KuppingerCole Report

EXECUTIVE VIEW

by Alexei Balaganski | September 2016

RSA NetWitness® Suite

RSA NetWitness Suite is a security monitoring solution that combines log and network traffic analysis with endpoint-based visibility and automated threat intelligence to detect and investigate sophisticated cyber-attacks.

by **Alexei Balaganski**
ab@kuppingercole.com
September 2016

Content

Related Research

Advisory Note: Real Time Security Intelligence – 71033

Executive View: RSA Archer GRC – 70888

Executive View: RSA Adaptive Authentication – 70889

1 Introduction

RSA is a computer and network security company headquartered in Bedford, Massachusetts, USA. Founded in 1982 by Ron Rivest, Adi Shamir and Len Adleman – the developers of the RSA public key cryptography algorithm, the company has strong roots in cryptography and is probably best known for RSA SecurID®, one of the most popular hardware token-based methods of two-factor authentication. In 2006, RSA was acquired by EMC Corporation and has been operating as a division within EMC. After the acquisition of EMC by Dell was finalized in September 2016, it has been announced that RSA became a direct subsidiary of Dell Technologies and will continue operating with enough autonomy to keep maintaining their own product ecosystem.

With over 1300 employees and regional offices in over 70 countries, RSA has a strong global presence, serving more than 30000 customers worldwide across all major industry verticals, including government and defense, financial services, utilities and many others. RSA Conference, an annual event organized by the company, is recognized as one of the leading conferences in the field of information security. Currently, the company offers a wide range of technology and business solutions in such areas as identity assurance, GRC (governance, risk and compliance), fraud detection and information protection, as well as security analytics and operations. In addition, the company provides consulting and advisory services.

With the continued adoption of mobile and cloud services and the profound impact of digital technologies on business models and processes (the notorious Digital Transformation), organizations are finding it increasingly difficult to protect their IT systems from attacks. As the very notion of the corporate perimeter has almost eroded, traditional security controls are no longer able to detect the increasingly sophisticated methods cyber criminals are using to mimic normal user behavior and to infiltrate corporate networks. Even worse, many of those criminals may, in fact, be malicious insiders.

All this has led to a massive paradigm shift in information security from perimeter protection towards monitoring and detecting malicious activities within networks in real time. A new generation of security analytics tools has emerged recently, utilizing machine learning and Big Data analytics to correlate large amounts of security data collected across the corporate infrastructure and enrich them with additional context data and external threat intelligence. In the end, a security researcher can deal with a manageable number of relevant security incidents, ranked by severity and enriched with valuable forensic information. As opposed to traditional log-centric SIEM solutions or signature-based antimalware tools, these Real-Time Security Intelligence solutions provide a unified real-time overview of the corporate security posture across endpoints, networks and services and enable early detection and mitigation of cyber-attacks to minimize the damage.

RSA has been active in this market segment for quite some time, offering a complete security analytics solution recently rebranded as RSA NetWitness Suite. The product provides a unified platform for log, network packet and NetFlow analytics recently expanded to include endpoints and to support incident remediation workflows. Provided as fixed high-performance hardware appliances, consumption-based appliances or software only versions, suitable for both hardware independent or virtual machine deployments, the solution is capable of meeting the most demanding scalability and high availability requirements regardless of the deployment model.

2 Product Description

RSA NetWitness Suite (formerly RSA Security Analytics) is a threat detection and response solution that helps analysts detect and investigate threats which are too sophisticated to be detected by traditional security tools. It provides an integrated platform for collecting both log-based security events from various sources (both on-premises and from the cloud) as well as traffic information from network devices. The company's endpoint threat detection and response solution, previously known as RSA ECAT, can be both an integrated part of the suite as well as a stand-alone offering under the new **RSA NetWitness Endpoint** name. This integration extends detection and forensic investigation capabilities to corporate endpoint devices as well.

Security data captured from various sources is then processed to normalize the raw security events, enrich them with valuable context information and metadata and apply current threat intelligence to identify the most recently discovered threat and attack methods.

For the latter, the solution includes **RSA Live** – the company's threat intelligence delivery system, which provides the latest security reports, community intelligence, information on the newly identified malware, suspicious domains and other threats. Powered by RSA Research and Incident Response laboratories, RSA Live ensures that customers receive actionable threat intelligence in the form of consolidated rules, which are directly fed into the analytics platform. A more recent addition to the suite is **RSA Live Connect** – the community-driven cloud-based threat intelligence service. It collects and analyzes threat information from RSA NetWitness installations around the world and provides reputation scores for IP addresses as well as helps identify other risks.

To ensure that the platform can handle extremely large amounts of security events, the platform is designed to be distributed and modular, able to scale with the needs of customers of any size. The architecture comprises several modules that can operate on data streams in parallel to capture and analyze them in real time, as well as additional support components, which extend the platform to provide more storage, facilitate multi-site deployments and so on. These modules are usually delivered as specialized hardware appliances, but can be virtualized as well. A particular deployment can start with a single hybrid appliance and then gradually scale to a multi-branch solution with several dozens of modules. The primary components of the security analytics platform are the following:

- **Decoders**, which capture and store raw log and network data. They generate metadata and enrich captured information with security context. At least one decoder per captured data type is needed.
- **Concentrators**, which store and index metadata to ensure fast queries and retrieval of raw security data. Concentrators are also data type specific.
- **Event Stream Analysis,** which implements the real-time correlation engine across multiple data types.
- **Security Analytics Server,** which provides the web interface for management, forensic analysis, reporting, etc.
- **Archivers**, **Warehouses** and **Capacity** modules provide additional storage and correlation capabilities.
- **Brokers** and **Virtual Log Collectors** facilitate information exchange between remote sites in large-scale deployments.

Such architecture enables real-time collection, analysis and investigation of security incidents, short-term storage of network, endpoint and log data for more in depth investigations, and long-term log retention for forensic analysis and compliance reporting. Inherently distributed and linearly scalable, it ensures that capacity requirements even for extremely large deployments can be met without problems.

Unfortunately, this modularity also means that the solution can be complicated to set up. This means that the product is primarily targeted towards large enterprises. RSA does provide professional services to help implement and manage product deployments. This may change later this year, however, as the support for AWS and Azure cloud deployments targeted towards smaller customers is planned for future releases.

As opposed to traditional SIEM tools, RSA NetWitness Suite utilizes Big Data analytics, behavioral analysis, and machine learning algorithms to correlate log, network, endpoint and external threat intelligence data in real time and thus detect suspicious activities without relying on predefined rules. Security events from different sources can be automatically correlated to detect a sophisticated attack spanning multiple attack vectors. This approach dramatically reduces the number of alerts a security analyst has to deal with and instead provide him with a manageable list of highly probable incidents ranked by their criticality according to the particular customer's business context. By giving the analyst necessary controls to drill into details and context of each incident, the solution can greatly simplify forensic analysis as well. These controls not only provide fast access to all captured data in reconstructed human-readable form, but also integrate 3rd party research, as well as the latest research from the RSA FirstWatch expert team (available as an additional subscription tier).

Another important aspect of the solution is automated compliance reporting. The suite provides built-in reports for multiple government and industry compliance frameworks like GLBA, HIPAA, NERC, PCI, Basel II and others. In addition, the product supports two-way integration with the RSA Archer® GRC platform: it can both supply data and reports to the centralized GRC solution and consume additional business context from it, such as the purpose and criticality of various IT assets.

All these functions, including security monitoring, forensic investigations, long term analytics, and compliance reporting are available via a single browser-based interface provided by the Security Analytics Server. The modern HTML5-based GUI is notable for its rich visualization capabilities and high degree of customization.

RSA NetWitness SecOps Manager, formerly a standalone solution, can now be deployed as part of the suite as well. RSA NetWitness SecOps Manager provides a complete orchestration framework for a Security Operations Center (SOC). It integrates with RSA's own products and other third party security monitoring and security information and event management solutions and provides complete incident response workflow management.

Thus, RSA NetWitness Suite delivers a complete threat detection, investigation and response platform across endpoints, networks and the cloud.

3 Strengths and Challenges

RSA NetWitness Suite combines log, network traffic and endpoint analytics to enable real-time detection and investigation of sophisticated cyber-attacks. Its unique, highly modular architecture ensures that the solution can scale linearly and meet capacity requirements of even the largest, geographically distributed enterprises. Now incorporating solutions such as RSA NetWitness Endpoint and RSA NetWitness SecOps Manager (previously available as standalone products), the RSA NetWitness Suite has become an integrated platform for creating an end-to-end enterprise security operations center.

Unfortunately, architectural complexity makes the solution less suitable for smaller companies, at least until a cloud-based managed offering is added to the company's portfolio.

Strengths	Challenges
• Integrated platform for log, packet, NetFLow and endpoint analytics, alerting and forensic analysis • Threat Intelligence integration via RSA Live • Incorporates RSA NetWitness SecOps Manager to manage incident response workflows • Modular and easily scalable appliance-based architecture • Unified HTML5-based interface with rich visualization capabilities • High degree of customization	• Complex architecture with multiple components most likely requires services engagements to be successful • No cloud-based managed offering available yet • Limited localization capabilities (only English and Japanese are available)

4 Copyright

The Future of Information Security – Today

KuppingerCole supports IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst company, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global Analyst Company headquartered in Europe focusing on Information Security and Identity and Access Management (IAM). KuppingerCole stands for expertise, thought leadership, outstanding practical relevance, and a vendor-neutral view on the information security market segments, covering all relevant aspects like: Identity and Access Management (IAM), Governance & Auditing Tools, Cloud and Virtualization Security, Information Protection, Mobile as well as Software Security, System and Network Security, Security Monitoring, Analytics & Reporting, Governance, and Organization & Policies.

For further information, please contact **clients@kuppingercole.com**

Kuppinger Cole Ltd.
Sonnenberger Straße 16
65193 Wiesbaden | Germany

Phone +49 (211) 23 70 77 – 0
Fax +49 (211) 23 70 77 – 11
www.kuppingercole.com