

WHITE PAPER

**Securing End-Points Against
the Insider Threat
May 2010**



Securing End-Points Against the Insider Threat - May 2010

Abstract

This paper explores whitelisting and blacklisting technologies, and how they are used to protect an enterprise's end-points from the activities of cybercriminals and malicious insiders, and from the unintentional exposure of these systems to threats resulting from end-users' inadequate adherence to security best practices. Advantages and disadvantages of each technology are examined, and the reasons for whitelisting currently being the least deployed security technology are discussed. A defense-in-depth strategy, applicable to many enterprises, incorporating whitelisting on relatively static end-points and in locked-down environments, while implementing blacklisting on typical end-user systems is presented. A specific example of blacklisting, implementing anti-virus, anti-spyware, and host intrusion prevention with comprehensive and customizable application blocking rules, is discussed, and its effectiveness is empirically measured. This approach is concluded to provide effective protection against threats posed by virus, worms, bots and Trojans and enforces an organization's unauthorized applications use policies on endpoints where whitelisting is neither appropriate nor desirable.

The Insider Threat

The 2010 Cyber Security Watch Survey conducted by CSO magazine concluded that the most costly or damaging attacks were attributed to insiders, defined as employees or contractors with authorized access. 51% of the 535 companies responding to the survey who experienced a cyber security event were victims of an insider attack. In the past 12 months the number of reported insider-related incidents increased by 16% and the monetary loss averaged \$394,700 per incident.^{1,2}

Given the increase in incidents originating with insiders, and the high average cost associated with each incident, are our endpoint protection strategies, particularly those centered around blacklisting technologies, like anti-virus and anti-spyware tools, sufficient for combating the insider threat?

Effectiveness of Anti-Virus and Anti-Spyware Technologies

A recent research report by Allen Corporation indicates that anti-virus and anti-spyware, while mature and effective technologies for detecting and mitigating threats posed by virus, worms, bots and Trojans, are much less effective at addressing threats posed by malware programs and tools commonly used by cybercriminals, particularly insiders, to compromise critical systems, to access sensitive information, and to leak that information out of the enterprise.

Continued...

Securing End-Points Against the Insider Threat - May 2010

Effectiveness of Anti-Virus and Anti-Spyware Technologies (Continued)

A high-detection rate of malware in combination with a low number of false-positives is one of the most important measures of the effectiveness of an anti-virus product. AV-Comparatives.org, an independent research organization, conducted on-demand detection tests in February and August 2009 of the anti-virus products of a number of leading manufacturers. The results for two of the most commonly used antivirus products, were as follows:

Symantec: ~98.6% detection, 20 false-positives
 McAfee: ~98.9% detection, 54 false-positive

The AV-Comparatives test set consisted of 1,562,092 instances of malware including: Windows viruses, macro viruses, script malware, worms, backdoors/bots, Trojans, and other malware.³

Another set of benchmarks conducted by Allen Corporation of America tested the ability of these same two vendors' products to detect the presence of various types of malware commonly used by insiders to compromise systems and access and leak business critical and confidential information.

Categories of malicious code and programs included steganography, Trojans, keyloggers, encryption, password crackers and wireless hacking. The categories and datasets were selected from those used in cases involving post-incident malware discovery over the past ten years with WetStone Technologies' Gargoyle Investigator™ – Forensics Pro, a leading digital forensics tool. WetStone Technologies is a subsidiary of Allen Corporation.⁴

Symantec Results – Anti-Virus and Anti-Spyware

Malware Category	# of .exes in dataset	# of files detected	% of files detected
Steganography	947	12	1.3%
Trojans	3151	2690	85.4%
Keyloggers	3222	1533	47.6%
Encryption	2583	2	0.07%
Password Crackers	1534	150	9.8%
Wireless	648	127	19.6%

Continued...

Securing End-Points Against the Insider Threat - May 2010

Effectiveness of Anti-Virus and Anti-Spyware Technologies (Continued)

McAfee Results – Anti-Virus (with Artemis) and Anti-Spyware

Malware Category	# of .exes in dataset	# of files detected	% of files detected
Steganography	947	8	0.8%
Trojans	3151	2674	84.9%
Keyloggers	3222	689	21.4%
Encryption	2583	23	0.9%
Password Crackers	1534	91	5.9%
Wireless	648	127	19.6%

As one might expect, the anti-virus/anti-spyware products from these leading security vendors successfully detected a high percentage of Trojans in the test dataset. However, these products were only modestly successful at detecting keyloggers and wireless hacking tools. They fared the worst at detecting password crackers, steganography, and encryption tools.

Since the capabilities tested were representative of blacklisting technology, is there a way to improve the success rate of blacklisting at detecting these particularly insidious forms of malware or is it time to consider other approaches, such as whitelisting?

Blacklisting versus Whitelisting

The most common technology for dealing with malware is known as blacklisting. In blacklisting protection models, signatures that identify the characteristics of known pieces of malware are distributed to endpoint-resident tools, and these tools attempt to detect, clean, quarantine, or delete the offending code. However, as more sophisticated intrusive software becomes widespread, particularly with regards to those variants of malware that continuously morph to obfuscate their identity, some security vendors are advocating a change in tactics. These vendors contend that instead of waiting for malicious code to run in the first place, only authorized software should be permitted to install and execute on an end-point. This technology, called whitelisting, can be a very effective in some instances. However, whitelisting often comes at a high cost that an enterprise must weigh prior to adoption. For IT administrators, maintaining a whitelist can be very expensive in terms of time and resources, and the system lock-down that results often runs into significant resistance from employees.⁵

What factors should be considered when determining whether whitelisting, or blacklisting, or a combination of the two is appropriate as an endpoint security tactic for a particular enterprise?

Securing End-Points Against the Insider Threat - May 2010

Types of Whitelisting Technologies

There are various approaches to whitelisting.

In cloud-based whitelisting solutions, when a piece of code attempts to execute on a locked-down endpoint the hash of that executable is compared with a list of hashes in a vendor-maintained master database. That database is accessed via WAN links. Thus, challenges include the network latency involved (and, is protection lost entirely when the WAN link is severed?), and the dangers posed by allowing malicious software to be run on an endpoint when the master database becomes compromised or “poisoned”. The currency of the database contents can also be a big issue, since one must wait to patch systems until the master database is updated with the hashes corresponding to the latest application or system software updates. One must also determine how to handle software that is not defined by the whitelisting vendor as malware but violates a subscribing organization’s unauthorized use policy.

Another whitelisting technology variant requires that a local database be built containing hashes of all the executables in the local network. Just like vendor-supported cloud-based whitelisting solutions, network latency can again be an issue as is the potential for database poisoning. An examination of every executable in the database is required to determine whether or not it is authorized, and while custom code can be more easily added to a locally maintained database than to one that is vendor maintained, the review process is time-consuming and error-prone. Another issue include the resources required to make database changes necessary to authorize new applications and updates to existing applications. This can result in delays to updating software on endpoints and require that protection be turned off while making database changes.

Host-based application whitelisting identifies and authorizes the set of executables loaded on the host or in a “gold-build” at the time that the whitelist application is run. A major disadvantage of host-based whitelisting is poisoning the whitelist with malware that is present at the time of whitelist creation. Like all whitelisting technologies, management can be resource-intensive, and the time required to relearn the whitelist on a new build, can delay the rollout of system and application updates.⁶

Factors in the Slow Adoption of Whitelisting

For all of the promise that whitelisting offers for protecting endpoints against the threat of metamorphic and polymorphic malware and unauthorized applications, a McAfee survey conducted in September 2009 of 600 IT executives worldwide identified it as the least widely adopted security measure, implemented by fewer than one-fifth of organizations.⁷

Continued...

Securing End-Points Against the Insider Threat - May 2010

Factors in the Slow Adoption of Whitelisting (Continued)

In general whitelisting has a reputation for being time-consuming, and difficult and costly to manage because it requires keeping the control list of whitelisted applications fully up-to-date on any end-point where it is deployed. While whitelisting does offer protection against malware and the use of unauthorized applications, it can get in the way of the immediate use of applications for which employees have a legitimate need, slowing business efficiency and stifling innovation. Thus, a major impediment to the acceptance of whitelisting is the corporate employee who rebels against it.

Whitelisting can be most useful when it is used on application and DNS servers, point-of-sale systems, ATM's, and highly-controlled or static corporate environments, such as call centers in which workers do not need to install applications on demand to get work done.^{8,9} For these reasons whitelisting should not be viewed as an all-in-one solution for end-point protection, but instead be a component of a defense-in-depth strategy.¹⁰

A Defense-in-Depth Approach to Securing Endpoints-Black Listing and Whitelisting

As has been noted, whitelisting may be an acceptable security tactic for a select number of endpoints in an enterprise, particularly those in a static or highly controlled environment, where the lock-down restrictions of whitelisting, and the complexity and cost associated with its implementation and administration can be justified. However, blacklisting technologies support greater user flexibility and can be used to enforce endpoint protection, including unauthorized use policies, by implementing anti-virus, anti-spyware, and host intrusion prevention on the remaining endpoints where whitelisting is not appropriate or desirable.

A case study of this approach was described in a December 2009 *Network World* article. A credit union experienced significant pushback from employees to the restrictions imposed by the deployment of whitelisting on end-user systems. In response, instead of locking down employee desktops completely, IT now enforces the credit union's unauthorized use policy by deploying a host-based intrusion-prevention system to blacklist applications such as P2P programs, games, and administration tools.⁸

Commercial solutions increasingly bundle anti-virus, anti-spyware, desktop firewall, and host-based Intrusion Prevention Systems (IPS), as well as application whitelisting and blacklisting. Most endpoint security solutions can examine the name, location, and/ cryptographic hash of a given executable to determine whether it should be permitted to run on the protected endpoint. The most effective of these tools offer custom whitelists and blacklists based on executable path, hash, or regular expression matching.¹¹

Securing End-Points Against the Insider Threat - May 2010

Using Host Intrusion Prevention with Custom Application Blocking Rules to Protect Endpoints

An example of a widely-deployed commercial endpoint security solution that bundles anti-virus, anti-spyware, personal firewall, and host-based IPS (HIPS) technologies, along with software whitelisting and blacklisting, is McAfee Total Protection for the Endpoint. The implementation of the various capabilities of this solution are well-documented by the vendor, and a discussion is outside the scope of this paper. However, as noted in the introduction to this paper, despite the strengths of the leading security vendors' blacklisting solutions for mitigating risks associated with viruses, Trojans, bots, and worms, out-of-the-box these solutions do not address the threats associated with unauthorized applications as fully as a locked down environment based on whitelisting. Given that whitelisting is often an unacceptable solution for end users, a process for improving the capability of the vendor's blacklisting technology to recognize and block the execution of unauthorized applications commonly deployed by cybercriminals and malicious insiders is required.

McAfee refers to some types of unauthorized software as potentially unwanted programs (PUPs). PUPs include such unwanted programs as Trojans, spyware and adware, along with other types of malware that may compromise an end user's privacy. Some antivirus and PC security software packages, like McAfee's VirusScan Enterprise and McAfee Anti-Spyware, will scan an endpoint and protect it from some PUPs.

There is no industry standard categorization of PUPs. McAfee Labs breaks PUPs down into 6 major categories and an OTHER category.

- **Spyware:** Software whose function includes the transmission of personal information to a 3rd party without the user's knowledge and explicit consent.
- **Adware Software:** Software whose primary function is to make revenue through advertising targeted at the person using the computer on which it is installed. In some cases personal information may be captured or transmitted as a function of the software.
- **Password Crackers:** Software designed to allow a legitimate user or administrator to recover lost or forgotten passwords from accounts or data files. These same tools, when used by an attacker, allow access to confidential information, and represent a security and privacy threat.
- **Remote Administration Tools:** Software designed to allow remote control of a system by a knowledgeable administrator. When controlled by a party other than the legitimate owner or administrator, remote administration tools are a significant security threat.
- **Dialers:** Software that redirects internet connections to a party other than the user's default ISP for the purpose of securing additional connection charges for a content provider, vendor, or other third party.

Continued...

Securing End-Points Against the Insider Threat - May 2010

Using Host Intrusion Prevention with Custom Application Blocking Rules to Protect Endpoints (Continued)

- **Jokes:** Software that has no malicious payload or use, and does not impact security or privacy states, but may alarm or annoy a user.
- **Other PUPS:** Many innocuous pieces of software, such as FTP servers, have been misused to assist the replication or payload behaviors of traditional malware.¹²

The presence of hacker tools such as virus kits and spam tools on a system probably indicates objectionable or even illegal (depending on the jurisdiction) activity originating from that endpoint. Allen Corporation's Cyber Security Division, WetStone Technologies, has provided a widely-used application, Gargoyle Investigator Forensic Pro, that digital investigators have used over the past ten years to detect and classify malware, including hacker tools, as part of the process of collecting forensic evidence. One can extend and refine the category of "Other PUPS" by using these Gargoyle categories. These include:

- **Anti-Forensic Programs:** Products used to circumnavigate computer forensic procedures. These products include drive erasers, internet history erasers, and evidence altering tools.
- **Botnet Programs:** Various programs that exploit vulnerable computers causing them to forward transmissions, including spam or viruses, to other vulnerable systems unbeknownst to their registered owners. These applications are becoming an increasingly popular method to launch Distributed Denial of Service attacks.
- **Credit Card Fraud Programs:** Products used to generate and validate credit card, ATM card and calling card numbers.
- **Denial of Service Programs:** Various products that can be used to disable, disrupt, or overload communication channels to a targeted computer.
- **Encryption Programs:** Products used to encrypt and decrypt various types of information and files. Most applications separately allow data files to be encrypted using an assortment of algorithms, key types, key lengths and passwords.
- **Exploit Scanning Programs:** Products used to detect vulnerabilities in local and remote systems. Other forms of malicious software can then exploit these vulnerabilities.
- **File Splitting Programs:** Products used to split files into fragments.
- **Gaming Program:** Dataset consists of various products that allow an individual to play games both online, against other individuals, or on a local computer. The games consist primarily of casino style games that allow for online gambling.
- **Key Logging Tools:** Products used to record, analyze and possibly playback, a set of keyboard keystrokes, mouse movement, and mouse clicks. Every program records the user actions to some degree and provides a reporting mechanism for reviewing them.

Continued...

Securing End-Points Against the Insider Threat - May 2010

Using Host Intrusion Prevention with Custom Application Blocking Rules to Protect Endpoints (Continued)

- **Peer-to-Peer (P2P) Programs:** Programs used to host, share, and easily transfer files amongst users communicating on a fixed protocol. P2P file-sharing programs are of concern for a number of reasons: They often act as the carrier for a wide variety of other adware and spyware, there may be legal liability for some users because of real or potential copyright violations and they are often a vector for viruses, which often copy themselves to shared P2P directories in the hopes of enticing another victim to install them.
- **Password Cracking Tools:** Applications used to break a password set on a computer or various files. Each application supports a specific type or set of types of files. Some applications are used to break BIOS passwords. Password cracking programs generally use one or more of four common methods: brute force attack, dictionary attack, common word attack, or weaknesses in the application password implementation.
- **Piracy Tools:** Products used to bypass copyright protection technologies. Programs primarily work against DVD movies but also will function with various software titles.
- **Remote Access Programs:** Products used to acquire access on systems remotely.
- **Rootkit:** Dataset consists of tools used to gain access to vulnerable systems at the kernel and application level.
- **Network / Packet Sniffer Programs:** Products used to capture and monitor network traffic.
- **Surveillance and Monitoring Programs:** Products used to covertly spy on computer systems.
- **Steganography Programs:** Various steganographic information-hiding tools used to create channels of hidden communication. The use of steganographic tools requires minimal technical knowledge.
- **Virus and Malware Toolkit:** Pre-packaged products used as a toolkit for building viruses and hacking systems.
- **Trojan Programs:** Various products that provide the ability for a client component to be covertly introduced onto a victim's computer. Once infected, a server component can remotely access the victim's system. Information can be taken or the system may be used to attack others. The dataset does not contain any viral applications, or ones that specifically are used to destroy files or reformat systems. Although it should be noted that these actions are possible with some of the client/server Trojans.
- **Wireless Surveillance:** Products used to detect wireless access points, capture wireless network traffic, plot on a map previously recorded access points, and possibly break the WEP encryption on an access point.

Continued...

Securing End-Points Against the Insider Threat - May 2010

Using Host Intrusion Prevention with Custom Application Blocking Rules to Protect Endpoints (Continued)

Utilizing the API's available through McAfee's Security Innovation Alliance Program, Allen Corporation extended and refined the categories of PUPs that can be detected by McAfee end-point protection solutions. The commercial product resulting from this integration is called Advanced Threat Identification – Preemptive Defense (ATI-PD). Using the large database of malware hashes from Gargoyle Investigator Forensic Pro, Host Intrusion Prevention (HIPS) policies with custom blocking rules are created with the McAfee security manager, ePolicy Orchestrator. The resulting policies implement rules that detect and prevent execution of malicious code in real-time. Endpoints can be more thoroughly protected against a larger universe of malicious and unauthorized programs without implementing the more restrictive whitelisting protection, as illustrated in the table below.

Malware Category	# of malware executables in test dataset	# of executables detected by Symantec	# of executables detected by McAfee	# of executables detected and blocked by McAfee + ATI-PD
Steganography	947	12 (1.3%)	8 (0.8%)	947 (100%)
Keyloggers	3222	1533 (47.6%)	689 (21.4%)	3222 (100%)
Encryption	2583	2 (0.07%)	23 (0.9%)	2583 (100%)
Password Crackers	1534	150 (9.8%)	91 (5.9%)	1534 (100%)
Wireless	648	127 (19.6%)	127 (19.6%)	648 (100%)
TOTAL	8934	1824 (20.41%)	938(10.5%)	8934 (100%)

Summary

Whitelisting will most often be an acceptable security tactic for endpoints having a static application environment, such as those in call centers, as well as DNS servers, application servers, POS terminals, ATM's, and that small subset of user-endpoints with especially critical information resident on them. Blacklisting technologies are considered less effective at blocking unknown threats than whitelisting, but require significantly less resources to administer, and permit greater user flexibility. Blacklisting can be used to enforce endpoint protection, including unauthorized use policies, by implementing anti-virus, anti-spyware, and host intrusion prevention with custom application blocking rules on the remaining endpoints where whitelisting is not appropriate or desirable.

Continued...

Securing End-Points Against the Insider Threat - May 2010

Summary (Continued)

An example was given of a credit union where, after significant pushback from employees to the restrictions imposed by whitelisting, instead of locking down employee desktops completely IT chose to enforce an unauthorized use policy. This policy prevents users from using P2P programs, games, admin tools or using USB devices by utilizing anti-malware tools and a host-based intrusion-prevention system, to blacklist unauthorized applications.

A widely-deployed commercial end-point protection bundle is McAfee Total Protection for Endpoint. McAfee refers to some unauthorized software as potentially unwanted programs (PUPs). PUPs include such unwanted programs as Trojans, spyware and adware, along with other malware that may compromise an end user's privacy. McAfee's VirusScan Enterprise and McAfee Anti-Spyware, will scan an endpoint and protect it from some PUPs.

Test results from AV-Comparatives and Allen Corporation, document that the anti-virus and anti-spyware technologies incorporated in commercial end-point protection solutions, such as those from leading vendors like Symantec and McAfee, are adept at detecting and mitigating risks posed by viruses, bots, worms, and Trojans. However, their abilities to detect and block the execution of other categories of malware, i.e., in the McAfee PUPs category, are less effective.

Allen Corporation demonstrated that it could significantly improve the detection and mitigation of PUPs by creating custom host intrusion system policies which integrate a comprehensive set of malware hash signatures as application blocking rules. The database of signatures on which this solution was based was the result of research conducted over a period of ten years in the computer forensics space.

About the Authors

Chet Hosmer is the Chief Scientist at Allen Corporation's Cyber Security Division, WetStone Technologies, and may be reached at chosmer@allencorp.com.

Carlton Jeffcoat is the VP of Cyber Security Technologies at Allen Corporation and can be reached at cjeffcoat@allencorp.com.

Securing End-Points Against the Insider Threat - May 2010

Sources

1. *2010 Cybersecurity Watch Survey*; www.cert.org/archive/pdf/ecrimesummary10.pdf; Conducted by *CSO* magazine in cooperation with the U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Deloitte; January 25, 2010.
2. *Operational Risk Management – Corporate Intelligence Unit (CIU) blog*; <http://operationalrisk.blogspot.com/2010/04/ciu-corporate-intelligence-unit.html>; April 1, 2010
3. *Anti-Virus Comparative- Summary Report 2009*; <http://www.av-comparatives.org/images/stories/test/summary/summary2009.pdf>; December, 2009
4. Geoff Barron and Matthew Davis, *ATI Dataset Research Report (Allen Corporation of America Internal Research Report)*; January 14, 2010
5. Jack M. Germain, *Blacklisting and Whitelisting: Color Coding Security*; TechNewsWorld; October 9, 2008; <http://www.technewsworld.com/rsstory/64756.html?wlc=1273002389>
6. David Thomason; *Whitelisting Done Right*; http://www.securityevangelist.com/Home/Blog/Entries/2009/4/1_Whitelisting_Done_Right.html; April 1, 2009
7. Stewart Baker, Shaun Waterman, and George Ivanov; *Critical Infrastructure Protection In the Crossfire -Critical Infrastructure in the Age of Cyber War*; http://newsroom.mcafee.com/images/10039/In%20the%20Crossfire_CIP%20report.pdf
8. Ellen Messmer; *Whitelisting Made Strides in 2009*; Network World; December 18, 2009; <http://www.networkworld.com/news/2009/121809-outlook-whitelisting.html>
9. Ericka Chickowski; *Is Your Information Really Safe*; BASELINE; March 20, 2009; <http://www.bwise.com/bwise/download/articles-2009/baseline-03-20-09.pdf>
10. Angela Moscaritolo; *The White Knight: Application Whitelisting Solutions Gaining Appeal*; SC Magazine; <http://www.scmagazineus.com/the-white-knight-application-whitelisting-solutions-gaining-appeal/article/159964/>; January 1, 2010
11. SANS, *Twenty Critical Controls for Effective Cyber Defense: Consensus Audit: Critical Control 2: Inventory of Authorized and Unauthorized Software*; <http://www.sans.org/critical-security-controls/control.php?id=2>; November 13, 2009
12. *Potentially Unwanted Programs – Spyware and Adware* (McAfee White Paper); http://www.mcafee.com/us/local_content/white_papers/wp_antispyware_shadesofgray.pdf; September 2005