White Paper

Enterprises Need Layered Security Framework to Defend Against Cyber Attacks

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

November 2014

This ESG White Paper was commissioned by Absolute Software and is distributed under license from ESG.

Contents

Executive Summary

Organizations of all sizes in all industries are experiencing highly damaging security breaches. According to the Privacy Rights Clearinghouse, over 243 publicly disclosed data breaches occurred in 2014, exposing more than 65 million records.[1]

Why are there so many data breaches and what can be done to better defend against cyber-attacks? This white paper concludes:

- **Almost all organizations face the same primary issues that exacerbate the frequency of data breach incidents.** The recent wave of data breaches is a product of the increasingly dangerous threat landscape, growing IT complexity, and the continuing dependence on status quo security controls, manual processes, and an overworked security staff. These are issues that most organizations face, making the ongoing cyberwar a profound mismatch from the start.
- **CISOs need a reality check.** Aside from coming to terms with cybersecurity realities, security managers must understand that signature-based security defenses are no longer adequate and that cyber-attacks can come from any threat vector. Once a single system is compromised, it could cascade into a costly data breach over time.
- **Many organizations need layered enterprise defenses.** It is not enough to randomly add new threat management tools or services—cyber adversaries have become quite adept at finding and exploiting the gaps between security controls. What's needed is a comprehensive layered defense spanning endpoints and networks alike. Additionally, this defense-in-depth architecture must offer the right integration, intelligence, and automation to provide wide-ranging coverage for incident prevention, incident detection, and incident response.

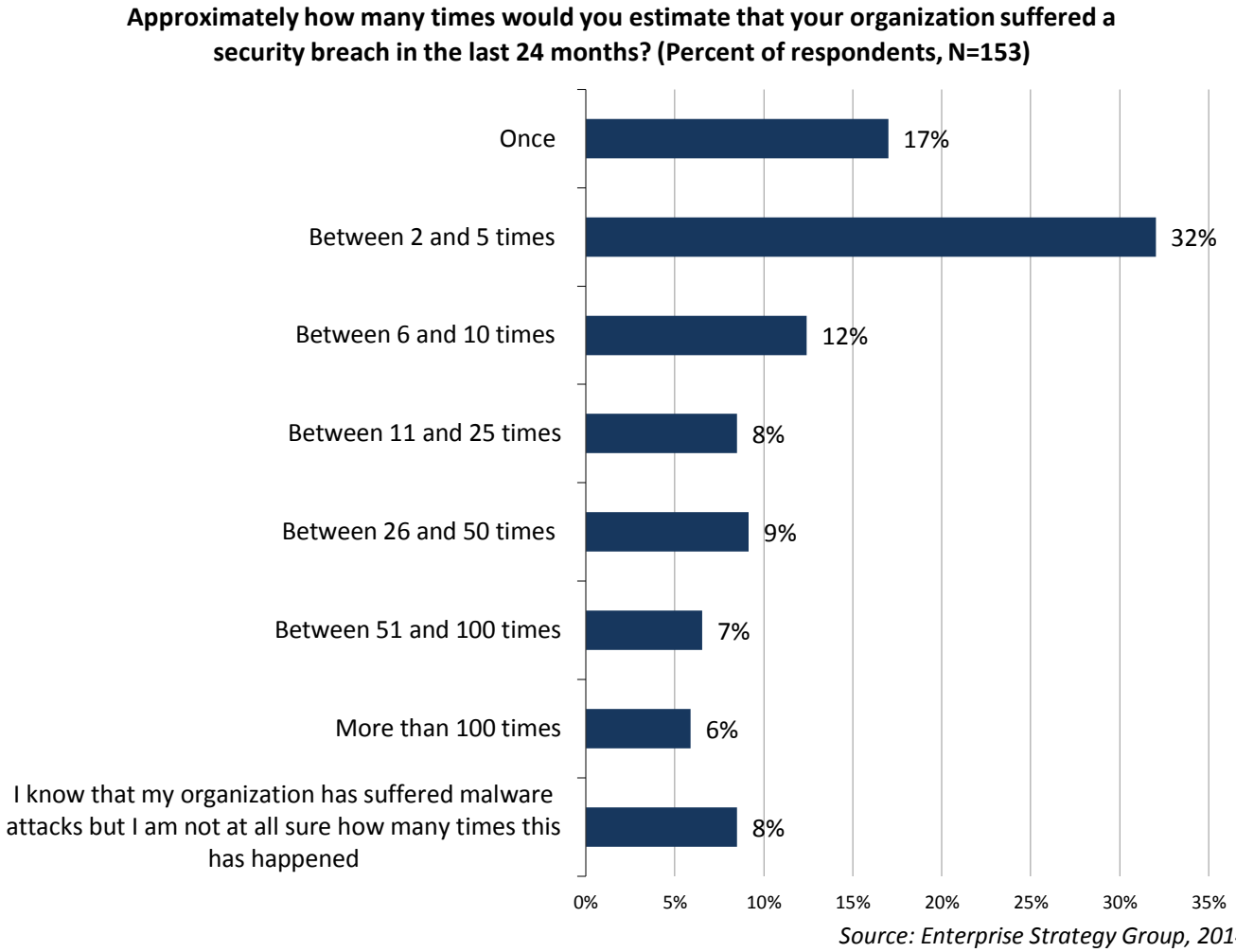
Enterprises Are Being Breached

Enterprise organizations are being breached at an alarming rate. According to ESG research, 49% of surveyed enterprise security professionals say that their organizations have been breached within the last 24 months.[2] Of those organizations suffering security breaches, 75% say they have been breached more than twice in that time frame. These numbers reflect the state of cybersecurity, and explain why enterprise CISOs often admit: "It's not *if* we will be breached, but *when* we will be breached."

[1] www.privacyrights.org

[2] Source: ESG Research Report, *Advanced Malware Detection and Protection Trends*, September 2013. All ESG research references and charts in this white paper have been taken from this research report.

Figure 1. Enterprises Are Suffering Security Breaches

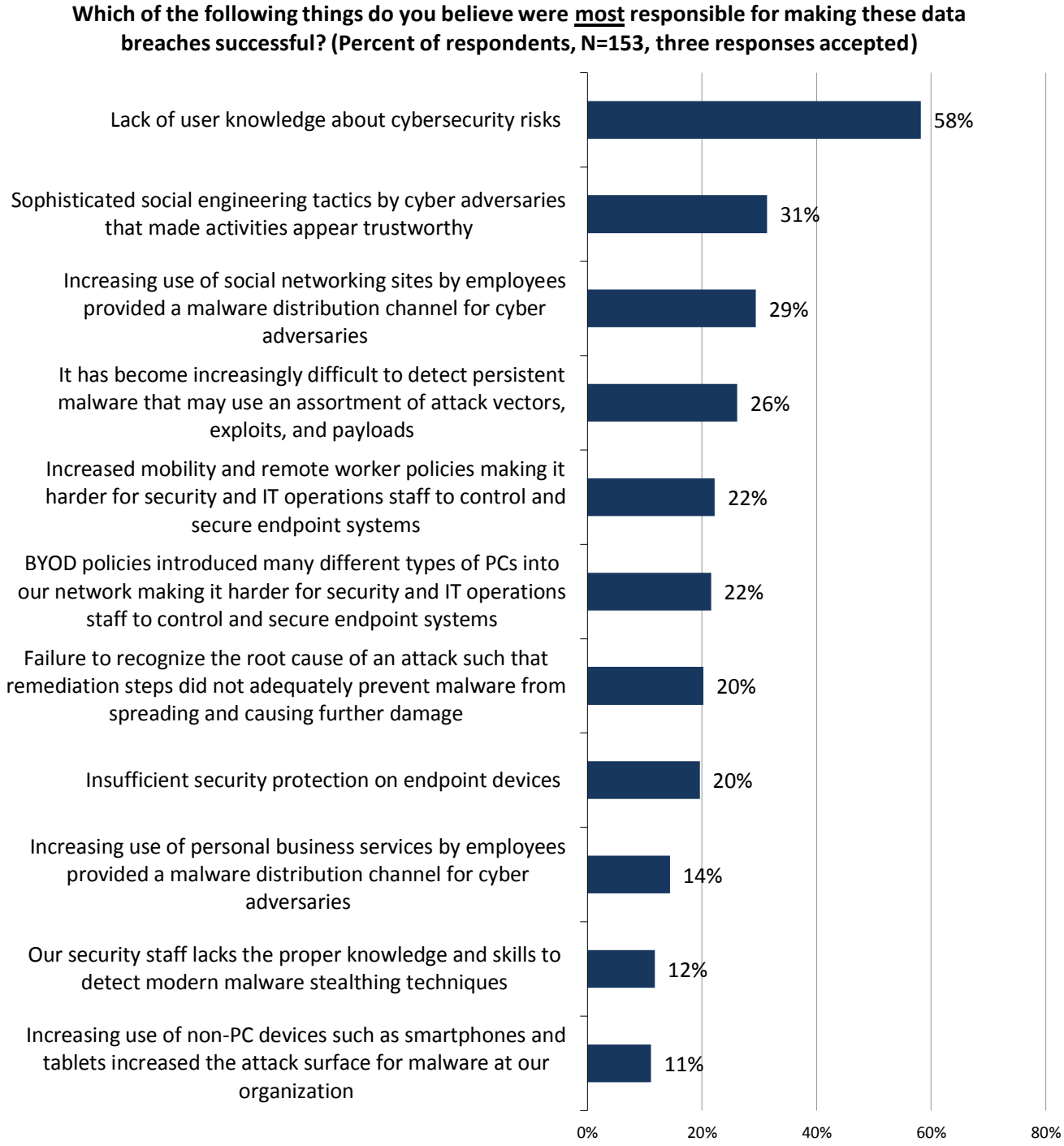


Source: Enterprise Strategy Group, 2014.

Why are breaches occurring at such a high rate? While many issues are certainly in play, ESG believes that the overall increase in security breach activity is due to three primary factors:

1. **An increasingly dangerous threat landscape and a lack of user knowledge.** ESG research indicates that 30% of respondent security professionals believe that the threat landscape became much worse between 2011 and 2013, while another 37% think that the threat landscape became somewhat worse during this timeframe. These perceptions are based on a number of dynamics like the rise in targeted attacks, the exposure of nation-state cyber espionage activity, and a wave of social engineering scams that seduce users with seemingly innocuous URLs (i.e., drive-by downloads), phishing sites, and files used for malware distribution. This issue is illustrated in a recent ESG research report: When asked to identify the factors most responsible for making data breaches successful, 58% of security professionals pointed to a lack of user knowledge about cybersecurity risk, 31% identified social engineering tactics, and 29% blamed an increasing use of social engineering sites by employees (see Figure 2).

Figure 2. Causes of Data Breaches



Source: Enterprise Strategy Group, 2013.

2. **Growing IT complexity.** Over the past few years, enterprise organizations have embraced a number of new IT initiatives including BYOD, cloud computing, SaaS services, social computing, and server virtualization. Unfortunately, many of these technologies carry new and previously unknown security vulnerabilities. For example, the adoption of BYOD has produced a long list of device types and operating systems that IT must secure. If the underlying legacy infrastructure is unable to support these devices, then IT will not have the tools needed to properly secure the mobile data. Finally, extremely lean security organizations often lack the necessary time or skills to oversee the security requirements inherent in constant IT change.
3. **Inadequate status quo security.** CISOs are now starting to realize that they can no longer rely on legacy security processes and technologies. Why? Overwhelmed security professionals frequently count on

manual processes and an army of point tools to get their jobs done. This creates an operational nightmare that doesn't scale. What's more, there is a global shortage of available cybersecurity skills, so organizations can't expect to simply add headcount to address their current problems. This leads to situations where CISOs mistakenly believe they are protected when just the opposite is true. For example, to bolster its security defenses, retail giant Target hired a team of security analysts and implemented network-based anti-malware gateways. Unfortunately, these investments were for naught when the security team failed to investigate a set of security alerts that ultimately led to the now infamous security breach.

Given these issues and the fact that security breach activity continues unabated, CISOs must face the reality that:

- **Signature-based defenses are not enough.** Endpoint and other security technologies such as gateway antivirus tools remain excellent at detecting and even blocking potential issues, but they aren't nearly as effective for detecting or blocking zero-day attacks.
- **Attacks can come through any vector at any time.** Endpoints are easier to attack because of their wide assortment of hardware and software configurations, and because end-users are prone to letting their guards down when using them. End-users can often be the biggest threat to an organization since IT must rely on them to safeguard devices and data while following corporate-approved security protocols. When matched against sophisticated social engineering tactics, industry research indicates that 60% to 80% of users will accept/open malicious files, visit rogue websites, inadvertently disclose encryption and other security passwords, download suspicious apps, or fall victim to phishing/social engineering attacks.
- **It only takes one compromised endpoint to cause major problems.** Enterprises can have thousands (or even hundreds of thousands) of endpoints accessing the network at any time. Cybercriminals are adept at compromising a single endpoint—either by stealing the device or accessing it remotely. Once this task is accomplished, they can use it as a staging point to remotely escalate privileges, conduct network surveillance, and exfiltrate valuable data.

Protecting Endpoints Demands Layered Security across the Enterprise

As previously described, many organizations rely on an assortment of independent point tools like encryption, AV software, IDS/IPS, and web threat gateways to protect endpoint systems. Unfortunately, hackers have found the holes between products and can now easily circumvent this traditional security approach.

So what's needed? An end-to-end security strategy based upon a foundation of automated, intelligent, and integrated security technologies spanning endpoints and the network. CISOs need to implement this strategy and technology architecture for (see Table 1):

1. Incident prevention
2. Incident detection
3. Incident response

Table 1. Enterprise Defense In Depth

Activity	Objective	What's Needed	Sample Technologies Used
Incident prevention	Decrease the attack surface across endpoints and networks, making the objective of cyber adversaries more difficult.	• A foundation of security controls • Industry-specific, advanced prevention • Threat intelligence integration	• Secure configurations • Network segmentation • Application controls • Port controls • ACLs
Incident detection	Detect anomalies, monitor activity, and maintain oversight.	• Endpoint and network data collection • Alerting capabilities for specific behaviors • Security analytics and forensics skills	• Endpoint security tools • Network and endpoint forensic tools • Security analytics engines for real-time detection and historical analysis
Incident response	Remediate compromised systems and minimize damages.	• Comprehensive, actionable intelligence • Remote security responses • A formal plan and feedback loop	• Security analytics engines • Endpoint data security measures • GRC systems • An asset database • CMDB

Source: Enterprise Strategy Group, 2014.

What's Needed for Incident Prevention?

In the past, most organizations spent the majority of their information security efforts on risk management and incident prevention. Typically, this was done by following security best practice guidelines like the SANS top 20 and implementing basic security controls like AV software and firewalls. These activities are still required, but they are not enough. To decrease the attack surface further, organizations need:

- **A foundation of tight controls and processes.** For starters, all systems must be deployed and maintained in secure configurations. Yes, some users will need the flexibility to download applications and files to get their jobs done, but it's best to map user roles to designated formal configuration options rather than make changes on an ad-hoc basis. Endpoint security should be supplemented with network-based controls like network segmentation and granular access controls. Security teams should also implement tools for continuous monitoring so they have real-time intelligence about the devices on the network and the security status of these systems. Vulnerable systems identified should be quarantined or redirected to a remediation VLAN with no delay.
- **To plan ahead.** CISOs should determine the behavior and conditions that would signify that a system is vulnerable and then ensure that the security team is alerted when these conditions occur. It is worthwhile to bring the entire IT and security teams together to brainstorm scenarios, study data breaches that have already occurred, and then determine what steps should be taken to protect the organization. Of course, unanticipated situations can (and probably will) occur, but even identifying a portion of these scenarios will help accelerate detection and response.
- **Industry-specific, advanced prevention.** Aside from basic controls, organizations should study threat intelligence to understand the specific types of attacks they may face. For example, leading industry

sources indicate that financial services are most often targeted with web application attacks; retail organizations are most often targeted with point-of-sales (POS) attacks; and entertainment companies most often face denial-of-service attacks. In the case of retail organizations, POS attacks are aimed at PCs used as cash registers. To address this threat directly, retail industry security professionals should arm POS systems with security defenses like application controls and file integrity monitoring (FIM), and limit POS network connectivity to specific IP addresses only. The value of the data can often be impacted by industry considerations. For example, health care information is considered highly valuable since a complete record (health records, payment, identification, and other personal information) can be worth up to $500 on the black market. This is why health care devices are often the target of cyber criminals.

- **Integration and automation based upon threat intelligence.** The threat landscape is in a constant state of change as hackers change malware distribution sites, command-and-control (C&C or C2) servers, malware variants, encryption techniques, and attack patterns. To get the most out of threat intelligence, some organizations are using it as a basis to automate security remediation activities. For example, when a threat intelligence feed identifies a malicious URL or IP address, these firms automatically generate firewall rules, URL filtering rules, or IDS/IPS signatures to block these malicious locations. And given the large percentage of employees that are mobile, automating threat intelligence off the network is also an imperative. If an endpoint strays geographically, locking down the device remotely until the potential threat is assessed may be the only way to ensure corporate data and networks are not compromised via the device. These measures can help organizations lower risk and stay one step ahead of the bad guys.

What's Needed for Incident Detection?

Advanced incident prevention will make attacks harder for cyber adversaries, but CISOs should assume that persistent hackers and cyber criminals will ultimately find a way to access devices, penetrate the network, and compromise data security. Given this, organizations need the right processes and technologies for incident detection, including:

- **Persistent data collection and processing.** To paraphrase an old management adage, "You can't secure what you can't measure." In other words, it's critical to monitor endpoint and network activity at all times in order to distinguish normal activities from suspicious behavior. To maintain "eyes and ears" on endpoints, organizations need to collect and process endpoint data (i.e., changes to user names, IP addresses, geographical locations, encryption status, and system-level activities like registry setting changes, executables, network connections, etc.) as well as network forensic data (i.e., NetFlow data and IP packet capture). This data provides an indisputable record of everything that happens on endpoints and networks, which can be used for security investigations.
- **Predefined conditions that signify a security incident.** Enterprises should take the time to document atypical behavior and data points that could point to vulnerability and train IT/security personnel on this information. They should also create alerts so the team is notified when these conditions occur because the sooner you can detect a threatening situation, the sooner you can respond.
- **Advanced security analytics.** While the reality of the security situation is captured in endpoint and network forensic data, it still must be processed and analyzed to be useful. CISOs need tools or services that can apply advanced analytics to this data in order to model "normal" system and network behavior, and then detect and detail anomalous activities in real time.
- **Security analytics and forensic skills.** Timely incident detection depends upon skilled IT personnel and security analysts who can make sense of an assortment of technical clues. For example, the security team may realize that the CEO's PC has been compromised based upon a breadcrumb trail of log and forensic data that could include a user name change, unauthorized physical movement of a device, certain e-mail attachments, software vulnerabilities, suspicious connections, specific file downloads, registry changes, and mysterious system processes. Organizations with limited security analysis and forensics skills should invest in building the skill set or find the right combination of technologies and partners.

What's Needed for Incident Response?

While organizations have invested in new tools for incident detection, many continue to miss the connection between incident detection and response. To some extent, this is exactly what happened with the infamous Target breach. Incident detection tools detected malware and generated alarms, but the Target security team couldn't figure out what they meant and chose to ignore them.

To bridge incident detection and response, the security team must make sure they have:

- **Comprehensive actionable intelligence.** Security analysts need specific information detailing everything that happened after an initial system compromise. This can help them piece together a sequence of events to understand what happened and when it happened, and then identify every system, process, individual, and connection that was involved. Armed with this analysis, the security team can prioritize actions throughout the remediation process.
- **A formal response plan.** Too many organizations still depend upon infosec analysts to assume the hero role and figure out a response plan on the fly. Given the sophistication and potential damage associated with modern security breaches, this is a fool's errand. Strong incident response plans should be approved by executive management and include a wide variety of participants including communications, HR, legal, IT, infosec, risk/compliance, and lines of business. Clearly, the security and IT team will take the lead on technical matters, but other stakeholders will be needed to work with law enforcement, communicate with business partners and customers, reassure employees, and alert regulators.
- **A feedback loop to improve risk management.** Once "the smoke clears," organizations should take the time to understand what happened, uncover the weaknesses that were exploited, and execute a continuous improvement plan to mitigate the risk of a similar attack in the future. The ability to understand how and why a security incident occurred will allow the organization to take the necessary measures to ensure it doesn't happen again. This action will serve the business well if the incident is publicized or if auditors or other regulators are involved.

The Role Played by Absolute Software

Absolute Software provides information security technology that can play a unique role in the layered security strategy described. Absolute provides solutions and services that can help organizations accomplish several goals including:

- **A persistent connection to the endpoint.** Employees are accessing critical data on their devices when they are off the network and outside the office, which is also when mobile devices are often lost or stolen, leading to a data breach or a reportable incident at the very least. With persistence technology built into the firmware of the device at the factory, IT can maintain a connection to the device in order to monitor, track, and investigate its behavior. Using Absolute Software, even if an unauthorized user attempts to remove the technology, it will simply reinstall. Most importantly, an organization can invoke remote security commands to delete sensitive information and determine if any data was accessed prior to wiping the device.
- **An alerting system based on meaningful conditions.** IT departments can identify specific scenarios that represent high risk to the organization and then build customized alerts so they are notified if these conditions occur. This gives Absolute a leading role with continuous monitoring for incident prevention.
- **SaaS-based security.** Absolute offers enterprises SaaS-based security, which provides coverage on and off the corporate network with no investment required for additional infrastructure.

The Bigger Truth

The World Wide Web and Internet at large are an increasingly dangerous neighborhood full of criminals, spies, and a host of other sordid characters. These cyber adversaries are growing in number each day and are using more sophisticated weapons as part of their targeted attacks. Unfortunately, they are often successful in their efforts to steal financial information, regulated data, and intellectual property with relative ease.

To quote Albert Einstein: "The definition of insanity is doing the same thing over and over and expecting different results." Alarmingly, this is exactly how many organizations are addressing cybersecurity. In spite of the dangerous threat landscape and increasing risk, they continue to defend endpoints and networks with manual processes, limited security skills, and basic security technology controls. It certainly appears that when it comes to enterprise cybersecurity, Einstein was right.

Organizations need to realize that they are really engaged in a cyberwar. Like kinetic warfare, defensive strategies must be adjusted as adversaries adopt new offensive tactics. With this in mind, CISOs must go beyond basic security controls and adopt a comprehensive strategy that includes incident prevention, detection, and response across endpoints and networks. The goals are simple:

1. **Decrease the attack surface, making a successful attack as difficult as possible.** This requires a hardened foundation, on- and off-network coverage, industry-specific controls, and automated remediation based upon up-to-date threat intelligence.
2. **Detect incidents in real time**. This demands the collection of extremely detailed data, as well as the ability to identify anomalous behavior and quickly uncover whether it is benign or malicious in nature.
3. **Create a formal, efficient, and comprehensive process for incident response.** Once the scale and scope of an attack is understood, organizations must have formal, documented processes for incident response in order to minimize technical and financial impact. This process should involve a cross-functional team of IT, information security, and business participants.

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