White Paper

Endpoint Security Must Include Rapid Query and Remediation Capabilities

By Jon Oltsik, Senior Principal Analyst and ESG Fellow

November 2018

Contents

Executive Summary 3
The State of Security Operations 3
What's Needed? 5
Toward a Consolidated Endpoint Security Architecture 6
Beyond Prevention and Detection Alone 6
Benefits of a Comprehensive Endpoint Security Architecture Including Rapid Query and Remediation 8
The Bigger Truth 9

Executive Summary

Organizations face several increasingly vexing security challenges. Despite annual investments, most firms recognize that they face significant risk of security events and data breaches. The overall situation is alarming—security professionals spend billions of dollars on security, yet cyber-adversaries continue to penetrate networks, infiltrate systems, and steal or hold data for ransom. Why is this happening, and can anything be done to alter the balance of power? This white paper concludes:

- **Today's security strategies are broken.** Many organizations anchor their cybersecurity efforts with an inadequately sized cybersecurity staff, manual processes, and an army of disconnected point tools. This ineffective strategy leaves firms at risk for security incidents, data breaches, and regulatory compliance violations.

- **Organizations need a comprehensive endpoint security technology architecture.** A best-of-breed security product strategy should be complemented with integration between security tools. This translates to tightly coupled endpoint security platforms designed for advanced prevention, strong incident detection spanning the "kill chain," and features/functionality for incident response.

- **Real-time query and remediation capabilities must be included.** Incident response is shared between security analysts and IT operations staff, so an endpoint security technology architecture should support the requirements of both of these organizations and their shared processes. Real-time query and remediation capabilities are designed for this purpose, providing on-demand querying of endpoint assets and their status and attributes. This can help security and IT build consistency into operational reporting and find and fix potential vulnerabilities and\or IT hygiene issues such as weak system configurations more proactively.

- **A solid endpoint security technology architecture can help improve security efficacy, operational efficiency, and business enablement.** Too often mutually exclusive outcomes, security efficacy, operational efficiency, and business enablement can only be realized by aligning the objectives of security and IT operations teams. Such alignment must be enabled by leveraging a shared toolset that provides these teams access to the same data and thus the same level of visibility into endpoint system status, including vulnerabilities. Unification of tools and data also serves to streamline remediation steps and provides consistent reporting, a capability CISOs will appreciate as they report on business and IT risk to "C-level" executives and corporate boards.

The State of Security Operations

According to ESG research, 72% of organizations believe that security operations were more difficult in July 2017 than they were two years earlier due to many factors like the increasingly sophisticated threat landscape, the growing volume of security alerts, and continuing security monitoring gaps.[1] In addition, many organizations report security challenges including (see Figure 1):

- **A cybersecurity skills shortage.** The global cybersecurity skills shortage presents the biggest challenge. According to research conducted by ESG for Carbon Black, only 30% of respondents say the skill level of their security operations staff is adequate in all cases while 19% indicate that their security operations staff size is adequate in all cases.[2] This situation can lead to overwhelming workloads as the SOC team struggles to keep up.

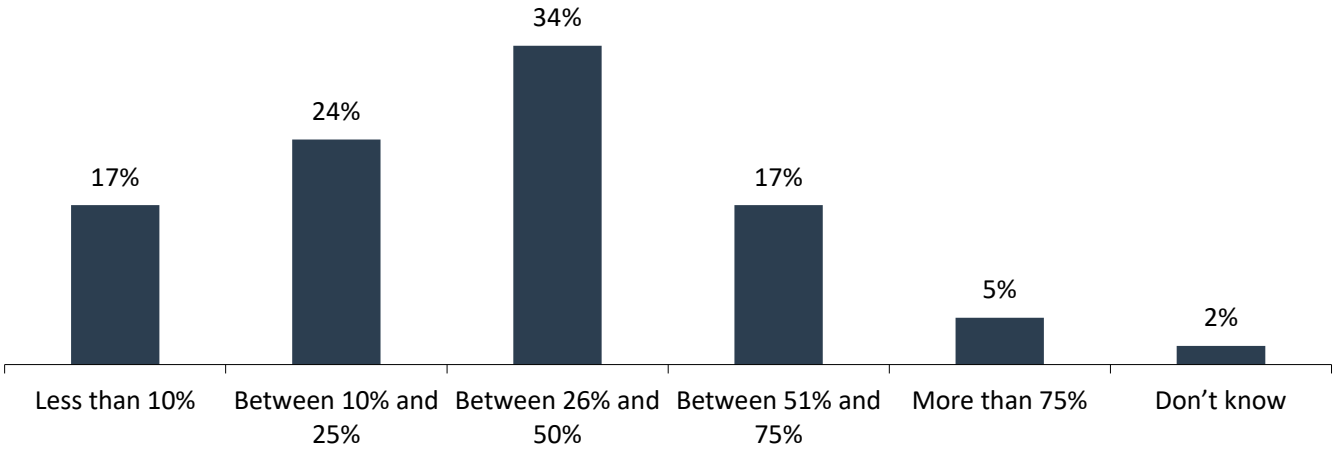
[1] Source: ESG Research Report, *Cybersecurity Operations and Analytics in Transition*, July 2017.

[2] Source: ESG Custom Research commissioned by Carbon Black, Inc., August 2018. All ESG research references and charts in this white paper have been taken from this custom research study, unless otherwise noted.

- Too many security alerts. Thirty percent of respondents estimate that their organization generates more than 1,000 security alerts monthly basis but many of these alerts are never investigated – even when security analysts would like to do so (see Figure 1).

Figure 1. Volume of Security Events/Alerts Organizations Ignore

What percentage of the overall volume of security events/alerts does your organization ignore, even though it would be beneficial to investigate, because it is impractical to investigate every alert? (Percent of respondents, N=201)

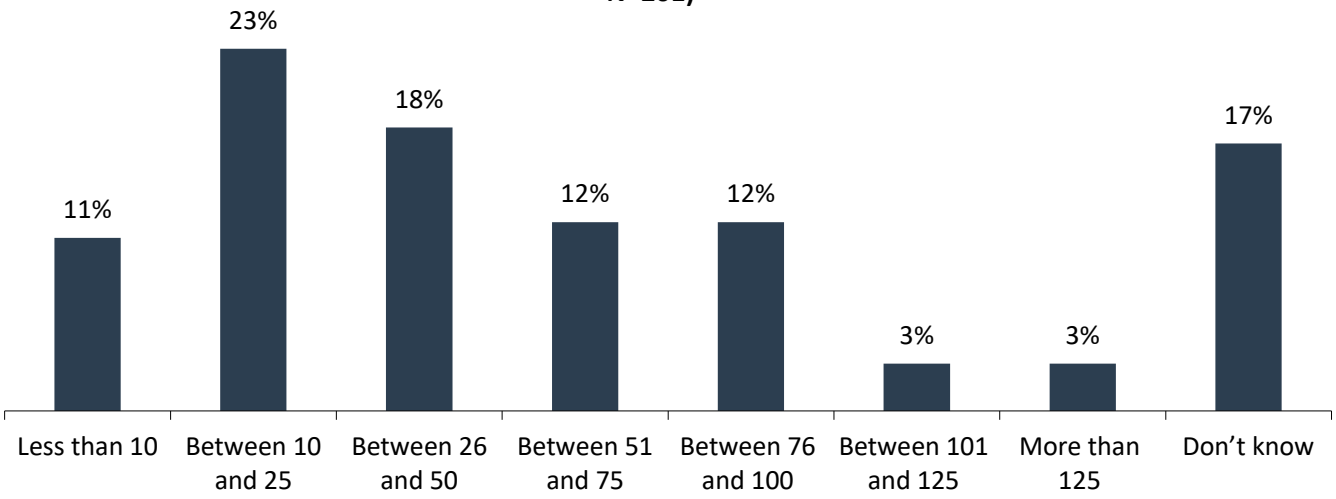


Source: Enterprise Strategy Group

- A dependence on disconnected point tools. Thirty percent of organizations use more than 50 discrete point tools to support their cybersecurity objectives (see Figure 2). In this situation, security analysts are forced to provide situational analysis by piecing together the output of disparate tools, reports, and UIs. Despite security analysts' best efforts, point tools-based security can be inefficient, ineffective, and inaccurate.

Figure 2. Number of Discrete Security Tools Used

Approximately how many different discrete or point security tools does your organization use today to manage, investigate, and respond to security threats? (Percent of respondents, N=201)



Source: Enterprise Strategy Group

These issues have inevitable and predictable ramifications—lengthy timeframes for threat detection and incident response. According to the Verizon Data Breach Investigations Report (DBIR), 87% of security compromises take minutes or less, yet more than two-thirds of these incidents remained undiscovered for months or more. And once incidents are detected, many security teams are unable to take surgical remediation actions due to a shortage of precise and timely information. Lacking detailed information and automated processes, many organizations simply reimage endpoints as a standard practice, wasting time and money. That is, even when aware of a cybersecurity incident, security analysts all too often lack specificity to minimize dwell time and prevent data loss and other forms of compromise. The solution to this problem is endpoint security solutions that provide precision, specifics, and surgical remediation capabilities to expedite incident investigations. These are an essential element of an incident response program.

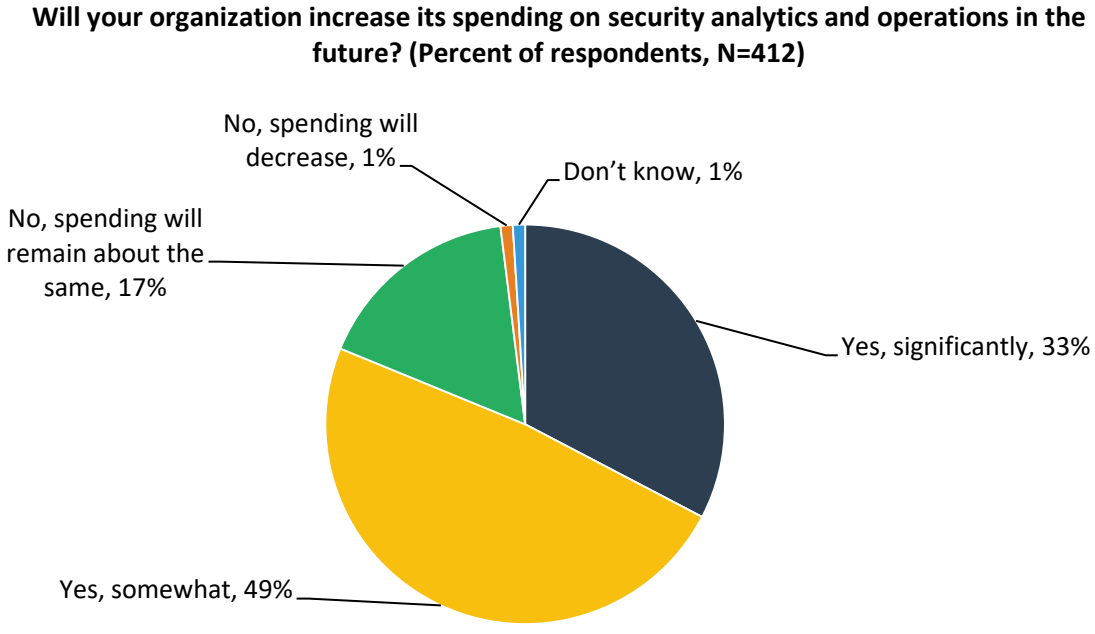
… endpoint security solutions that provide precision, specifics, and surgical remediation capabilities to expedite incident investigations are an essential element of an incident response program.

Overall, this situation should alarm organizations as it greatly increases the risk of a system compromise, data breach, or regulatory compliance violation. CISOs and CIOs must work collectively and diligently, address the issues described above, and unify security and IT operations processes as soon as possible.

What's Needed?

Organizations recognize that they must move security operations beyond the status quo. As a result, 82% of firms plan to increase spending on security operations through actions like adding headcount, modernizing security technologies, and working more with third-party service providers (see Figure 3).[3]

Figure 3. Increased Spending on Security Analytics and Operations



Source: Enterprise Strategy Group

[3] Source: ESG Research Report, *Cybersecurity Operations and Analytics in Transition*, July 2017.

Increasing security operations spending can be beneficial, but only if organizations can realize strong and near-term return on investment. For example, some organizations plan on adding new tools for threat detection, including endpoint detection/response (EDR), network behavioral security analytics, and user behavior analytics (UBA). While these technologies may provide some help, they can also exacerbate the challenges associated with managing point tools previously described. In this case, more tools can equate to more problems.

A comprehensive set of endpoint security controls, including those that provide real-time system state information and remediation capabilities, is an essential part of a strategic cybersecurity objective that helps bridge operating gaps between security analyst and IT operations teams.

Furthermore, threat detection improvements alone are not sufficient. Organizations must also include vulnerability assessments and remediation to reduce their attack surface, along with advanced prevention and incident response improvements. It is worth noting that addressing vulnerabilities requires the identification of both known software vulnerabilities and an ongoing assessment of system configurations requiring instrumentation of endpoint status. A comprehensive set of endpoint security controls, including those that provide system state and remediation capabilities, is an essential part of a strategic cybersecurity objective that helps bridge operating gaps between security analyst and IT operations teams.

Toward a Consolidated Endpoint Security Architecture

Rather than dabble in tactical solutions, CISOs should take a more strategic approach with a technology architecture that spans prevention, detection, and response. ESG also suggests that CISOs eschew complex multi-layered security technologies and instead concentrate their strategy across the endpoint security. Why? Endpoints act as a beachhead for nearly every type of cyber-attack. Therefore, it makes sense to focus efforts by bolstering endpoint security first. This can help improve prevention, detection, and response while delivering measurable ROI.

A complete endpoint security solution should span the entire security event lifecycle by including:

- Innovative advanced prevention capabilities. CISOs should start by looking for innovative types of next-generation antivirus capabilities that can help them block threats before they can compromise endpoint systems. These types of tools go beyond AV signatures alone by blocking exploits and malware using heuristics, threat intelligence integration, machine learning, and anti-exploit technologies. By blocking a much higher percentage of threats, organizations effectively decrease their attack surface, leading to fewer incidents to investigate and systems to reimage.

- Comprehensive endpoint behavior monitoring and reporting for full lifecycle threat detection. Even the best next-generation AV solutions will miss some types of sophisticated or zero-day cyber-attacks. This requires endpoint behavior monitoring to record all endpoint activities for further analysis. The best endpoint detection and response (EDR) tools will also be instrumented with rules programmed specifically to help analysts detect malicious activities like registry setting changes, lateral movement across networks, suspicious file downloads, or connections to rogue domains or IP addresses.

Beyond Prevention and Detection Alone

An endpoint security architecture composed of next-generation antivirus and EDR is a good start for threat prevention and detection. Unfortunately, these tools don't go far enough on their own. What's missing? Real-time query and remediation capabilities that can be used and shared by security analyst and IT operations staff.

To illustrate this shortcoming, suppose a cyber-adversary launches an attack using an exploit designed to take advantage of a recently discovered software vulnerability. The exploit easily circumvents any and all network perimeter defenses and

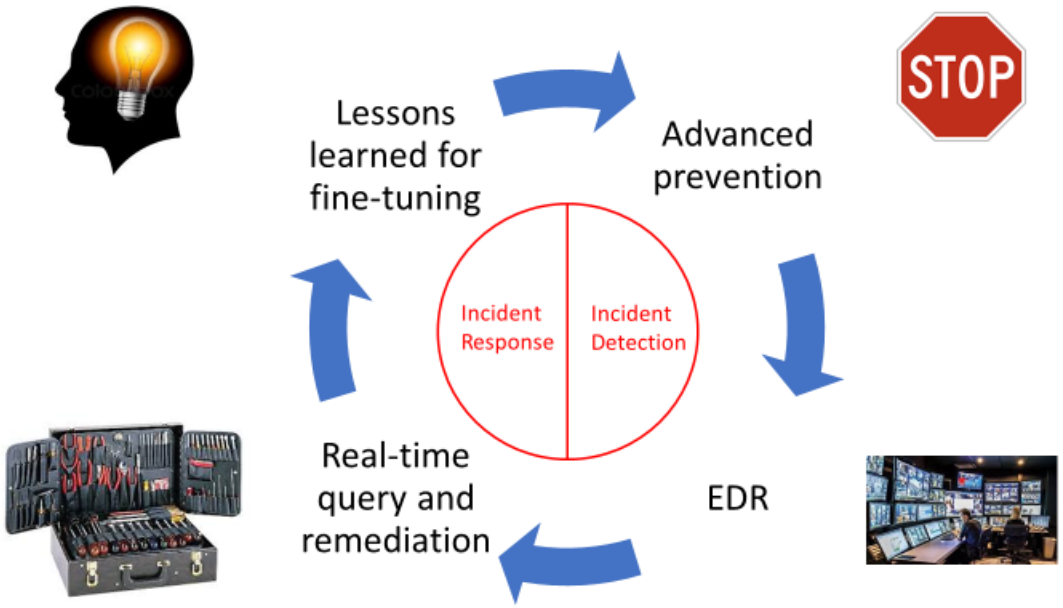
then targets the CEO's Windows PC, which is instrumented with leading next-generation antivirus and EDR software. Due to the sophistication of this attack, the exploit is not blocked by NGAV and thus compromises the system.

A few days after the initial compromise, the system starts to exhibit anomalous behavior. Perhaps it downloads a file from a rogue web domain and starts to propagate this file to other systems on the network. Of course, this behavior is enough to cause the EDR software to detect suspicious activities and generate alarm bells and provides security analysts with enough evidence for them to identify a cyber-attack in progress.

What happens next? To determine the scope of the attack, security analysts and IT operations professionals begin looking for answers to numerous crucial questions like:

- How many other systems on the network have a similar software vulnerability and haven't been patched yet?
- Where are these systems located and who owns them?
- Have other systems downloaded the same file or similar files that may or may not have been executed?
- How can we remediate systems as quickly as possible without disrupting user productivity?
- Which systems should be prioritized for further remediation?

Figure 4. Comprehensive Endpoint Security for Prevention, Detection, and Response



Source: Enterprise Strategy Group

In the past, security and IT personnel queried asset management systems, vulnerability scanners, system logs, and Active Directory as part of lengthy investigations to answer questions like those above. Data was often imported into spreadsheets, adding time for data collection and spreadsheet maintenance. Yes, some tasks could be automated with scripts, but this meant writing and maintaining scripts—a difficult task when endpoints are constantly moving around the network, changing configuration settings, or accessing networks remotely.

To better address these requirements, organizations need common tools for real-time query and remediation. Armed with these kind of tools, security analysts and IT operations professionals can accelerate security investigations and incident response processes around:

- Asset management. As part of incident response, security and IT personnel need continuous knowledge about the location and state of all endpoints. Real-time query and remediation tools are designed to provide this information based upon simple queries that can be facilitated by junior staff members. This capability can help organizations improve collaboration and accelerate IR processes. Asset management also includes an element of license management by providing an inventory of products running across an inventory and location information for those products being used.

- Problem scoping. Real-time query and remediation tools can help security teams perform IoC searches, file searches, and vulnerability scans at any time. This information can help organizations identify and mitigate risk while determining the scope of a cyber-attack.

- Swift remediation. Rapid query and remediation tools provide a map of all compromised and vulnerable endpoints across the network. With this information in hand, security and IT operations teams can then prioritize remediation tasks based upon business and IT risk factors like asset value, location, owner, etc. This level of specificity and focus effectively expedites remediation steps.

- Fine-tuning threat prevention. As organizations acclimate to rapid query and remediation tools, they can develop improved methodologies for threat hunting and risk identification. These lessons learned can then be directly applied to security controls for advanced prevention to further decrease the attack surface. In the future, endpoint security vendors will monitor these kinds of security operations behaviors across organizations and then share best practices operations templates amongst the customer base.

It is important to note the complementary nature of EDR solutions and real-time query and remediation tools based on their roles in performing these tasks. EDR solutions provide critical historical information to investigate root cause by capturing, analyzing, and retaining endpoint system activity while real-time query and remediation tools offer a view of the current state of endpoints, as well as the ability to remediate issues.

As such, on-demand rapid query and remediation tools can also help organizations build consistency and structure into operational reporting—a big improvement from existing practices of ad-hoc reporting related to emergency responses and ongoing cyber-attacks. In this way, organizations can run scheduled queries to track security status on a regular basis. This can help security teams improve risk assessment and reporting for CISOs and business executives.

Benefits of a Comprehensive Endpoint Security Architecture Including Rapid Query and Remediation

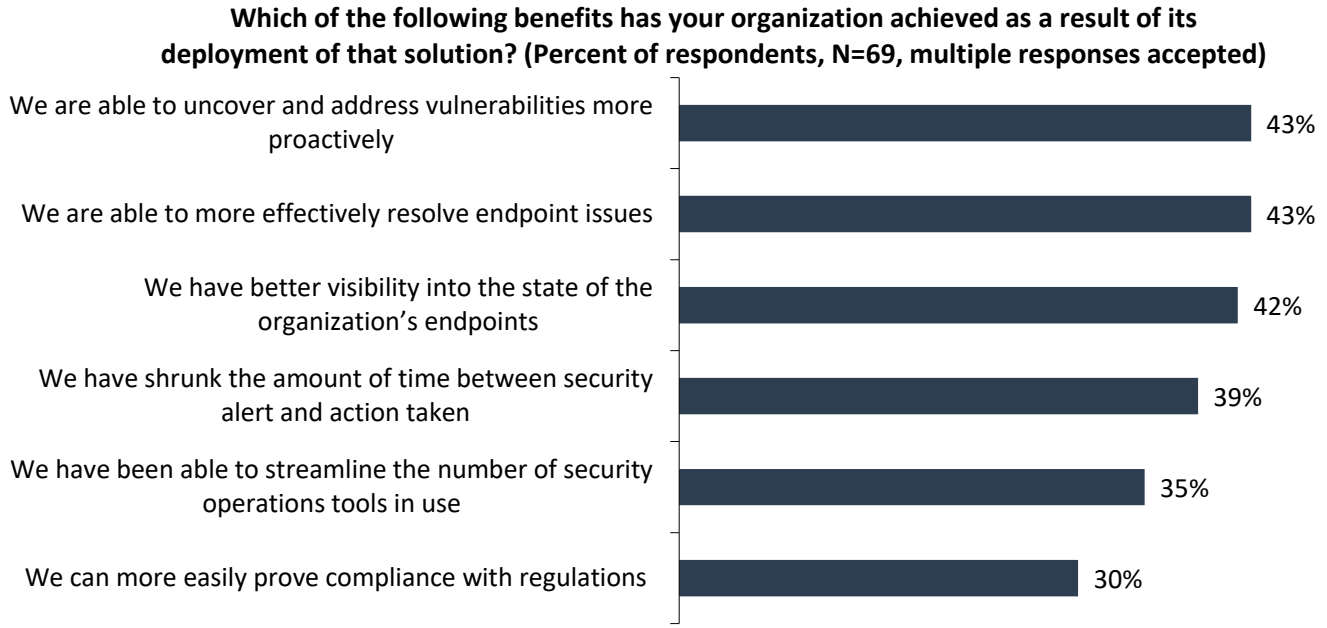
All CISOs have three common goals: 1) strong security efficacy, 2) operational efficiency, and 3) business enablement. A comprehensive endpoint security technology architecture, one that spans the full spectrum with advanced prevention, EDR, and on-demand endpoint query, can help organizations achieve these goals. In fact, the research points out that the addition of on-demand endpoint query can help organizations:

1. Uncover and address vulnerabilities proactively. On-demand endpoint query tools can be used to find vulnerable systems, isolate their location, and help IT operations teams prioritize patching schedules.

2. Resolve endpoint issues. Large enterprises often complain that they are constantly juggling hundreds of endpoint issues at any one time. Using on-demand endpoint query tools, IT operations teams can triage problems, fix minor issues, and manage open tickets more effectively from creation to completion.

3. **Gain visibility.** Endpoint visibility is often a journey, dependent upon multiple monitoring and asset management systems that are often out of synch with one another. With real-time endpoint query tools, IT teams have the ability to view granular endpoint configuration and security status whenever they need to.

Figure 5. Benefits of an Endpoint Query Tool



Source: Enterprise Strategy Group

The Bigger Truth

A famous quote says that the definition of insanity is doing the same thing repeatedly and expecting different results. Regrettably, this is exactly what many CISOs are doing. To address cyber-risks, many organizations continue to add layers of independent security controls and monitoring tools. Understaffed security and IT operations teams are then tasked with managing growing security technology chaos with manual processes and haphazard collaboration. This informal approach to threat prevention, detection, and response simply can't scale to address today's requirement, thus reaching its breaking point.

Organizations need new strategies based upon integrated security technology architectures built for security efficacy, operational efficiency, and business enablement. Supplementing a comprehensive endpoint security technology architecture with real-time query and remediation capabilities can align with this strategy and help bridge the operational gap between security and IT operations teams.

Given these benefits, CISOs and CIOs should review their current staff and technology capabilities while assessing cross-organizational process gaps and bottlenecks. Once existing issues are well understood, security managers should then see how a comprehensive endpoint security technology architecture with rapid query and response can help them address challenges and facilitate improvements in all areas.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides actionable insight and intelligence to the global IT community.

 www.esg-global.com

 contact@esg-global.com

 P. 508.482.0188