule-based engine that can “understand” HTML, scripts and all the programmatical components that make up HTTP-based content, at a level similar to compiler analysis. This engine is driven by highly detailed rules that capture the essence of the various possible vulnerabilities in any of the following software applications or systems:

- Internet-related applications, such as Internet Explorer and Microsoft Outlook
- Windows operating system, services, file system and runtime libraries
- Various protocols or applications that can be accessed by any type of active content coming into the user’s PC over the network such as FTP, Windows Media Player, etc.

MCRC analyzes the vulnerabilities and using Finjan’s unique, proprietary **Vulnerability Description Language (VDL)**, Finjan creates behavioral rules which translate into operational instructions that feed the **Vital Security SDK** scanning engines. These rules enable the scanners to identify, for a given vulnerability, a wide range of possible attacks that

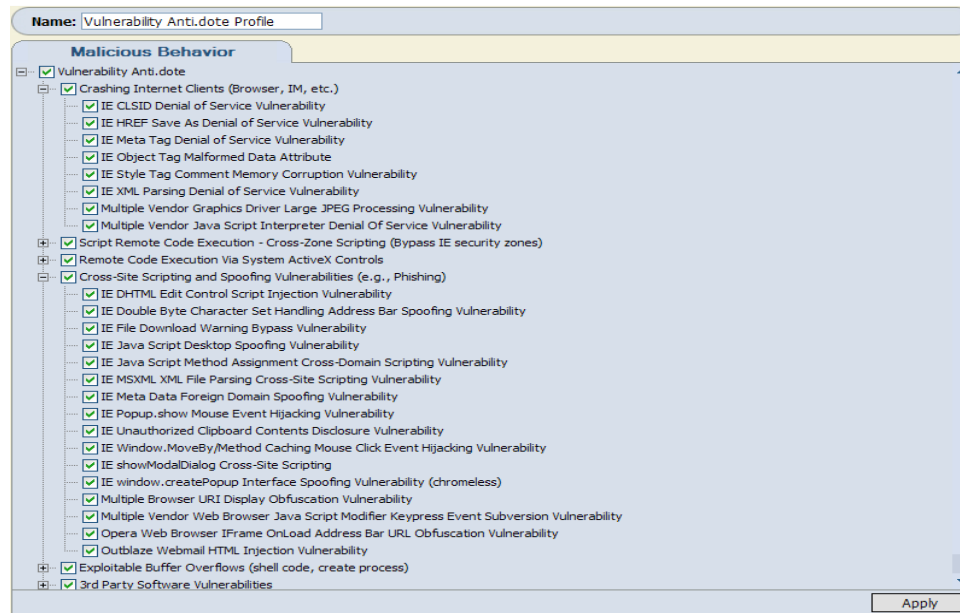
will try to exploit this vulnerability, or a combination of two or more vulnerabilities. Thus, from inception, once a certain vulnerability has been encoded in Finjan VDL and fed into the engine, the engine can discover and protect against multiple viruses that will inevitably be written to exploit this vulnerability. This is the core of Finjan's breakthrough **Vulnerability Anti.dote** technology.

The vulnerabilities are logically arranged into categories, for ease of management. The following example is a screen-shot of the **Vital Security** management console, showing the **Vulnerability Anti.dote** panel, with some of the vulnerability categories partially expanded.



Vital Security™ Management Console - Vulnerability Anti.dote™

The following screen-shot shows an example of just one of the sub-categories (URI Vulnerabilities) fully expanded. The full list contains hundreds of items, and is continuously updated and maintained by Finjan.



URI Vulnerabilities

Anti-Spyware Engine

The **Vital Security™ SDK** protects your customers from known and unknown Spyware attacks at the gateway, before it infiltrates their networks. Finjan's **Anti-Spyware engine** leverages patented **Application-Level Behavior Blocking** technology which has been customized specifically to block spyware attacks, together with URL blacklists. This highly focused **Anti-Spyware** solution provides organizations with comprehensive and layered protection against Spyware, without compromising user productivity or performance. Finjan's solutions are field-proven in their ability to identify and block unknown Spyware before updates are issued by anti-virus companies.

As opposed to traditional viruses, Spyware is an application-level threat and must be handled at this level. Packet inspection products, such as IDS and IPS, cannot predict how a given web page will behave when loaded into a browser, because they never "see" the web page -- they only see individual packets. Finjan's Anti-Spyware solution works at the application level, which means that it determines the full set of behaviors that a given piece of content will exhibit when loaded into the browser. Finjan's scanning technologies inspect the application-level traffic that might carry spyware, and analyzes the behavior of the code itself - before it begins to run on the target computer.

Finjan's **Anti-Spyware engine** uses multiple layers and techniques to directly address the Spyware threat, ensuring the highest level of protection:

- Proactive behavior-based solution that operates in real-time to block **unknown** spyware by using Finjan's unique technology to detect and prevent malicious Spyware operations such as:
 - Attempt to install spyware
 - Attempt to steal information from desktop
 - Attempt to manipulate information
 - Attempt to use backdoor
 - Attempt to "phone home"
 - Attempt to steal user names, password by keylogging
 - Attempt to send information to remote server
 - Attempt to modify OS setting
 - Attempt to affect execution of desktop products
 - Attempt to add code to existing installed application on desktop
- Proactive behavior-based solution that operates in real-time to block **known** spyware
 - Block known spyware by auto updated list of known Spyware (by CLSID and previously detected and cached Spyware)
 - Block known spyware by auto updated list of known URLs hosting spyware
- Detects Spyware that tries to exploit known vulnerabilities
- Minimizes over-blocking to allow business as usual
- Centralized web-based management and single point of provisioning
- Extensive reports provide valuable network information
- Blocks already-installed Spyware from "calling home" to known Spyware websites
- Automatic security updates and product upgrades enhance security and reduce total cost of ownership

Research-Driven Security Policy

The **Vital Security™ SDK** operates in accordance with Finjan's default security policy, reflecting the extensive security knowledge and expertise of Finjan's MCRC researchers. MCRC is Finjan's leading research department, dedicated to the discovery of security vulnerabilities in Internet and email applications that could be exploited for malicious purposes. MCRC's goal is to continue to be steps ahead of hackers attempting to exploit open platforms and technologies to develop malicious code such as worms, Trojans, viruses and spyware. MCRC researchers work with the world's leading software vendors to help patch their security holes, as well as contributing to the development of next generation defense tools for Finjan's proactive secure content management solutions.

The security policy is comprised of Behavior-Based Security and Vulnerability Anti.dote rules, as well as Spyware objects, which are defined and updated by MCRC. For example, based on Finjan's extensive database of known vulnerabilities, Finjan's MCRC security experts create behavioral rules that enable the Vulnerability Anti.dote scanners to identify and block any attempt by active content to exploit one or more vulnerabilities.

Additional SDK Features and Benefits

- **Comprehensive Logging** – The SDK scanning engines accumulate transaction information and download to a central logging server. The extensive logging capabilities provide IT managers with easy access to critical operational information.
- **Flexible Reporting** - An advanced reporting infrastructure allows the SDK customers to offer predefined reports or user defined reports that may be generated on known information (e.g. list, actions, transactions, policy, rule, filter, etc). The reports may be displayed at different levels (vulnerabilities, active content types, etc.) for different types of users.
- **Security updates** - Finjan provides weekly security updates which leverage the unparalleled knowledge and expertise of our MCRC security researchers to continually refine and update the level of security in our Vital Security Web Appliances. The security updates include the following:
 - Updates to Vulnerability Anti.dote™ rules to provide customers with virtual patches against newly discovered or published vulnerabilities
 - Updates to Behavioral rules, e.g., in the case of a new type of attack for which new behavior needs to be detected
 - Updates related to new Spyware objects

Finjan's security updates further enhance the value of the **Vital Security™ SDK**, keeping Finjan customers/OEM partners steps ahead of the increasingly sophisticated hacker community.

- **Multi-Threading** – This feature lets vendors run multiple threads of the SDK in parallel for separate pieces of content, thus enhancing system performance.
- **Dedicated SDK Support** – Finjan offers dedicated support services for the SDK. Integration support is provided by Finjan's R&D team, while security support is provided by MCRC. In addition, educational training (non-technical) is available related to the specific capabilities of the behavior-based security and Vulnerability Anti.dote scanning engines (in coordination with Finjan).
- **Supported Platforms:**, Linux, FreeBSD, Windows

Advantages over Packet Level and Other Types of Security Solutions

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.

Conclusion

In light of the growing magnitude and increasing sophistication of web-based security threats, such as Spyware, businesses require intelligent, proactive security solutions. These solutions must be able to analyze and identify the behavior of Active Content in real time, in order to block malicious and inappropriate content from reaching corporate desktops, while allowing appropriate business content to flow in a transparent and uninterrupted manner.

By integrating Finjan's **Vital Security SDK** within their existing content management systems, gateway vendors will be able to offer their customers the highest available level of Internet security against the new generation of malware threats. The **Vital Security SDK** incorporates Finjan's patented behavior-based and revolutionary Vulnerability Anti.dote technologies to provide unmatched proactive security against new, unknown attacks and vulnerabilities before software vendors issue a patch and before the first virus or exploit of a specific vulnerability is even born.

These unique capabilities are the reason why the Pentagon, FBI and most of the federal banks in the Western world use Finjan's security solutions to protect their vital assets and information. In businesses and organizations where security truly matters, Finjan is the intelligent choice.

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.