WHITE PAPER

Introducing RSA NetWitness® Detect AI

Cloud Analytics for Superior Threat Detection

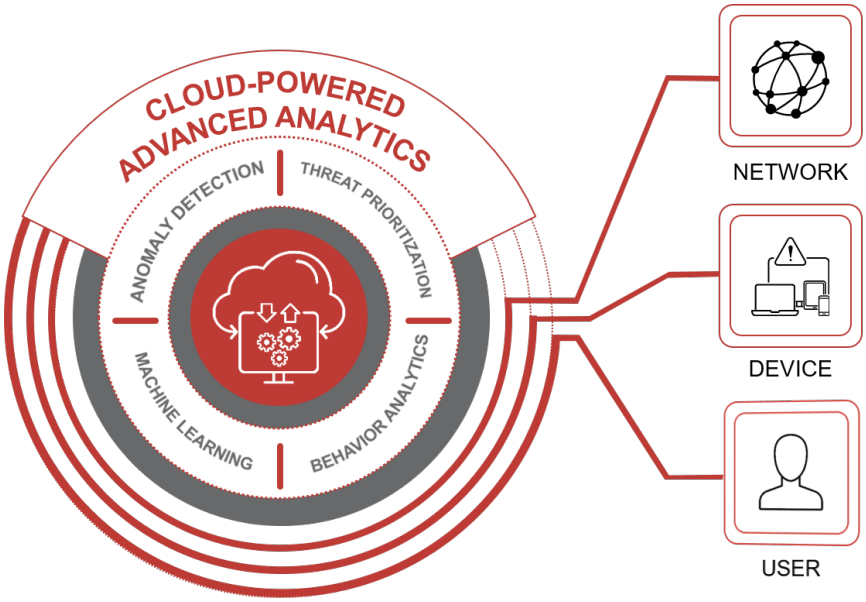
The Relentless Pace of Cybersecurity Innovation

The history of cybersecurity is one of rapid and continuous invention, as advances in attack methods continuously drive innovation in cyber defenses.

This dynamic has led to the development of sophisticated security operations centers (SOCs) built on industrial-grade cyber defense solutions like RSA NetWitness Platform. A leading SIEM and XDR solution, RSA NetWitness Platform is used by many of the world's largest, most complex and security-conscious organizations, who rely on its powerful threat detection, incident response and security automation capabilities to identify the stealthiest threats in their earliest (and least destructive) stages.

Taking RSA NetWitness Platform into the Cloud

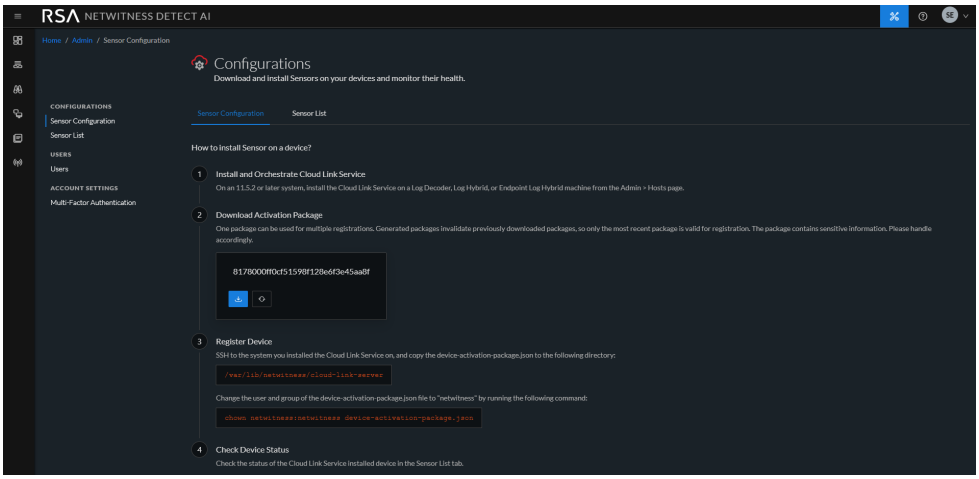
The release of RSA NetWitness Detect AI represents a decisive step in extending the power of RSA NetWitness Platform to the cloud. RSA NetWitness Detect AI takes RSA NetWitness Platform's industry-leading analytics capabilities and offers them as an easy to use software-as-a-service solution.



RSA NetWitness Detect AI uses advanced behavior analytics and machine learning to quickly reveal unknown threats, leveraging log, network, endpoint and IoT/ICS data monitored by RSA NetWitness Platform. It creates baselines of an organization's behaviors and IT usage and identifies anomalies that indicate suspicious behaviors and sophisticated threats.

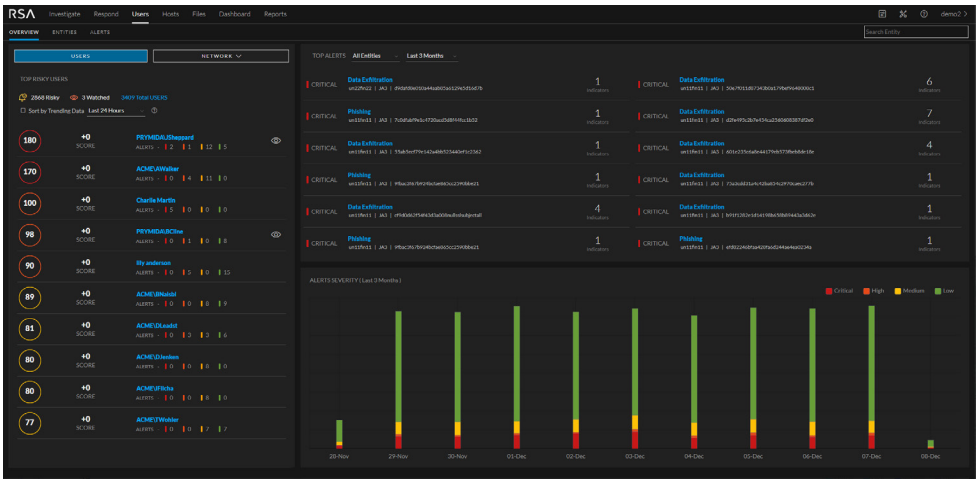
RSA NetWitness Detect AI's cloud architecture provides immediate value to analysts. Cloud elasticity, scalability and processing power drive RSA NetWitness Detect AI's unsupervised machine learning algorithms across a wide range of use cases, including detection of insider threats, brute force authentication and machine operated activities. RSA NetWitness Detect AI combines its proprietary machine learning algorithms with an innovative risk scoring model designed to alleviate alert fatigue for analysts by only alerting on high fidelity and high priority threats. This leads to faster attack investigation and response times, and drives more efficient and complete incident management.

Because it's cloud-based, RSA NetWitness Detect AI requires no pre-deployment resource sizing, no additional hardware, and very little configuration—all of which make setup simple and straightforward. Ongoing maintenance is equally simple since there's no physical or virtual hardware to manage and updates are automatically pushed out.



Once initiated, RSA NetWitness Detect AI starts processing data immediately and begins establishing behavioral baselines within hours. It rapidly scales to process millions of data points and becomes smarter and more accurate with each unit of data it ingests.

RSA NetWitness Detect AI can accommodate the processing requirements of organizations large and small. The elastic nature of the cloud means that the service only consumes the resources it requires, without the need to keep capacity in reserve for traffic spikes or incident response activities. Flexible licensing options make planning and budgeting easy, even as situations and use cases change.



RSA NetWitness Detect AI provides continuous behavior-based detection for unknown threats, meaning it doesn't rely on rules, signatures, or require manual analysis. It gets continuously smarter about the specifics of your environment as more data flows through, and its machine learning algorithms are regularly refined and updated by RSA data scientists, so your analysts don't have to worry about tuning them. Thus, RSA NetWitness Detect AI performs the hard work of detection and correlation, freeing up analysts to focus on proactive threat hunting activities and giving them meaningful data and insights they need to accelerate incident resolution.

The Future of RSA NetWitness Platform

RSA NetWitness Platform is built to perform in the most demanding enterprise security environments and to address the most intractable challenges security teams face, including:

The ever-expanding attack surface – RSA NetWitness Platform provides organizations with the most complete visibility across logs, network, endpoint and IoT/ICS systems, regardless of whether those systems runs in the cloud or on premises.

Inconsistent data formats across security prevention platforms – RSA NetWitness Platform centralizes network and endpoint analysis, behavioral analysis, data science techniques and threat intelligence on a single platform, allowing security teams to eliminate redundant security tools and data. It uses unique, patented technology to dynamically parse, enrich and index log data at capture time, creating sessionized metadata that dramatically accelerates alerting and analysis.

Inconclusive monitoring technologies and noisy detection platforms – RSA NetWitness Platform enriches log data with threat intelligence and business context to identify high-priority threats and reduce false positives. In addition, it aggregates multiple indicators of suspicious activity, then applies a dynamic statistical risk scoring model to produce higher-fidelity alerts triggered only when a risk score exceeds established thresholds.

RSA NetWitness Detect AI is RSA's latest innovation in threat detection and response. Continued investment in RSA NetWitness Platform evolved SIEM and XDR will, as always, focus on making RSA NetWitness Platform smarter, faster, and easier to use, with cloud capabilities to support the full range of industrial-grade SOC use cases, including SaaS, hybrid and private cloud deployments. We remain committed to providing analysts with advanced solutions to defend against sophisticated and well-funded threat actors.

For more information, visit **rsa.com/detect-ai** or contact your RSA sales representative.

About RSA

RSA, a leader in cybersecurity and risk management solutions, provides organizations with technology to address challenges across security, risk management and fraud prevention in the digital era. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user access control; and reduce operational risk, fraud and cybercrime. RSA protects millions of users around the world and helps more than 90 percent of the Fortune 500 companies thrive and continuously adapt to transformational change.

©2021 RSA Security LLC or its affiliates. All rights reserved. RSA and the RSA logo are registered trademarks or trademarks of RSA Security LLC or its affiliates in the United States and other countries. All other trademarks are the property of their respective owners. RSA believes the information in this document is accurate. The information is subject to change without notice. 1/21 White Paper, W437406.