

RSA acknowledged by Frost & Sullivan for excellence and innovation in its network security forensics product

JOHANNESBURG – June 27, 2016 –RSA, The Security Division of EMC, has been determined by Frost & Sullivan as winner of the 2016 Global Frost & Sullivan Enabling Technology Leadership Award in Network Forensics for RSA Security Analytics.

According to a statement released by Frost & Sullivan, RSA Security Analytics was chosen based on its outstanding achievement in product leadership, technological innovation, customer service, and product development. Industry analysts compare market participants and measure performance through in-depth interviews, analysis, and extensive secondary research. Frost & Sullivan identified thirty-one products offering network security forensics, and RSA Security Analytics was selected due to its superior capabilities and for best addressing customer needs for network security forensics.

RSA Security Analytics is designed to improve threat detection, investigations and response by consuming network flow data, full packet capture (PCAP), logs, and endpoint data, as well as information from other security systems, external threat intelligence and IT assets. Additionally, RSA Security Analytics applies multiple advanced analytics engines, including behavioural analytics, and investigative interfaces to this data to help detect attacks before they can impact the business.

Networks Unlimited, a value-added distributor, distributes RSA in 23 African countries.

One of the unique aspects of the architecture is RSA Security Analytics' support of RSA's Event Stream Analysis (ESA) technology, which is engineered to deliver advanced analytics by enabling both correlations and more sophisticated machine learning-based techniques to detect and provide prioritised alerts on security incidents, as well as providing the

full scope of an attack campaign.

Furthermore, RSA Security Analytics is designed to enable forensic investigations that make it simpler for security teams to determine the root cause of an incident in the broader scope of an attack campaign. RSA Security Analytics regularly receives fresh threat intelligence information and other content continuously through its RSA Live service, which is included with the product. The RSA Live service provides machine-readable threat intelligence thus making the intelligence actionable immediately.

One other distinguishing capability of RSA Security Analytics is the ingestion of RSA ECAT data, providing endpoint threat detection and response. When used together, the combined solution provides security teams with visibility, threat detection and response capabilities from endpoints to the cloud.

"Network-based security monitoring is not just important for the detection of malware; it is critical for the detection and investigation of a broad set of security incidents using multiple forms of telemetry and analytics," explains Frost & Sullivan research analyst, Christopher Kissel. "RSA Security Analytics provides a comprehensive set of capabilities for incident detection and security forensics. Metadata generation and full network packet capture gives RSA Security Analytics depth and real-time visibility to determine the security posture of the enterprise as traffic traverses its network."

"RSA's solution is ahead in the technology race, creating significant advantages for security monitoring teams," adds Kissel. "When a potential breach is detected, the ideal forensics system helps the security analyst act swiftly to contain the threat. RSA's central management of incidents, generation of metadata across multiple data sources, session replay to view exactly what occurred and what was exfiltrated, and the use of advanced analytics and machine learning enables exemplary threat detection and response."

“Networks Unlimited congratulates RSA on its Frost & Sullivan accolade. Distributing technology products that are leading the innovation curve is a boost to the future economic prosperity of Africa and a step in the right direction to curbing the growing cyber attacks that affect all demographics, regions and industries,” says Anton Jacobsz, MD of Networks Unlimited.