NETWITNESS

DATA SHEET

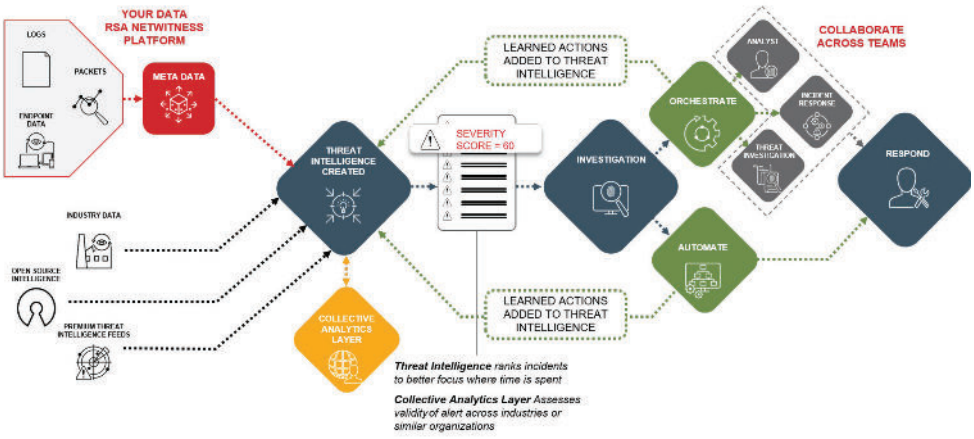
NetWitness® Orchestrator

Focus on the threats that matter most

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 and time-consuming activity. Not all threats are created equal, and not all deserve your attention. Yet disconnected silos of prevention, monitoring and investigation technologies fail to weed out false positives; eliminate manual, repetitive actions; and focus responses. Security teams need a comprehensive solution that enables security operations centers (SOCs) to automate processes effectively, and detect and respond to threats that matter most.

NetWitness® Orchestrator Built on ThreatConnect™ is a comprehensive security operation and automation technology that combines full case management, intelligent automation and orchestration, and collaborative investigation. NetWitness Orchestrator brings consistency and efficiency to threat investigation, hunting and response. By leveraging playbooks and integrated threat intelligence, it not only enriches but also automates analyst workflow, collaboration and response. NetWitness Orchestrator serves as the connective tissue for the NetWitness Platform—and a security operations team's entire security arsenal.

Threat Intelligence at the Center of Orchestration and Automation



Key

- Integration with the NetWitness Platform
- Threat intelligence-driven incident management
- Indicators of compromise (IOC) relevancy determinations
- Enhanced playbook control for better quality of service
- Real-time execution
- Streamlined collaboration across teams and tools
- Auto-documentation
- Scalable and secured multi-tenant platform
- Extensible integration framework
- Flexible on-premises and cloud Completely attack deployment

Key Benefits

- Automation: Empower software to do task-oriented "human work" and automate threat hunting
- Orchestration: Automate or systematize decision-making
- Dashboard and reporting: Visualize threat intelligence-driven metrics
- Incident management and collaboration: Provide end-to-end incident management
- Response time: Speed response time and reduce errors, improving analyst productivity and minimizing mean time to remediation (MTTR)

Redefine incident management

NetWitness Orchestrator enables security operations teams to collect isolated alerts from the organization's security arsenal and transform them into context-rich, correlated incidents containing critical data. It takes user reputation, system, IP, network, related incidents, repeat offenders and threat intel, empowering analysts to make informed decisions quickly. It serves as a foundation for security operations decisions, with a well-structured, consistent and automatically documented incident management process that brings together, correlates and enriches security alerts across the incident management lifecycle.

Automate the known. Detect the unknown.

Visibility is key to effective threat detection. NetWitness Orchestrator features more than 500 apps and integrations enabling countless security actions, including joint, transparent investigations that reduce resolution time per incident. Security analysts can accelerate enterprise-wide threat detection and response using comprehensive data across logs, network, endpoint, security and non-security solutions. Take advantage of a rich, pre-configured playbook, or customize your own for consistent and precise incident response. Use NetWitness Orchestrator to automate handling of known and low-risk threats, speeding containment and eradication—and freeing analysts to investigate higher-risk issues.

Threat intelligence-powered orchestration and automation

Unlike solutions that use intelligence only to trigger specific workflows, NetWitness Orchestrator leverages threat intelligence across all orchestration and automation functions, for rich context and playbooks that adapt continually. The platform also leverages the full value of any intelligence, with support for cross-team coordination within workflows.

Combining threat intelligence, orchestration, automation and response, NetWitness Orchestrator delivers holistic system-wide insight, enabling security operations to:

- Alert, block and quarantine based on relevant threat intel. Even for lower-level tasks such as alerting and blocking, relevant threat intelligence is important. You can automate detection and prevention, but you need multisourced, validated threat intel to make sure you're getting alerts for—and blocking—the right things.
- Increase accuracy, confidence and precision. Situational awareness and historical context are key to decision-making. Working directly from threat intelligence allows you to work faster, and to prevent more attacks before they happen. The more you can automate up front, the more proactive you can be. Eliminating false positives and using validated intelligence help you take more accurate actions—which in turn improves speed and precision.
- Understand context and improve over time. Automate tasks based on threat intelligence thresholds (such as indicator reputation scores), then memorialize all that information—and you can strategically look at your processes and see how to improve.

NetWitness Orchestrator System Requirements

Physical Instance

- Physical server requirements
  - —Application server (no playbooks)
    - Memory: 16GB
    - CPU Cores: 8 (2GHz)
    - Estimated storage: 50GB
  - —Application server (playbooks)
    - Memory: 48GB
    - CPU cores: 8 (2GHz)
    - Estimated storage: 150GB
  - —Database server (< 2 million indicators)
    - Memory: 12GB
    - CPU cores: 6 (2Ghz)
    - Storage: 20GB
  - —Database server (2-5 million indicators)
    - Memory: 16GB
    - CPU cores: 8 (2Ghz)
    - Storage: 40GB
  - —Database server (5-10 million indicators)
    - Memory: 32GB
    - CPU cores: 12 (2Ghz)
    - Storage: 60GB
  - —Elasticsearch® server (< 2 million indicators)
    - Memory: 12GB
    - CPU/vCPU cores: 6 (2Ghz)
    - Storage: 20GB
  - —Elasticsearch server (2-5 million indicators)
    - Memory: 16GB
    - CPU/vCPU cores: 8 (2Ghz)
    - Storage: 40GB
  - —Elasticsearch server (5-10 million indicators)
    - Memory: 32GB
    - CPU/vCPU cores: 12 (2Ghz)
    - Storage: 60GB

- **Orchestrate with confidence.** Native sense-making analytics on external threat intelligence allows for more accurate alerts with fewer false positives, blocks and quarantines. Unfortunately, you can't just ingest lots of threat intel feeds, or act from a shared IOC. You need to make sense of them at scale, using adaptable scoring and contextualization to drive action, and to know whether action is needed.
- **Build organic intelligence from security operations and response.** Your team and your data are the ultimate intelligence sources. You want to be able to capture insights, artifacts and sightings from operations and response engagements, then immediately refine them into intelligence, in the form of new IOCs, adversary tactics and techniques, and knowledge of security gaps.
- **Adjust processes automatically as information and context change.** You should be able to adapt your orchestration capabilities to changing threat intelligence, automatically adjusting internal processes in response to indicator classification and threat assessment scores. Dynamically update these processes and workflows to make your team's efforts more relevant and effective.

Flexible and scalable deployment

NetWitness Orchestrator is designed from the ground up to support deployments in multi-tenant, single-tenant and true on-premises environments. No matter the deployment, data is securely segregated, with easy options for both vertical and horizontal scaling. NetWitness supports orchestration across multiple network environments with centralized management.

Typical security orchestration and automation technologies struggle to scale to handle the workload volume and breadth needed to maximize SOC automation and enrichment. That leaves security teams able to automate only a few use cases, leaving many manual workflows remaining. NetWitness Orchestrator provides a truly scalable architecture that allows orchestration and automation workloads to grow along with the SOC. Security teams can prioritize execution, dedicate resources to specific playbooks and add additional playbook servers as workload demands increase.

The NetWitness platform

With more than 30 years of security expertise, NetWitness continues to lead the market with an innovative solution that addresses the biggest challenges of security operations for the largest global organizations. NetWitness Orchestrator extends the NetWitness Platform and its threat detection and response capabilities, leveraging its pervasive visibility across logs, network, endpoints, netflow and IoT devices.

NetWitness Orchestrator System Requirements

- Operating system: Red Hat® Linux variant—either Red Hat Enterprise Linux (RHEL) or Community Operating System (CentOS) 6 or 7
- Oracle® Java® Development Kit (JDK): Access to a local installation of Oracle Java 8 or OpenJDK (JDK version 1.8)
- Java Cryptography Extension: Version 8
- Elasticsearch: Elasticsearch server 6.3.0
- Python®: Installation of Python 3.6.x only: Refers to CPython
- Python SDK: TCEX version 1.0+
- Redis: Installation of Redis 4.0.10
- Database (select from one of the following):
  - MySQL®: Installation of MySQL 5.7.x Community or Enterprise Edition
  - SAP S/4HANA®: Installation of SAP S/4HANA 2.0 SPS 02
  - PostgreSQL: Installation of PostgreSQL v11

NOTE: Install only one as the working database.

About NetWitness

NetWitness, an RSA® Business, provides comprehensive and highly scalable threat detection and response capabilities for organizations around the world. The NetWitness Platform delivers complete visibility combined with applied threat intelligence and user behavior analytics to detect, prioritize, investigate threats, and automate response. This empowers security analysts to be more efficient and stay ahead of business-impacting threats.

NETWITNESS