COLLECT, MANAGE, AND ANALYZE ALL SECURITY ACTIVITY IN YOUR ENVIRONMENT

With today's rapidly evolving threat environment, one of the keys to securing your organization is the ability to see and understand everything that is happening on your network. Real-time visibility and high-powered analytics along with long term data retention are required to fulfill detection, investigation, analysis, forensic, and compliance needs. The RSA Security Analytics solution makes this a reality via two primary infrastructure elements: the capture infrastructure and the analysis and retention infrastructure.

The capture infrastructure is made up of three core components: Decoders (both for logs/NetFlow and packets), Concentrators and Brokers. Each component has a critical role in providing scalability and achieving an organization’s security monitoring goals. In order to enable application layer traffic analysis in real-time at high data rates, the capture infrastructure must scale out as well as scale up. The distributed and hierarchical nature of the Security Analytics infrastructure enables an organization to incrementally add data collection, analysis, and archiving as-needed. In higher throughput environments, the ability to separate primary read and write-to-disk functions allows Security Analytics to maintain both high capture rates as well as fast analytic response times.
THE CAPTURE ARCHITECTURE

DECODER

The Decoder is the cornerstone and the frontline component of the enterprise-wide network, log, and NetFlow collection, and analysis infrastructure of Security Analytics. The Decoder is a highly configurable appliance that enables the real-time collection, filtering, enrichment, and analysis of all network packet, log and NetFlow data. Position the Decoder(s) wherever you require on the network: egress, core, or other segment.

The Packet Decoder collects, extracts metadata, fully reassembles and globally normalizes network traffic at layers 2-7 of the OSI model, for real-time, full session analysis. The appliances can be operated in continuous, rapid capture mode or used tactically to consume network traffic from any source.

The Log Decoder leverages the same proven, highly scalable architecture used for log/NetFlow collection and indexing - recognizing over 250 Event Source Types.

The Decoder’s patented technology represents a breakthrough in security monitoring by dynamically creating a complete data structure of searchable metadata across all network layers, logs, events, and applications. Combined with log data, RSA Security Analytics also delivers compliance reporting, long term archiving and analysis.

CONCENTRATOR

Concentrators are designed to aggregate metadata and to hierarchically enable scalability and deployment flexibility. This enables implementations across various organization-specific network topologies and geographies. As a result, Concentrators can be deployed in tiers across multiple Decoders to provide and accelerate visibility.

BROKER AND ANALYTICS SERVER

The Broker operates at the highest level of the infrastructure hierarchy. Its function is to facilitate queries across an enterprise-wide deployment where two or more Concentrators are employed. Brokers provide a single point of access to all the Security Analytics metadata and are designed to operate and scale in any network environment, independent of network latency, throughput, or data volumes.

The Security Analytics (SA) Server is generally deployed with a Broker and hosts the security analyst’s user interface that enables incident detection, investigation, reporting and administration, among other analysis functions. It also includes support for role based access control and strong authentication. In addition, the SA server enables reporting on data held in the Pivotal powered RSA Analytics Warehouse as well as Archiving storage.

THE ANALYSIS & RETENTION ARCHITECTURE

ARCHIVER FOR LONG TERM RETENTION
The Archiver enables long term log archiving by indexing and compressing log data and sending it to archiving storage. The archiving storage is then used for long-term data retention, forensic analysis, and compliance reporting.

**EVENT STREAM ANALYSIS / CORRELATION**

The Security Analytics Event Stream Analysis (ESA) offering provides correlation at high throughputs and low latency. ESA is capable of processing large volumes of disparate event data that cannot be achieved by traditional correlation engines. Unlike other tools, ESA is able to correlate data across logs, packets, NetFlow and endpoints.

ESA is designed to handle the vast data volumes of today’s organizations and brings meaning to the events flowing through your enterprise. ESA’s advanced Event Processing Language (EPL) allows you to express filtering, aggregation, joins, pattern recognition and correlation across multiple disparate event streams. Event Stream Analysis is at the heart of Security Analytics’ ability to perform powerful incident detection and alerting. It also hosts Security Analytics’ incident triage and management capability for managing alerts across analysts.

**BIG DATA WAREHOUSE**

The RSA Analytics Warehouse powered by Pivotal HD provides a massively parallel computing infrastructure where computing power is scaled upon a standardized hardware platform or node. The Warehouse is specifically designed to manipulate large amounts of data and run complex queries for advanced analysis that is not be feasible without a big-data security analytics architecture.

**ADDITIONAL PLATFORM OPTIONS**

To meet the specific needs of an organization and its security use cases, RSA Security Analytics is available in a series of deployment options:

**ALL-IN-ONE APPLIANCE**

The All-In-One appliance brings the RSA Security Analytics experience to smaller enterprises or more narrowly scoped implementations in larger organizations. The All-In-One is a fully integrated, self-contained Security Analytics appliance that resides on the customer's premise. The appliance contains the Decoder and Concentrator software as well as the Security Analytics Server and is offered in a packet-only or log-only implementation. Included in each All-In-One appliance is 10 TB of capacity. This appliance capacity can be expanded.

**DECODER / CONCENTRATOR HYBRID**

For optimizing branch monitoring and lowering the total cost ownership, the Security Analytics Hybrid provides the functionality of a Decoder and Concentrator pair on a single appliance that can be hosted on the branch premises. The Hybrid enables the branch office or small security team to scale to next-generation requirements and still meet important operational security initiatives for responsive incident management and threat mitigation. A Hybrid offering is available for either packets or log collection. The use of a separate Security Analytics Server is required in a Hybrid deployment either in a Hybrid-only deployment or as part of a larger enterprise implementation which includes Hybrids. The Hybrid can be expanded with a single DAC of 22TB or 32TB.
EXPAND AND INTEGRATE

SCALABILITY
RSA Security Analytics unique architecture allows organizations to collect and analyze large amounts of data and expand linearly. The federated infrastructure allows organizations to scale, while still maintaining the ability to analyze and query seamlessly across the system. In order to enable application layer traffic in real-time at high data rates, the capture infrastructure must scale out as well as scale up. The distributed and hierarchical nature of the Security Analytics infrastructure enables an organization to incrementally add data collection, analysis, and archiving as-needed. In higher throughput environments, the ability to separate primary read and write-to-disk functions allows Security Analytics to maintain both high capture rates as well as fast analytic response times.

OPEN API
To scale beyond RSA Security Analytics offerings users can create their own custom security solutions by using Security Analytics’ open REST API. This open API enables other tools to integrate with the Security Analytics platform and extends the value of their existing security investments.