ESG Solution Showcase

Raytheon Is Addressing the Transformation in Enterprise Security

Date: April 2015 **Author:** Jon Oltsik, Senior Principal Analyst

Abstract: Information security is getting more difficult all the time. Why? Enterprises continue to address the dangerous threat landscape with point tools and manual processes while corporate IT grows more complex with the addition of cloud computing, mobile computing, and software-defined data centers. As a result, many large organizations suffer costly data breaches each year. ESG believes that CISOs must assume that their organizations will be breached and redouble their efforts on improving their ability to detect and respond to threats as quickly as possible. This will require a new approach for security data analytics focused on gaining actionable intelligence from data collection, processing, and analysis.

Overview

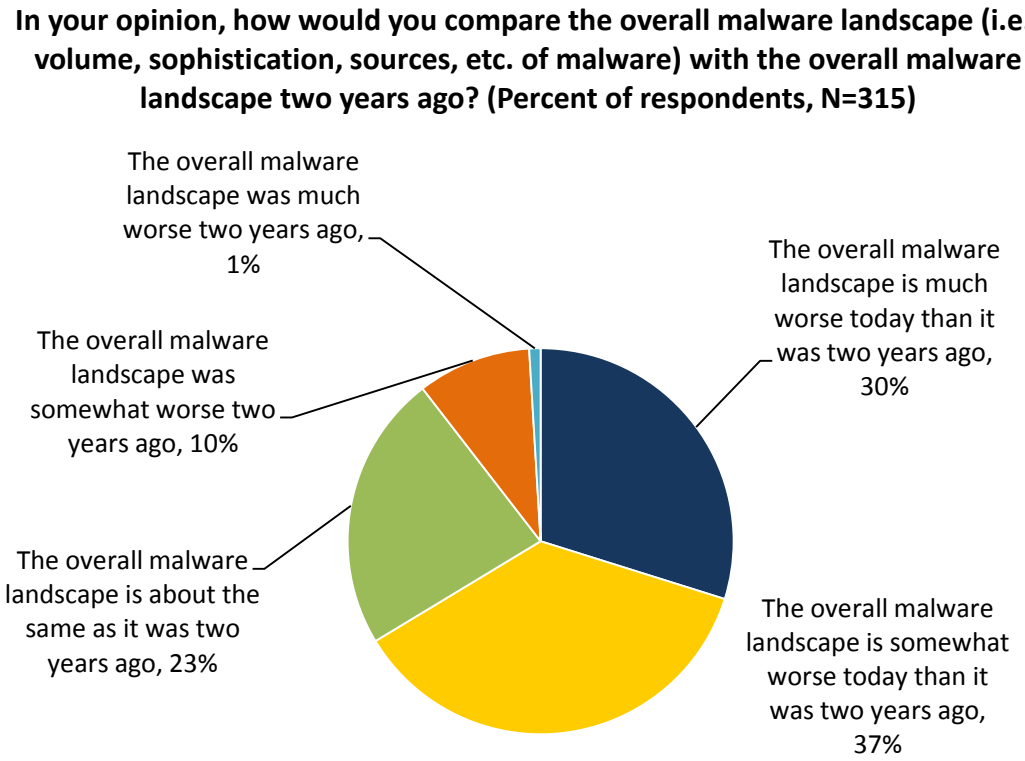
Ask any CISO and she will tell you that information security is growing more cumbersome on an annual basis. This difficulty isn't simply related to one aspect of info sec: It is happening everywhere. For example, ESG research indicates that 79% of security professionals working at enterprise organizations (i.e., more than 1,000 employees) believe that network security has become more difficult than it was two years ago.[1] The same is true with regard to endpoint security—80% of enterprise security professionals believe that endpoint security management and operations is more difficult today than it was in the past.[2]

Why is information security growing more difficult? While there are a multitude of reasons, ESG believes the primary causes include:

- **The increasingly dangerous threat landscape.** Enterprise organizations are constantly confronted by a new assortment of sophisticated cyber-adversaries intent on stealing their sensitive data. In fact, the population of bad actors (i.e., nation states, cyber-criminals, hacktivists, etc.) continues to grow in number and expertise across the globe. Furthermore, cyber-crime activity is more organized, specialized, and market-oriented than in the past, making black hats more adept at finding and exploiting an organization's vulnerabilities with highly effective malware that can easily circumvent security controls or remain "under the radar" of common security monitoring and analysis tools. Clearly enterprise security professionals share this belief— in 2013, 67% reported that the malware landscape was worse than it had been in the previous two years (see Figure 1).[3]

[1] Source: ESG Research Report, *Network Security in the Era of Cloud and Mobile Computing*, August 2014.
[2] Source: ESG Research Report, *The Endpoint Security Paradox*, January 2015.
[3] Source: ESG Research Report, Advanced Malware Detection and Protection Trends, September 2013.

FIGURE 1. Network Security Is Getting More Difficult



Source: Enterprise Strategy Group, 2015.

- **IT complexity.** While security professionals struggle to keep up with the threat landscape, their peers in IT are pursuing a host of new IT initiatives around cloud computing, mobile computing, and software-defined data centers. These projects introduce new layers of hardware, software, and interoperability challenges that expand the threat surface and expand the existing cybersecurity workloads.

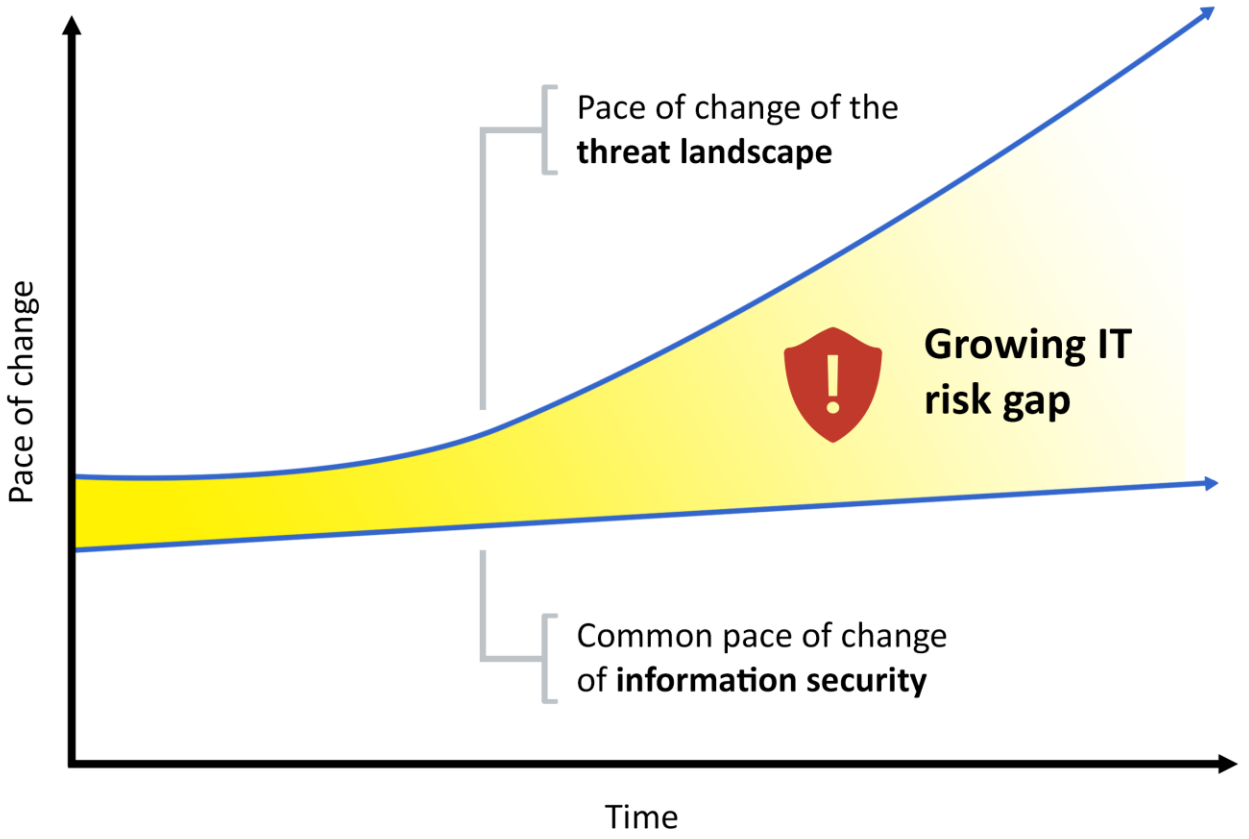
- **Legacy security tools, processes, and attitudes.** Enterprise security has grown organically over the past decade, built on the back of perimeter security controls (i.e., firewalls, IDS/IPS, threat gateways), host security software (i.e., antivirus software, HIDS/HIPS), and security monitoring and compliance tools (i.e., SIEM, log management, etc.). In this model, many organizations prioritized threat prevention with the intent of blocking attacks at the network perimeter and endpoint computers while threat detection was handled by SIEM correlation rules and dashboards. Unfortunately, this tactical approach is no match for today's multi-dimensional threats. Why? Disparate point tools aren't integrated to provide a multi-layered, tightly coupled defense, creating gaps between each tool. The security team is often bogged down with manual processes, creating operational overhead. Finally, static SIEM rules lack the analytics capabilities cyber-analysts need to leverage the data to make decisions and take action.

In addition to these issues, CISOs face another challenge: the global cybersecurity skills shortage. According to ESG research, 28% of security professionals' state that they have a problematic shortage of information security skills at their organization.[4] In many cases, enterprise organizations simply deal with their cybersecurity needs with an info sec team that is understaffed and under-skilled.

[4] Source: ESG Research Report, *2015 IT Spending Intentions Survey*, February 2015.

ESG believes that many organizations now face a frightening situation. While cyber-adversaries make rapid improvements to their tactics, techniques, and procedures (TTPs), enterprises respond with nominal, incremental enhancements to their cybersecurity defenses and oversight. In other words, cyber-adversaries are advancing their offensive capabilities at a more rapid pace than corresponding enterprise defenses. This imbalance is driving a growing IT risk gap at many enterprise organizations (see Figure 2).

FIGURE 2. The Growing IT Risk Gap



Source: Enterprise Strategy Group, 2015.

Enterprise Security in Transition

In the past, enterprise security was often anchored by security controls designed to prevent security attacks. While these kinds of security controls are still necessary, CISOs should assume that their security defenses will ultimately be breached. Given this, enterprise organizations need to move beyond SIEM alone and develop skills and expertise for threat detection and response. To address this requirement, enterprise security professionals must:

- Understand attacker behavior throughout the kill chain. Once a cyber-adversary compromises a system, he will take additional actions to advance his attacks, including downloading/installing additional software, moving laterally throughout the network, stealing user credentials, and creating rogue administrator accounts. Security analysts must have the right combination of skills and tools to identify and investigate suspicious behavior across the entire kill chain as efficiently as possible.

- **Concentrate on reducing "dwell time."** According to the 2014 Verizon Data Breach and Investigation Report (DBIR), 62% of breaches were not discovered until months after the initial compromise. This lag time gives cyber-adversaries ample time to become familiar with corporate networks, find the data they seek, and slowly steal terabytes of sensitive data over time. While security professionals may not be able to prevent malware attacks and system compromises, they can still prevent data breaches if they can reduce the amount of time that cyber-adversaries reside on the network (i.e., dwell time). In fact, ESG believes that all CISOs should track and measure dwell time metrics to strive for continuous improvement.

- **Improve network egress traffic monitoring.** Many organizations spend the bulk of their security monitoring on ingress traffic as it enters the corporate network. Yes, this is important, but the fact remains that cyber-attacks depend upon network egress traffic like system beaconing, command-and-control communications, and ultimately data exfiltration. Thus, organizations can improve threat detection and response by understanding attack patterns, developing network forensic skills, and continuously monitoring all network egress traffic for suspicious/malicious sessions.

What's Needed?

The requirements outlined depend upon a greater commitment toward continuous monitoring and situational awareness. In other words, CISOs must know everything they can about the network—which systems are connected, how these systems are interacting, where network traffic is going, what type of files reside in network packets, etc. Getting to this level of security analytics depends upon:

- **Holistic data collection and processing.** SIEM systems base their analysis on log files, security alerts, and network flow in some cases. These data sources are a good start but are no longer enough alone. To gain greater intelligence, enterprises need to collect and correlate this data with data from other sources both within and outside the enterprise. These data sources include other types of security systems such as those focused on endpoint and network forensics as well as general enterprise databases containing personnel records, supply chain data, and customer information. Additionally, external referential data may be needed to enrich the enterprise data with additional context. These sources can include external threat intelligence feeds, industry ISACs, and social networks. Beyond threat detection, security analysts need access to this broad array of data so they can pivot across data sets as they connect anomalous activities across systems, networks, files, and applications distributed across the enterprise. Further, as the threat landscape evolves and bad actors find new ways to attack, new data sources will be added to provide a more complete picture. Enterprises needs a highly adaptive cybersecurity infrastructure that is capable of quickly adding and correlating new data in combination with existing information.

- **Malware analytics.** Over the past ten years or so, many organizations started the process of malware analysis by sending files through AV gateways and web sessions through URL filtering tools. Good start, but these security controls can't keep up with over 300,000 new malware variants per day and can be ineffective against targeted attacks. In addition to the old guard, enterprises need static and dynamic malware analysis tools that open and execute files to search for malicious behavior. When malware is identified, security analysts can use additional data analytics to determine which systems have been infected, how they behaved after the initial exploit, and where they connected. This information can then act as a blueprint for remediation.

- **Intelligent algorithms.** Rather than depend on homegrown SIEM correlation rules and dashboards, CISOs need more proactive intelligence from their security analytics tools to help them improve threat detection and response. This means that security analytics tools must offer features like machine learning algorithms for better

anomaly detection. Superior security analytics tools will provide nested algorithms that sequence multiple behavioral anomalies together before issuing an alert. This not only reduces false positive alerts, but also can provide a timeline of details to the SOC team for investigations and response. Finally, improved security analytics and visualization can help bolster the security team's productivity—an effective countermeasure for coping with the global cybersecurity skills shortage.

Burgeoning security data analytics requirements can be difficult and require advanced skills, so CISOs must plan accordingly. For instance, security analytics tools should be evaluated not only for their security efficacy but also for their ease of use. In other words, these systems should be easy to deploy, require little training or customization, and provide GUIs and workflows that support the security analyst team. The best tools will offer leading-edge visual analytics rather than standard charts and network topologies in order to empower analysts and speed investigations. Finally, CISOs must recognize when and where they need help and work with security vendors offering professional services, staff augmentation, or even managed security services.

Enter Raytheon

While Raytheon may not be the first information security vendor that comes to mind, the company has actually been deeply involved with government agencies on cybersecurity for many years. Raytheon also leverages this experience and knowledge with a portfolio of cybersecurity products and services for the private sector that features:

- **An integrated product suite.** Like many enterprise CISOs, Raytheon recognizes that disparate security point tools are no match for today's dangerous threat landscape. As an alternative, Raytheon offers its SureView Suite, which brings together its products for insider threat protection and security analytics into an enterprise security architecture. Large organizations can also leverage APIs to build connections and interoperate SureView with their existing security infrastructure.

- **End-to-end security data collection, correlation, and analytics.** As part of its SureView suite, Raytheon includes data from endpoints, networks, malware analysis, cross-functional divisions, and external threat intelligence. The goal? Gather and analyze comprehensive data from multiple sources to improve threat detection, identify suspicious activities like lateral movement, reduce dwell time for cyber-adversaries, and improve response processes.

- **A progressive commitment to visual analytics.** In addition to algorithms and analytics, Raytheon continues to invest heavily in an advanced user experience and interface to make analytical teams more productive and help its customers address the cybersecurity skills shortage. The new GUI, easily used by security analysts and junior staff members, actually includes visual analytics and a visual language that applies the latest findings in cognitive research and neuroscience. It is also designed to reduce overload by visually emphasizing the most important elements unique to each investigation. The interface highlights actionable intelligence in order to transform raw data into efficient processes that accelerate detection and response time. In other words, this is a visual approach focused on information rather than security controls, allowing the analyst to quickly interpret the data and take action.

Raytheon's real focus goes beyond analytics. SureView is results-centric in that it is designed to process and analyze data to identify problems and then provide security analysts with the analytics and tools needed to take immediate action.

Raytheon may not be the most familiar name to cybersecurity professionals in the private sector, but given its SureView Suite, experience, and innovative visual analytics, CISOs would be wise to see how the company aligns with their cybersecurity strategy moving forward.

The Bigger Truth

In the past, cybersecurity was a tactical endeavor. When faced with a new type of threat, most organizations simply added new network gateways or host-based security software. In other words, each threat simply demanded a new defensive technology countermeasure. Unfortunately, this incremental approach to cybersecurity is no longer effective: Skilled cyber-adversaries can easily circumvent most security controls, and cyber-attacks designed to resemble normal traffic fly under the radar of most security monitoring tools.

French military and political leader Napoleon Bonaparte once stated, "War is 90% information." The same can be said of cyberwar today. Defending against modern cyber-attacks demands a comprehensive commitment to collecting, correlating, and analyzing security data from a multitude of sources. The key here is to turn intelligence into action. This means detecting threats as quickly as possible, conducting efficient investigations, and remediating problems before they progress into damaging data breaches.

This transition won't be easy, so CISOs must build their cybersecurity strategies by selecting technologies that are powerful, enhance their existing security infrastructure, are easy to use, and deliver near-term results. Raytheon's SureView Suite is designed to meet these types of enterprise requirements.

Enterprise Strategy Group is an integrated IT research, analysis, and strategy firm that is world renowned for providing actionable insight and intelligence to the global IT community.