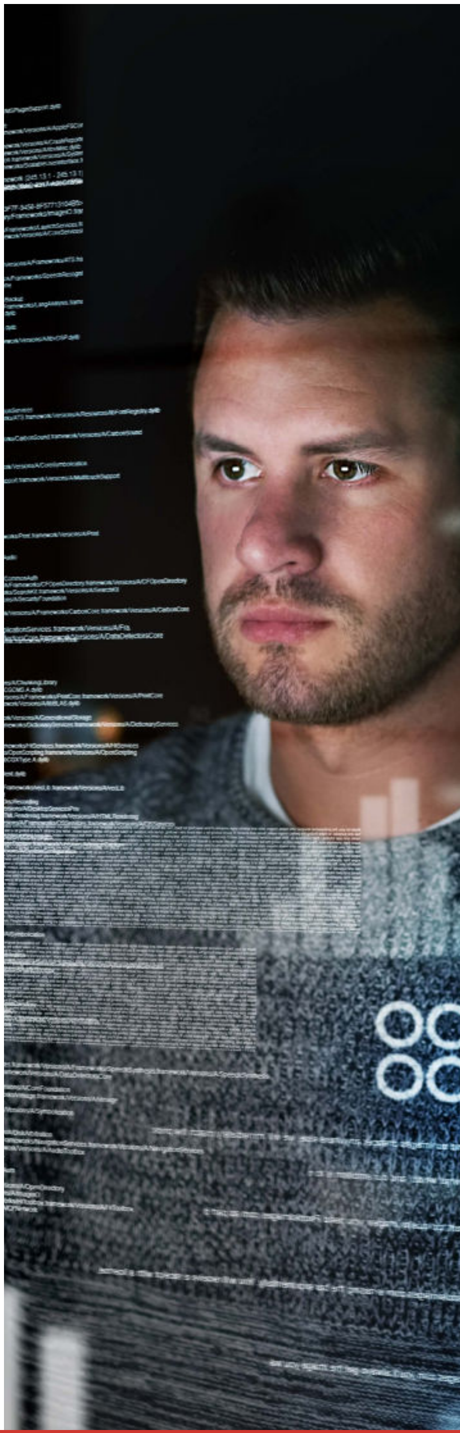
NETWITNESS

SOLUTION BRIEF

# The NetWitness® Platform

## Accelerated Threat Detection and Response from Endpoint to the Cloud



In order to stay ahead of the growing number of sophisticated emerging threats, organizations need to find ways to gain visibility, effectively investigate incidents while avoiding false positives that waste time, and collaborate across the security team to take the proper action quickly and efficiently.

In the past, organizations needed to correlate data from multiple systems, often working in silos. This consumed time working through mundane tasks, resulting in security analyst burnout or potential threats slipping through the cracks. Organizations need to combine full visibility and analytics with business context and threat intelligence to detect and respond to the threats that matter most and have an efficient organized way, leveraging task automation, to resolve issues with speed and consistency.

## The Struggle to Keep Up with the Ever-Growing and More Sophisticated Threat Landscape

Security teams need to evolve to stay in front of attackers and the latest threats, but in recent years this has become even more difficult. Attackers continue to advance and use sophisticated techniques to infiltrate organizations that no longer have well-defined perimeters. Attackers spend significant resources performing reconnaissance to learn about organizations and develop techniques specifically designed to bypass security tools.

Sophisticated threat actors and the expanding attack surface make it nearly impossible for already overburdened security teams to discover and understand the full scope of threats quickly enough to respond before they negatively impact the business.

The sophisticated and ever-expanding attack surface of a modern IT infrastructure has evolved beyond the capabilities of legacy security information and event management (SIEM) systems. Security teams need capabilities to rapidly discover compromises and understand their full scope, to respond before threats impact the business.

Attackers are gaining access to an organization's infrastructure—usually within minutes—and are extracting sensitive data within a matter of days. These same breaches can take months to discover and are often found by external authorities instead of internal security systems.

Organizations struggle to rapidly detect and respond:

- Disproportionate reliance on preventative controls and log-centric SIEMs
- Blind spots across the network, at the endpoint and into virtual and cloud infrastructure
- Siloed data sources, with no correlation or analytics across multiple data sets
- A lack of threat intelligence and business context enrichment of security data

The threat landscape is more sophisticated:

- As applications, data and everyday computing migrate to the cloud, there is varying visibility into events.
- Attackers are well resourced, targeted and understand organizations' blind spots.
- Attackers only have to be correct once; security teams must be right every time.

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

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

The NetWitness® Platform applies the most advanced technology to detect, prioritize and investigate threats in a fraction of the time of other security products.

## The Visibility You Need to Effectively Respond to Known and Unknown threats

The NetWitness® Platform applies the most advanced technology to detect, prioritize and investigate threats in a fraction of the time of other security products. Through a unique combination of behavioral analysis, data science techniques and threat intelligence, it detects known and unknown attacks. It exposes the full scope of an attack by connecting incidents over time, prioritizing incidents quickly, and delivering deeper insights from both automation and machine learning.

The NetWitness Platform brings together Evolved SIEM and Threat Defense solutions that deliver unsurpassed visibility, analytics and automated response capabilities as the centerpiece of the security operations center (SOC). It enables security teams to detect and resolve known and unknown attacks.

- Offers unparalleled visibility across logs, network, endpoint, user behavior, NetFlow data, and IoT devices, enriched with business context and threat intelligence
- Aligns business context to security risks, ensuring that IT security is optimized to support an organization's strategic goals
- Identifies new, targeted and unknown threats with real-time, data science and machine-learning analytics to identify any attack

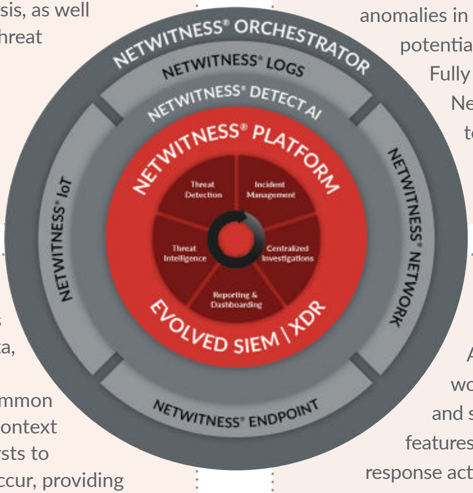
- Empowers security teams to accelerate investigations by quickly drilling down from logs into recreated sessions to identify what occurred
- Provides immediate understanding of the full scope of an attack and powers SOC teams to be more efficient and effective at detection and response by better correlating threat data with context
- Scales from the smallest to the largest organizations

### ADVANCED ANALYTICS

Detects and identifies threats using sophisticated rules, threat intelligence and malware analysis, as well as behavior analytics. Sophisticated threat detection algorithms operate across disparate data types and sources, for fast identification and correlation of indicators of compromise (IOCs) and real-time prioritization of true threats.

### TRUE UEBA

User and Entity Behavior Analytics (UEBA) detects anomalies in behavior patterns, highlighting potential exploits or insider threats. Fully automated and " zero touch," NetWitness UEBA is proprietary technology that is integrated into the platform's common data model and analyst toolset.



### BROAD VISIBILITY

Provides unsurpassed visibility across logs, packets, endpoints, NetFlow data, and IoT devices, across on-premises, virtual and cloud environments. A common data model, enriched with business context and threat intelligence, enables analysts to correlate anomalies wherever they occur, providing fast insight into the full scope of an attack.

### AUTOMATION & ORCHESTRATION

Automation security tasks and analyst workflows to increase SOC efficiency and speed. NetWitness Orchestrator features playbook-driven automated response actions, and machine-learning insights that integrate your entire security arsenal.

### BUSINESS-DRIVEN SECURITY

As organizations embrace Digital Transformation, digital risk becomes business risk. The NetWitness Platform aligns business and security risks, integrating risk factors such as asset criticality and user identity, and orchestrating incident response across your organization.

## Advanced Analytics:

Detects and identifies threats using sophisticated rules, threat intelligence and malware analysis, as well as behavior analytics. Sophisticated threat detection algorithms operate across disparate data types and sources, for fast identification and correlation of indicators of compromise (IOCs) and real-time prioritization of true threats.

## User and Entity Behavior Analytics (UEBA)

User and entity behavior analytics solution integrated as a central part of the NetWitness Platform. UEBA leverages unsupervised statistical anomaly detection and machine learning across logs, network packets and endpoint data, eliminating the need for security analysts to constantly tune and train the solution for a "zero touch" management. The NetWitness UEBA provides comprehensive detection for unknown risks, highlighting potential exploits and insider threats, by detecting and grouping anomalies to provide a reliable risk score allowing security analysts to address real threats and minimize time wasted chasing false positives.

### Broad Visibility

Provides unsurpassed visibility across logs, packets, endpoints, NetFlow data, and IoT devices, across cloud, virtual and on-premises environments. A common data model, enriched with business context and threat intelligence, enables analysts to correlate anomalies wherever they occur, providing fast insight into the full scope of an attack.

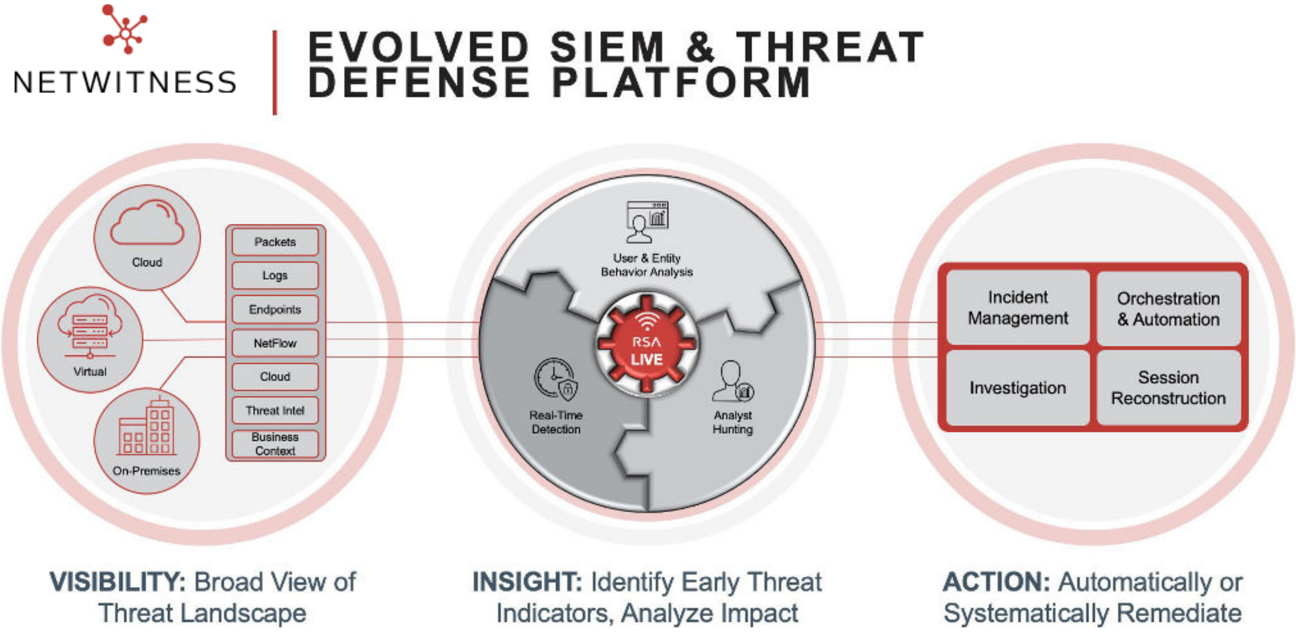
### Automation and Orchestration

Allows the whole security operations team to address potential threats quickly and efficiently, unifying people and technology around the same game plan. Security operations can easily collaborate and respond through cross-team coordinated efforts, leveraging automation to perform repetitive tasks, consistently freeing up analysts' time to be spent on tasks that matter and minimizing replication or tasks being missed during an investigation. By aggregating all relevant information and insight throughout the course of an investigation, decision-makers can easily communicate risk to stakeholders and act quickly.

By aggregating all relevant information and insight throughout the course of an investigation, decision-makers can easily communicate risk to stakeholders and act quickly.

### Business-Driven Security

As organizations embrace digital transformation, digital risk becomes business risk. The NetWitness Platform aligns business and security risks, integrating risk factors such as asset criticality and user identity, and orchestrating incident response across your organization.


NETWITNESS
EVOLVED SIEM & THREAT DEFENSE PLATFORM
Cloud
Virtual
On-Premises
Packets
Logs
Endpoints
NetFlow
Cloud
Threat Intel
Business Context
User & Entity Behavior Analysis
RSA LIVE
Real-Time Detection
Analyst Hunting
Incident Management
Orchestration & Automation
Investigation
Session Reconstruction
VISIBILITY: Broad View of Threat Landscape
INSIGHT: Identify Early Threat Indicators, Analyze Impact
ACTION: Automatically or Systematically Remediate

### Flexible & Scalable Platform

The NetWitness Platform is a modular threat detection and response solution that is the centerpiece of an evolved security operations team. It enriches data at capture time, creating metadata to dramatically accelerate alerting and analysis and quickly understand the full scope of an attack. Core NetWitness Platform capabilities include its common data model, radical scalability and flexible deployment options, as well as its sophisticated analyst toolset, forensic capabilities and reporting engine.

## NetWitness Logs

NetWitness Logs provide fundamental visibility into all the relevant log sources, including various industry-leading network and security devices, popular applications and operating systems, in order to defend against a broad threat landscape. NetWitness Logs is a security monitoring solution that collects, analyzes, reports on and stores log data from a variety of sources to speed threat identification and support security policy and regulatory compliance initiatives.

## NetWitness Network

NetWitness Network collects and analyzes network data in real time to enhance a security team's capabilities to detect and respond to today's advanced threats. The solution indexes, enriches and correlates network packet data at capture time to provide immediate deep visibility. NetWitness Network provides rich forensic value like session reconstruction so analysts can reconstruct an email from network data to reveal threats in ways that preventative solutions cannot.

## NetWitness Endpoint

Continuously monitor and respond on the endpoint—such as laptops, desktops, servers and virtual machines—to provide deep visibility and powerful analysis of all threats on an organization's endpoints. NetWitness Endpoint leverages unique, continuous endpoint behavioral monitoring and rich response components to dive deeper and more accurately and rapidly identify new, targeted, unknown and even file-less attacks that other endpoint security solutions miss entirely.

## NetWitness Orchestrator

Address threats quickly and consistently, unifying people and technology around the same game plan. Collaborate and respond through coordinated efforts, automating repetitive tasks quickly and consistently. Decision-makers can easily communicate risk and act quickly with relevant insight, and investigations are enhanced with contextualized threat intelligence at the heart of the solution. This ensures security teams have an immediate understanding of all related indicators, correlated from massive amounts of data from broad sources, to make faster decisions.

## NetWitness Detect AI

Augments your existing security team by providing rapid detection of unknown threats and anomalous behavior at every step of the attack lifecycle. Its powerful machine learning engine provides high-fidelity threat detection across a range of uses case. 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.

## NetWitness Professional Services

NetWitness offers three advanced services to support customer cybersecurity efforts:

- The NetWitness Risk and Cybersecurity Advisory Practice helps customers implement solutions that protect against risk, ensure compliance and accelerate business objectives.
- The NetWitness Advanced Cyber Defense (ACD) Practice offers services that span planning, implementation and ongoing operational effectiveness for SOCs and Cyber Incident Response Centers (CIRCs).
- The NetWitness Incident Response (IR) Practice delivers experienced, expert response services, to help organizations quickly identify and eradicate threats. IR services are available on a retainer or engagement basis.

Security operations teams turn to the NetWitness Platform to stay ahead of new and emerging threats as an advanced threat detection and response solution that empowers security teams to rapidly detect and understand the full scope of a compromise. The platform aligns business context to security risks to close the gaps of technology-only solutions and ensure that IT security is optimized to support an organization's strategic goals. The NetWitness Platform delivers the most complete visibility, integrating logs, network data and endpoints, and applying threat intelligence and behavior analytics to analyze, prioritize, investigate threats and automate response. This unsurpassed breadth of visibility and depth of technology make security analysts more effective and efficient.

- 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.
- Create a more efficient and effective security team—without adding staff.

## 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.

Learn more about the NetWitness Platform at NetWitness.com.

NETWITNESS