RSA

DATA SHEET

RSA NETWITNESS® ORCHESTRATOR

DETECT THREATS. REDUCE DWELL TIME. AUTOMATE RESPONSE.

KEY FEATURES

- *Intelligent automation*
- *Collaborative investigation*
- *ChatOps powered war room*
- *Machine learning powered security bot*
- *Evidence collection and journaling*
- *Threat intelligence hub*
- *Variety of integrations including SIEM, firewalls, EDR, sandboxes, forensics, and more*
- *Robust command line interface*
- *Customizable map of related incidents across time*
- *Customizable visualizations of reports and dashboards*
- *Open and extensible platform (Python, Javascript)*
- *Comprehensive SLA tracking and metrics*
- *Regulatory compliance features*
- *Flexible deployment*

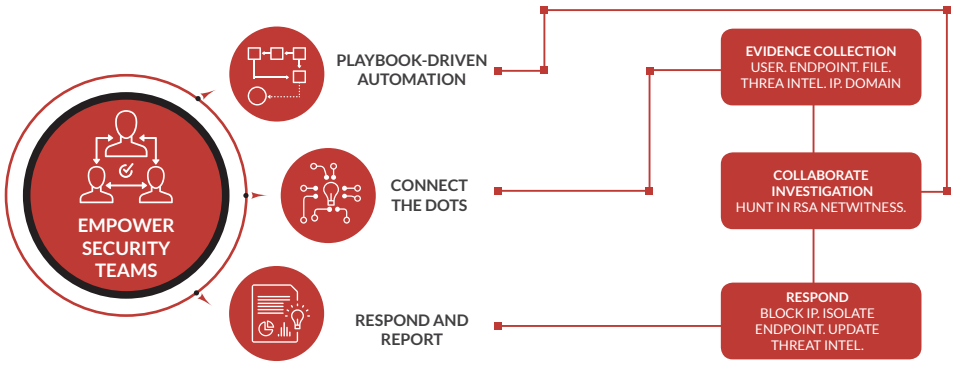
KEY BENEFITS

- *Enhance team performance*
- *Reduce MTTR*
- *Faster response*
- *Fewer errors*
- *Higher analyst productivity*
- *Automated threat hunting*

A force multiplier for SOCs to standardize, scale, measure and continuously adapt their security operations, by automating repetitive tasks and empowering security analysts to respond faster.

In an era of ever-expanding attack surfaces, protecting against threat actors—from commodity malware, insider threats and crimeware to state-sponsored exploits, hacktivists and terrorists—has become an increasingly complex activity. Not all threats are created equal, yet disconnected silos of prevention, monitoring or investigation technologies continue to fall short in empowering security operations centers (SOCs) to rapidly weed out false positives and eliminate manual, repetitive actions. What's needed is a comprehensive solution that enables security analysts to detect and respond to threats that really matter to the organization.

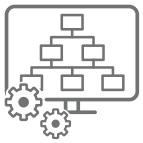
RSA NetWitness® Orchestrator is a comprehensive security operation and automation technology that combines full case management, intelligent automation and orchestration, and collaborative investigation capabilities. RSA NetWitness Orchestrator enables SOC analysts to have consistent, transparent and documented threat investigation and threat-hunting capabilities by leveraging playbook-driven automated response actions, automatic detection and machine-learning powered insights for quicker resolution and better SOC efficiency. RSA NetWitness Orchestrator acts as the connective tissue—not only for the RSA NetWitness Platform but across a SOC's entire security arsenal.



REDEFINE INCIDENT MANAGEMENT

RSA NetWitness Orchestrator enables SOC teams to collect isolated alerts from the organization's security arsenal and transform them into a context-rich, correlated incident containing critical data, including user reputation, system, IP, network, related incidents, repeat offenders, threat intel and many more customizable, out-of-the-box indicators. RSA NetWitness Orchestrator's Incident Management is the foundation for security operation decision, bridging orchestration, correlation and enrichment of security alerts across the entire incident management lifecycle, featuring a well-structured, consistent and automatically documented incident management process.

RSA



SYSTEM REQUIREMENTS

- *Physical or virtual server*
- *Linux OS: Ubuntu 14.04 and 16.04, CentOS 7.x*
- *8GB RAM minimum (16GB desired)*
- *8 CPU cores minimum (16GB desired)*

ENGINE PROXY (OPTIONAL)

- *Linux OS: Ubuntu 14.04 and 16.04, CentOS 7.x, Windows*
- *4GB RAM minimum*
- *Dual core CPU minimum*

DETECT UNKNOWN THREATS. AUTOMATE THE KNOWN.

Increase visibility. With visibility being the key to effective threat detection, RSA NetWitness Orchestrator features 160+ integrations and 500+ security actions. This empowers security analysts to accelerate enterprise-wide threat detection and response with comprehensive data across logs, network, endpoint, security and non-security solutions.

Up-level your SOC. Boost the productivity of all your analysts—from hunters to less skilled security staff—with joint, transparent investigations that reduce resolution time per incident. Gain maximum value from your entire SOC analysts' skill set.

Go beyond automation. Execute incident response processes and procedures with consistency and precision by leveraging a rich, preconfigured playbook portfolio. RSA NetWitness Orchestrator enables automated handling of known and/or low-risk threats, allowing swift containment and eradication. This frees and better positions analysts to investigate unknown threats that pose greater risk to the organization, across the entire IT infrastructure.

MACHINE LEARNING POWERED ENGINE

RSA NetWitness Orchestrator leverages the power of machine learning through an integrated "security chatbot" that primes SOCs for the future. RSA NetWitness Orchestrator learns from all interactive commands, playbook executions and secured execution of other actions to better position the analyst in future investigations. A real-time command-line execution interface alongside incident owner recommendations and task-analyst matching assists SOC analysts and precludes the need for tiresome documentation exercises.

Machine learning cuts across all three pillars: incident management, intelligent automation and orchestration, and interactive investigation. As both the security bot and analysts grow smarter with each incident, the marginal time to predict, contain and respond to threats decreases.

FLEXIBLE AND SCALABLE DEPLOYMENT

Deployed either on-premises or in cloud environments, RSA NetWitness Orchestrator was built from the ground up as a multi-tenant environment with data segregation, completely isolated both in execution and at-rest containers, for a superior adaptive and scalable architecture. The dedicated engine proxy better governs segmented networks in a secured fashion for ease of deployment and management.

THE RSA NETWITNESS PLATFORM

With over 30 years of security expertise, RSA continues to lead the market with an innovative solution that addresses the biggest challenges of security operations for the largest global organizations. The new RSA NetWitness Orchestrator product extends the RSA NetWitness Platform and its Evolved SIEM and Threat Defense offerings, leveraging its pervasive visibility across logs, network and endpoints.

Check our website for all the latest integrations, case studies and best practices.