NETWITNESS

DATA SHEET

NetWitness® UEBA

Detect threats faster. Reduce dwell time. Automate response.

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 activity. Not all threats are created equal, yet disconnected silos of prevention, monitoring and investigation technologies continue to fall short in empowering security operations centers (SOCs) to rapidly weed out false positives and provide focused indicators as opposed to openended siloed alerts. What's needed is a comprehensive and collaborative solution that enables security analysts to detect and respond to threats that really matter to the organization.

NetWitness® UEBA is a purpose-built, big data-driven, user and entity behavior analytics solution integrated as a central part of the NetWitness Platform. By leveraging unsupervised machine-learning algorithms, across a large breadth of use cases, NetWitness UEBA provides comprehensive detection for unknown threats based on behavior, without the need for analyst tuning. NetWitness UEBA augments your existing security team to provide rapid detection and actionable insights at every step of the attack lifecycle. NetWitness UEBA is core to the NetWitness Platform to help with full attack investigation lifecycle and breach resolution.

Detect threats across all terrains

NetWitness UEBA boosts the NetWitness Platform threat-detection capabilities. Leveraging native and core to the NetWitness Platform network capture, log collection, endpoint visibility and a unified metadata enrichment at machine-learning speed, security analysts can flush out attackers—whether inside or external—via clear, focused alerts. NetWitness UEBA leverages artificial intelligence and a superior machine-learning mathematical approach to baselining users and user groups, entities and organization-wide behaviors, which can separate normal, benign activities from malicious deviations for true, actionable incident response.

Answers. Not open-ended quest ons.

NetWitness UEBA assists security analysts in identifying sources of compromise and suspicious outlier activities via identity-based chronological visualization, highlighting suspicious indicators aligned with the MITRE ATT&CK™ framework, for a more efficient, complete incident response.

Key features:

- Patented recursive, unsupervised behavioral machine learning
- Native data collection
- Innovative feature-weighting system
- Simplified risk-scoring engine
- Breadth of use cases
- Identity-context visualization
- Automated false-positive reduction algorithms

Key benefits:

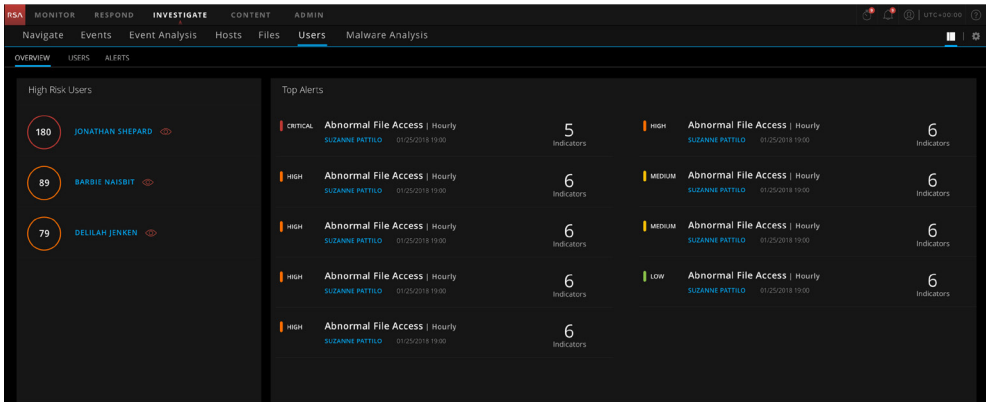
- Reduce MTTD & MTTI
- Accelerate incident response
- Fewer false positives
- Identity-based context enrichment
- Quickly pinpoint risky users

Better combat evolving destructive threats, regardless of the terrain in which they operate.

Hands-off detection firepower

Automated and continuous monitoring accelerates time to detection of both rogue insiders and cybercriminals who are using compromised accounts—without rules, signatures or manual analysis. NetWitness UEBA features powerful data science models to strengthen organizations' ability to detect yet-to-be-seen tools, techniques and processes (TTPs), and provides end-to-end investigations that enable analysts to pivot from raw analytics findings to their organization's overall risk posture.

Leveraging a big-data, scalable technology architecture, NetWitness UEBA provides a powerful threat-detection engine capable of connecting disjointed events to surface abnormal activities and previously unknown user threats—all in a single user interface.



UEBA. Core to the Platform.

Focused, actionable and context-aware alerts zero in on user behaviors that are likely indicators of suspicious activity and will ultimately pack more punch for security analysts. NetWitness Platform introduces adaptive user and entity behavior analytics that can operate with the same agility and speed as evolving threats. The NetWitness Platform is capable of capturing unattended log data to enable security analysts to unmask attackers—leveraging dynamic, nondeterministic detection algorithms, baselining, behavior modeling and peer group analytics.

UEBA use cases:

- Insider threat
- Brute force
- Account takeover
- Compromised account
- Privilege account abuse and misuse
- Elevated privileges
- Snooping user
- Data exfiltration
- Abnormal system access
- Lateral Movement
- Malware activity
- Suspicious behaviors

NetWitness UEBA starts getting smarter the moment you turn it on, revealing anomalous behaviors quickly, accurately and without constantly demanding your attention to fine-tune.

NetWitness UEBA and UEBA Essentials surface events of higher priority, correlated in real time across log events, network traffic and endpoint visibility to empower SOC teams to lower MTTD (Mean Time To Detect) and MTTI (Mean Time To Investigate), reduce alert fatigue and false positives, and better provide more accurate threat forecasts and predictive analytics.

The NetWitness Platform

With more than 30 years of security expertise, NetWitness continues to lead the market with innovative solutions that address the biggest challenges of security operations across the globe. NetWitness UEBA extends the NetWitness Platform and its threat detection and response capabilities, leveraging its pervasive visibility across logs, network, endpoints, netflow and IoT devices.

Visit NetWitness.com for more information.

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