11 REASONS TO LOVE RSA NETWITNESS® PLATFORM 11.x EVOLVED SIEM

RSA NetWitness Platform 11.x provides significant functionality to address customers' threat detection and response needs. Take a look at 11 reasons why you'll love RSA NetWitness Evolved SIEM.

1 UEBA

RSA NetWitness® UEBA leverages unsupervised machine learning and includes machine learning models based on log data and deep endpoint process data, to rapidly detect anomalies in users' behavior and uncover unknown, abnormal and complex evolving threats.

2 ENDPOINT

The RSA endpoint detection and response (EDR) solution, RSA NetWitness® Endpoint, is fully integrated with the RSA NetWitness Platform to provide additional context for detection and response, and a free RSA NetWitness Endpoint Insights Agent to capture static endpoint data and Microsoft Windows logs.

3 ORCHESTRATION & AUTOMATION

Native response workflows and SOAR capability in RSA NetWitness® Orchestrator. RSA NetWitness Orchestrator is a force multiplier for security operations centers (SOCs) to standardize, scale, measure and continuously adapt its security operations.

4 A REDESIGNED AND INTUITIVE UI

Easy to use for both experts and less experienced analysts.

5 NODAL VIEW

Visual representation of threats to speed recognition of threat dynamics and identify the full scope of attack.

6 AUTOMATED AND DYNAMIC LOG IDENTIFICATION

Forget about the days of unknown devices and unparsed logs when using the new out-of-the-box log parsing capabilities.

7 CLOUD SECURITY

Provides cloud visibility by capturing data from third-party cloud providers such as Amazon Web Services, Azure vTAP and many others.

8 DECODE

Ability to find and decode base64 and hex, and deep dive into network sessions with redesigned network investigations.

9 INSIGHTS INTO ENCRYPTED TRAFFIC

Inbound SSL decryption, parsing of compressed webpages and entropy measurements to help organizations gain valuable insight and metadata into encrypted traffic; without this visibility, the attacker has the clear advantage.

10 BUSINESS CONTEXT

Delivered in both Respond and Investigate workflows, with asset criticality from RSA Archer® Suite and threat-aware authentication with RSA SecurID® Suite, to help analysts prioritize their investigations and drive more informed authentication decisions.

11 THE ABILITY TO RUN ANYWHERE

Ability to run on RSA appliances, customer-provided hardware, virtual environments and in the cloud. Now with expanded HA failover capabilities for RSA NetWitness® Platform server host as well as a seamless backup and restore process for your entire environment.

See RSA NetWitness Platform in Action