WHITE PAPER

Specialized Threat Analysis and Protection Technologies: Vendor Landscape Addressing Advanced Threats Is Growing Significantly

Sponsored by: Comodo

Robert Westervelt
February 2016

IDC OPINION

The specialized threat analysis and protection (STAP) market continues to gain traction with widespread adoption of both SaaS subscription and on-premise sandboxes and a renewed focus on emerging advanced endpoint and network security technologies. These solutions examine network traffic as well as user, system, file, and application behaviors in an attempt to identify threat indicators associated with targeted attacks, custom malware, and sophisticated tactics. IDC estimates that the market in 2014 had revenue of $930 million. It is forecast to grow to over $3 billion by 2019, with a total market compound annual growth rate (CAGR) of 27.6%. The number of security vendors with STAP products is growing significantly. Established security vendors are taking steps to modernize their portfolio to meet customer demand for new approaches to protect sensitive corporate data and identify threats that evade detection from traditional signature-based network and endpoint products.

IDC estimates that the market in 2014 had revenue of $930 million. It is forecast to grow to over $3 billion by 2019, with a total market CAGR of 27.6%.

This IDC paper examines the competitive market for STAP technology and aims to identify the participants and significant trends that will impact the broader market for endpoint, network, messaging, and Web security products and services. In this paper, IDC also discusses Comodo's STAP market offerings which span across the STAP endpoint, STAP boundary, and STAP internal network analysis submarkets.

Existing Security Investments Must No Longer Be Siloed

There have been significant changes to corporate environments in recent years, from the adoption of cloud services and the widespread use of mobile devices to growing end-user demand for support of emerging collaboration services and other technologies designed to further productivity. Criminals are seizing on the complexity born from these changes and the inability of existing security solutions to extend protection to a fluid perimeter and distributed corporate assets.

While businesses are scrambling to adopt these modern technologies, attackers are investing heavily to further their own methods. Financially motivated cybercriminals are now using sophisticated targeted attacks and cyberespionage campaigns. Attackers are well organized and share their resources and expertise. Security researchers have observed a growing number of multi-staged attacks that begin with reconnaissance activity to identify and target employees with privileges to

sensitive resources. Attacks use custom malware, including remote access Trojans designed to maintain persistence on the corporate network in order to monitor and document processes and potential weaknesses that can be exploited.

The increasing variety and pace of new data breaches illustrate the fact that enterprises are struggling to defend against these sophisticated attacks. The defense challenge is compounded by previous investments in security products and point solutions that fail to share threat intelligence or take a holistic approach to an organization's security posture. The challenge has proven costly. Forensics investigators interviewed by IDC consistently state that they find basic missteps, employee mistakes, and the failure to implement and maintain basic security best practices are often leading causes of these costly security incidents.

Bridging Security Controls

Interest and adoption of STAP market products are growing significantly, driven in part by the need to identify advanced threats as well as the need to bridge gaps in the existing security architecture. Sandbox technology, once an esoteric tool used by malware analysts, is now incorporated into both on-premise appliances and subscription-based services. In the sandbox, suspicious files are detonated, examined, and documented to provide protection. STAP solutions generally examine files from messaging, endpoint, and Web activity, tying together security products deployed to cover the various attack vectors.

Many modern advanced endpoint solutions employ some level of behavior analysis, typically using an endpoint client to monitor system calls, examine executable files, and assess applications for unusual behaviors. Security vendors are also adding automated response functionality and data collection to support incident responders and forensics specialists. The endpoint information is often correlated with network traffic inspection to gain visibility into botnet communication with criminal command and control servers, identify unusual spikes in traffic that may represent data exfiltration, and create protection for unified threat management appliances, intrusion detection and prevention products, and secure Web and messaging gateways.

STAP products represent the first significant advancement in the security stack in some time, and IDC predicts that organizations will continue to deploy these products through on-premise devices, endpoint clients, via private and public clouds, or in some combination of these models. The three STAP subsegments that IDC is tracking — endpoint, boundary, and internal network analysis— have strong enterprise interest and adoption. Trends in each subsegment consist of the following:

- **Endpoint.** Endpoint STAP products use a wide variety of methods to improve threat detection and prevention capabilities. Emerging solutions collect data for analytics processing either on-premise or in the cloud, to provide visibility into endpoint activity. Isolation and containment of suspicious or unknown files and local sandboxing are other advanced techniques being used by this new breed of STAP endpoint solutions. Some solutions also include integrated forensics capabilities for rapid incident response while others rely on third-party integration for remediation. The market is evolving to include a level of automated remediation. Endpoint is the fastest-growing market, with a CAGR approaching 48% through 2019. Examples of security vendors providing Endpoint STAP products include Bromium, Carbon Black, Comodo, CrowdStrike, Cylance, Intel Security, Invincea, Symantec, and others.
- **Boundary.** The interest in boundary technology has been prompted primarily by the success of companies delivering sandboxing and other identification techniques on the network as well as secure Web gateway solutions. This is the largest STAP market segment and is expected to

reach $2 billion in vendor revenue by 2019. Adoption of subscription-based offerings are a significant driver in this market segment. Examples of vendors providing boundary protection include Ahnlab, Blue Coat, Comodo, Cisco, Fidelis, FireEye IBM, Lastline, Palo Alto Networks, Trend Micro, Websense, and others.

- **Internal Network Analysis.** Internal network analysis STAP products are primarily focused on botnet detection and determining if malware has infected the network. These products rely on user behavior, flow traffic, and DNS traffic to monitor east-west traffic flow and determine whether there is malicious behavior on the network. Internal network analysis solutions are expected to grow slightly faster than the overall STAP market with a CAGR of 28.9% through 2019. Examples of security vendors providing internal network analysis STAP products include Blue Coat, Comodo, Cisco Systems (Lancope), Damballa, IBM, RSA, and Trend Micro.

CONSIDERING COMODO

Comodo has developed solutions that address all three segments of the STAP market. The company offers its STAP products as a bundled solution called Comodo 360 which integrates technology components, security intelligence, and management. The Comodo 360 approach provides a Default Deny platform that relies on a layered strategy to prevent, detect, and respond to malware threats. Comodo has leveraged its position as the world's largest Certificate Authority to allow known good applications, or whitelisting. At the same time, the company also draws on the 85 million endpoint installations it has to ensure known bad files are instantly blocked or blacklisted. All other files are considered unknown and suspicious, and are safely run in a container temporarily until detailed analysis is completed.

Valkyrie

The key to Comodo's STAP solution is its cloud-based Valkyrie platform, which delivers global intelligence across all Comodo enterprise solutions. Valkyrie conducts both static and dynamic analysis of files, and supports a manual analysis capability as well. Valkyrie takes an average of 45 seconds to render a verdict on unknown files. The solution supports all currently supported versions of Windows and Windows server.

Endpoint: Comodo Advanced Endpoint Protection

Comodo Advanced Endpoint Protection (AEP) layers modern STAP capabilities such as Comodo's patent pending automatic containment technology, VirusScope behavioral- and action-based analysis on the host, and Valkyrie cloud-based sandbox integration, on top of a full suite of traditional endpoint security such as host firewall, HIPS, AV, Web URL filtering, file reputation, and persistent VPN.

Comodo AEP automatically contains untrusted processes and applications in a secure container locally, allowing users the freedom to run even unknown and possibly malicious applications safely while still denying potential malware the system access required to deliver its payloads, thus preventing infection even from zero day threats.

Comodo's automated containment technology has fully customizable capabilities. The technology can be set to automatically force all unknown applications to run in containment, thereby protecting corporate data. The containment system has no CPU dependencies and is hardware-agnostic unlike other containment solutions on the market, and supports Comodo's philosophy to only contain temporarily and as a last resort unknown files until a verdict can be reached. This approach allows Comodo to avoid the problems often experienced with other containment and micro-virtualization solutions and deliver a better user experience. The solution supports all currently supported versions

of Windows desktop, Windows server, Android, iOS and is targeting support for Apple OS X and Linux midyear 2016.

The Comodo Client is managed with Comodo IT and Security Manager (ITSM), which unifies both IT and security management into a single console, and allows for the configuration of security policies and visibility into the health and control of the endpoint, with device monitoring, anti-theft and even takeover capabilities. Organizations can choose to auto contain all applications or prevent the impact to the endpoint by virtualizing applications in certain folders. Comodo ITSM also extends controls to mobile devices and provides customers with security management functionality to check the health status and fix problems remotely. With Comodo ITSM, system administrators can get an enterprise view of all unknown files running in automated containment, and even execute an enterprisewide malware scan.

Boundary: Comodo Dome

Comodo's cloud-delivered secure Web platform, Comodo Dome, acts primarily as a malware containment gateway, leveraging the cloud-based Valkyrie File Analysis Platform and Comodo's patent pending portable containment technology. The platform also supports URL filtering and other Web gateway functions. Comodo Dome can be deployed from a private cloud or through ISP or MSP infrastructure-as-a-service. The company plans to add modules for data loss prevention, firewalling and additional capabilities to Comodo Dome in the near future.

Internal Network Analysis: cWatch

Comodo's cWatch provides internal network analysis capabilities. Endpoint and network data is collected via sensors deployed at a distribution switch in the environment, where the collected data is analyzed in the manager to identify malicious as well as legitimate application data providing detailed cloud and shadow IT visibility. Advanced signature and anomalybased intrusion detection continuously monitors network activity, logs and connections. Collected data is normalized, classified and correlated by Comodo to create a range of meaningful security intelligence and alerts that ensure network security at all times.

CHALLENGES/OPPORTUNITIES

While Comodo did have a relatively late entry into the STAP market, the company's Advanced Endpoint Protection is complete. The Valkyrie verdict-driven File Analysis Platform is tightly integrated across all Comodo solutions to deliver global intelligence for enhanced effectiveness and speed. Comodo Dome and Comodo cWatch are newer offerings and will continue to evolve and provide a broader range of capabilities. Comodo will need to make up overall market share against more established vendors. On the plus side, Comodo benefits by having integrated solutions in all three STAP categories, reducing the need for reliance on outside integration partners and developing the technology and solutions in-house. Since Comodo is among the very few security vendors that has competitive offerings in all three STAP categories, the company is setting itself up to be a unique security and IT management solution for both larger enterprises and small to mid-sized business across industries.

CONCLUSION

STAP solutions show potential in leveling the playing field between defenders and attackers and IDC has projected significant growth in the market over the next five years. The combination of endpoint, network security, and internal network analysis provides visibility and context into threats to help incident responders reduce "dwell time" — the amount of time it takes to detect and contain a threat after the initial infection. STAP solutions help bridge the mostly rigid and siloed security solutions, creating the cohesion necessary to give security teams situational awareness.

Buyers should consider the following guidance when considering STAP security products:

- Carefully assess all existing security infrastructure to determine if solutions are properly configured and maintained. Determine requirements and whether they can be truly solved with a STAP security investment.
- Identify the organizational changes required as a result of deploying STAP products in the environment. Security operations and incident response processes may require changes.
- Thoroughly evaluate STAP products to determine their performance impact on the business environment and any potential for end user disruption. Identify security functionality in the organization's existing architecture that may not be turned on.

Buyers should seek to bolster their existing security infrastructure by making an investment in products designed to detect advanced threats from each of the three STAP submarkets: endpoint, boundary, and internal network analysis. Some vendor solutions provide functionality from each of the submarkets, integrating analysis products designed to identify suspicious files with behavioral analysis to identify function calls and suspicious file activity on the endpoint, and network analysis to detect attacker reconnaissance activity and lateral movement within the network.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com