IDC VENDOR SPOTLIGHT

Modern Endpoint STAP Solutions Offer Innovative Threat Defense

October 2016

Adapted from Worldwide Endpoint Security Forecast, 2016–2020 by Robert Westervelt, IDC #US41825816

Sponsored by Cylance

Attackers are increasingly using malware designed to evade traditional, signature-based antivirus solutions to gain entrance into an organization's IT environment. In response, many enterprises are embracing endpoint specialized threat analysis and protection (STAP) solutions, which can detect and prevent modern threats from executing on endpoint devices. This Vendor Spotlight looks at the challenges encountered by early adopters of endpoint STAP solutions and discusses how to effectively evaluate these solutions for an enterprise deployment. The paper also explores how Cylance's next-generation antivirus offering, CylancePROTECT, delivers on the goals of modern endpoint STAP solutions and uses an innovative approach to mitigate many of today's targeted attacks and zero-day threats.

Endpoint Specialized Threat Analysis and Protection Is Mainstream

Criminals' cyberattack techniques are growing ever more creative. Consider the rise of ransomware as a tool to extort money from organizations and severely cripple business operations while IT teams race to recover. These attacks — and other advanced threats that gain access to critical resources — often enter the corporate network through employee laptops and other endpoint devices. Now, the latest threats are finally forcing enterprises to identify modern endpoint security solutions that can level the playing field and to seek outside help in preventing these exploits rather than purely detecting and responding to them.

Modern endpoint security solutions designed to augment or replace traditional antivirus are the fastest-growing segment of the STAP market. What vendors of these products generally have in common is the use of host monitoring, machine learning, and other non-signature-based detection capabilities to identify never-before-seen threats. But a smaller subset of this group has upped the ante and is gaining attention by providing innovative ways to detect signs of threat activity, usurping exploits before they get a chance to run malicious code.

The STAP market consists of three segments: endpoint, boundary, and internal network analysis. Endpoint STAP is the most rapidly growing segment, with CAGR forecast to approach 48% through 2019. This segment encompasses products designed to harden and protect endpoints (PCs, Macs, servers, smartphones, and tablets), making them less vulnerable to advanced attacks. For endpoint STAP, a client or local agent is required even when many of the functions (such as analytics and calculations) are often performed at a central server or in the cloud. Endpoint STAP products can identify threats in memory and prevent the manipulation of underlying application processes. The endpoint client typically monitors and records system processes and may be capable of blocking suspicious files from executing.

Enterprises Widely Adopting Modern Endpoint Security Products

Emerging endpoint security vendors are having an impact on the traditional endpoint security software market. Enterprise adoption of these modern solutions has shifted from deployments that run side by side with standard antivirus offerings to deployments that completely upend traditional, signature-based endpoint security solutions. Established security vendors have struggled to address revenue disruption on several fronts: declining consumer antivirus products, market penetration of emerging endpoint security start-ups with innovative detection and prevention technologies, and significant growth in ransomware infections that disrupt business operations.

IDC is documenting a significant disruption of established endpoint security vendors. Some of these longstanding vendors are being displaced following production testing of these modern endpoint security solutions running side by side with their traditional, signature-based antivirus offerings. Signature-less file analysis is capable of stopping malware before execution, so it can provide more reliable endpoint protection compared with other products, which act only after malicious files are executed. Enterprises gain by not having to update signature database files. This enables laptops and other devices to remain protected regardless of whether they are connected to the organization's network.

Enterprises that have standardized on large, established security vendors are also fitting these modern endpoint security solutions into their stack by simply turning off standard antivirus over time. They note that some modern endpoint security solutions are easy to use and preconfigured out of the box for fast, transparent, and interruption-free deployment. These enterprises aren't making a significant strategy change. They are continuing to leverage encryption, patching, vulnerability and configuration management, and other security capabilities that have been adopted from these large platform security vendors. In fact, enterprise adopters of these modern endpoint security solutions consistently cite the efficacy and efficiency of the new product they deployed. They tell IDC that they don't believe that the security solution is working in their environment because there are few, if any, help desk calls, noting that the modern endpoint security solution they have adopted is extremely transparent to the end user.

The latest IDC *Security Trends* survey found widespread acceptance of endpoint STAP solutions, with some vendors experiencing significant growth and successfully displacing long-established endpoint security vendors. Conducted jointly with The Channel Company in July and August 2016, the survey reached more than 350 security consultants, systems integrators, and resellers and found that modern endpoint and network security products topped the list of customer priorities over the next 12 months, along with data loss prevention and data security technologies. What is driving the demand? IDC interviews with enterprise CISOs, CIOs, and IT directors found ransomware as the primary driver for freeing up spending for modern endpoint solutions. The fact that ransomware severely disrupts business operations even if the organization has a functional recovery plan in place has raised the urgency of putting a modern endpoint solution in place.

Interviews with dozens of enterprises that have adopted modern endpoint security solutions found some maintaining antivirus and augmenting it by running the modern antimalware solutions side by side. Many have taken the next step of replacing existing antivirus altogether, relying entirely on the modern endpoint security solution. These enterprises put their faith in solutions that offer greater reliability and real-time monitoring that is transparent to end users. The rapid pace of adoption and shedding of traditional antivirus from established vendors suggests to IDC that these solutions have matured rapidly and will have a greater impact on the endpoint security market over the next 12 to 18 months as organizations enter their laptop refresh cycles and/or begin upgrading to Windows 10. IDC offers the following guidance based on these interviews:

- **Embrace the cloud.** Identify solutions that use a cloud-based database and analytics engine and provide a web-based management console. The results are typically faster updates, less maintenance, and a reduced datacenter footprint.

- **Improve rapid malware identification.** Identify solutions that have an engine capable of examining file characteristics to identify advanced threats rather than relying on identifying attacker tactics or abnormal system behavior. Add the ability to monitor system memory for signs of malicious activity.
- **Enhance detection and prevention.** Identify solutions that not only alert and provide policy management but also can block threats and provide responders with the context required to investigate and remediate other potential avenues at risk of similar attacks. Customers also desire products that provide the choice to enable or disable prevention functions, such as application control, which is helpful on datacenter servers, point-of-sale systems, industrial control systems, and kiosks.

Key Threat Trends

Targeted attacks are often multistaged and carefully planned and frequently use sophisticated tools, tactics, and procedures designed to evade common defenses. Most attacks begin with a simple phishing campaign or web-based attack to gain an initial foothold in an organization. Once a staging ground is established, attackers carefully seek to elevate privileges, often stealing account credentials to appear as legitimate users on the corporate network. These kinds of targeted strikes enable criminal groups and nation-state-sponsored attackers to spider out across the whole environment. Their aim is to steal information that is valuable to them — which may be credit card numbers, merger and acquisition plans, or technical design specifications.

The success of the targeted nature of attacks has prompted interest in modern endpoint security solutions. Criminals have improved their social engineering tactics and are extremely successful in targeting senior managers and key support personnel, such as a payroll clerk or business partner specialist. Phishing, ransomware, and spyware were ranked as the top 3 threats experienced in enterprise networks, according to the latest IDC *Security Trends* survey. Laptops and workstations led the list of high-risk areas in enterprise environments, followed by employee errors and mobile device risks, illustrating the impact that ransomware infections are having on enterprise security strategies.

Ransomware is prompting organizations to assess their data governance strategy and driving interest in modernizing endpoint security and data protection capabilities. Ransomware is a dangerous and disruptive threat that encrypts data on PCs and network file shares, and it has grown to be a significant problem to enterprises of all sizes. The security survey validated the problem with 59% of survey respondents identifying ransomware as a significant threat to their customer networks.

Threats Fuel Services Interest

The fact that modern attacks can evade conventional perimeter and network security measures creates an atmosphere in which cybersecurity and business continuity are top of mind. The barrage of media reports about advanced persistent threats (APTs), distributed denial-of-service (DDoS) attacks, zero-day malware, and other threats feeds the flames of corporate anxiety. Executives, IT managers, and CISOs are looking for expert guidance. With more flavors of security services available every month, each claiming to be better than or different from the next, it's challenging for executives to know what to do. Adopters of modern endpoint security solutions have sought services from a variety of sources:

- **Professional security services (includes consulting and integration).** Outside professional services organizations are available from some endpoint security vendors to assist in configuring and managing advanced security detection technologies. The value in these services is to make an assessment prior to deployment to aid in proper configuration and ensure that the full value of the technology is being achieved. These services can also include triage assistance with alerts, detailed forensics investigations, and post-breach assessment capabilities. Some security consulting firms that specialize in breach, incident response, and forensic analysis can be placed on retainer ahead of time rather than organizations obtaining these services at a time of crisis.

- **Consulting security services.** Some consultative services specialize in risk assessments, penetration testing, and identifying data governance weaknesses. They may assist with developing and testing an incident response plan or help manage breach notification or disaster recovery procedures. They may also provide security awareness training to help build up a culture of security within the organization.
- **Threat intelligence services.** Outside threat intelligence services that are tailored to an organization's industry vertical can help bolster the detection of APTs, attacks that are unknown, targeted, low and slow, and adaptive. They can also serve to provide additional context behind specific alerts and aid the remediation process to bolster prevention. Organizations should look for threat intelligence services that can be customized and provide timely and actionable data.

The increased volume of good threat and endpoint visibility information also has an increased level of noise, or alerts that do not represent malicious activity. The alert noise generated by some solutions presents a challenge to already overburdened incident responders. IDC believes organizations must develop and cultivate a security program that reduces the attack surface and has the ability to quickly detect and contain attacks before they move into the next stage of the attack life cycle. The challenging hiring environment for skilled security professionals will no doubt continue to drive interest in external security services to identify threats and aid incident response. No organization has the perfect strategy. The focus should be on solidifying basic security best practices and developing and thoroughly testing incident response (IR) procedures.

Considering Cylance

According to IDC research, CylancePROTECT is a market revenue leader in the endpoint STAP marketplace with an advanced threat prevention solution that has been adopted by more than 1,000 customers in 2016. Cylance calls its product "next generation antivirus" because it is categorized under the Microsoft Virus Initiative as an antimalware solution. Cylance also lists its product as PCI DSS Section 5 compliant.

A key differentiator of CylancePROTECT is its approach of efficiently conducting pre-execution static analysis of file types rather than focusing exclusively on system or application behaviors to detect threats. Cylance places an agent on the host that uses mathematical models to make decisions. The algorithm does this without the need for behavioral, heuristic, or signature-based techniques. It examines file characteristics to determine the malicious or benign nature of a file by extracting unique characteristics from potentially hazardous files and applying analysis to determine a file's intention. The agent can also function autonomously and continue classifying threats when an endpoint system is offline. The agent receives minimal, noninvasive updates, with new software improvements issued every few months. There is no need for a daily DAT file download or constant cloud-based lookups because Cylance doesn't use signatures.

Cylance terminates exploit attempts and can be set to quarantine unsafe applications before they run. It also provides alerts and context about the malware it identifies to incident responders. Cylance is working on a remediation tool to support remediation activity.

Cylance Consulting is also available to organizations requiring a professional services engagement. Cylance's ThreatZERO Services offers complete implementation and configuration support of CylancePROTECT to begin blocking threats relatively quickly. Cylance consultants provide risk assessments and vulnerability and penetration testing. This includes an array of services associated with incident response and forensics, red teaming, IoT/embedded systems security attestation and assessments, and industrial control systems security assessments, planning, and design.

Challenges

- Cylance has experienced rapid growth and, as a result, it must scale its internal organization to address customer support, indirect sales partners, and product management and operations to meet growing needs. About 30 people staff Cylance's customer support team, and the company has ongoing plans to address support workflow for handling customer support requests between time zones.
- Cylance does not offer an on-premises management server for organizations that have an aversion to a cloud management console. The company is transparent about the data it collects and the security protecting its database systems and associated backups. Cylance collects and retains minimal customer data, and no data is shared between customers.
- The optional Memory Protection component requires additional proactive management capabilities to exclude custom scripts and applications from being blocked. Cylance says memory protection can coexist with other solutions already present on the machine, but it makes no guarantee that all third-party security solutions can function normally.

Conclusion

Attackers are easily evading legacy security solutions, such as signature-based antivirus, and using social engineering tactics that aim straight at human fallibility and the misjudgments that create the opportunity for a costly data breach. A wide variety of serious problems and areas need to be secured (malware, endpoints, mobile, etc.), and most organizations are struggling to keep pace with the rapidly evolving threat landscape. A growing number of endpoint STAP vendors are adding automated response capabilities designed to quarantine or remove threats.

Not all modern endpoint security solutions prevent malicious code from executing on an endpoint device. Enterprises should identify solutions that focus on preventing malware from running on the endpoint and thoroughly test the solutions to ensure the prevention capabilities don't interfere with business processes and employee workflow. Organizations should seek assistance in assessing the state of their existing security policies and enforcement controls. Far too many businesses lack established security best practices and an effective data security strategy as part of maintaining a comprehensive security program.

Some security vendors are responding by building out their internal professional services capabilities, and organizations are encouraged to contact their security vendor or channel provider for assistance. In addition, emerging threat intelligence management platforms can help incident response teams organize and gain more value from security vendor and other third-party threat intelligence feeds.

ABOUT THIS PUBLICATION

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

For more information on IDC, visit www.idc.com. For more information on IDC Custom Solutions, visit http://www.idc.com/prodserv/custom_solutions/index.jsp.

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com