RSA® Security Analytics

Discover & Investigate Advanced Threats.

INFRASTRUCTURE

HIGHLIGHTS

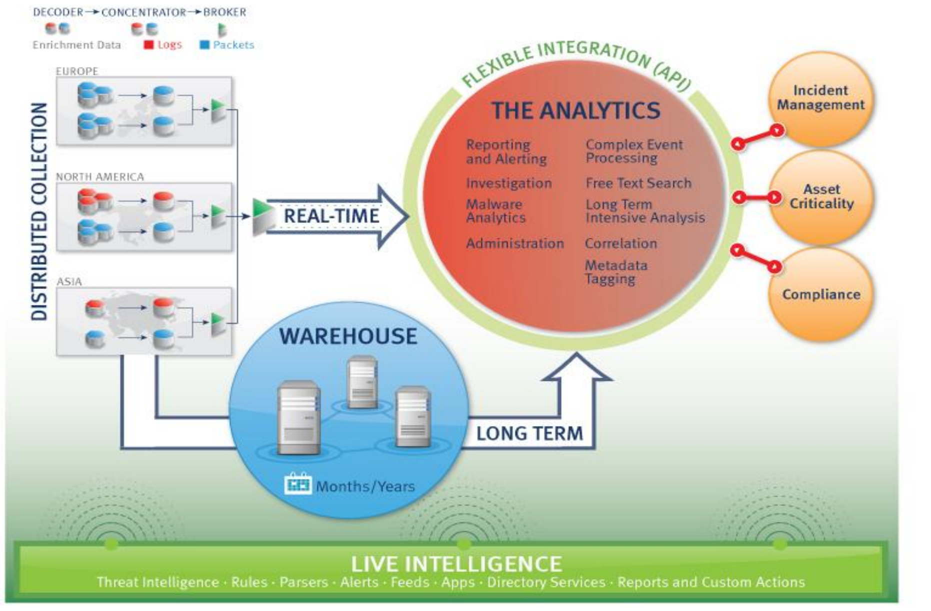
The RSA Security Analytics Infrastructure

- Modular architecture for distributed collection
- Metadata-based for efficient indexing, storage and search-ability
- Leverages RSA NetWitness infrastructure for analytics and investigations
- Warehouse provides long term archiving and intensive analysis

THE ABILITY TO COLLECT, MANAGE, AND ANALYZE EVERYTHING OCCURRING ON YOUR NETWORK

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

The capture infrastructure is made up of three core components: Decoders (both for packets and logs), 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 allows an organization to incrementally add data collection and Warehouse nodes for data retention 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.



SECURITY ANALYTICS INFRASTRUCTURE

DATA SHEET

THE CAPTURE ARCHITECTURE

DECODER

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

The Packet Decoder collects, 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 capture mode or tactically to consume network traffic from any source.

The Log Decoder leverages the same proven, highly scalable architecture used for network traffic recording and indexing - but for more than 200 devices and common log and event formats.

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

CONCENTRATOR

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

BROKER AND SECURITY ANALYTICS SERVER

The Broker operates at the highest level of the hierarchical infrastructure. 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 Server is generally coupled with a Broker and hosts the security analyst's user interface that enables discovery, investigation, reporting and administration, among other analysis functions. It includes support for role based access control and strong authentication. In addition, the SA server enables reporting on data held in the Security Analytics Warehouse.

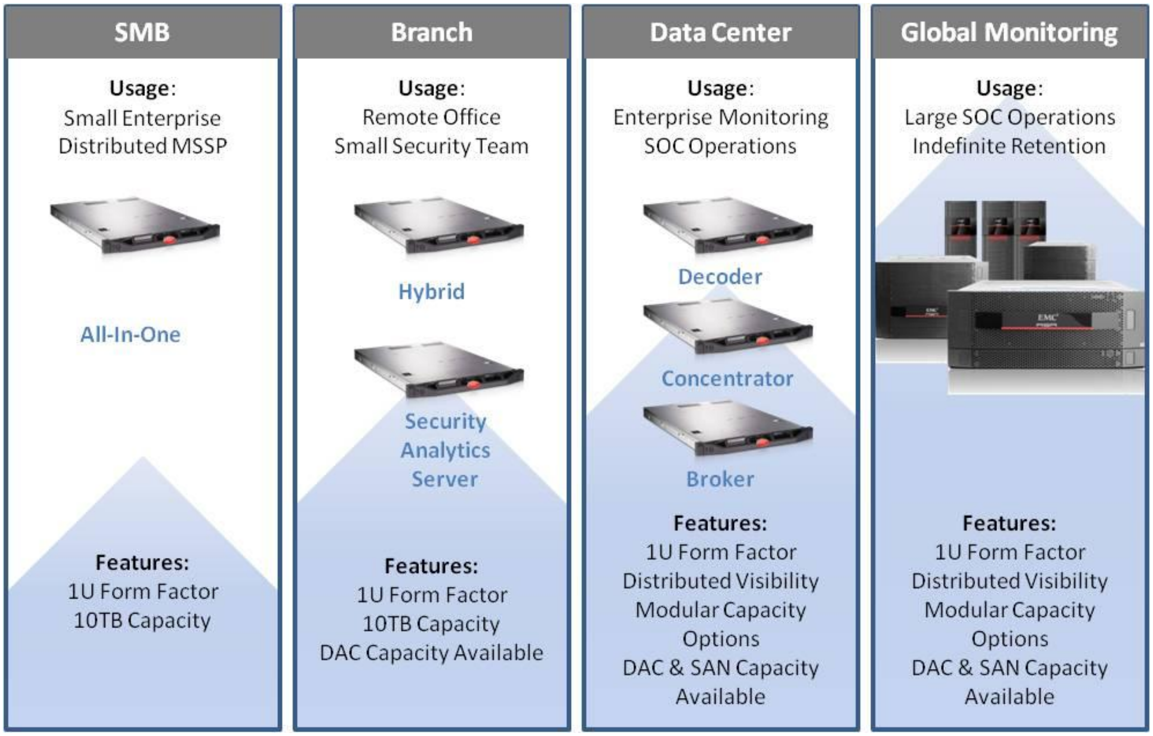
THE SECURITY ANALYTICS WAREHOUSE

LONG TERM RETENTION AND INTENSIVE ANALYSIS

The Security Analytics Warehouse is specifically designed for long term archiving, forensics, sophisticated analysis and reporting of many types. Leveraging Hadoop as a basis for an extensible platform, the Warehouse provides a massively parallel computing infrastructure where computing power is scaled in conjunction with storage capacity upon a standardized hardware platform or node. Unlike a traditional SIEM's retention model that can only scale by storage, the Security Analytics Warehouse retention capacity is local to each Warehouse node and is sized proportionately to the computing performance for the appliance node. Warehouse nodes can be incrementally added to deliver better compute performance increased archiving capacity, or both.

PLATFORM

OPTIONS



SMB

Usage:
Small Enterprise
Distributed MSSP

All-In-One

Features:
1U Form Factor
10TB Capacity

Branch

Usage:
Remote Office
Small Security Team

Hybrid

Security Analytics Server

Features:
1U Form Factor
10TB Capacity
DAC Capacity Available

Data Center

Usage:
Enterprise Monitoring
SOC Operations

Decoder

Concentrator

Broker

Features:
1U Form Factor
Distributed Visibility
Modular Capacity Options
DAC & SAN Capacity Available

Global Monitoring

Usage:
Large SOC Operations
Indefinite Retention

Features:
1U Form Factor
Distributed Visibility
Modular Capacity Options
DAC & SAN Capacity Available

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:

SMALL-MEDIUM ENTERPRISE

Bringing the RSA Security Analytics experience to smaller enterprises or more narrowly scoped implementations in larger organizations is the All-In-One appliance. 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. The appliance can be expanded with a single DAC of 22TB or 32TB.

BRANCH OFFICE

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 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.

DATA CENTER

For high performance enterprise-wide environments, the Security Analytics Decoder, Concentrator and Broker appliances offer the flexibility to meet bandwidth, events-per-second (EPS), and archiving performance requirements of the organization. The hierarchical architecture allows geographically dispersed locations to be sized appropriately while maintaining enterprise-wide, centralized operational standards for real-time situational awareness and long term archiving.

GLOBAL SCALE MONITORING

For the most demanding environments that require unlimited scalability and global security analytics, this RSA platform brings industry-leading technology and experience to support any security operations team. From a global organization operating their own backbone to service providers, RSA Security Analytics offers an extensible platform to maximize investment value and deliver the operational performance needed to inform, improve incident response and enable better risk management and business decisions.

FLEXIBLE INTEGRATION

Users can create their own custom applications by using Security Analytics' open API to integrate with the Security Analytics platform and to extend the value of their existing security investment. By having relevant information immediately accessible, organizations have the agility to respond to emerging threats and forensic investigations, identify broken business processes, mitigate malicious data exfiltration and adapt to tomorrow's challenges. Security Analytics represents the intersection of network telemetry, logs, threat intelligence, and rich application layer content and context that differentiates it from any other solution on the market.