Enterprise Strategy Group | **Getting to the bigger truth.™**

White Paper

Rethinking Endpoint Security

By Jon Oltsik, Senior Principal Analyst
With Kyle Prigmore, Associate Analyst

February 2015

This ESG White Paper was commissioned by RSA Security and is distributed under license from ESG.

Contents

Executive Summary 3

Rethinking Endpoint Security 3

Endpoint Security Challenges Abound 5

Endpoint Security in Transition 7

RSA and Endpoint Security 8

The Bigger Truth 9

Executive Summary

Mention endpoint security to an infosec professional and he or she will likely think of antivirus software, vulnerability scanning, and patch management. These three areas have made up the essence of endpoint security since organizations first connected to the Internet. Antivirus software, vulnerability scanning, and patch management remained relatively effective at detecting and blocking routine malware like viruses and Internet worms from the mid-1990s through the early 2000s.

Over the past few years, however, many legacy enterprise security methodologies, in particular those focusing on the endpoint, have started to show their age. While signatures and software updates remain important to patch common vulnerabilities and block pedestrian malware, new types of targeted attacks and sophisticated malware can easily circumvent traditional endpoint security controls and contribute directly to major data breaches.

Endpoint security as a category is now in a rapid state of transition. Key conclusions in this white paper are:

- **Endpoint security strategies are changing to address new types of threats.** Cyber-adversaries have adopted new tactics, techniques, and procedures (TTPs) using stealthy malware, spear phishing, social engineering, and other techniques designed to circumvent traditional endpoint security controls. These advances have led to the recent wave of publicly disclosed, massive data breaches at organizations such as Home Depot, JPMorgan Chase, and Sony Pictures, prompting security and business executives to increase their focus on cybersecurity... As a result, many organizations are rethinking their endpoint security strategies and budgets and are now crafting endpoint security strategies to address malware threats and cyber risks.
- **Endpoint security challenges remain.** While organizations have many new endpoint security initiatives, they continue to be hamstrung by existing endpoint security challenges such as a shortage of endpoint security skill, IT operations inefficiencies, and continued dependence on legacy infosec controls. Unfortunately, these challenges are only leaving them further and further behind, increasing IT risk.
- **Large organizations are embracing new endpoint security controls, oversight, and analytics.** ESG research indicates that many CISOs are adding new endpoint security controls to prevent, detect, and respond to sophisticated malware threats. In addition, large organizations are implementing endpoint forensics tools to capture and analyze security data in real time. Finally, firms are integrating endpoint, network packet, and log data to broaden their security visibility and analyzing this data with big data security analytics techniques.

Rethinking Endpoint Security

Endpoint security used to be a fairly mundane area at many enterprise organizations. The IT operations team would provision PCs with an approved gold image and then install AV software on each system. Of course there were periodic security updates (vulnerability scans, patches, signature updates, etc.), but the endpoint security foundation was generally straightforward and had become relatively easy to manage.

Firms are integrating endpoint, network packet, and log data to broaden their security visibility and analyzing this data with big data security analytics techniques.

More recently, however, organizations are increasing their focus on endpoint security and its associated people, processes, and technologies. This is reflected in the fact that 57% of organizations have increased their endpoint security budgets over the last two years. Endpoint security strategies are also in a state of transition. ESG research reveals that endpoint security strategy is being driven by (see Figure 1):[1]

- **The need to address new types of malware threats**. Nearly one-third (31%) of respondents report that one of the two most significant influences on their organization's endpoint security strategy moving forward is

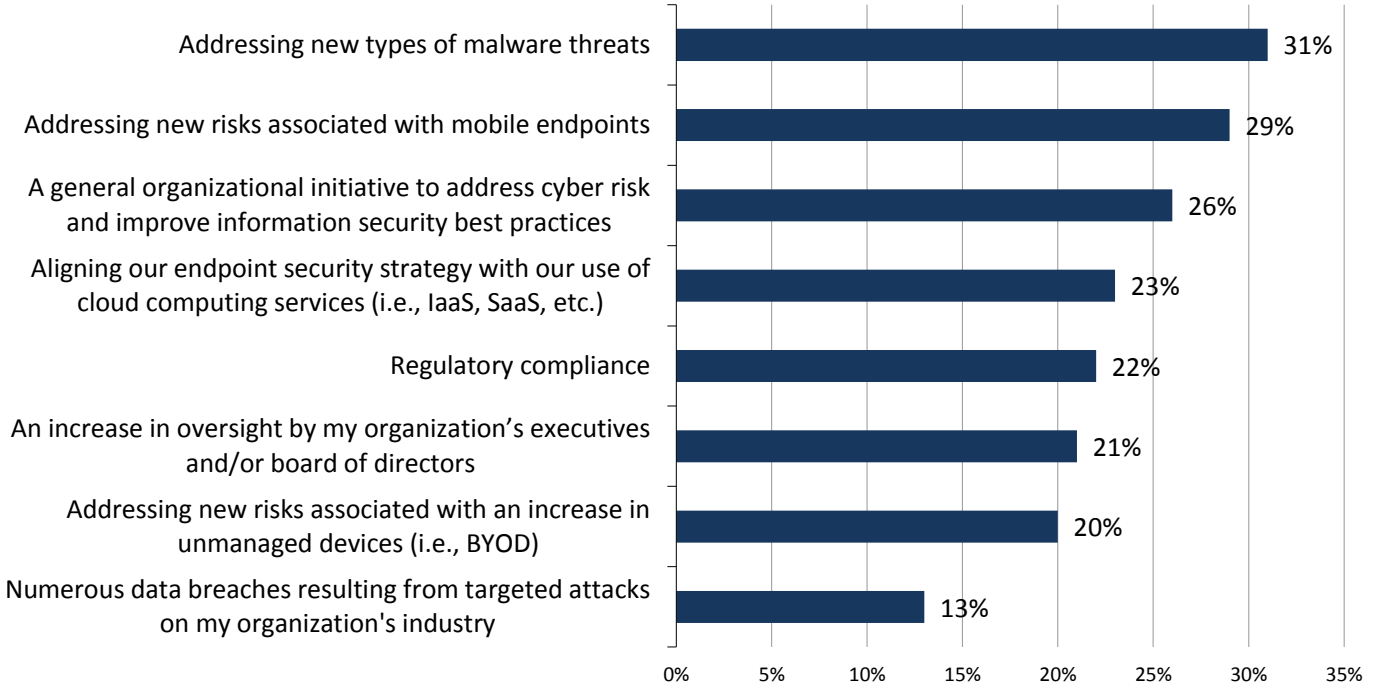
[1] Source: ESG Research Report, *The Endpoint Security Paradox*, January 2015.

addressing new types of malware threats. This is not surprising as the volume and sophistication of attacks has never been higher and the landscape is steadily becoming more dangerous. The sophistication and efficiency of the cybercriminal underground, the threat of state-sponsored cyberattacks, and the increasing ease of access that would-be criminals have to sophisticated malware tools are an intimidating combination, driving the need for new security strategies. Organizations are rightly concerned about their ability to rebuff these threats and stay a step ahead of their attackers, and they do not believe AV can do the job alone.

- **Problems caused by the volume and diversity of devices.** Twenty nine percent (29%) of respondents say that addressing new risks associated with mobile endpoints is a top endpoint security strategy requirement, while an additional 20% say that they need to manage new risks associated with unmanaged devices. This will only increase with the addition of more cloud, mobile, and Internet-of-Things (IoT) technologies.
- **Addressing cyber risk and improving information security best practices.** Just over one-quarter (26%) of respondents say that their endpoint security strategy is greatly influenced by an organizational initiative to address cyber risk and improve information security best practices. This is a clear indication that what they are doing today is not working.

Figure 1. Considerations That Have the Most Significant Influence on Organization's Endpoint Security Strategy Moving Forward

Which of the following considerations would you characterize as having the most significant influence on your organization's endpoint security strategy moving forward? (Percent of respondents, N=340, two responses accepted)



Source: Enterprise Strategy Group, 2015.

It is also worth noting that 21% of respondents said that endpoint security strategy is influenced by an increase in oversight by their organization's executives and/or board of directors. ESG interprets this as an indication of the growing importance of sound endpoint security policies, processes, and technologies.

Endpoint Security Challenges Abound

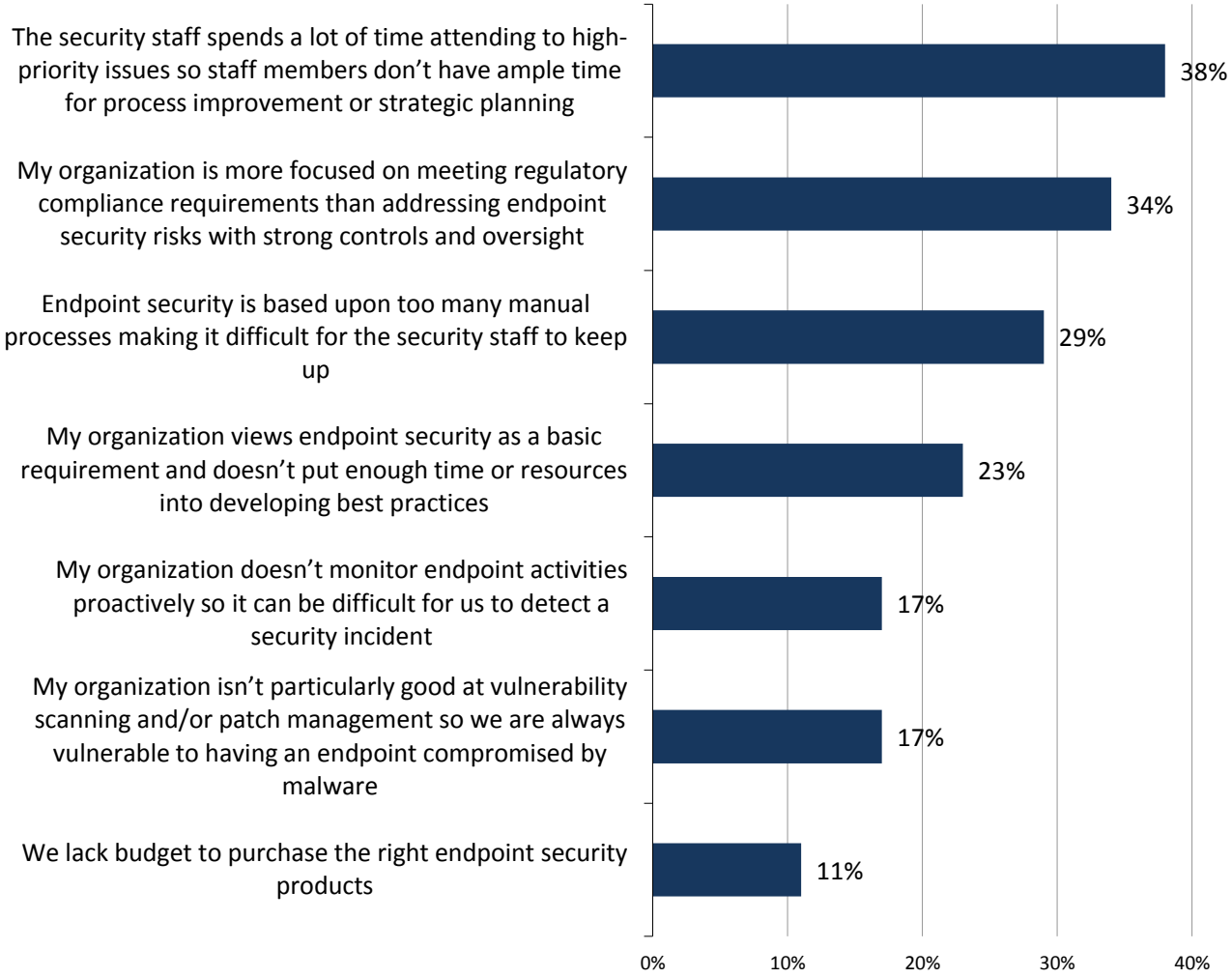
While ESG research indicates endpoint security strategies are driven by the numerous factors discussed, many organizations still struggle to address endpoint security vulnerabilities and threats with legacy processes and technologies. For example (see Figure 2):[2]

- **Security teams spend too much time putting out fires.** Thirty eight percent (38%) of respondents say that their security staff spends a lot of time attending to high-priority issues so staff members don't have sufficient time for process improvement or strategic planning. This challenge is something of a paradox. Strategic improvements cannot and should not come at the expense of the security team failing to respond to these high-priority issues, creating a purgatorial quandary for many organizations: They know they need an endpoint security overhaul, but cannot afford to dedicate ample time at the expense of day-to-day security tactics. Effective endpoint tools must address this head-on by improving both the strategic and day-to-day position of the security team.
- **Organizations remain overly focused on regulatory compliance.** More than one-third (34%) of respondents report that their organization is more focused on meeting regulatory compliance guidelines than addressing endpoint security with strong controls and oversight. Regulatory compliance should come as a result of strong security, and endpoint security cannot be achieved with a compliance-centric approach.
- **Endpoint security is fraught with too many manual processes and controls.** Endpoint security has undergone a major technical transition, but many organizations continue to rely on legacy products and processes to combat these new challenges. It is often cheaper and easier for organizations to layer new products on top of legacy products as needs arise, but this unfortunately bogs down security teams with haphazard layers of security processes and tools which can create a security operations nightmare.

[2] Source: ESG Research Report, *The Endpoint Security Paradox*, January 2015.

Figure 2. Endpoint Security Challenges

In your opinion, which of the following presents the biggest endpoint security challenges to your organization? (Percent of respondents, N=340, two responses accepted)



Source: Enterprise Strategy Group, 2015.

In addition to these issues, many organizations also find that their security teams are understaffed, conduct too many repetitive tasks manually, and lack critical malware and endpoint security skills for detecting and responding to cyber-attacks. All in all, ESG research points to a situation where the predominant endpoint security approach is not an adequate countermeasure for addressing the complexity and sophistication of modern threats.

Endpoint Security in Transition

ESG data strongly suggests that enterprise organizations do not view antivirus as a viable technology for blocking sophisticated attacks. As a result, many organizations are supplementing their AV products with newer and more robust technologies that offer more functionality across incident detection, response, and remediation. ESG research shows that enterprises are implementing new endpoint security technologies such as:

ESG data strongly suggests that enterprise organizations do not view antivirus as a viable technology for blocking sophisticated attacks.

1. **Advanced antimalware products.** Nearly three-quarters (73%) of organizations have already deployed or are testing advanced antimalware detection/prevention products on their endpoints (in addition to AV). The top reasons that organizations acquire advanced antimalware solutions are because it is recommended to them by their service providers (i.e., compliance auditors, penetration testers, etc.), the organizations are reacting to intelligence that they may be targets and want to add another layer of security, or they have seen industry peers add antimalware solutions with some success and they decided to follow suit.
2. **Continuous endpoint monitoring**. Fifty nine percent (59%) of organizations have purchased and implemented tools for endpoint monitoring over the last two years. While many continuous monitoring initiatives are in their nascent stages, the ESG data indicates that enterprise organizations are making slow and steady progress in this area.
3. **Endpoint forensics.** Sixty nine percent (69%) of organizations surveyed by ESG have deployed endpoint forensic solutions to some degree. And similar to real-time monitoring, organizations are deploying endpoint forensic products based on need, not cost. For example, 29% of respondents indicate that their organization deployed endpoint forensics because they thought it would improve their efficiency and effectiveness related to incident response, while another 29% indicated that the reason their organization deployed the technology was to reduce the time it takes for incident detection.

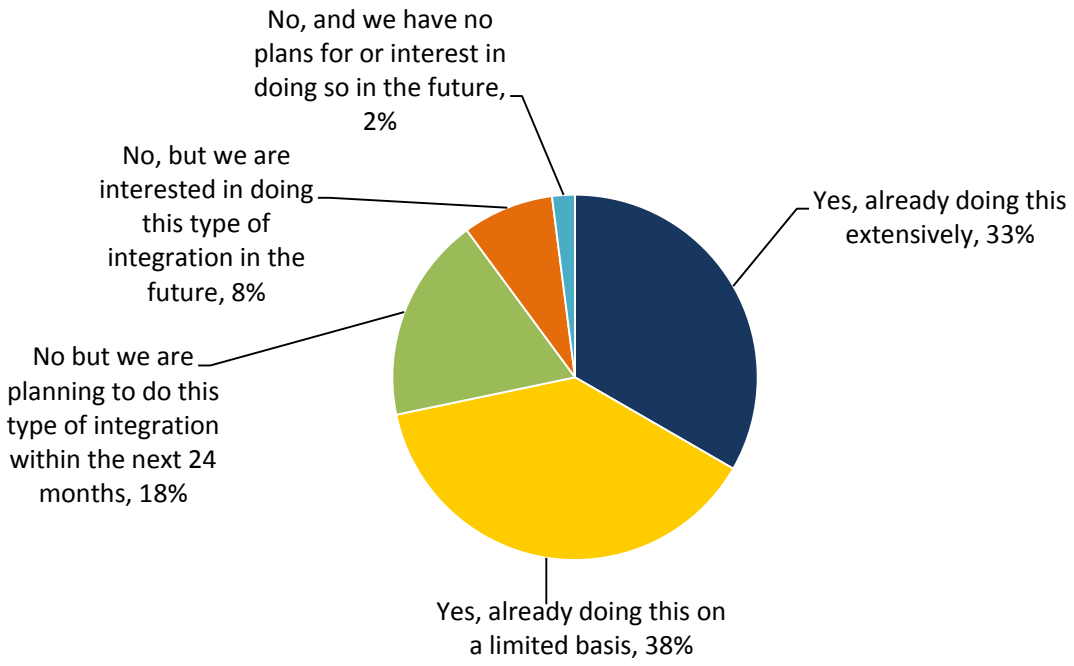
Finally, ESG found that 71% of organizations are integrating endpoint data with network security analytics. This gives them a more comprehensive and integrated view of security activities across networks and host systems (see Figure 3).[3]

ESG found that 71% of organizations are integrating endpoint data with network security analytics. This gives them a more comprehensive and integrated view of security activities across networks and host systems.

[3] Source: ESG Research Report, *The Endpoint Security Paradox*, January 2015.

Figure 3. Interest in Integration Between an Endpoint Forensics Solution and Other Types of Security Analytics Systems

Some organizations are integrating endpoint forensics solutions with network-forensics and/or security analytics tools (i.e., SIEM, big data security analytics systems, etc.). Is your organization doing or planning to do any type of similar integration between an endpoint forensics solution and other types of security analytics systems? (Percent of respondents, N=291)



Source: Enterprise Strategy Group, 2015.

RSA and Endpoint Security

Endpoint security has grown well beyond AV alone. Many organizations are implementing new types of tools to improve their incidence detection and response effectiveness and efficiency. Unfortunately, many CISOs continue to take a tactical approach. While layering on new tools may improve some aspects of endpoint security, it also adds complexity and operational overhead. Rather than approach endpoint security on a piecemeal basis, ESG believes that a prudent endpoint security strategy must be strategic and tightly integrated with the organization's enterprise-wide incident detection and response strategy.

RSA Security, a veteran information security vendor, has recently added endpoint security to its robust portfolio of incident detection, investigation, and response related products and services. RSA's endpoint security approach is based on:

- **RSA ECAT.** RSA acquired Silicium Security in 2012 and has recently released a major new version of the software, RSA ECAT 4.0. RSA ECAT is an endpoint threat detection solution that exposes malware and other threats, highlights suspicious activity for fast investigation, and instantly determines the scope of a compromise. With continuous monitoring of endpoint activity, organizations can gain the real-time visibility needed to detect and respond to threats faster. Unlike AV, RSA ECAT does not rely on signatures to detect malware. Instead, RSA ECAT gains a deep view of endpoint activity, looking for and flagging suspicious behavior for review. RSA ECAT can collect the critical endpoint data needed for investigations and enables security teams to focus their investigations and quickly confirm infections. In this way, RSA ECAT can capture endpoint forensic details to improve incident investigation and response, without requiring physical access to machines.

- **Integration with RSA Security Analytics.** RSA Security Analytics can help security operations teams gain visibility and control over their network. It is integrated with and thus can be paired with ECAT to bring together network-, log-, and endpoint-level security visibility and provide organizations with the data collection, aggregation, and analytics tools needed for enterprise SOC teams.
- **RSA Professional Services.** CISOs challenged by the complexity of improving their incident detection and response capabilities generally and endpoint security in particular can contract with RSA to help assess current capabilities, plan and design an appropriate endpoint security strategy, and deploy RSA ECAT alone or with RSA Security Analytics to better address the needs of their security team

The Bigger Truth

Endpoint security is changing to meet new demands. Organizations are struggling to hire the right staff, choose the right technologies, and respond to the many challenges of modern threats. The scale and diversity of these challenges can appear overwhelming, but organizations that take the time to devise and execute solid, integrated endpoint strategies can see rich returns. ESG believes that organizations that are seeking to overhaul their endpoint security should integrate their endpoint security technologies with their network-level and log monitoring in order to improve incident detection, prevention, and response, while also streamlining the work of their security operations team. RSA may be fairly new to endpoint security, but the company has taken an enterprise approach combining security products and services that aligns with burgeoning endpoint security needs. Given this, CISOs can benefit from an investigation of RSA's endpoint security offering.

Enterprise Strategy Group | **Getting to the bigger truth.**

20 Asylum Street | Milford, MA 01757 | Tel: 508.482.0188 Fax: 508.482.0218 | www.esg-global.com