RSA

SOLUTION BRIEF

RSA NETWITNESS® EVOLVED SIEM

RSA

OVERVIEW

A SIEM is technology originally intended for compliance and log management. Later, as SIEMs became the aggregation points for security alerts, they began to be more broadly used to detect and investigate attacks. However, SIEMs have several inherent flaws that make it difficult to detect more complex, successful attacks, and make it even more complicated to effectively investigate them in a timely manner.

SIEMs give security personnel some level of visibility into what is going on across the enterprise by highlighting anomalies across different sets of logs. However, logs alone ultimately lack the deep visibility and important detail required to fully understand what is happening in an environment—from data deep on the endpoint to packet capture that highlights what goes on between the log connection intervals.

An evolved SIEM accelerates threat detection and response, provides additional depth of visibility, and incorporates both threat intelligence and business context to help prioritize threats and security incidents. It provides:

- Unparalleled visibility to see threats anywhere
- Capabilities to instantly detect the full scope of an attack
- Business context to enable analysts to rapidly respond to the threats that matter most

Despite increasing investments in security, breaches are still occurring at an alarming rate. Whether the result of cybercriminals sending phishing or malware attacks through company emails, nation states targeting organizations' intellectual property or insiders misusing sensitive data, we live in a world where prevention of breaches has become impossible. Given the speed with which cybercriminals are able to create and execute new security threats globally, companies must change their approach to security.

It is time for the centerpiece of our security operations to evolve!

WHY IS EVOLVED SIEM REQUIRED?

The sophistication of threat actors and the ever-expanding attack surface of a modern IT infrastructure have evolved beyond the capabilities of legacy SIEMs and related tools. Security teams need capabilities to rapidly discover compromises and to understand their full scope, so they can respond before these threats impact the business.

Attackers are gaining access to an organization's infrastructure faster than ever—usually within minutes—and nearly all are extracting sensitive data within a matter of hours. However, these same breaches can take weeks or even months to discover and usually not by internal security systems and controls but rather by external sources such as customers or authorities.

RSA

Organizations struggle to rapidly detect and respond due to:

- Disproportionate reliance on preventative controls
- Blind spots across the network, at the endpoint, and into virtual and cloud infrastructure
- The flood of data from silos of data sources, with no correlation or analytics across them
- A lack of threat intelligence and business context enrichment of their security data
- Inexperienced and scarce analyst resources

The threat landscape is more sophisticated:

- As organizations migrate applications, data and everyday computing to the cloud, they have varying limited visibility into events occurring outside traditional network environments.
- Attackers are well resourced, targeted and understand organizations' blind spots.
- Attackers only have to be right once; security teams have to be right every time.

Security teams are struggling to be efficient and effective in detection and responding:

- Technical experts struggle to keep up with the flood of alerts with limited prioritization.
- Security analysts rely on manual correlation, detection and investigations.
- It takes too long to understand how security incidents are affecting the overall business.

RSA

RSA NETWITNESS EVOLVED SIEM

RSA NetWitness evolved SIEM empowers security teams to detect and understand the full scope of a compromise because it analyzes data and behavior across an organization: logs, packets and endpoints as well as the NetFlow of activity generated by people and processes. The solution transforms that data into more useful information through the real-time enrichment with business context and threat intelligence delivered from a variety of sources. The evolved SIEM utilizes a unified taxonomy across the entirety of this intelligent data to accelerate the detection of both known and unknown threats.

The RSA NetWitness evolved SIEM features powerful capabilities built on machine learning, user and entity behavior analysis (UEBA), and advanced threat intelligence. RSA NetWitness evolved SIEM provides rich, role-based orchestration and workflow for threat detection and response activities as well as flexible deployment models (cloud, virtualized or appliance) to support modern IT infrastructure.

This comprehensive and flexible platform enables RSA NetWitness evolved SIEM to dramatically optimize threat detection and response processes. In an environment where security expertise is scarce and expensive, the RSA NetWitness evolved SIEM makes security analysts far more effective in protecting their organizations against advanced cyber threats.

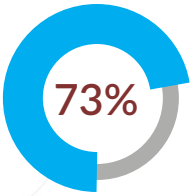
RSA NetWitness evolved SIEM key capabilities include:

- **Single, Unified Platform for All Your Data.** It is the only solution that combines threat detection analytics and response with log and event monitoring, endpoint telemetry, investigation and threat intelligence capabilities across all your data. With "dynamic parsing," RSA NetWitness Advanced SIEM delivers instant value for new and unknown sources, without requiring custom parsers or coding.
- **Integrated Threat and Business Context.** By adding business context to threat analysis, organizations can prioritize threats based on the potential impact to their businesses. In addition, intelligence gathered from industry research and crowdsourced from our customer base and the organization's own data is fully aggregated and operationalized at ingestion to better detect the unknowns that are prime indicators of compromise.
- **Automated Behavior Analytics.** Our unique Advanced Analytics Engine looks for potentially malicious issues across logs and NetFlow as well as correlates data across full network packets and endpoints—all prime attack vectors for today's advanced threats. By analyzing all these data sources together and searching for attack behaviors, and applying UEBA, RSA NetWitness evolved SIEM can dramatically speed threat detection and response. RSA NetWitness UEBA Essentials extends the power of the RSA

RSA

RSA NetWitness® evolved SIEM is the threat detection and response solution that gives you the fastest path to fully understand, then ultimately eradicate, threats prior to business impact, regardless of the attack vector.

- *Know that you have visibility across all systems in order to detect threats before they can damage the business*
- *Match business context to security risks, closing the gaps of technology-only solutions*
- *Have confidence that you have the right understanding of the full scope of the threat*
- *Achieve efficiency by managing analyst workflows and supporting compliance objectives*
- *Minimize business impact by quickly responding and taking action*
- *Create a more efficient and effective security team—without adding staff*



of organizations rate their threat detection capabilities as inadequate

Source:
RSA Cybersecurity Poverty Index 2016

NetWitness evolved SIEM by targeting threats that manifest themselves in user and entity behavior.

- **Rapid Investigations.** The RSA NetWitness evolved SIEM provides an advanced analyst workbench to triage alerts and incidents, including an interface designed specifically for security investigations. Utilizing deep insight into data from across the infrastructure allows analysts to natively and visually reconstruct a network attack or data exfiltration in its entirety. The evolved SIEM empowers analysts to connect incidents over time in order to expose and better understand the full scope of an attack.
- **Automation and Orchestration.** This platform enables security operations center (SOC) analysts to have consistent, transparent and documented threat investigations 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.
- **Flexible, Scalable Architecture.** By offering a wide range of flexible deployment options, the RSA NetWitness evolved SIEM can scale incrementally according to an organization's needs and security priorities. Whether deployed as a single appliance or dozens, partial or fully virtualized deployments, on-premises or in the cloud, RSA NetWitness evolved SIEM can support it all.
- **End-to-End Security Operations.** The RSA NetWitness evolved SIEM is the only platform that unifies logs, network telemetry and endpoint telemetry along with advanced threat intelligence and SOC runbooks and management to fully operationalize security operations programs from end to end.