RSA® Security Analytics

Detect & Investigate Threats.

OVERVIEW

HIGHLIGHTS

Introducing RSA Security Analytics, Providing:

- Security monitoring
- Incident investigation
- Compliance reporting

Providing Big Data Security Analytics

Enterprise-wide collection of network traffic and log event data is fused with automated threat intelligence and leveraged with high-powered analytics to enable fast threat discovery and investigations

ADVANCED SECURITY THREATS DEMAND MORE EFFECTIVE SECURITY MONITORING

To raise their game security teams need more effective threat detection and significantly faster investigations. Security teams need a system that can collect and manage a huge volume and wider scope of security data which will lead them to the most pressing security risks for their enterprise in the shortest amount of time. In the same vein, security teams need automated access to the best threat intelligence about the latest tools, techniques, and procedures in use by the attacker community and have this intelligence be immediately actionable through automated-enrichment on ingestion of telemetry. And they need this in one integrated security system, not multiple ones. When prevention fails all that is left is fast detection, investigation and remediation.

DEEP VISIBILITY DRIVES DETECTION

RSA Security Analytics is a security solution that helps security analysts detect and investigate threats that are often missed by other security tools. By combining big data security data collection, management, and analytics capabilities with full network and log-based visibility and automated threat intelligence, security analysts can better detect, investigate, and understand threats they could often not easily see or understand before. Ultimately this improved visibility and speed helps organizations reduce an attackers' free time in their computing environment from weeks to hours, thus dramatically reducing the likely impact of an attack.

RSA Security Analytics is a solution which provides converged network security monitoring and centralized security information and event management (SIEM).

Unlike perimeter or signature based security solutions, which struggle to keep up with current risks, especially targeted attacks, RSA Security Analytics helps analysts discover "interesting" or "anomalous" behavior without being dependent on having foreknowledge of the attackers specific instances of malware or attack steps.

RSA's security approach is akin to removing the "hay" (known good) until only "needles" (likely bad issues) remain, as opposed to traditional security approaches which attempt to search for needles in a giant haystack of data. Furthermore RSA Security Analytics helps analysts quickly understand alerts and unusual activity by correlating them with with network, log and event data as well as the most up-to-date threat intelligence.

The highly visual interface of RSA Security Analytics unifies security analysis, such as detection, investigation, alerting, reporting, and content and system administration into a single browser-based interface which puts enterprise-level visibility directly into the hands of the security analysts. This significantly increases the efficiency and effectiveness of the analysts as they don't have to flip from security tool to security tool to do their jobs. In short RSA Security Analytics takes traditional log-centric SIEM and re-conceives it and brings it forward to address the realities of today's threat landscape.

HIGH POWERED ANALYTICS FOR ANALYSTS

RSA Security Analytics enables comprehensive security monitoring, incident investigation, long term archiving and analytics, malware analytics, and compliance reporting via a unified, browser-based interface. It enables security analysts, whether part of a Security Operations Center (SOC), incident response team or neither, to be more effective and efficient in their job of protecting the organization's digital assets and IT systems.

MONITORING & ANALYTICS

- Provides a single platform for capturing and analyzing large amounts of network, log, event, and other data
- Powerful streaming analytics for incident detection and alerting.
- Integration with RSA ECAT to extend detection and investigations to endpoints.
- Integration with RSA Security Operations Management for incident remediation.
- Automatically generates alerts to suspicious behavior by applying analytics and by leveraging external threat intelligence (delivered via RSA Live) fused with internally collected security data.
- RSA Live provides: security reports, open source community intelligence, command & control reports, exploit kit identification, blacklists, APT tagged domains, suspicious proxies, and others.
- Applies business context to security investigations helping analysts better prioritize their work.

INCIDENT INVESTIGATION

- Accelerates security investigations by enabling analysts to pivot through terabytes of meta-data, log data, & recreated network sessions with just a few clicks.
- Uses the industry's most comprehensive and easily understandable analytical workbench
- Leverages the best 3rd party research and research created by RSA FirstWatch®, RSA's elite, highly trained global threat and intelligence research team

BIG DATA ANALYTICS

- Provides a distributed computing architecture for sophisticated, advanced analysis of long term security data, delivering high performance and scalability.
- Scales linearly through the addition of high performance or high capacity compute nodes.
- Free text searching enables powerful retrieval of documents, information within or metadata about documents
- Provides an open interface for programmatic data access, transformation, and analysis.

COMPLIANCE REPORTING

- Built-in compliance reports, covering a multitude of regulatory regimes (GLBA, HIPAA, NERC, SOX…) and industry requirements (PCI, BASEL II, ISO 27002…).
- Automates regulatory or governance focused reporting. Also allows security teams to take advantage of business context gathered as part of their compliance program.
- Ties into the wider compliance reporting system through two-way integration with RSA Archer GRC. RSA Security Analytics supplies data and reports for compliance related control reports and consumes business context information about the value and purpose of individual IT systems and assets.

MALWARE ANALYTICS

- Combines four distinct malware investigation techniques, including sandboxing, community intelligence, file content, and network behavior analysis to help the malware analyst discern if a file is malware or not.
- Identifies executable content wherever it exists, answers questions about the behavior of files taking into consideration where the malware was found and how it arrived into the IT environment.
- Incorporates anti-virus signatures only as one of multiple factors in determining the nature of the prospective malware.

UNIFIED BROWSER-BASED DASHBOARD

- HTML5 based user interface which enables customizable analysis and monitoring user interfaces.
- Monitoring, detection, investigation, and administration in a single integrated and customizable interface, driving analyst efficiency.
- Customized views based on the particular roles of the security analysts.

BIG DATA SECURITY ANALYTICS INFRASTRUCTURE

REAL TIME COLLECTION, ANALYSIS & INVESTIGATIONS

- Distributed collection infrastructure for simultaneous log and full network packet capture.
- Metadata parsing and management enables the blending of log, events, network, and other data for automated analytics, reporting, and analyst-driven investigations.
- Event Stream Analysis engine provides advanced stream analytics such as complex event processing and correlation at high throughputs and low latency.
- Distributed data management optimized for near real-time analysis, reporting, and investigations.

LONG TERM COLLECTION ARCHIVING, FORENSICS, ANALYSIS, & REPORTING

- Archiving engine enables long-term log archiving which is then optimized for long term data retention, forensic analysis and compliance reporting.
- Distributed warehouse and analytic engine for analysis, and reporting on security data, including logs, log meta data, network packet meta data, and select other content.
- Linearly scalable by adding warehouse nodes as analytic performance and capacity needs increase.

KEY ARCHITECTURAL COMPONENTS

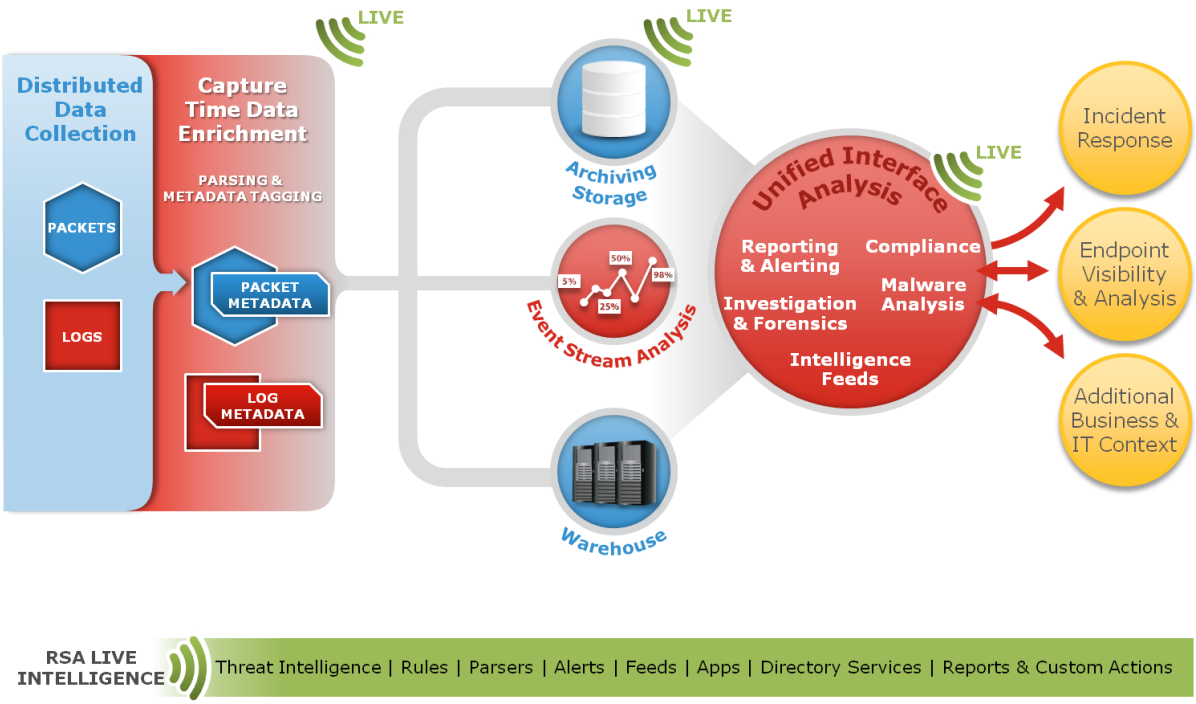
RSA Security Analytics is a distributed and modular system that enables highly flexible deployment architectures that scale with the needs of the organization. Key components of the architecture are:

- DECODER - Captures, parses, and reconstructs, all network traffic from Layers 2-7 or log and event data from hundreds of devices.
- CONCENTRATOR - Indexes metadata extracted from network or log data and makes it available for enterprise-wide querying and real-time analytics while also facilitating reporting and alerting.
- ANALYTIC SERVER/BROKER - Hosts the web server for reporting, investigation, administration, and other aspects of the analyst's interface. Bridges the multiple real-time data stores held in the various

decoder/concentrator pairs throughout the infrastructure. Also enables reporting on data held in the Warehouse and in archived storage.

- EVENT STREAM ANALYSIS ENGINE - Processes large volumes of disparate event data and brings meaning through correlation to the events flowing through your enterprise.
- ARCHIVER - Indexes and compresses log data and sends to archiving storage. The archiving storage is then optimized for long term data retention through compression, forensic analysis, and compliance reporting.
- WAREHOUSE - Hadoop based distributed computing system which collects, manages, and enables advanced analytics and reporting on longer term sets of various security data. The Warehouse can be made up of 3 or more nodes depending on the organization's analytic, and resiliency requirements.
- CAPACITY - RSA Security Analytics has a modular-capacity architecture, enabled with direct-attached capacity (DACs) or storage area networks (SANs), that adapt to the organization's short-term investigation and longer-term analytic and data-retention needs.

THE SECURITY ANALYTICS INFRASTRUCTURE



DEPLOYMENT FLEXIBILITY

RSA Security Analytics provides large deployment flexibility as it can be architected using as many as multiple dozens of physical appliances down to a single physical appliance, based on the particulars of the customers' performance and security-related requirements. In addition the entire RSA Security Analytics system has been optimized to run on virtualized infrastructure.

CONTACT US

To learn more about how EMC products, services, and solutions can help solve your business and IT challenges, contact your local representative or authorized reseller—or visit us at www.EMC.com/rsa.