



Eric Ogren

92 Robert Road

Stow, MA 01775

m: 978-618-9240

eric@ogrengroup.com

Endpoint Security: Moving Beyond AV

An Ogren Group Special Report

July 2009

Introduction

Application whitelisting is emerging as the security technology that gives IT a true defense-in-depth capability, filling in the gaps that anti-virus (AV) was never designed to cover. Organizations have invested heavily in traditional AV solutions, often stacking AV filters from multiple vendors along the data path in the desperate hope that one of the products would stop malware from infecting the corporate or government endpoints. While AV plays a crucial role in identifying known malware and cleaning infected systems, the reality is that relying on layers of the same defense mechanism leaves organizations completely exposed to attacks and data theft from unknown or designer malware that can be delivered in web-based active code, downloaded encrypted code fragments, and persistent botnets. Security teams that know they need more than AV are now deploying application whitelisting technology to protect laptops, desktops, server and Point-of-Sale endpoints from unidentified malicious code as well as undetected code injections - and they are finding significant operational benefits due to fewer interruptions responding to infected endpoints.

Whitelisting defines a trusted application environment that prevents any unknown or unwanted software, including sophisticated and unknown malware, from executing. The underlying mechanism for this enforcement is fundamentally different from traditional blacklisting AV technologies. Application whitelisting is characterized by the ability to identify authorized executables and associated files and to treat as an attack any program or file that is not on the authorized whitelist. This allows IT professionals to establish a policy based on a reference configuration model of operating system, business applications, and user executables with the ability to deflect any attempts to change the approved configuration such as attacks burrowing into existing files to evade AV scanners. Recent advances in application whitelisting, including automatically approving files from trusted sources (e.g. Microsoft or corporate IT) to reduce administrative overhead or allowing end-users to personalize their endpoint for greater user acceptance, has made application whitelisting an attractive choice for augmenting AV.

AV utilizes signature-based pattern matching schemes to detect known malicious attacks. While this approach provides a good understanding of what known bad applications have infiltrated a system, the usefulness of AV as a frontline defense is continuously diminishing. Developers of malicious code know that AV vendors cannot push out signature updates in time to stop an attack, cannot readily recognize Internet and USB-borne attacks, and are not even very good at detecting attacks that are sitting on the disk of the endpoint. If AV does recognize an attack, it is good at blocking the attack and at erasing symptoms of the attack, but AV comes with an unacceptably high cost and a shockingly low catch rate. Many security teams have come to the realization that they need more than AV to be protected against today's malware threats.

This Ogren Group Special Report, *Endpoint Security: Moving Beyond AV*, commissioned by Lumension, presents the market demand for application whitelisting with recommended actions for security decision makers. Information in this report derives from Ogren Group research and interviews with enterprise security executives of global organizations.

Why AV is Not Enough

IT organizations are finding that they have placed too much trust in the ability of anti-virus products to protect desktops and servers from malicious attacks. AV, pioneered in the 1980's, has captured large chunks of the corporate security budget with anti-virus subscriptions for endpoints, gateway devices, mail servers, and service provider networks. However, this has amounted to organizations spending their product and support budgets on redundant technologies that are not effectively protecting the technical infrastructure for the business.

The evidence, as presented in Exhibit I, is clear and compelling. There is a pandemic of malicious code that completely overwhelms IT architectures that depend on identifying each and every attack. If AV was capable of blocking malware, the world would not be experiencing more than 16 million cyber-attacks per year. Software development of malicious programs has become a vibrant industry largely because the malware products can easily evade detection by anti-virus scanners to achieve their goal of stealing identities or other confidential information. Unfortunately, malicious code development is big business, and it is big because not enough organizations have recognized the limitations of AV and continue to rely on limited technology to thwart new and emerging threats.

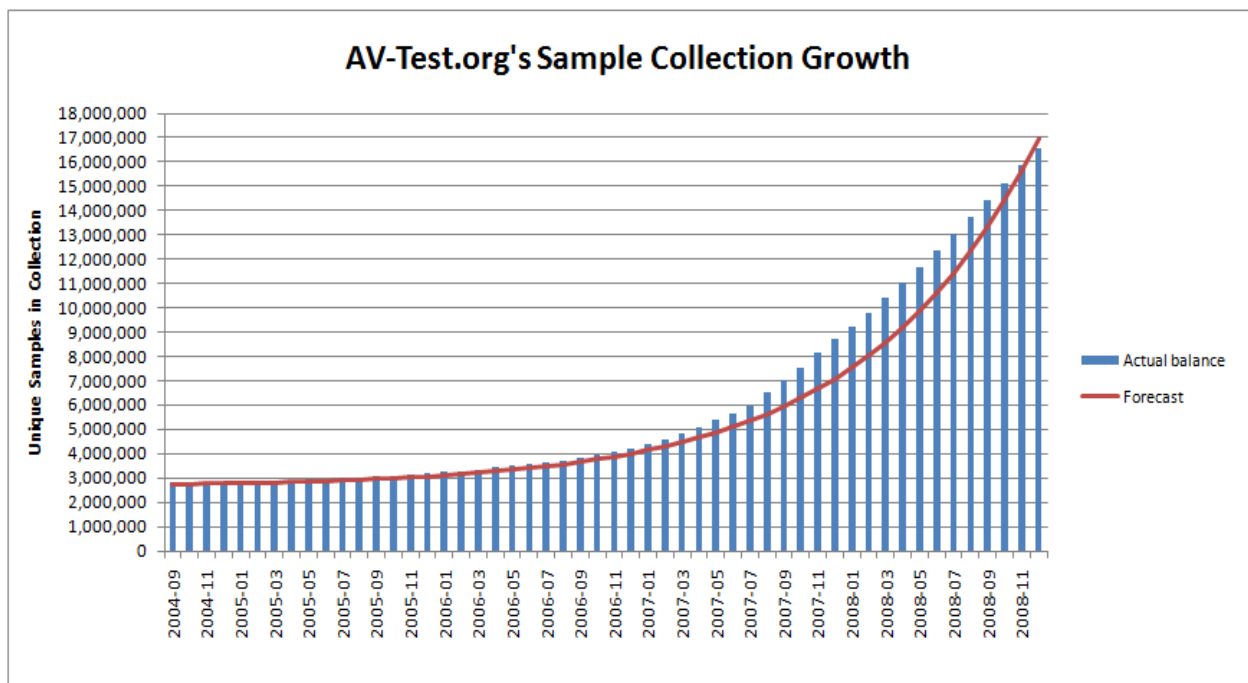


Exhibit I

The explosive growth in malicious programs depends on an over-reliance on AV

Attackers know AV does not work as the primary endpoint defense. In fact, professional attackers use an array of anti-virus products in their quality assurance testing to be sure the attack will not be detected. The botnets, trojans, and targeted attacks are designed to steal sensitive information, and depend on the false security of AV. The problems with anti-virus are not easily fixed and include:

- **The *Window of Vulnerability* is always open.** The window of vulnerability is defined as the time between the launch of an attack and the time signature updates are received at the endpoint. (This is also the zero day attack which is malware without a corresponding AV signature). There is a window of vulnerability caused by the delays to discover the existence of a new attack, analyze the attack to plan an antidote, develop a defensive attack signature with eradication logic, and distribute

the new signature to all subscribing endpoints. No matter how efficient the AV vendor is, the attack will always spread quickly before the window of vulnerability can be closed.

- **Anti-virus approaches are not effective against attacks that penetrate via active code in browsers, or are carried in on USB devices.** Unfortunately, anti-virus was originally designed for scanning files as they are created and not for today's Internet world. Internet-borne attacks that penetrate through the browser show the sharpest growth rate of all attack classes for 2009. Similarly, infected USB devices are seldom scanned for malware when connected and easily defeat AV systems. Two recent examples include Conficker worm, which leverages USB devices as one of its methods for propagation, and the US Army incident where an infected USB device spread malware over government networks, causing the Department of Defense (DoD) to issue a ban on the use of USB devices.
- **Behavioral techniques are not deterministic and generate unacceptable amounts of false positives that security teams must investigate.** AV products try to augment signature scanning with behavioral methods that look for anomalies in the processing of the endpoint, such as executables creating files in system folders or programs exhibiting unusual network traffic. The main problem with behavioral methods is that AV software cannot always differentiate between attack code and valid application logic, which leads to IT spending precious time to investigate erroneous reports of an attack. Even if there is an attack, a behavioral approach will not be able to tell what damage occurred before the anomalous behavior was detected, and hence cannot clean the attack from the endpoint.
- **Users and administrators may install software that takes the endpoint out of compliance.** Insiders show initiative when installing software or modifying endpoint configurations to execute unauthorized applications. IT needs a means of protecting the system components of the endpoint to minimize the risks of malware infections from user error and malicious intent.

Malicious programs must exist on the endpoint's disk if the malware is to survive reboots and on/off power cycles. In some cases the attack creates new files in system folders that users cannot recognize; in other cases the malware modifies known executables to embed attack code. Not only does AV miss the attack upon penetration, AV also usually fails to detect the attack during full disk scans conducted well after the infection.

The result of a successful attack is the business disruption of an IT cleaning operation to reset the endpoint to a compliant state after an attack. Users notice performance degrading and place a call to the service desk, security responds by investigating the problem, IT refreshes the endpoint with a new desktop image, and then documents the service call. The true cost of malicious attacks includes substantial IT time and effort to clean infected endpoints. One organization, John C. Lincoln Health Network determined that each year, 15% of their computers would require service; 30% required reimaging and 70% needed the installation of more memory. The direct costs that John C. Lincoln Health Network incurred from reimaging each PC were \$250.00. The indirect costs associated with reimaging a PC were estimated at \$150.00. Added up over the course of a 4 year time frame, by leveraging whitelisting technology, John C. Lincoln Health Network has been able to reduce costs associated with helpdesk and endpoint cleanup from malware or unauthorized configurations by \$860,000; this includes headcount reduction, cost of computer reimaging, cost of computer upgrading, and cost to replace computers.¹

IT organizations recognize that they need more than AV to maintain compliant configurations, to reduce costs from security incidents associated with infected endpoints, and to protect sensitive information from loss due to targeted attacks.

¹ The Total Economic Impact of Lumension Security's Sanctuary Application And Device Control. September 2007.

The Evolution of Application Whitelisting

Application whitelisting has evolved to be the choice for security organizations to protect laptops, desktops, and servers when they need more than AV. Anti-virus technology is good at the perimeter to filter known attacks from legitimate network traffic, and it is required to identify and categorize an attack to clean the endpoint after infection. However, application whitelisting provides the proactive help that AV needs to secure endpoints, reduce the risk of exposing confidential data, and control escalating costs from malware-induced security incidents.

The most attractive feature of application whitelisting is its capability to close the window of vulnerability without false positives or adverse affects on the business. Application whitelisting does not react to attack notifications – it treats any unexpected changes to the endpoint configuration as an attack and acts to block the change before any damage can occur. Since IT and security teams define the whitelist of approved application executables, files and operating system components, the whitelisting approach does not suffer from false positives and is completely controlled by IT. Application whitelisting does not need to know the specifics of an attack, it knows that there is a violation of security policy and automatically blocks the offending action in real time.

Application whitelisting is a mature technology that has seen significant evolution that makes the approach suitable for complementing AV on laptops and desktops as well as servers across the enterprise. The top three innovations in application whitelisting include:

- **Excellent performance, especially when compared to AV.** Whereas anti-virus has to check a list of more than 16 million attack signatures plus testing for anomalous behavior, application whitelisting can process a much shorter list of executables that are allowed to run and system files that are allowed to be modified. The higher performance of application whitelisting makes it a particularly good fit for locking down server configurations and for securing end-user computers without impeding response times.
- **IT administration is simplified by associating protected applications with trusted sources.** Application whitelisting has evolved to allow files from a trusted source to automatically appear on the whitelist without the need for IT or security to review. For instance, all software from Microsoft including executables, files, and patches are transparently added to the whitelist and are allowed to execute. Similarly, security can define in-house development as a trusted source of applications to facilitate the identification of programs that are allowed to execute. This saves IT and security teams significant administrative effort, while keeping a strong security profile through application patching and upgrades.
- **End-users can still personalize the endpoints while IT protects privileged areas of the endpoint.** IT needs to accommodate the needs for end-users to run personal applications on the endpoint without weakening security and operational controls. Application whitelisting locks down servers where IT can specify a software bill-of-materials of executables and files that will seldom change. Similarly, application whitelisting protects the core elements of desktops and laptops while optionally allowing the end-user to add to the list of acceptable programs, IT ensures the integrity of the operating system and business application components, allowing the end-user to include personal applications for a customized look and feel.

The security benefits of application whitelisting are apparent – with minimal IT overhead the security software enforces application usage policies across the entire organization. Organizations needing more than AV to protect their servers and end-user endpoints are finding that application whitelisting tightens security around endpoints against attacks and even inadvertent administrative changes. IT also removes costs from supporting the infrastructure dues to decreases in malware-related service desk calls, cleaning endpoints after an infection (including complete system refreshes), and extra reporting procedures for compliance. In fact, EC Suite, a Lumension customer in the credit card processing business, estimates that application whitelisting generates *annual* savings of \$40,000 by blocking attacks and reducing end-user calls to the IT service desk.²

² Lumension Security: a Case Study in Proactively Managing Endpoint Risk. November 2008.

In addition, application whitelisting supports an integrated approach between IT, security, and application teams. Because application whitelisting focuses on the applications and systems that drive the business (and not peering into the underworld to focus on attacks like AV), whitelisting offers substantial operational benefits to enterprises in the areas of application discovery, policy enforcement, application usage auditing, and compliance reporting as shown in Exhibit 2.



Exhibit 2
Lumension application whitelisting operational benefits

Organizations stand to benefit from the increased security of not executing unwanted programs as well as the operational benefits of greater control over endpoints.

1. **Discover applications and files in use on endpoints.** Application whitelisting helps build an inventory of *actual software in use* throughout the organization. This intelligence gathering is an essential first step in creating acceptable use application whitelisting policies, as well as providing valuable information for software licenses deployed throughout the enterprise.
2. **Ensure compliant configurations through application whitelisting policy enforcement.** The security software ensures that attacks do not execute, configurations do not drift with unauthorized software installations, and attacks cannot hide by modifying protected files. End-users suffer fewer disruptions due to infected devices while IT finds that security incidents consume less time from the service desk and security personnel.
3. **Monitor activity to keep application whitelisting in tune and to understand application usage patterns.** The application needs of an organization are dynamic and shift over time. Application whitelisting captures application usage intelligence for requested executables and correlates with user role definitions to allow security policy to easily evolve with business needs. The monitoring of application usage allows IT to optimize whitelists for business performance and gives IT specific insight into which applications are most useful to the business.
4. **Automatically generate compliance and acceptable use reports.** Compliance mandates that IT control critical resources against malicious code and subsequent loss of sensitive data. Application whitelisting generates correlated reports that save IT time and energy in documenting the state of compliance of endpoints, and compliance with enterprise-wide software licensing terms.

Conclusion

Anti-virus technology is no longer up to the task of being the primary means of securing laptop, desktop, and server endpoints against the new generation attacks from Internet-borne active code, coordinated botnets, or encrypted designer code downloaders . Relying primarily on AV in today's dynamic threat environment, leaves businesses at increased risk due to data theft from malicious code executing on endpoints. Signature-based approaches cannot keep pace with new attacks nor have any winning chance of recognizing a new variant of a historically effective attack.

Leading IT organizations are now augmenting AV with application whitelisting to better control desktop and server infrastructures and detect and block inappropriate actions before serious damage occurs. Anti-virus software still has its purpose but businesses need more than AV on endpoints to protect against all forms of malicious attacks. IT teams would do well to investigate endpoint security technology that includes application whitelisting, and pilot the solution in a controlled datacenter environment to measure the results. At a minimum, organizations should deploy whitelisting solutions on mission critical servers where static configurations are easy to lock down and the performance penalties of signature suites are unacceptable. IT and security teams are advised to re-examine application whitelist innovations in personalization support and trusted application sources while placing the technology on laptop and desktop endpoint. Malware designers have had the upper hand for too long – it is now time for endpoint security to move beyond AV.