IDC Analyze the Future

IDC Solution Brief

Assessing the Business Value of Endpoint Specialized Threat Analysis and Protection Solutions

Sponsored by: Cisco

Utsav Arora
Matthew Marden
Christian A. Christiansen
Robert Westervelt

July 2016

OVERVIEW

Criminal groups behind today's cyberattacks have become better organized, introducing reconnaissance activity, custom malware, evasion techniques, and other sophisticated tactics that place a burden on traditional security defenses. The litany of high-profile data breaches is impacting every industry and prompting organizations of all sizes to respond by modernizing their IT security infrastructure. The battlefield continues to be at the endpoint, where attackers typically strike to gain initial access to the corporate network. Most organizations have been waging this battle using traditional antivirus at the endpoint, a solution that has received a lot of improvements over its more than 25 years of existence but clearly isn't keeping up with attacker sophistication. Emerging endpoint specialized threat analysis and protection (STAP) products can either replace or complement antivirus by adding behavioral analysis and continuous system and user activity monitoring to identify new and sophisticated malware designed to evade long-established security controls. Modern endpoint STAP products have become an essential part of enterprise risk mitigation strategies. They provide the visibility necessary to support rapid incident response and the ability for security teams to determine the scope of an attack and contain it before a breach takes place.

This IDC Solution Brief leverages IDC's research into the value of IT security solutions, including endpoint STAP solutions such as Cisco Advanced Malware Protection for Endpoints (Cisco AMP for Endpoints). IDC's research shows that organizations can achieve significant value by deploying solutions such as Cisco AMP for Endpoints as components of their security strategies by providing a more secure operating environment and reducing the risk to their business operations. In particular, endpoint STAP security solutions can enable organizations to better identify, neutralize, and eradicate malware seeking to enter their systems through end-user devices before creating operational risk or harm. As a result, organizations can reduce the frequency of malware-related security breaches and other incidents, identify more threats proactively, resolve incidents in less time, and decrease the impact of security-related issues on business operations, which enables them to achieve business value by:

- Preventing security-related breaches or incidents from harming business outcomes or operations or damaging organizational reputation
- Enabling business agility by providing confidence in the security of data and business applications
- Improving end-user productivity by limiting the impact of downtime and other security-related incidents

- Making IT staff teams more effective and productive by enabling more proactive identification of security threats and helping them spend less time responding to security threats and incidents

SITUATION OVERVIEW

Enterprises are investing in more robust security solutions to proactively defend against targeted attacks and zero-day threats. Emerging products are rapidly gaining interest as CISOs and CIOs seek to modernize the IT security architecture to provide comprehensive protection against these threats. IDC tracks these solutions in a competitive market called specialized threat analysis and protection. Endpoint STAP is one of three segments of STAP, a competitive market that also consists of boundary STAP (sandboxing solutions for suspicious file analysis) and internal network analysis STAP (NetFlow and network packet inspection solutions).

Modern endpoint security solutions make up the fastest-growing segment of STAP. These products shed the traditional signature-based approach for threat detection and typically incorporate an agent that conducts continuous monitoring over system resources and application behavior. The latest endpoint STAP solutions combine a variety of functions such as behavioral analysis, file integrity monitoring, telemetric heuristics, and containerization to 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.

Cisco Advanced Malware Protection for Endpoints is one of the modern endpoint security solutions on the market that can increase visibility into executable and file activity. The product does more than monitoring, recording, detecting, and alerting. It can also automatically block malware in real time as well as contain it and remediate it before damage can be done.

Cisco AMP for Endpoints is fueled by threat intelligence supplied by the Cisco Talos Threat Security Intelligence and Research Group. Talos is made up of 250+ leading threat researchers and security experts who are on the frontlines, gathering and analyzing millions of new malware samples and terabytes of threat data per day. Talos then delivers that information in the form of detections, behavioral indications of compromise (IoC), and more to AMP for Endpoints via its cloud-based design, providing the most up-to-date protection.

Cisco AMP for Endpoints initially inspects files at the point of entry using a variety of detection mechanisms, including one-to-one and one-to-many signature matching, machine learning, static and dynamic analysis, indications of compromise, and other intelligence built into the product. If the files are deemed malicious, AMP will automatically block the malware in real time. Unknown files can be sent to AMP's built-in sandboxing technology to analyze file behavior and return a comprehensive report, which can prompt a "block" or "allow" decision.

Cisco AMP for Endpoints also supports retrospection for historical analysis. For the files deemed good or unknown and then allowed inside the endpoint, AMP for Endpoints will still continuously analyze and record their activity and behavior, regardless of file disposition. If a behavioral indication of compromise is detected at some point in the future, AMP alerts the security operations team and shows the entire recorded history of the malicious file's behavior over time. The team can see where the malware came from as well as where it has been and what it is doing across all endpoints. This allows investigators to quickly understand the full scope of the compromise, so they can quickly block and quarantine it using AMP's built-in remediation capabilities.

Organizations deploy AMP for Endpoints via a lightweight connector to protect PCs, Macs, Linux systems, and mobile devices. The autonomous connector continues to function regardless of whether the system is on or off the corporate network. Organizations have the option of a cloud-based and cloud-managed deployment or management through a private cloud virtual appliance built for organizations with especially stringent privacy requirements.

Fragmented Versus Integrated Advanced Security Solutions

IDC's interviews with CISOs from a variety of industries found that the selection process for modern endpoint security solutions often requires the integration of the new solution into the existing IT security architecture. Organizations are seeking ways to gain more value out of existing security investments and link often siloed or fragmented security systems to create more cohesive security defenses. Cisco supports this with an API enabled on AMP for Endpoints to integrate with third-party security tools.

Also being considered in product evaluations is each vendor's complete modern defense portfolio for seamless integration with a suspicious file analysis sandbox, threat intelligence engine, security analytics offering, and core threat detection services for comprehensive protection over Web, messaging, and cloud-based resources. Beyond just Cisco AMP for Endpoints, Cisco AMP can be deployed in other ways across the extended network, including on Cisco FirePOWER next-generation intrusion prevention appliances (AMP for Networks), on the Cisco next-generation firewalls (AMP for Firewalls), and on the Cisco Email Security Appliance (AMP for ESA) and Cisco Web Security Appliance (AMP for WSA). All of these integrations with other Cisco security products allow different AMP deployments to share and correlate information, communicate threat information to the security team in common formats, eliminate the need for manual correlation, and make it easier to understand the full scope of a compromise across the extended network. All of these products are also linked to the Cisco AMP Threat Grid malware analysis and threat intelligence engine. By integrating these solutions, organizations are bolstering their security posture and eliminating bottlenecks and runaway alerts that often wrangle incident response teams and hamper their ability to rapidly investigate and contain threats before a breach takes place.

THE BUSINESS VALUE OF ENDPOINT STAP SECURITY SOLUTIONS

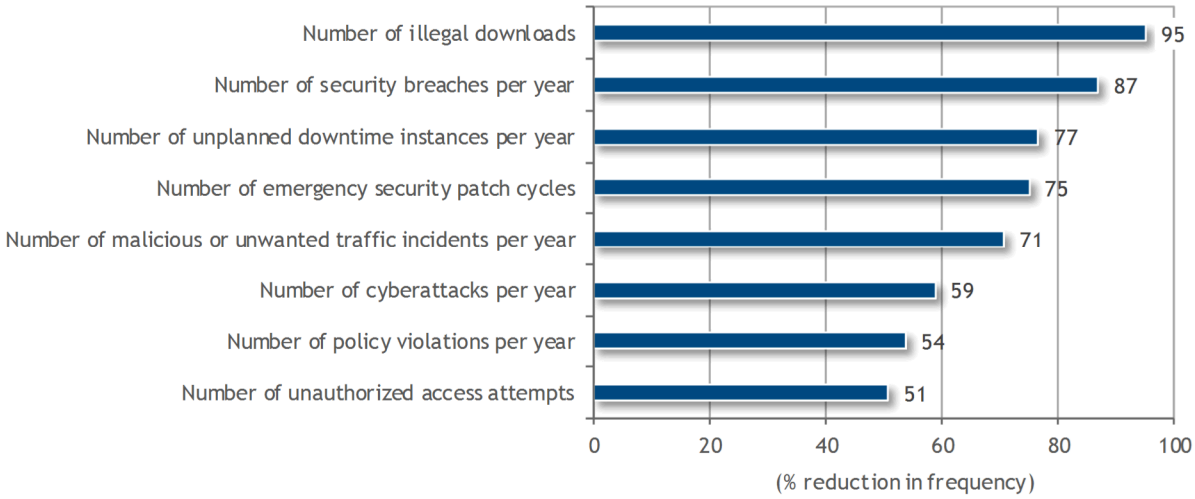
To evaluate the business value of endpoint STAP security solutions such as Cisco AMP for Endpoints, IDC analyzed key security-related metrics based on interviews with organizations that have deployed such solutions as a component of their security strategies. Endpoint STAP security solutions such as Cisco AMP for Endpoints offer capabilities such as improved ability to analyze the nature of incoming files, identification of unusual patterns and activity, early and accurate detection of possible breaches, and blocking malware from penetrating internal and external networks. Most organizations face demand to provide access to more applications to more users on more types of devices, making it increasingly important that the organizations have solutions that can deliver these capabilities and minimize risk related to accessing data and systems through endpoints.

IDC's analysis demonstrates that organizations can use security solutions that include endpoint STAP security solutions to quickly identify and resolve substantially more security threats, including malicious or unwanted traffic, security breaches, cyberattacks, illegal downloads, and policy violations. Figure 1 demonstrates the scale of potential benefits. IDC's research shows that organizations can reduce the number of security breaches they experience by an average of 87%, malicious or unwanted traffic incidents by 71%, cyberattacks by 59%, and unauthorized attempts to access their IT environments by

51%. Additional details of improvements to key security-related issues realized from the use of security solutions that include endpoint STAP security solutions are provided in Figure 1.

FIGURE 1

Security-Related Incident KPIs for Organizations Using Security Solutions That Include Endpoint STAP Security Solutions



Source: IDC, 2016

These security-related improvements can enable organizations to capture significant business value by reducing the risk of security incidents to their business operations, increasing the confidence of business teams in their security postures, and increasing the productivity of users and IT staff. Based on research with organizations that are using endpoint STAP security solutions such as Cisco AMP for Endpoints, IDC has identified four primary areas of benefit, which are discussed in the sections that follow.

Reduced Business and Operational Risk

IDC's research shows that organizations utilizing endpoint STAP security solutions such as Cisco AMP for Endpoints can significantly reduce their exposure to business and operational risk. Many organizations view compromising or losing customer or data or experiencing customer-facing business outages as a substantial business risk. As demonstrated in recent years, security breaches and other security incidents can cause significant and enduring reputational harm, as well as substantial financial losses in terms of revenue or fines. This makes it imperative that organizations do all they can to prevent these types of events from occurring. Meanwhile, IT security teams must establish and maintain strong security while facing continual demand from lines of business to extend access to data and business applications to more employees and partners using more types of devices.

Organizations interviewed by IDC that use endpoint STAP security solutions alongside other security solutions reduce the frequency of security-related incidents that can lead to harmful data losses or business outages (refer back to Figure 1). IDC's research shows that organizations can benefit from the capabilities associated with such solutions, including improved detection capabilities, more

pervasive visibility, and the ability to take steps such as sandboxing threats to prevent suspicious activities from becoming serious security threats or incidents. Given that many security incidents are self-induced (i.e., they occur because of actions taken by employees), proactively identifying more threats (42% more) and limiting the frequency with which events such as illegal downloads (95% fewer), unwanted traffic incidents (71% fewer), or policy violations (54% fewer) occur can greatly reduce an organization's exposure to these types of events that can carry heavy business and operational risk.

Supporting Business Agility

Security-related concerns can also limit an organization's ability to act with the agility needed to achieve the best possible business outcomes. Increasingly, competing robustly and addressing new business opportunities require that organizations deliver applications and services to more users and customers on more devices and in less time. This can create security concerns when potentially sensitive data becomes more broadly available and when more potential entry points exist for malware infections. To the extent that organizations conclude that they cannot sufficiently or cost effectively address gaps in their security postures, they may choose to sacrifice agility for security, which can mean missing out on business opportunities or operational efficiencies.

Endpoint STAP security solutions such as Cisco AMP for Endpoints can provide the confidence organizations need in their security postures to meet business and operational challenges. With this confidence, organizations can focus on serving their customers and address business opportunities rather than slowing the pace of their innovation to address security-related concerns. Of the interviewed organizations using endpoint STAP security solutions considered for this analysis, more than half of them attributed value to achieving greater agility, citing peace of mind of improved security and the ability to have employees focus more on business-critical aspects of their work as driving this value.

Allowing Users to Be More Productive

Users need reliable access to their organizations' devices, networks, and applications to ensure maximum productivity. Through continuous monitoring and analysis of the nature of incoming files, and alerting IT departments of malware and possible breaches, organizations using solutions such as Cisco AMP for Endpoints can reduce the frequency and duration of security-related incidents and threats impacting end users. As a result, users experience fewer disruptions that keep them from accessing their devices, critical files and data, enterprise networks, and business applications. For example, organizations considered for this analysis reported that users are losing 67% less productive time while security breaches are being resolved and 65% less productive time to unplanned outages since deployment of security solutions that include endpoint STAP security solutions. This means that their users are spending more time creating value, which can translate into significant financial benefits for organizations, including higher revenue.

Making IT Staff More Effective and Productive

The use of endpoint STAP security solutions can have a significant impact on IT departments. IT staff members become more productive when they can proactively identify and resolve more security- and malware-related incidents – not only do they need to spend less time on remediation, but they are also helping better minimize operational risk and ensure business continuity. Solutions such as Cisco AMP for Endpoints support IT staff efficiencies by providing deeper visibility into user and file activity, automatic detection of malware, and easy remediation once malware has been isolated. All of these capabilities enable IT teams to identify and resolve potential malware attacks on end-user devices

more proactively, meaning that they spend more time supporting the business rather than supporting users or resolving problems once they have occurred.

ESSENTIAL GUIDANCE

Organizations and attackers are engaged in an arms race; the more sophisticated attacks are, the more comprehensive and proactive the security response should be. Traditional security technologies continue to provide some protection but may require support from modern security solutions that introduce more robust capabilities for identifying threats. The following guidance can help organizations gain endpoint visibility and put the tools in place to support rapid incident response:

- Consider advanced security technologies that monitor the integrity of files and system resources and identify indicators of suspicious activity. Solutions should be supported by internal and external threat intelligence and a component designed to monitor network activities for signs of anomalous behavior.
- Identify endpoint STAP products that, in addition to detecting and alerting, can prevent malicious code execution and be configured to block threats. Determine whether the solution produces a risk score for any alerts generated at the endpoint and whether that score can be customized based on the enterprise's security posture. Examine the reporting capabilities and context being provided to incident responders.

  A comprehensive solution to this problem requires the integration of products from all three STAP segments: endpoint STAP, boundary STAP, and internal network analysis. Ensure that the provider of the endpoint STAP solution offers API to enable customers to use third-party tools and analytics.

As always, prior to adopting new technology, organizations should have a clear understanding of the most critical data to the business and document where the data resides and what employees have access to the information. Conduct a comprehensive risk assessment that takes into account internal and external threats and asset vulnerabilities. Prioritize and create a plan to remediate the identified risks.

APPENDIX: METHODOLOGY

IDC compiled the data used in this study from interviews it has conducted in the past year with organizations using endpoint STAP security solutions such as Cisco AMP for Endpoints in the context of their broader security strategies. Information was gathered by conducting interviews designed to obtain qualitative and quantitative information about the impact of these security solutions on organizations' security, business operations, staff, and costs.

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