IDC
Analyze the Future

IDC TECHNOLOGY SPOTLIGHT

The "Patient Zero" Problem and the Need for Modern Endpoint Protection

June 2017

Adapted from *IDC MarketScape: Worldwide Endpoint Specialized Threat Analysis and Protection 2017 Vendor Assessment,* IDC #US42385717

Sponsored by Palo Alto Networks

Today's digital transformation reality differs greatly from the cyber reality of the recent past. Current signature-based defenses provide little protection in a world of malware with singular targets, referred to as the "patient zero effect." This paper examines modern endpoint protection, describing how the evolution of malware has created a need for a modernized approach to endpoint protection. It also looks at the role of Palo Alto Networks Traps offering in this critical market.

Introduction

In the PC era, endpoint security was based on signatures. Virus and other malware signatures are essentially digital patterns of malicious code. Signature-based approaches were conceptually simple: Security products such as antivirus would scan files for signatures of known malware and subsequently block those known malicious files.

Signature-based approaches offered reasonable protection. The discovery of malware on "patient zero" (the first known victim of the malware identified by security researchers) led to the creation of a signature and subsequently broad distribution of that signature. Given the low number of malware variants and widely distributed malware, commonly referred to as "spray and pray," signature-based approaches provided efficient protection and limited the number of infections.

However, today's digital transformation reality differs vastly from the cyber reality of the recent past. Mobility, big data, cloud, and social media are the four pillars of the compute reality that has created a massive transformation in our digital lives.

The exponential increase in scale had an equally powerful impact on network security as Stuxnet gave birth to targeted attacks. The forefather of advanced threats, Stuxnet was an attack by U.S. and Israeli governments on an Iranian uranium enrichment facility in 2009 and was the first accredited instance of a cyberattack specifically tailored to attack a targeted entity. The term "targeted" additionally implies sophisticated as the attack focused on taking advantage of four specific weaknesses in the Iranian IT systems to cripple the uranium enrichment facility. Such weaknesses were later referred to as "zero-day vulnerabilities" because they were unknown before the attack.

PC-era signature-based endpoint protection techniques do not work in today's reality.
The fundamental weakness in the signature-based approach is "patient zero": Signatures typically depend on the discovery of malware on an infected endpoint to create the signature, a reactive approach based on known threats. Patient zero is the sacrificial lamb of the approach. When a low number of malicious binaries are widely distributed, an "acceptable" infection rate results. Targeted malware results in an exponential increase in the number of malicious binary variants. Ultimately, the reactive signature approach succumbs to an explosion of malware variants.

Life and Cybersecurity Are Not So Simple

In life, good people sometimes do bad things. Likewise, in cybersecurity, seemingly good files or applications do bad things. We give these types of attacks the moniker of "exploit." Taking advantage of a vulnerability in a browser or in Microsoft Word to launch PowerShell commands on a remote endpoint to take control of the device is an example of an exploit. Exploits are challenging for signature-based defenses because there is often a lack of any discernible malware and the exploit often targets an unknown vulnerability.

Exploits are especially vexing because they are sophisticated attacks that can be used by the unsophisticated. Exploits are typically implemented using exploit kits that reside on web servers. An exploit kit identifies software vulnerabilities on endpoints and then uploads and executes malicious executables to the endpoint in an automated fashion. Creating an exploit kit requires sophistication; using an exploit kit does not. Easy-to-use, packaged exploit kits are readily available on the dark web for as little as $500 per month and thus are popular among cybercriminals today.

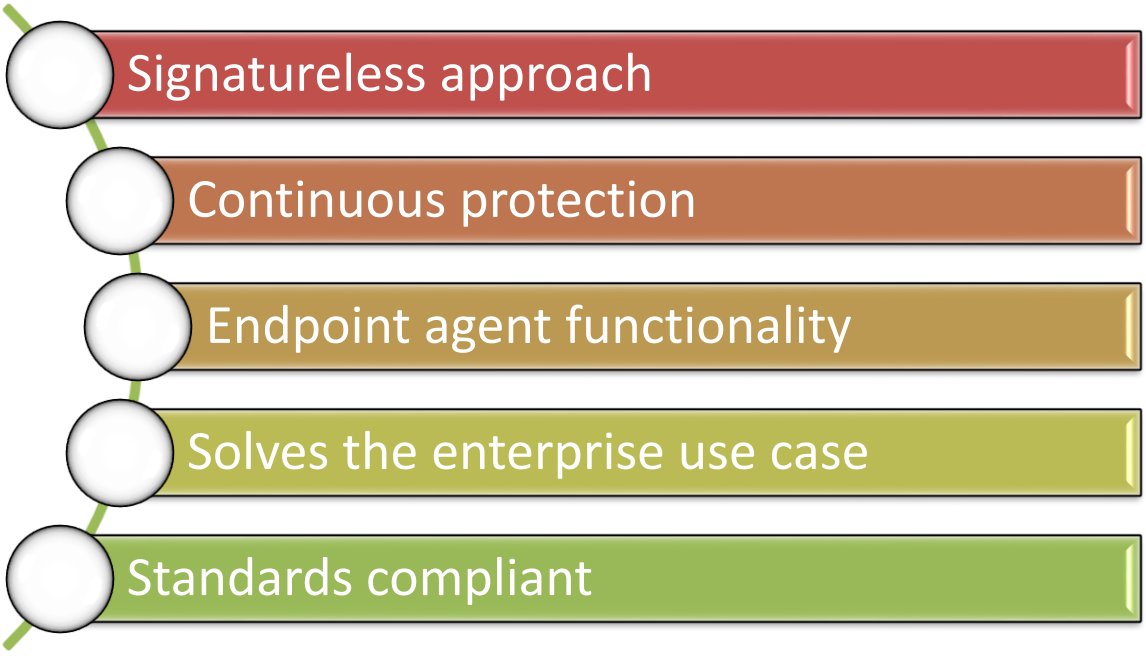
As we approach the point where malicious binaries can be easily customized to have a single target, whether malware or exploit based, all endpoints are potentially "patient zero."

Solving the Patient Zero Effect with Modern Endpoint Protection

Given the acute problem presented by the patient zero effect, legacy approaches to endpoint protection become unsustainable. New approaches are necessary. In today's cybersecurity reality, IDC's fundamental rules for modern endpoint security include the features illustrated in Figure 1.

FIGURE 1

IDC's Rules for Modern Endpoint Security



Source: IDC, 2017

Signatureless Approach

Modern endpoint security products must use a signatureless approach as their primary technology for threat detection and prevention. After all, such products are purchased to thwart targeted, advanced or sophisticated attacks that use zero-day malware and nonmalware attacker tactics. Ideally, protection includes a multilayered approach:

- **Static analysis** evaluates the potential maliciousness of a file based on file inspection.
- **Heuristic rules** prevent potential malicious actions by blocking exploits such as detecting and alerting on the manipulation of Windows PowerShell or other underlying system administrative tools. Such rules will ideally provide the ability to protect good processes from exploitation as well as prevent malware from running.
- **Behavioral analysis** evaluates the maliciousness of a file based on the functions performed. Malicious behavior can be implemented by the sequential stringing together of seemingly benign activities. Often, advanced malware can be detected only by analyzing the sequence of operations that it performs. The two primary forms of behavioral analysis are code emulation and sandboxing. Code emulation has the advantage of rendering verdicts quickly and placing little demand on compute resources. The drawback is that code emulation is easily evaded. Sandboxing uses an isolated analysis environment to create a virtualized endpoint with the goal of detonating a binary and observing it for malicious behavior. Sandboxing is significantly more resource intensive than emulation, often requiring 5–8 minutes for a valid verdict. However, higher resource requirements result in dramatic improvements in efficacy.

Continuous Protection

Endpoint security products must provide continuous protection of endpoint system and file behaviors. Stopping malware from doing bad things is important; stopping "good" files and applications from doing bad things is equally important. Advanced attacks are stealthy and sophisticated, actively looking to evade detection. Such attacks cannot be stopped with one-time analysis. Analysis needs to be constant and vigilant to catch the nastiest of malware.

Endpoint Agent Functionality

Modern endpoint security products should provide an agent that detects malicious activity and can be configured to block regardless of endpoint device connectivity. Additionally, endpoints are often mobile and live on batteries, so memory (both volatile and nonvolatile) and CPU requirements of the endpoint client are important considerations.

Solves the Business Endpoint Security Use Case

A solution sounds simple, but many current offerings tend to be point products that address singular attributes of a solution, pushing responsibility for the integration of the products and ownership of the effectiveness of the solution onto the end user. A modern endpoint security vendor should be able to provide static analysis, heuristic rules implementation, and behavioral analysis and not require customers to cobble those components together themselves. A solution needs to work "out of the box" with minimal customization or configuration required without compromising the flexibility to enable the varying security needs of an enterprise.

A solutions approach becomes critical as it relates to leveraging intelligence, as the ability to learn quickly from unknown activity throughout the environment (including network, endpoint, and cloud/SaaS) and convert the intelligence into prevention. Automation is a must!

Maintenance and management overhead of a "solution" cobbled together in a grouping of point products is a nightmare, especially given the shortage of qualified information security professionals. Ease of updates and ease of maintenance are fundamental requirements because misconfigured security products offer little real security. Also, role-based administration and Active Directory integration are definite pluses.

A single pane of glass for managing endpoints, including multiple endpoint operating systems, is critical. Enterprise networks are a heterogeneous mixture of endpoint type. The ability to protect multiple types of endpoints (i.e., Windows, Mac, Android) is a fundamental requirement.

A subtle yet critical factor of a solution is not only its efficacy in discovering malicious files but also its ability to minimize false positives. Security professionals are drowning in a sea of alerts. A robust modern endpoint security solution delivers low false-positive rates with minimal tuning to provide low maintenance for operations.

Standards Compliant

The ability to satisfy compliance requirements is a must in any reality. Certainly, security efficacy is critical. However, implementing a solution that does not satisfy compliance regulations and standards is impractical because it would result in a need for two solutions: a security-focused endpoint solution and a compliance-focused endpoint solution. Managing two endpoint clients when one will suffice is folly.

Frankly, today's compliance standards are hard to satisfy. Modern endpoint security solutions should satisfy the compliance needs of an enterprise, such as Payment Card Industry Data Security Standard (PCI-DSS). Compliance regulations and standards will become only more stringent. Selection of a modern endpoint solution should consider the long-term ability of the organization to satisfy not only the ongoing needs of current regulations and standards but also the needs of new regulations and standards as they become relevant.

Considering Palo Alto Networks Traps

Traps from Palo Alto Networks is a modern endpoint protection solution that was built from the ground up to address the endpoint security needs of enterprises. To build Traps, Palo Alto Networks leveraged its $200 million acquisition of Cyvera, a cybersecurity company that focused its core prevention engine on identifying techniques that attackers use to exploit software vulnerabilities. Traps focuses on protecting the endpoint, operating independently of any other defenses, such as next-generation firewalls (NGFWs) or deception (honeypots).

Traps natively includes cloud-based sandboxing, which is directly integrated into the endpoint client. Palo Alto Networks WildFire threat analysis service provides for both static analysis and detonation of potentially malicious binaries in a virtual environment and bare-metal hardware for in-depth analysis. Sandbox analysis is commonly a great feature of NGFWs, but today's environment necessitates such behavioral analysis during roaming. Traps directly leverages the capability at the endpoint. The other benefit of providing WildFire support directly to the endpoint is that WildFire additionally integrates security intelligence to share insights that may have been gained from other parts of the network, third-party providers, and other subscribers to the service and automates prevention.

Advanced attacks are not just about malware. The Traps endpoint agent is equipped with a series of exploit prevention modules that are injected into system and third-party processes to block different exploit techniques from executing. Traps protects both vendor-published and in-house-developed applications on physical, virtual, and mobile endpoints. The core focus of Traps is prevention of *both exploits and malware*, known and unknown.

Security professionals are always pressed for time, and not stopping good processes is as important as stopping malicious processes. Thus Traps includes trusted publisher identification, allowing organizations to identify executable files published by trusted and reputable software publishers. These executable files can run without impact on the user experience.

Although Traps provides standalone endpoint security that operates completely independent of any network-based security protection, integration synergies were enabled. Having WildFire as a foundational intelligence component of both network and endpoint protection security tools essentially creates a communication framework. Thus enforcement occurs at scale as Traps and Palo Alto Networks NGFWs can subsequently become enforcement points throughout a network. Additionally, protection occurs at network speed, so the scaled protection is implemented in seconds.

Palo Alto Networks continues to innovate Traps. Recent improvements introduced in version 4.0 include malware and exploit prevention for Mac devices, protection for Android devices, Office macro protection, enhanced child process protection, exploit kit fingerprinting protection, and kernel privilege escalation protection.

Challenges

Traps provides robust modern endpoint protection that is tailored to the needs of large enterprises or smaller enterprises with sophisticated cybersecurity capabilities. Traps includes default policies so that it is ready to go "out of the box" as much as possible. However, Traps also includes granular controls to tune the product to the needs of a sophisticated cybersecurity organization. Small and medium-sized businesses without security professionals dedicated to an endpoint protection should consider an offering that provides more standardized features.

Additionally, at the time of this analysis, the Palo Alto Networks Traps management console is primarily deployed on-premises. This stands in contrast to some competitive offerings, which primarily leverage cloud-based management consoles.

Conclusion

Signature-based endpoint security simply cannot provide effective protection against the new wave of cyberattacks targeting endpoints. Given the acute problem presented by the "patient zero effect," new approaches are essential. Built from the ground up to address modern endpoint security needs, Palo Alto Networks Traps provides modern endpoint protection that can be implemented either as an independent, standalone solution or as part of an integrated security ecosystem with the accompanying integration synergies that its next-generation security platform can provide. Palo Alto Networks Traps commands consideration from organizations seeking modern endpoint threat prevention capabilities.
