PROTECT YOURSELF FROM ANTIVIRUS

Despite attempts to pivot from outdated security methodologies, traditional antivirus continues to fail in preventing security breaches on the endpoint. Although AV satisfies many regulatory, governance and compliance requirements by layering on multiple products, it saddles organizations with hidden costs while providing questionable security value. Case in point: although traditional AV solutions "protect" nearly every endpoint and server in the world, security breaches are still on the rise. Organizations that choose to replace traditional AV with more advanced technologies should select a security product that not only provides superior security value at the endpoint but also complements and natively integrates with a security platform to provide even higher levels of security across the environment.

This document highlights some of the hidden costs of operating an antivirus system – costs that may be intangible, difficult to quantify or unquestioned due to precedence. It also outlines five security requirements that any AV replacement technology or product must meet to prevent security breaches on the endpoint. The document concludes with a discussion of how Palo Alto Networks® Traps™ advanced endpoint protection enables organizations to replace their legacy antivirus with a multi-method approach to prevention that protects their endpoints from both known and unknown threats.

Table of Contents

Antivirus No Longer Offers Meaningful Security Value	3
The Hidden Costs of Antivirus	3
5 Security Requirements of AV Replacement	4
Traps Replaces Antivirus	5
Conclusion	7

Antivirus No Longer Offers Meaningful Security Value

By most accounts, traditional AV has existed since 1987.[1] Signature-based scanning of files has been the cornerstone of AV's ability to detect malicious content ever since. In the late 1980s and throughout the 1990s, signature-based antivirus provided adequate protection for endpoints and servers, given the nature, sophistication and frequency of attacks of that era. However, the effectiveness of this technology has diminished over time as operating systems, networks and applications have evolved. Today, there are simply too many variations of new and unknown threats for a signature-based approach to identify and block them in a timely fashion.

Legacy AV vendors have been slow to adopt new technologies and continue to rely on outdated methods to bolster the effectiveness of their offerings. Many have begun adding new capabilities, such as machine learning, to their endpoint security products. A deeper look into these additions, however, reveals that many are underdeveloped, disabled by default, or deliver only incremental improvements in malware coverage. Some require multiple products with separate endpoint agents to compensate for the shortcomings of the new additions. In fact, technologies such as digital signatures, virus scanning and heuristic analysis remain at the core of "new" endpoint solutions offered by most traditional AV vendors.

Attackers rely primarily on two attack vectors to compromise endpoints: malicious executables (malware) and vulnerability exploits. These vectors are used individually, or in various combinations, but are fundamentally different in nature:

- Malware is an often self-contained malicious executable designed to perform nefarious activities on a system.
- Exploits are weaponized data files or content designed to leverage software flaws or bugs in legitimate applications to provide an attacker with remote code-execution capabilities. Successful exploitation enables an attacker to remotely execute malware on a targeted endpoint.

To prevent attackers from compromising endpoints and servers, a security technology or product must prevent both malware and exploits, known and unknown. Signature-based scanning and traditional AV are woefully inadequate at detecting exploits, and cannot identify or prevent malware or exploits for which they have no signatures.

The Hidden Costs of Antivirus

Security technologies must balance the benefits they provide an organization with operational costs. The costs of operating an AV system extend beyond tangible staffing, operational, and licensing and support costs to areas that may be intangible, difficult to quantify or unquestioned due to precedence.

Operational Agility

As mentioned, traditional AV still relies heavily on signature-scanning technology that is not particularly flexible in supporting new applications, systems or platforms. Organizations that continue to rely on AV will invariably encounter obstacles in deploying and securing new technology that may offer significant business advantages (e.g., virtual desktop infrastructure).

Opportunity Costs

Supporting, operating and maintaining AV systems requires staff, time and resources that might otherwise be used to support projects with greater ROI. Security teams are frequently expected not only to support aging AV systems but also to cobble together capable security from different vendors and solutions that may take longer to integrate and ultimately offer lower security effectiveness than a single, natively integrated security platform.

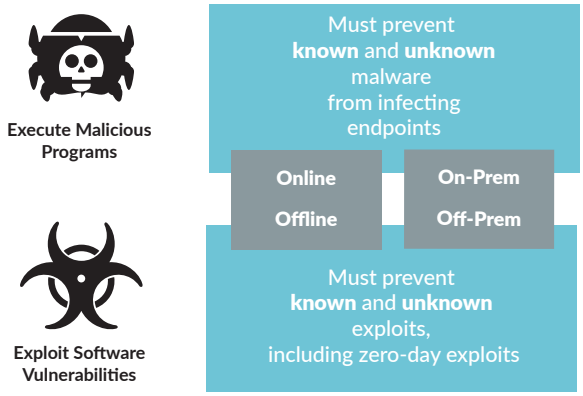

Figure 1: Effective endpoint security must prevent both malware and exploits

Increased Operational Burden

Traditional AV typically relies on heuristics and behavioral monitoring to detect exploits and evasive malware. These techniques are error-prone, generating alerts that falsely identify benign processes as malicious – commonly referred to as "false positives." As traditional AV vendors pivot to home-grown machine learning technologies, security teams are tasked with handling the potential influx of additional false positives common to many machine learning solutions. Enterprises may discover they simply do not have the staff to accommodate the increased operational burden. Given the security failures of traditional AV solutions, organizations may decide to abandon these vendors in favor of an automated next-generation security platform.

Unmitigated Risks Despite Compliance

Most security professionals would agree that regulatory compliance does not equal security. Although many compliance and regulatory frameworks, such as PCI DSS (Payment Card Industry Data Security Standards) and HIPAA (Health Insurance Portability and Accountability Act), require organizations to use various functions of traditional AV solutions, compliance does not guarantee security risks are sufficiently mitigated. As discussed earlier, maintaining traditional AV may force security professionals to deploy other technologies and products to mitigate security risks that AV cannot address. This, in turn, imposes additional tangible and intangible costs on the organization.

In addition, as advanced endpoint security offerings receive third-party validation for assisting in compliance with such regulatory frameworks and standards as HIPAA and PCI DSS, the decision to retain traditional AV solutions becomes harder to justify.

Fortunately, security practitioners now have access to superior technologies and products that both eliminate the need for traditional AV and far surpass it in security value.

5 Security Requirements of AV Replacement

Organizations that choose to replace their traditional AV with more advanced technologies should select a security product that provides the five capabilities that follow.

1. **Focus on Prevention First**

   As cyber breaches continue to increase in frequency, variety and sophistication, the whole security industry has struggled – and more often, failed – to prevent successful breaches. The industry's collective focus on EDR (endpoint detection and response) solutions is partially to blame for this. Better detection only narrows the window of time during which an attack is detected and does little to address the need for protecting valuable information before a compromise occurs. According to the Verizon 2016 Data Breach Investigations Report,[2] 81.9 percent of cyberattacks successfully compromise their targets within minutes. The recent increase in successful ransomware attacks highlights the shortcomings of legacy AV and EDR solutions in protecting systems during an ever-shrinking window of opportunity to detect and respond to cyberattacks.

   Breach detection and incident response do offer security value, but they must be secondary priorities compared to prevention. A focus on prevention is the only effective, scalable and sustainable way to reduce the frequency and impact of cyber breaches.

2. **Prevention of Known and Unknown Malware**

   A complete solution for preventing security breaches on the endpoint must also prevent the successful execution of malware, both known and unknown. To avoid the shortcomings of signature-based antivirus and minimize the operational impact of responding to false positives from behavioral monitoring, the malware prevention capabilities of the ideal product should not involve signatures or require prior knowledge of an instance of malware to prevent its execution. Additionally, effective prevention of both common and advanced malware necessitates the deployment of multiple analysis and prevention methods that can be tuned for maximum effectiveness.[3]

3. **Prevention of Known and Zero-Day Exploits**

   Threat actors who pursue the most effective means to circumvent existing endpoint security measures rely on exploits, especially those that leverage unknown software vulnerabilities (commonly referred to as "zero-day exploits"). Embedded in specially crafted data files and content, such as Adobe® PDF and Microsoft® Word documents, zero-day exploits manipulate legitimate applications to carry out nefarious activities. Their ability to evade traditional AV and a lack of vendor security patches often leave organizations with little in terms of preventive measures against exploits, especially the zero-day variety. A complete solution to preventing security breaches on the endpoint must therefore prevent known and unknown exploits from subverting legitimate applications.

4. **Automatic Integration of Threat Intelligence**

   With the proliferation of free and low-cost tools, threat actors can quickly generate new and unique attacks that evade detection by traditional signature-based antivirus. Organizations must use the threat intelligence gained elsewhere through encounters with new and unique attacks to prevent security breaches in their own environments. A replacement for AV must natively integrate and leverage threat intelligence from global resources to automatically detect known malware and quickly identify unknown malware, blocking both from infecting systems. It must also reprogram the entire environment quickly and without human intervention to ensure defenses are in place to block subsequent attacks that may deploy previously seen malware.

5. **Ubiquitous Protection**

   Organizational workforces are becoming more mobile. They are connecting to internal resources from points around the globe that are outside the organizational network perimeter. They use cloud-based SaaS (software as a service) and storage solutions to process and share data, even when disconnected from the organization's network. These services and solutions can sync and distribute files, including malware and exploits, across an organization's entire employee population. A complete solution to preventing security breaches on the endpoint must therefore prevent both malware and exploits from compromising a system regardless of its online status, its connectivity to the organizational network, or its physical location (on-premise or off).

Additional Considerations

The security capabilities of a product are often the primary considerations for organizations seeking to replace traditional AV. However, other non-security considerations may affect a product's ability to meet an organization's AV replacement needs.

Operational Efficiency

The intrusive nature of AV file scans remains a major source of irritation for users and IT administrators alike. An optimal AV replacement product must therefore be minimally intrusive – ideally, transparent to users – while placing minimal demands on memory, bandwidth and CPU resources.

Support for Unpatchable Systems

Not every organization is able (or willing) to upgrade existing production systems. Organizations may choose not to apply available system updates and security patches because doing so would interfere with, diminish or eliminate critical operational capabilities. Alternatively, they may not be able to apply such updates because a system or software has reached its end-of-support and the vendor no longer provides system and security updates. A complete AV replacement product must therefore support and protect these systems and software applications that have become essentially "unpatchable."

Customizability to Meet Business Requirements

Organizational business requirements for AV replacement can vary widely. In this case, one size does not fit all. A flexible, blended, multi-method approach to prevention accommodates business needs that are likely to vary across organizations and internal user groups. An ideal AV replacement product must provide such flexibility to tune security to an organization's business requirements.

Traps Replaces Antivirus

Even as traditional AV vendors attempt to incorporate such new technologies as machine learning into their solutions, their continued reliance on old approaches like scanning limits their effectiveness against today's cyberthreats. Fortunately, organizations can now secure their endpoints without tolerating the hidden costs of traditional antivirus solutions.

Traps replaces legacy antivirus with a multi-method approach to prevention that deploys a unique combination of the most effective, purpose-built malware and exploit prevention methods to prevent known and unknown threats before they compromise an endpoint.

Multi-Method Malware Prevention

Traps prevents malicious executables with a unique approach that maximizes coverage against malware while simultaneously reducing the attack surface and increasing the accuracy of malware detection – without reliance on virus signatures or resource-taxing scanning. This approach combines several layers of protection (Figure 2) that instantly prevent known and unknown malware from infecting a system:

- **WildFire threat intelligence:** Palo Alto Networks WildFire™ cloud-based threat analysis service is the world's largest distributed sensor system focused on identifying and preventing unknown threats. Over 17,000 customers, third-party feeds and technology partners contribute threat intelligence to WildFire.

Figure 2: Traps multi-method malware prevention

WildFire continually analyzes this threat intelligence, and Traps automatically uses the resulting knowledge and prevention controls to identify and prevent malware previously seen elsewhere. When Traps encounters a file it has never seen (such as a piece of malware or an Office file containing a malicious macro), it queries WildFire with the hash of that file before allowing the file to run. If the file is deemed malicious, Traps automatically terminates it, reprograms itself to prevent the execution of that file from that moment on, and optionally quarantines it.

- **Static analysis via machine learning:** This method delivers an instantaneous verdict on any unknown file before the file is allowed to run. By examining hundreds of the file's characteristics in a fraction of a second, this method determines if it is likely to be malicious or benign, and does so without reliance on signatures, scanning or behavioral analysis. Palo Alto Networks uses the threat intelligence contained in WildFire to train a machine learning model to autonomously recognize malware and malicious macros – especially unknown variants – with unmatched effectiveness and accuracy. The training of the machine learning model takes place in the cloud environment, while unknown file analysis happens on the local machine; hence, the name "local analysis." This method is especially useful if users are not connected to an organization's network and cannot take advantage of WildFire.
- **WildFire inspection and analysis:** In addition to local analysis, Traps submits unknown files to WildFire for full analysis. Named a "Leader" for Automated Malware Analysis by Forrester, WildFire brings together four independent techniques to discover even the most evasion-resistant malware in as few as five minutes:
    - **Dynamic analysis:** WildFire observes files as they detonate in a custom-built, evasion-resistant virtual environment to detect never-before-seen malware and malicious macros using hundreds of behavioral characteristics.
    - **Static analysis:** WildFire instantly identifies variants of existing malware by comparing the characteristics of the file with known malware patterns.
    - **Machine learning:** WildFire extracts thousands of unique features from each file to identify new malware.
    - **Bare metal analysis:** WildFire automatically routes evasive malware to a real hardware environment for detonation, which eliminates an adversary's ability to deploy virtual machine evasion techniques.
- **Malicious process control:** Traps delivers fine-grained control over the launching of legitimate applications (like script engines and command shells) that can be used for malicious activities. For example, Traps can prevent Internet Explorer® from launching a specific script interpretation engine or an administration tool, such as PowerShell®, as a sub-process – a common technique used by ransomware attacks.

The above methods and capabilities enable Traps to prevent malware and malicious Office macros from compromising a system, and give organizations the flexibility to fully customize this prevention to meet their varying business needs.

Multi-Method Exploit Prevention

Many targeted attacks begin with an exploit delivered as a data file through a website, via email or over the network. When the user opens the file, embedded malicious code leverages a vulnerability in the application opening the file, manipulating it to execute the attacker's instructions. Because this type of attack is difficult to distinguish from normal application behavior, it typically bypasses traditional antivirus and most endpoint security solutions. In addition, if the application being exploited is allowed by IT security policy, the attack will bypass any whitelisting controls.

Traps implements a multi-method approach to exploit prevention, combining several layers of protection to block exploit techniques (Figure 3):

- **Pre-exploitation prevention:** Traps prevents attempts by exploit kits before they begin, by blocking their initial vulnerability profiling actions. This profiling, sometimes called "fingerprinting," involves collecting information about an endpoint before initiating an attack to identify specific operating system or application vulnerabilities and match the optimum attack to leverage against them. Traps blocks fingerprinting, preventing exploits before they begin.

Figure 3: Traps multi-method exploit prevention

- **Technique-based exploit prevention:** Although there are many thousands of exploits, they all rely on a small set of exploitation techniques that change infrequently. Each exploit – known or unknown/zero-day – must use a series of these techniques to successfully subvert an application. Traps renders these techniques ineffective by identifying and preemptively blocking them the moment they are attempted. Organizations using Traps can run any application, including those developed in-house or that no longer receive security support, without the imminent threat to their environment.
- **Post-exploitation prevention:** Traps prevents attackers from exploiting the operating system. A common kernel exploitation technique involves the creation of a malicious process that steals the credentials of a privileged process, allowing the malicious process to run with system permissions. Traps identifies and blocks this technique, and with it, various other kernel exploits.

These methods enable Traps to efficiently, continuously and transparently prevent both known and zero-day exploits from compromising a system. This prevention protects applications and systems whether or not they receive security patches, and regardless of network connectivity or physical location.

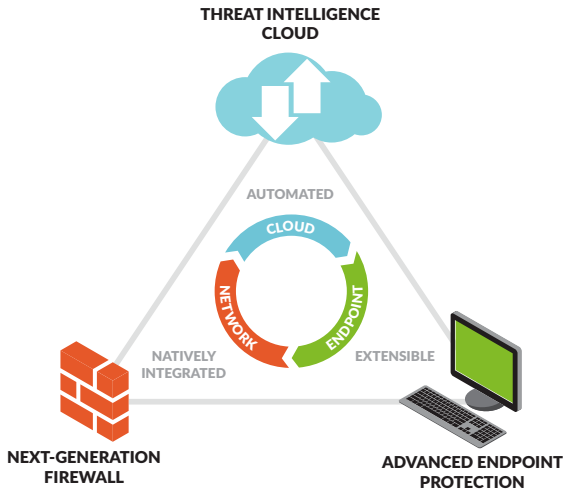

Figure 4: Next-Generation Security Platform

Next-Generation Security Platform

As an integral component of the Palo Alto Networks Next-Generation Security Platform (Figure 4), Traps benefits from the platform's capabilities even in environments where no other Palo Alto Networks technology is deployed. As mentioned earlier, WildFire draws upon multiple threat intelligence resources, analyzes the collected intelligence using its multi-technique approach, and delivers prevention controls to Traps. This integration with WildFire is automatic and included with Traps, enabling customers to block malware that has first been seen elsewhere by other customers on any of their Palo Alto Networks components, including next-generation firewalls, Aperture™ SaaS security service and Traps. In effect, Traps customers benefit from the insights gained by the global community of Palo Alto Networks customers as they encounter new and never-before-seen threats.

Conclusion

Traditional AV no longer offers meaningful security value because it is no longer an effective means to prevent security breaches. Organizations now have access to a superior technology that eliminates the need for traditional AV; far surpasses it in terms of security value; and avoids the intangible, difficult-to-quantify, unquestioned costs of antivirus. Palo Alto Networks Traps replaces legacy antivirus with a multi-method approach to prevention that preemptively blocks malware and exploits, known and unknown, before they compromise an endpoint.

To learn more about Traps, download the Traps Datasheet or the Traps Technical Overview. Alternatively, see Traps in action by attending an Ultimate Test Drive event or by contacting your sales representative to schedule an in-house evaluation for your organization.

1. https://en.wikipedia.org/wiki/Antivirus_software
2. http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/
3. Advanced malware includes those that deploy targeted or multiple infection mechanisms, triggers, and payloads and utilize stealth strategies such as self-encryption and polymorphism.
4. https://www.paloaltonetworks.com/company/press/2016/palo-alto-networks-named-a-leader-in-automated-malware-analysis-report

4401 Great America Parkway
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com