White Paper

Information-driven Security and RSA Security Analytics and RSA ECAT

By Jon Oltsik, Senior Principal Analyst

September 2014

This ESG White Paper was commissioned by RSA, The Security Division of EMC Corporation and is distributed under license from ESG.

Contents

Executive Summary

Large organizations are under constant cyber-attack and many are breached each day. How many? Aside from the infamous breaches at Neiman-Marcus, the New York Times, and Target in 2013, ESG research indicates that nearly half of all enterprise organizations experienced at least one successful malware-based attack over the past two years that resulted in some type of internal action (like re-imaging a system), and/or external damage control (like notifying trusted customers about the breach).[1]

Although security breach activity is always troubling, enterprise CISOs are often especially frustrated since they've spent millions of dollars on security defenses that cybercriminals have no apparent difficulty getting around. This being the case, what is the current state of enterprise security and what can CISOs do to better protect their organizations? This paper concludes:

- **Large organizations face significant struggles with incident detection and response.** Many CISOs now assume that their organization will be breached regardless of their defenses. While this type of realistic perspective calls for strong incident detection and response processes and technologies, many enterprises continue to struggle in each of these areas. ESG research shows that many firms say they aren't very good at incident detection/response tasks like performing forensic analysis to determine the root cause of a problem, performing remediation to contain the scope of security events, and analyzing security intelligence to help accelerate the detection of security incidents. CISOs need to assess and address their organizations' limited incident detection/response capabilities in response to the increasingly dangerous threat landscape.
- **Enterprises need information-driven security.** While large organizations will (and should) continue to deploy firewalls, implement antivirus software, and segment networks, they also need a continuous understanding of their security status and the threats that they face. This leads directly to information-driven security—the collection, processing, analysis, and storage of real-time and historical security-relevant data. Using this approach, the data can lead CISOs to conclusions on what to prioritize for improved incident detection and response as well as prevention.
- **Information-driven security is anchored by big data security analytics.** In addition to the collection, processing, and storage of security data, organizations must also have the right actionable analytics to detect suspicious activities, investigate the scope of attacks, prioritize activities, and respond quickly and efficiently to all security events. Accomplishing these goals will require a big data analytics architecture built for automation, intelligence, and massive scale. Furthermore, big data security analytics must enable real-time incident detection/response as well as historical investigations. Finally, big data security analytics must align with the responsibilities, processes, and workflows needed by security analysts, security operations, and the business at large.

Over the past few years, big data security analytic systems have been a work-in-progress where industry hype has vastly outweighed available product capabilities. With the introduction of RSA Security Analytics 10.4 and RSA ECAT 4.0 however, RSA can now deliver multiple products that integrate into an end-to-end enterprise security analytics architecture and thus anchor information-driven security initiatives.

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

Enterprise Security in Transition

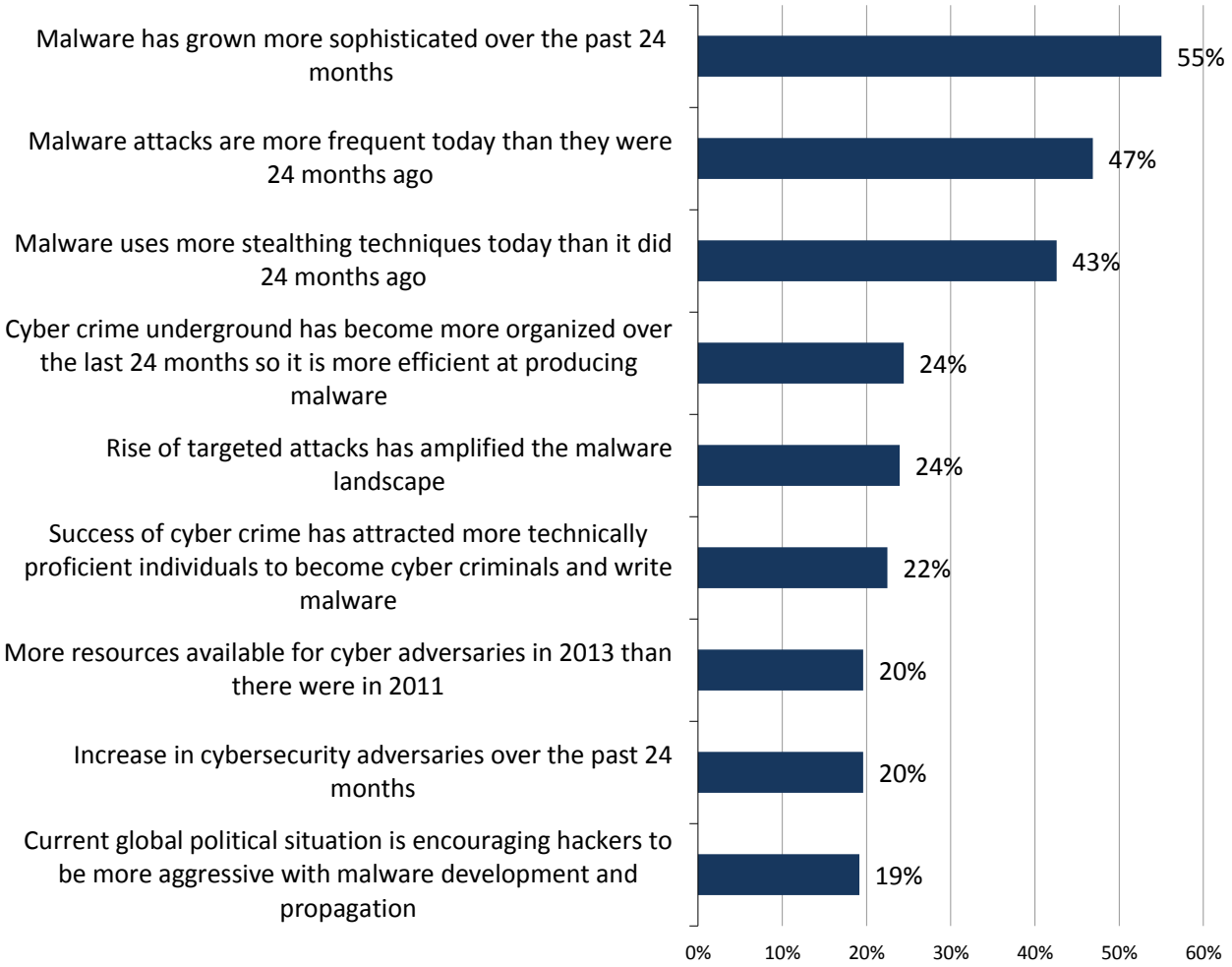
According to ESG research from 2013, 49% of enterprise organizations had experienced a successful malware-based attack over the past two years. In this context, the word "successful" indicates that malware actually compromised an IT asset and that security, IT, and even business personnel had to take some type of action as a result (i.e., conduct an investigation, remediate a system, work with law enforcement, notify customers, etc.). Even more concerning is that 22% of enterprise organizations claimed that they experienced more than 25 successful malware attacks over the past two years.

While security breaches are a big concern, they are especially troubling given that many enterprise organizations continue to experience them in spite of spending millions of dollars in security technology investments over the past few years. Regrettably, security breaches continue to plague enterprises because:

- **Large organizations rely too much on prevention.** Many enterprise security strategies and budgets remain skewed toward preventive controls like firewalls, IDS/IPS, and endpoint antivirus software. Yes, these are important components of a defense-in-depth security infrastructure, but these security technologies tend to rely on signatures, static configurations, and simple rule sets. Furthermore, many security technologies operate independently of one another, so they defend against threats across one or few vectors (e.g., e-mail or web browsing) only. When cybercriminals find a way to circumvent any single preventive technology, they are able to penetrate networks and compromise hosts. At that point, prevention technologies add little, if any, incremental value.
- **The threat landscape is getting worse.** According to ESG research, 67% of enterprise security professionals surveyed in 2013 said that the malware threat landscape was much worse or somewhat worse than it was two years earlier. Why do so many security professionals share this belief? More than half (55%) say that malware has grown more sophisticated, 47% point to the increasing frequency of malware attacks, and 43% say that modern malware has become more stealthy than in the past (see Figure 1).

Figure 1. Reasons Why Security Professionals Believe the Threat Landscape Is Getting Worse

You indicated that you feel like the overall malware landscape is worse than it was in 2011. Which of the following reasons are most responsible for this feeling? (Percent of respondents, N=209, three responses accepted)

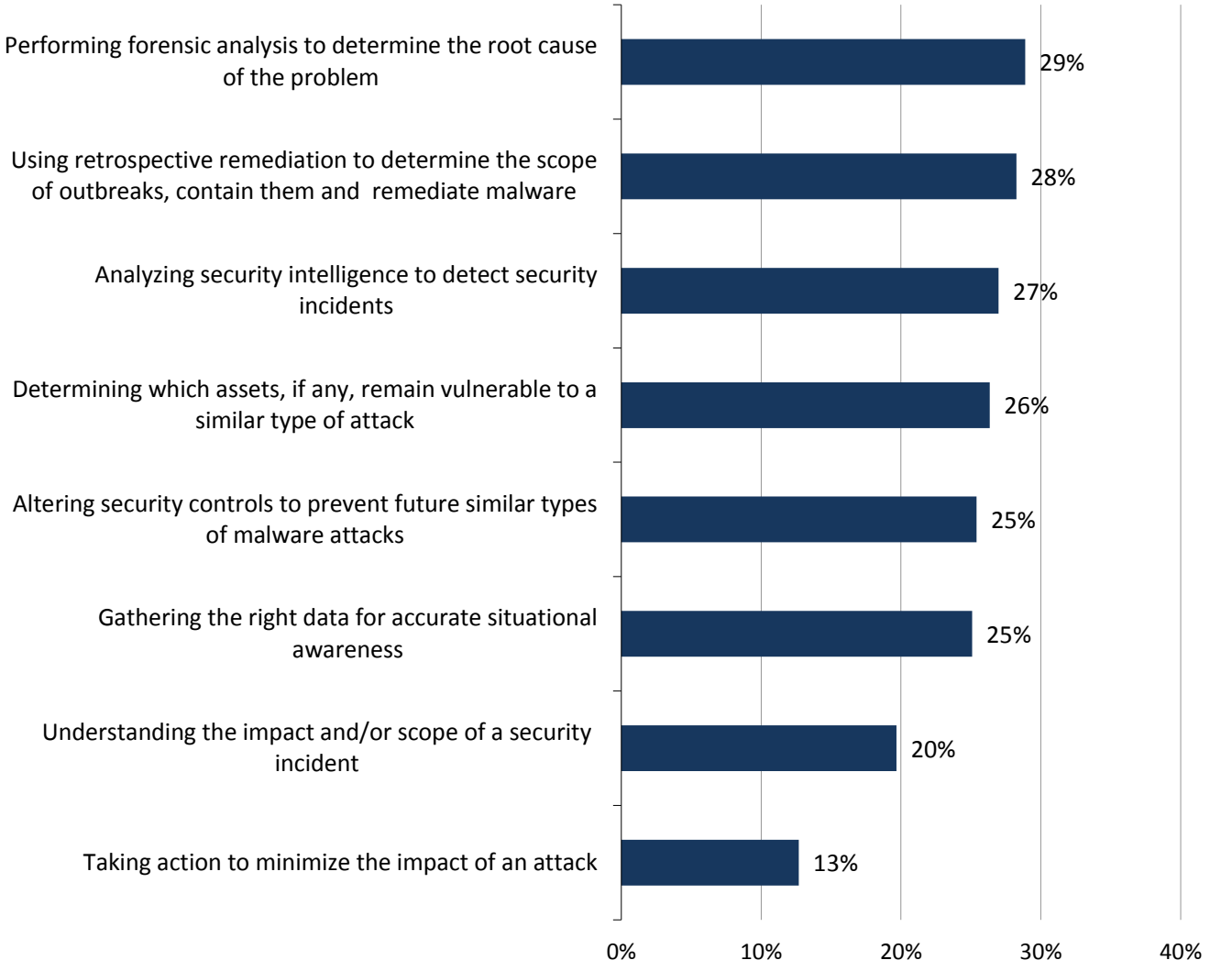


Source: Enterprise Strategy Group, 2013.

- **Organizations remain challenged by incident detection and response.** Once malware-based attacks circumvent preventive controls, it is up to security analysts to detect, investigate, and respond to the incidents in order to minimize the damage associated with them. Unfortunately, many enterprises also struggle in these areas. ESG research shows that 29% of enterprises are relatively weak when it comes to performing forensic analysis to determine the root cause of a problem, 28% find it difficult to perform retrospective remediation to contain the scope of security events, and 27% have shortcomings with regard to analyzing security intelligence and using it to help them accelerate the detection of security incidents (see Figure 2).

Figure 2. Reasons Driving Increased Threat Perception

Please consider this list of incident detection/response tasks. Which three are your organization' biggest areas of weakness (i.e., which are you worst at)? (Percent of respondents, N=315, three responses accepted)



Source: Enterprise Strategy Group, 2014.

Aside from the problems described in Figure 2, many organizations have a more fundamental problem: They don't have the right cybersecurity skills or staff resources to adequately address their organization's needs. In fact, ESG research indicates that 25% of organizations say they have a problematic shortage of IT security skills today.[2] This leads to a predictable situation where the infosec team can't keep up with day-to-day responsibilities. Furthermore, security teams are often overwhelmed by a constant barrage of security alerts and emergency response procedures mixed with day-to-day operational tasks. Security professionals try their best to triage problems and prioritize their activities, but many spend their days putting out fires rather than managing to any kind of security best practices.

The Increasing Need for Information-driven Security

CISOs tend to base their infosec strategies on tried-and-true best practices derived from risk management frameworks and approaches such as the CISSP Common Body of Knowledge (CBK) and well-known security

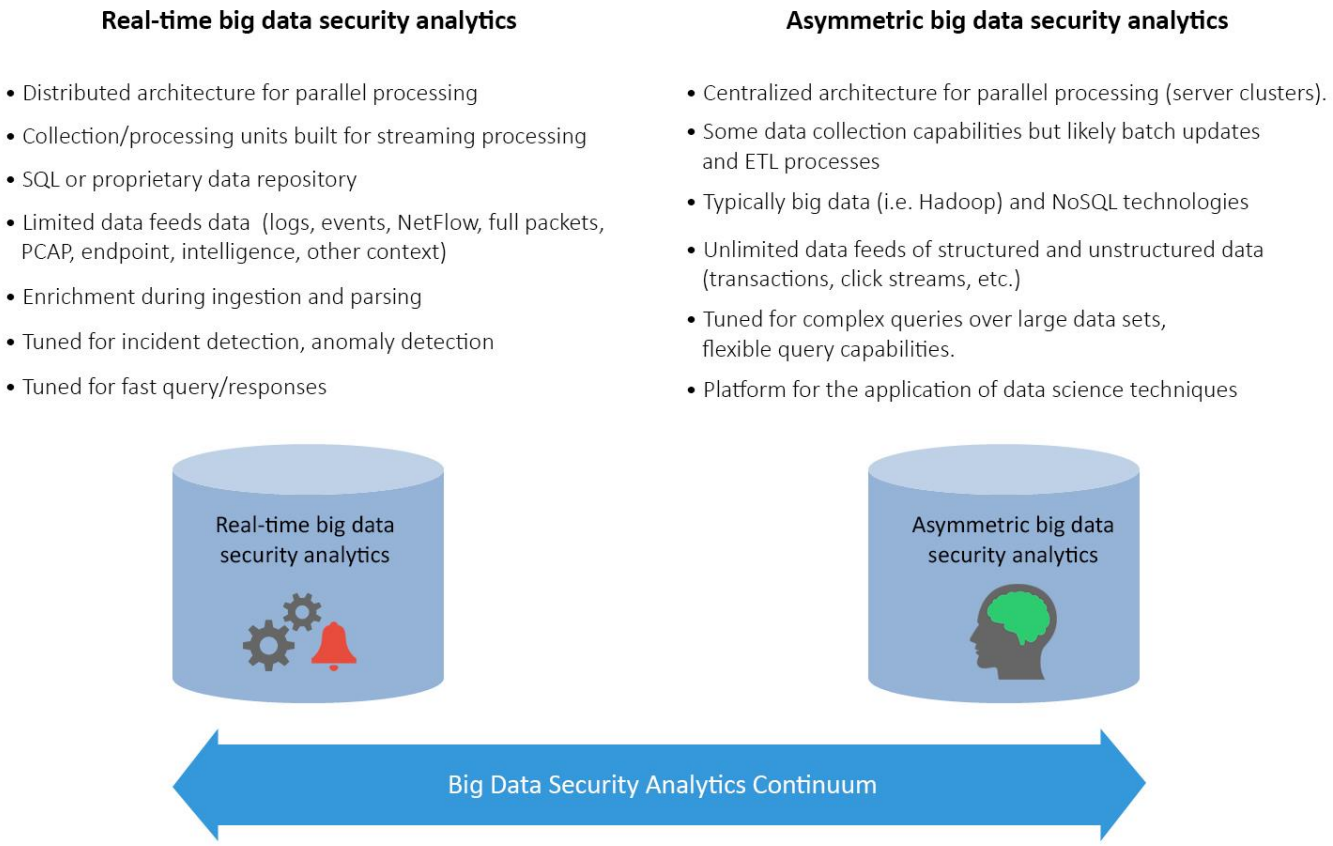
[2] Source: ESG Research Report, *2014 IT Spending Intentions Survey*, February 2014.

technology controls like network firewalls, endpoint security software, and security information and event management (SIEM) systems. These security guidelines and technologies will continue to be important within an enterprise infosec strategy, but security teams need help beyond the basics.

So what's needed? To address the security challenges described, CISOs should move toward an information-driven security strategy where decision making is based upon advanced big data security analytics. In other words, day-to-day security tactics must be anchored by accurate information built upon:

- **The collection, processing, and storage of both internal and external intelligence**. In the past, security analysis was derived from a handful of data feeds like event logs, IDS/IPS alerts, and open source threat intelligence, but these data sources are no longer adequate on their own. To address today's risk management and incident detection/response needs, organizations need to collect, process, and store a plethora of data sources including asset data, identity information, network traffic (via full packet capture), NetFlow, endpoint forensic information, etc. This data volume is in part what transforms yesterday's security analysis into today's big data security analytics. Furthermore, information-driven security must be closely aligned with external threat intelligence in order to correlate anomalous internal activities with new attacker tools and techniques that are "in the wild." ESG believes this last detail is critically important. Enterprise organizations need threat intelligence to keep up with cybercrime activity in general and to track specific attack patterns that may target their industry or firms in their particular geographic location.
- **Real-time and asymmetric data analysis**. Enterprises need security analytics across a continuum. One side of the continuum is designed and tuned for real-time analytics used for fast incident detection/response and based upon events, logs, NetFlow, network packets, and activity on endpoints. The other side of the continuum is for asymmetric data analysis of security anomalies and the associated investigations that may span several months or years (see Figure 3). This type of asymmetric security investigation may require analysts to sift through massive quantities of disparate historical data to piece together patterns, detect malicious behavior, and trace the root of these activities. With asymmetric big data security analytics, security analysts will use an assortment of analytics methods including queries, data science, visual analytic GUIs, and dashboards as they discover and investigate "low-and-slow" attack patterns.

Figure 1. The Big Data Security Analytics Continuum



Source: Enterprise Strategy Group, 2014.

- **Advanced intelligent security analytics algorithms.** Current security analytics tools can spot obvious policy violations but struggle to look across multiple data sources to understand when several seemingly innocuous independent actions represent a security threat when considered in combination. To bridge this gap, big data security analytics systems must offer "contextual-security" by correlating data, modeling "normal" behavior, and offering a multitude of analytics algorithms designed for high-speed and accurate incident detection. The best systems will use "nested-algorithms" that analyze anomalies across multiple algorithms in order to eliminate false positives, pinpoint problems, and provide security analysts with the right details so they can prioritize and expedite remediation processes.
- **Improved visualization, and query technologies for security analysts.** As previously mentioned, many organizations don't have the right cybersecurity skills and remained understaffed. Given this reality, big data security analytics systems must help security analysts work smarter, not harder. To accomplish this, big data security analytics must include easy-to-use GUIs, comprehensive reports, and intuitive navigation. The best systems will integrate modern visual analytics with 3-D images and simple pivoting across dimensions rather than a standard assortment of spreadsheets and charts.
- **Integrated workflow and data sharing to align incident detection/response with security operations.** Security analysts work hand in hand with IT and security operations teams once incident detection processes transition to incident response. Unfortunately, this is where many organizations bog down, burdened by a poor communications, incompatible tools, and a lack of end-to-end oversight. To overcome this problem, big data security analytics should offer the right workflow tools to manage the incident detection/response process independently or interoperate with existing security and IT operations tools.

Information-driven security can be viewed as a recipe: Take a wide range of disparate internal and external data feeds; add advanced analytics algorithms, visualization, and workflow; and make the data investigable and "actionable" to improve the time and efficiency of incident detection and response. Certainly, some experienced organizations may be able to improvise a bit, but the main ingredients of the recipe are not optional.

Introducing RSA Security Analytics 10.4 and RSA ECAT 4.0

As cyber threats grow more sophisticated and stealthy, it is becoming increasingly clear that *all* large organizations will need to adopt information-driven security and big data security analytics. Unfortunately, this set of new security approaches has led to massive confusion in the market. CISOs aren't quite sure what they need to supplement existing tools, while security vendor messaging makes it confusing to separate real enterprise-class solutions from industry hype.

With its September 2014 product announcement, RSA Security may actually bring some clarity to information-driven security with an advanced big data security analytics architecture and the introduction of RSA Security Analytics 10.4 and RSA ECAT 4.0. RSA recognizes that security teams need help attaining the right level of visibility, analyzing mountains of data, and turning these activities into immediate action. To that end, RSA Security Analytics 10.4 and RSA ECAT 4.0:

- **Includes new data sources for analysis.** With its new version, RSA Security Analytics adds NetFlow and integrated endpoint monitoring and forensic data consumption to existing data sources including full packet capture, log data, and external threat intelligence feeds. This helps RSA deliver, combine, and intersect visibility about what's happening on internal networks and "in the wild." This also helps customers customize data collection and analytics to their organization's needs. How? Security teams can perform full-packet capture at critical network intersections to ensure that they have all the data needed for real-time and historical needs. In addition, they can collect NetFlow data, giving them an appropriate level of visibility into less-critical subnets or remote offices while maintaining visibility as threats traverse the network.
- **Supports real-time and asymmetric big data security analytics needs.** Since its acquisition of NetWitness in 2011, RSA has helped organizations analyze network traffic to improve incident detection and response. RSA Security Analytics 10.4 builds upon this heritage in a few ways. For one, it includes integration with RSA ECAT, allowing correlation between network and endpoint activity. RSA also improved its endpoint threat detection capabilities with the release of RSA ECAT 4.0, which enhances product scalability, performance, and native analytics, and introduces real-time monitoring and alerting. RSA Security Analytics can also tie into threat intelligence for correlation of suspicious internal and external behavior. Aside from these real-time capabilities, RSA Security Analytics 10.4 also adds big data science and analytics capabilities with Pivotal (an enterprise-class Hadoop distribution) for historical detection and investigation across massive amounts of data. With real-time and asymmetric big data security, RSA Security Analytics can cover the entire big data security analytics continuum.
- **Adds built-in analytics and algorithms.** With security skills at a premium, security analytics tools need to provide a helping hand with built-in algorithms, data correlation, machine learning, and anomaly detection and prioritization. RSA Security Analytics 10.4 adds these capabilities on top of Pivotal with algorithms for multifaceted security analytics like detecting suspicious domains and discovering host beaconing to malicious command and control (C&C) servers. RSA is committed to adding more of these kinds of algorithms in the future.
- **Eases security analytics and operations.** RSA put a lot effort into understanding security analysts' job responsibilities and instrumented RSA Security Analytics 10.4 and RSA ECAT 4.0 with features and functionality to help them improve and automate processes. For example, RSA redesigned the GUI and dashboards to help analysts focus their investigations on suspicious activities first. In addition to these visual enhancements for incident detection, RSA also added native incident triage management so security analysts can pivot from finding to fixing problems immediately. Finally, RSA Security Analytics 10.4 is also tightly integrated with its RSA Security Operations Management product. This integration should help

organizations streamline remediation processes and use operational metrics to bolster security controls on a continuous basis.

Aside from the products themselves, RSA also is also committed to a modular security analytics architecture. RSA products such as RSA ECAT, RSA Security Analytics, and RSA Security Operations Management can deliver value on their own, integrate with third-party products like SIEMs, or work together to form a comprehensive big data security analytics architecture. In this way, CISOs can work with RSA to address pressing requirements as they develop and execute a two- to three-year security modernization plan for their enterprise.

The Bigger Truth

ESG believes that enterprise security has reached a tipping point. Status quo defenses and analytics are no longer effective at addressing the insidious threat landscape. Large organizations are suffering extremely damaging security breaches as a result. This status quo approach should be considered unacceptable to any responsible senior business manager or CISO.

To address increasing IT risk, organizations need a comprehensive improvement in risk management and incident prevention, detection, and response, but CISOs can't count on hiring an army of cybersecurity specialists to help them dig out. Rather, they will need to find technology solutions that can help them work smarter; not harder.

ESG believes that enterprise cybersecurity systems will be anchored by information-driven security moving forward. This means that CISOs will need to capture, process, and store growing volumes of internal/external data; analyze the data in a way that correlates all data feeds; contextualize the data so it aligns with their organization, IT, and business processes; and finally, act upon the data in real time in order to detect malicious behavior, respond to security breaches, and continually improve their defenses.

Many organizations have some but not all of the pieces they will need to form an enterprise-class big data security architecture. As a result, they will need to surround existing technologies with additional capabilities and glue all the piece parts together into a cohesive and integrated architecture. RSA designed RSA Security Analytics 10.4 and RSA ECAT 4.0 with enterprise security analytics challenges like these in mind, as the products offer strong analytics capabilities on their own and can be integrated together to form a key part of an end-to-end security analytics architecture. Based upon this, CISOs should seek out RSA to explore how RSA Security Analytics 10.4, RSA ECAT 4.0, and other RSA products and services can help them address their security analytics needs and also lower risk, improve security operations, and better align their security with their business processes and priorities.

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