NETWITNESS

SOLUTION BRIEF

NetWitness® Platform Evolved SIEM

Information security has been a major challenge for organizations since the dawn of the digital era. Today, however, several factors have combined to make security more challenging than ever before:

- The rapid industry transition to virtualized and cloud-based infrastructure has effectively broken the traditional perimeter-based security approach.
- Cyber threats have been commercialized for mass use, with many exploits originating in nation-state intelligence organizations.
- Managing cyber risk has been elevated to a core business responsibility, not just an IT problem.

NetWitness recognizes and understands these challenges and offers evolved SIEM and threat defense tools and services that help organizations rapidly detect and respond to threats in this continuously evolving environment.

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

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.

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.

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 limited or no correlation or analytics across them
- A lack of dynamic 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 gain scalable infrastructure but are more vulnerable and have 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.

NetWitness Platform evolved SIEM

The NetWitness Platform evolved SIEM empowers security teams to detect and understand the full scope of a compromise because it analyzes data and behavior across an organization's logs, packets and endpoints as well as the behavior of the people and processes on the network. The solution transforms that data into actionable threat insights through real-time enrichment with business context and threat intelligence delivered from a variety of sources. The evolved SIEM creates a unified taxonomy across the entirety of this intelligent data to accelerate the detection of both known and unknown threats.

The NetWitness Platform evolved SIEM features powerful capabilities built on machine learning, user and entity behavior analytics (UEBA), correlation rules and advanced threat intelligence. The NetWitness Platform evolved SIEM provides 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 the NetWitness Platform evolved SIEM to dramatically optimize threat detection and response processes. In an environment where security expertise is scarce and expensive, the NetWitness Platform evolved SIEM makes security analysts far more effective in protecting their organizations against advanced cyber threats.

The NetWitness Platform evolved SIEM key capabilities include:

- **Single, Unified Platform for All Your Data.** It is the only solution that combines threat detection analytics, log and event monitoring, and endpoint and network visibility with investigation and threat intelligence capabilities across all your data. With "dynamic parsing," the NetWitness Platform evolved 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 for faster detection of threats.

- **NetWitness Detect AI** is a cloud-based behavior analytics solution that applies unsupervised machine learning to data captured by the NetWitness Platform to rapidly detect unknown threats, no matter where they occur in the attack lifecycle. High-fidelity anomaly detection empowers your existing security team to work more efficiently and effectively, with fewer false positives and noisy alerts. NetWitness continuously tunes the machine learning algorithms so you don't have to, and so that NetWitness Detect AI is ready to reveal anomalous behaviors quickly and accurately the moment you turn it on.

- **Rapid Investigations.** The NetWitness Platform 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, analysts can natively and visually

NetWitness Platform evolved SIEM is the threat detection and response solution that enables security teams to fully assess then ultimately eradicate threats before they impact your business.

- Visibility across all systems to quickly detect threats
- 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 automating analyst workflows and supporting compliance objectives
- Comprehensive detection for unknown threats based on behavior. Threat-aware authentication for defining authentication policies that act upon suspicious activity and elevate trust.

197

DAYS

Mean time of organizations to identify a breach

Source: *Ponemon Institute 2018 Cost of a Data Breach Study* reconstruct a network attack or data exfiltration in its entirety. The evolved SIEM empowers analysts to connect incidents over time to expose and better understand the full scope of an attack.

- **Automation and Orchestration.** NetWitness® Orchestrator is a comprehensive security operation and automation technology that combines full case management, intelligent automation and orchestration, and collaborative investigation capabilities. 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.
- **Flexible, Scalable Architecture.** By offering a wide range of flexible deployment options, the NetWitness Platform 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, the NetWitness Platform evolved SIEM can support customers' specific architectures.
- **End-to-End Security Operations.** The NetWitness Platform evolved SIEM is the only platform that unifies analytics, log and event monitoring, and endpoint and network visibility with advanced threat intelligence and automated incident management to optimize security operations.

About the NetWitness Platform

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. For more information, go to **netwitness.com**.

NETWITNESS
An RSA Business