Product Brief

RSA ECAT 4.0 for Endpoint Forensics and Enterprise Security Analytics

Date: November 2014   **Author:** Kyle Prigmore, Research Associate and Jon Oltsik, Senior Principal Analyst

Abstract: *In September 2014, RSA announced the release of RSA ECAT 4.0, an endpoint security analytics solution aimed at improving organizations' ability to detect, prioritize, investigate, and remediate threats. In a move toward integration, ECAT rounds out RSA's product line alongside its web threat detection, GRC, and IAM solutions for data protection, security analytics, and now endpoint security as well. This approach to endpoint security widens RSA's footprint in the enterprise security market, providing customers with end-to-end integration between their networks and endpoints.*

Announcement Overview

RSA took a big step toward establishing its endpoint security products when it made a major product announcement unveiling ECAT 4.0. ECAT 4.0 offers new and improved functionality, including:

- **Real-time monitoring and alerts**. In the past, ECAT relied on periodic scanning, which left customers somewhat vulnerable in between scanning cycles. RSA rectified this as ECAT now boasts live monitoring of endpoints. IT administrators will be able to see which devices are on their network at any given time, and there will be no delay between the detection of anomalous behavior and a security alert.
- **The ability to X-ray endpoints' processes, tasks, and communications.** ECAT can drill into an endpoint at any time to collect a complete information set regarding what the device is doing, whom it is talking to, and what operations it has executed. The ability to collect this type of data from an endpoint gives IT admins more granular insight into endpoint activities—investigating security incidents is faster and easier when security experts can establish context including what tasks an endpoint executed in a given timeframe, what the endpoint's provisioned state was at the time of the incident, the geographic location of the endpoint during a particular login session, and more.
- **High scalability.** With ECAT 4.0, RSA claims that only one hardware device is needed to manage 50,000 endpoints. Furthermore, ECAT management consoles can be federated for larger deployments. This is appealing to enterprise organizations that want to collect and integrate their endpoint data in real time, but have difficulty finding endpoint and network security products that can integrate and scale simultaneously.
- **Ease of use.** The well-documented security skills shortage can make it difficult for understaffed organizations to use cutting-edge security products because the best products are often the most difficult to implement and manage. ECAT is specifically designed to be easy to use even for understaffed organizations seeking to implement and gain immediate value from endpoint analytics solutions for the first time.
- **Mac OS Support.** Organizations seeking to enable their workforces through BYOD initiatives often find that supporting different platforms and operating systems can become a major security challenge. RSA has built-in Mac support, which is one less factor organizations need to worry about before making a decision.
- **Actionable use of RSA live threat intelligence.** RSA's threat intelligence feed can collect network and endpoint data and integrate other intelligence feeds to alert security admins about suspicious files/websites that should be avoided. ECAT's advantage is that security teams can use this data to easily discover which machines have been exposed to malicious IP addresses, domains, files, etc. and use that information to automatically kick off a scan of the compromised machines. This simplified search-and-discover mechanism makes it much easier for IT admins to investigate security incidents.

RSA fully launched ECAT in mid-September (sans ECAT for mobile, which remains in development as planned and will launch at a later date).

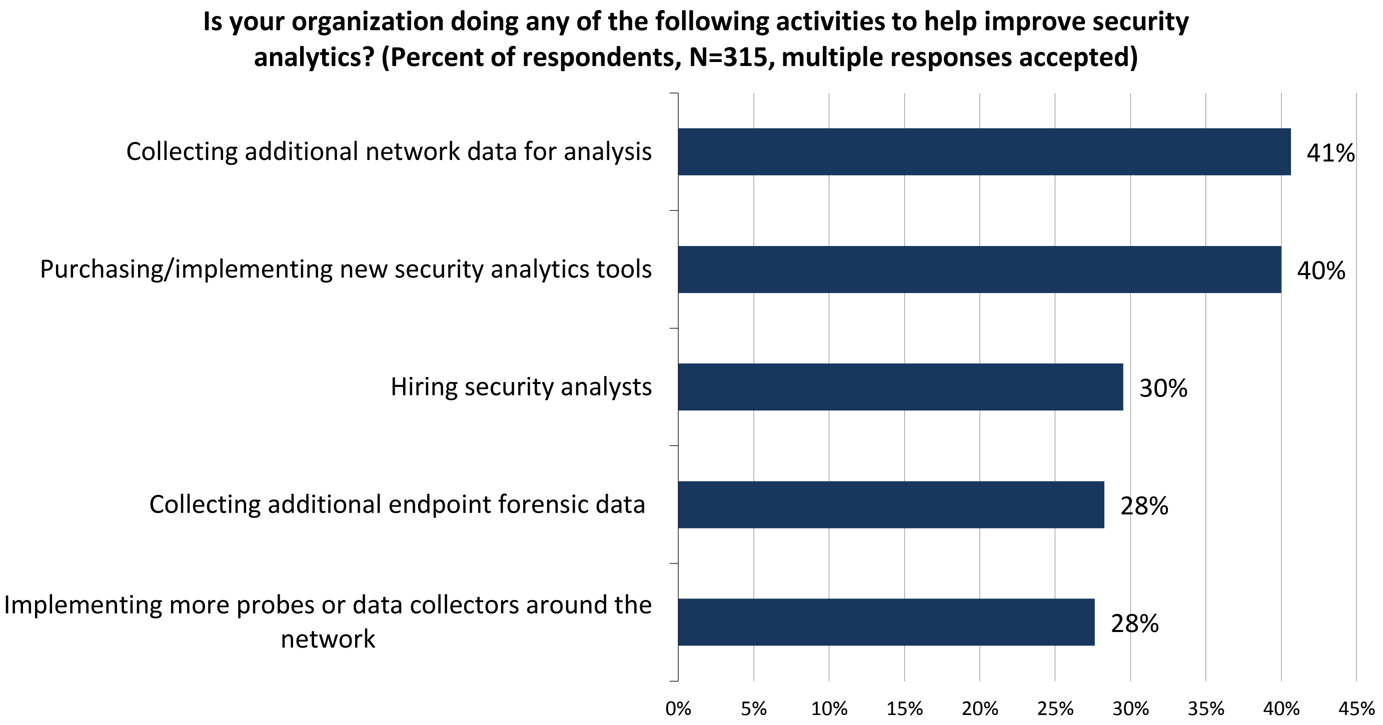
RSA Joins the Detection-as-prevention Trend

RSA is one of a growing number of vendors that believe prevention techniques or perimeter defenses are no longer the best way to secure an endpoint. While the truth of "prevention is dead" remains up for debate, there is no doubt that the market for new endpoint security solutions (advanced detection and endpoint analytics specifically) is very strong. Organizations want to collect more information from their endpoints and integrate that information with other network security data. Trying to stay ahead of the bad guys' constantly evolving attack techniques has proven nearly impossible, hence the relatively poor reputation of signature-based prevention at the moment. Minimizing the post-breach damage may prove more successful, hence the excitement around detection and response. ECAT's value proposition is aimed toward the detection/response camp.

Detection-as-prevention may indeed be a path to security solvency: If endpoint data is constantly collected and analyzed, and endpoints can be scanned/queried, then any changes to the state of the device or any suspicious behavior can be identified and investigated much more quickly. Why and how? Most enterprise security teams are overworked and overwhelmed by security alerts that lack context, meaning that they are chasing down problems that may be minor while unintentionally procrastinating on major incidents. When security teams have lots of data to work with, and the data can be viewed in context, analysts can respond to high-priority incidents as quickly as possible while leaving low-priority incidents for a later time. Smart organizations solve this by seeking to maximize their security teams' efficiency, and RSA should be able to demonstrate how exactly ECAT can help them to do just that.

Despite the many possible advantages that endpoint analytics solutions such as ECAT can bring, the question remains: Is the market prepared to jump to endpoint analytics as a main-line endpoint security solution? Yes. ESG data points to the fact that many CISOs are not sitting still, but are already engaged in a number of activities intended to help them improve their security analytics. Specifically, 41% are collecting additional network data for analysis, 40% are purchasing/implementing new security analytics tools, 30% are hiring security analysts, and 28% are collecting additional endpoint forensic data (see Figure 1).[1] RSA is enhancing ECAT at exactly the right time

Figure 1. Top Five Steps Organizations Are Taking to Help Improve Security Analytics



Source: Enterprise Strategy Group, 2014.

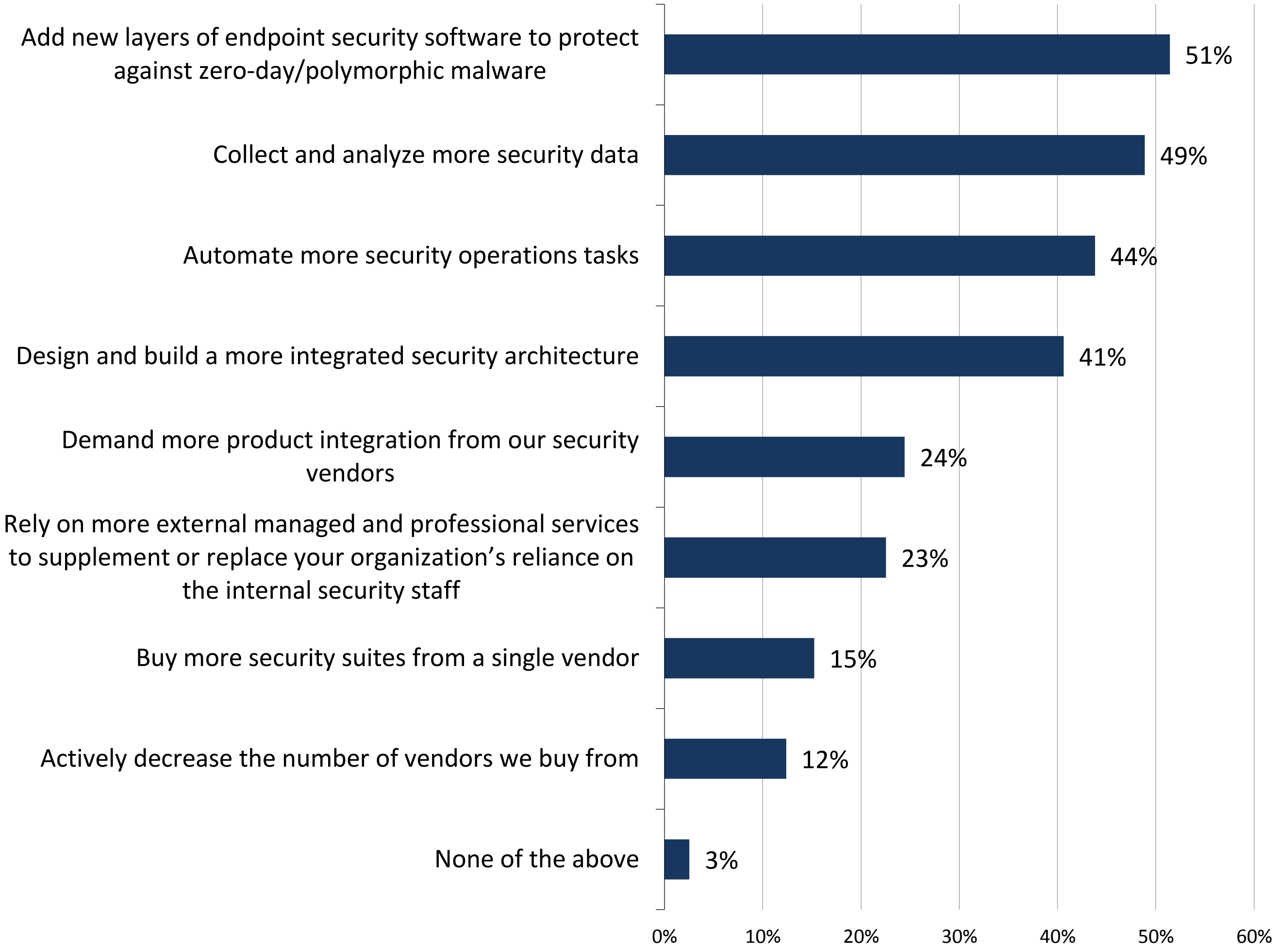
[1] Source: ESG Research Report, *Advanced Malware Detection and Protection Trends*, September 2013. All ESG research references and charts found in this brief have been taken from this research report.

The Bigger Truth

CISOs and their equivalents are seeking to streamline their operations by reducing their manual operations and increasing their efficiency. According to ESG research, 44% of organizations intend to automate more security operations tasks, and 41% want to design and build a more integrated security architecture. Doing so is the only way to free up their task-strapped employees enough up to pursue predictive defense and truly turn the tide moving forward.

Figure 2. Planned Changes of Security Technology Decisions

In which of the following ways will your organization change its security technology strategy decisions over 24 months in order to respond to the current cybersecurity and threat landscape? (Percent of respondents, N=315, multiple responses accepted)



Source: Enterprise Strategy Group, 2014.

This is arguably ECAT's greatest strength: It is an endpoint security solution that can seamlessly integrate with network security tools and help organizations perform a wide variety of tasks ranging from endpoint management to security investigations to threat intelligence improvements. Recognizing this fact, RSA has begun to weave a compelling security story by releasing ECAT in step with its Security Analytics 10.4 update.

To build upon its product momentum and thoughtful enterprise security strategy, RSA must:

- **Develop security analytics that can help organizations form new policies.** One of the unique benefits of security analytics for endpoint security is that after anomalies are spotted and responded to, the information can be used to decrease the network attack surface moving forward. Behavior rules, provisioning adjustments, and more can be changed on the fly with ECAT—a feature that many traditional endpoint solutions lack. To gain a market advantage, RSA should help customers utilize these capabilities based upon their industry, skill sets, and network architectures.

- **Convince the market that ECAT can save an organization's time.** In a world where 34% of organizations say they do not have enough employees on their IT security teams, speed and efficiency matter. RSA's ECAT 4.0 can help organizations establish faster, more targeted response timelines by capturing device information and integrating that information with automated response options. RSA must quantify and communicate these benefits.
- **Build a link between better cybersecurity and better business processes.** Security analytics are not only on a path to faster detection and response, but also to better business processes. The more organizations know about how their endpoints and users behave, the more they can fine-tune security policies to prevent false-positive situations and reduce remediation downtime. Once again, RSA can benefit from this link if it can back it up with metrics and case studies.
- **Improve SIEM value.** Organizations that deploy SIEMs understand their usefulness and limitations. ECAT can feed endpoint data directly into the SIEM and, as mentioned, more information can equate to better security and processes. RSA should trumpet its SIEM integration loudly. Yes, this strategy may delay security analytics deals, but it gets RSA in the proverbial door. Furthermore, its SIEM affinity will pay dividends as CISOs move beyond SIEM alone toward a big data security analytics architecture.

RSA's ECAT release is part of a wave of products that seek to further integrate endpoint and network security solutions. Organizations seeking to improve their detection and response capabilities on endpoints can look to ECAT as a possible solution that can improve security capabilities and streamline security operations.