Advanced Persistent Threats: Moving from Detection to Prevention and Response

October 2015

Adapted from Worldwide Specialized Threat Analysis and Protection Forecast, 2015–2019: Defending Against the Unknown, IDC #256354

Sponsored by Symantec

New modern threats and multistaged attacks are now impacting every industry. The FBI estimates losses associated with a single recent attack at more than $100 million. Increasingly, difficult-to-detect attacks are changing the security protection landscape and, subsequently, the enterprise security posture. These attacks occur at multiple different points across the network, making it more difficult for companies to detect and respond to them. The limitations of signature-based security products are well known, and advanced models of threat detection are on the rise. This paper examines the specialized threat analysis and protection (referred to by IDC as STAP) market along with technology that can help protect companies from the rise of advanced, sophisticated, and tailored malware. It also considers the offerings of technology vendor Symantec in this growing and strategically significant market.

Introduction

To ensure that enterprise network, application, data, and endpoints can remain secure (clean of malware and breaches), antimalware products and services are evolving. Advancements focus on the increasingly sophisticated threats, relying less on signatures and adopting other forms of detection. While many products are incorporating some of these capabilities, dedicated products provide the best security and focus for advanced threats. The STAP market overlays the functional security markets (endpoint, messaging, network, and Web). The key distinguishing factor to determine whether a solution falls within the STAP category is that the malware (or similar type of threat) detection or prevention method does not rely on standard signature detection (i.e., blacklisting). STAP solutions must also be highly automated.

The high demand for specialized threat analysis and protection solutions is reflected in supply-side market growth, which IDC predicts will increase from $930 million in 2014 to $3.14 billion in 2019, representing a CAGR of 27.6%.

Definitions

Advanced Persistent Threat

Threat intelligence services grew out of security services providers developing threat detection capabilities to address the challenge of detecting advanced persistent threats (APTs), advanced malware, previously unidentified attacks, and other threats.

Specialized Threat Analysis and Protection

STAP products help protect enterprises from new malware attacks that cannot be detected by traditional signature-based techniques. These products use a variety of non-signature-based protection methods — including sandboxing, behavioral analysis, file integrity monitoring, telemetric
heuristics, containerization, netflow analysis, and threat intelligence — that can detect a malware attack or compromise by identifying attacker activity or subtle system process changes. Some of the products only detect and alert, while others may contain malware to prevent it from causing damage.

**Intersection of APTs and STAP**

APTs are a combination of malware, delivery mechanism (e.g., phishing), and data exfiltration. Advanced persistent threats should best be considered as an attack process. Threat intelligence–based STAP solutions analyze, alert, and/or remediate parts or all of this attack chain. STAP products investigate each of the attack chain layers, such as reconnaissance, infiltration (“low and slow” attack types seem to be more prevalent than "smash and grab" attack types), and exfiltration of targeted information.

**STAP Submarkets**

IDC has identified two particularly relevant STAP submarkets: boundary and endpoint. These submarkets are not specifically based on technology; rather, they are based on where in the network the protection process is performed.

**Boundary**

This category of product monitors and analyzes files for malware or malicious indicators (such as known command and control locations) that will enter the enterprise network. Boundary covers all types of traffic (e.g., HTTP, SMTP, TCP/IP). The boundary category is composed of messaging, Web, and unified threat management (UTM)/firewall products. Most boundary solutions consist of security appliances, but some functions will be handled in the cloud. Boundary STAP, the largest area, is expected to reach $2 billion in vendor revenue by 2019.

**Endpoint**

This category encompasses products that are designed to harden and protect endpoints (computers, servers, smartphones, and tablets), making them less vulnerable to advanced attacks. For endpoint, some type of client is required even when many of the functions (such as analytics and calculations) are performed at a central server or in the cloud. If there is no client, the STAP solution would fall under boundary or internal network analysis. Endpoint STAP has the fastest-growing demand, with a supply-side CAGR approaching 48%.

**What Are the Benefits?**

How do you defend against something that's never been seen before? That's the key question with which organizations are struggling. Malware today is targeted, polymorphic, and dynamic. To solve this increasingly complex problem, a new category of products has emerged that leverage a variety of techniques to collect information around behavior, communication, activity, reputation, and other factors in order to detect the seemingly undetectable.

The ultimate goal of today’s attacks is typically data exfiltration, which lends itself to a “low and slow” approach where attacks can go unnoticed for long periods of time. Organizations are struggling to identify and contain advanced threats before they become data breaches. Dwell time, the time between an initial point of infection and the point in which a threat is detected (sometimes days or weeks later), is far too long, giving criminals the ability to steal data quickly and move on to a new target.

A focus on reducing dwell time will motivate organizations to invest in STAP solutions to identify threats and address them at a faster pace. STAP solutions increase visibility and also support incident response efforts by providing enough context behind threats for responders to recognize the criticality of a threat and enough knowledge to take immediate action.
Security is being embedded into applications so that by 2018, 25% of security capabilities previously purchased will be incorporated into applications. The model has been to add security on top of a function. There are dedicated security solutions for authentication, network, Web applications, messaging, and endpoints. This could create performance and usability issues. As a result, many independent software vendors have determined that it is better to incorporate security into their products to not only add value to the products but also make them more resistant to attack. For customers, this reduces systems acquisition and integration costs and may require fewer IT professionals as consolidation creates efficiencies.

The monitoring of network flow or other traffic to discover anomalies within the network has been adopted mainly to support performance optimization efforts. A surge in interest in solutions that address the risks posed by the Internet of Things (IoT) could fuel interest in internal network analysis solutions.

**Key Trends**

**SaaS**

The rising adoption of SaaS services, driven by the 3rd Platform (cloud, mobile, social, big data and analytics) makes it very difficult for organizations to have complete control over their data and applications. Enterprise security is lagging the pace of architecture changes.

Some organizations will withdraw from investing in STAP products or rely on SaaS providers to carry the security burden. STAP products may also become less effective as distributed architectures make them easier to bypass. Investments must be made to provide adopters with additional capabilities and seek integration with other security partners. Organizations will buy STAP products that can integrate with existing security investments and support the creation of a cohesive security system.

**Improved Sandboxes**

The mounting losses from cybercrime are helping drive broad acceptance of sandboxes. Sandboxes have been integrated into so many different network security solutions that the value of having a protected environment in which to detonate and monitor suspicious binaries is no longer disputed. While this area is being commoditized quickly, its market opportunity is expanding drastically. Network security providers offer virtual sandboxes at their core to analyze suspicious files and identify advanced threats. Appliances use emulation or virtualization sandboxes to detect attacks.

**Risk Versus Reward Spending**

Security buying decisions are increasingly becoming risk management decisions driven by business objectives. These investments are increasingly weighed against the value of the risks facing the enterprise. It is difficult to mitigate attacks without understanding threats, asset value, and vulnerabilities.

Organizations seeking to maximize the return on their security investments should develop and implement a process for prioritizing security initiatives based on the specific vulnerabilities and threats detected and validated in their own business, thus avoiding the trap of responding first to the loudest or the latest clanging gong.

Process changes and other risk mitigation efforts could have a great effect in reducing the attack surface. No security product is a silver bullet, and despite the need for STAP technologies to detect advanced malware, many serious breaches stem from basic security lapses. STAP products have limited value when an attacker uses stolen or weak passwords or takes advantage of vulnerabilities and configuration weaknesses.
**Endpoint Spending**

The endpoint is high-priced real estate at most enterprises, and a lot of security solutions are vying for their own place. Enterprises must be extremely careful about adopting new security solutions that may provide flash-in-the-pan comfort but cause performance or productivity problems. While growth in endpoint STAP is high, the overall numbers are still fairly low. IDC expects this space to shake out considerably as enterprises make their strategic partner choices.

**Considering Symantec Security Products**

In the $30+ billion worldwide security products market, Symantec remains the largest security vendor and offers products in nearly every functional area, dominating endpoint security with a 31.5% share and garnering top share in messaging security. Symantec is addressing the need to unify products for enhanced threat detection at lower operating costs and embrace emerging technologies such as cloud without compromising on security. Threat protection, information protection, and security analytics are the three key needs driving Symantec’s unified security strategy.

The company is expanding its focus from prevention to detection and response to solve the advanced threat detection problem in a distinguished manner. Symantec Advanced Threat Protection, which fits IDC’s classification of STAP, represents Symantec’s shift into analytics. This solution incorporates threat prevention, detection, and response across endpoints, email, and networks under a common platform and integrates with the Symantec Endpoint Protection agent and Symantec Email Security.cloud. This allows customers to have a single console for breach management, hunting, and forensics to more quickly respond to potential issues and without the need for additional endpoint security agents or software, providing customers with immediate access to critical capabilities, knowledge, and skill sets during incident response scenarios. Having the ability to monitor breaches across multiple control points allows for a faster response and further insight into what caused the breach.

According to the company, only Symantec's Global Intelligence Network provides the volume and variety of threat data analytics to detect advanced threats, vulnerabilities, and malicious behavior. Organizations can leverage analysis of their own local network activity with security intelligence from Global Intelligence Network to get detailed, relevant, and actionable data needed to respond to critical security events in a quick and effective manner.

Customers implementing Symantec’s Advanced Threat Protection have the option of engaging the Symantec Services team to ensure a successful deployment, and assisting with management of their environment, interpretation of incident impact, and overall reduction in risk and threat posture. The company’s team of experienced security professionals holds various industry certifications, including the Certified Information Systems Security Professional (CISSP)-credential.

Symantec's highest value to enterprises will be in the company's ability to combine separate technologies into a coherent and consistent security estate, eliminating hand-off between disparate products and making security easier to manage. Only a handful of firms worldwide have the resources to deliver on such a critical role for enterprises. More importantly, a comprehensive solution suite allows Symantec to raise its entry point into prospective clients from the IT management level to the CISO or CIO level — and have the right set of follow-up conversations.
Challenges

The biggest challenge for Symantec in the next 6 to 12 months — as it evolves into a separate security company — is strategy execution. Symantec is in a better position to accomplish this as it becomes a focused, standalone security company.

Symantec also has to work through the shift in business model from licensing to services, subscriptions, and SaaS. Though not unique to ISVs, it's another bridge that Symantec needs to cross.

Conclusion

By 2017, 75% of large enterprises will receive custom threat intelligence information tailored to their industry, company, brand, and environment. Threat intelligence will be one of the fastest-growing data-as-a-service offerings built on the 3rd Platform. The capability to integrate external threat data, internal security log data, system vulnerabilities, and functional IT activities will require a software platform for full visibility and integration of this data. Various security products will need to be configured to share information and be able to automatically respond to that knowledge. Emerging approaches to detection and containment have largely proven their value to early adopters. Over the next several years, organizations will purchase STAP products not only because they want to bolster existing security investments but also because they are attracted to the benefit of creating a cohesive security system capable of adapting to the rapid pace of change associated with the 3rd Platform.

Market leaders for the next generation of security providers will have to focus on an intelligence-led and platform-driven approach as opposed to the traditional security software markets that we have come to know and understand over the past 20 years. CISOs constantly complain about the fragmented security estate that they have to manage, a problem that could be solved with the "unified security" approach from Symantec. Assuming Symantec can address the challenges described in this paper, IDC believes that the company is well positioned in developing technology and gathering information globally to succeed in the current business environment.