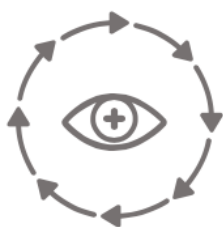# NetWitness® Endpoint

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 open-ended siloed alerts. What's needed is a comprehensive and collaborative solution that enables security analysts to detect and respond to the threats that matter most to their organization.

Given today's mobile workforce, which is increasingly off-premises on untrusted networks and then logged back in to trusted environments, endpoints—now more than ever—remain the most vulnerable attack vector.

NetWitness® Endpoint is a fully integrated endpoint detection and response solution, a core product offering within the NetWitness Platform, that provides continuous monitoring of endpoints to equip security analysts with deep visibility into and powerful analysis of all threats on an organization's endpoints. Instead of signatures or rules, it leverages unique, continuous behavioral monitoring and advanced machine learning to dive deeper into endpoints to better analyze and identify zeroday, hidden and non-malware attacks that other endpoint security solutions may miss entirely.

Featherweight. Not your average agent.

NetWitness Endpoint provides a single, scalable and fast tamper-proof agent that delivers immediate insights, response actions and metadata ingestion from both windows logs as well as endpoint core processes. This depth of visibility and actionable insights offers an organization wide view of all endpoints for full attack lifecycle and incident-response investigations across Windows, macOS and Linux operating systems.

Key Features

- EDR, NDR, SIEM, behavior analytics, O&A in one complete platform
- Process visualization
- Continuous threat-aware authentication
- Single tamper-proof agent for logs, endpoint kernel and metadata collection
- Broad behavior analytics detection algorithms
- Innovative and customizable risk-scoring engine
- Can be deployed on-premise or in public cloud like AWS and Azure

Key Benefits

- Reduce Mean Time To Detect, Investigate and Respond
- Accelerate incident response and reduce dwell time
- Unparalleled visibility into endpoint behavior anomalies for early threat detection
- Threat-aware authentication pinpoints suspicious users and compromised accounts
- Faster root cause analysis
- Assess the full scope of the attack across endpoint and network

The NetWitness Platform helps SOC and IT teams gain insights into the full scope of an attack across both network and endpoint and delivers the actionable intelligence security analysts require to streamline threat analysis and response actions.

Analyze user and entity behaviors at a deeper level

NetWitness Platform provides machine-learning models based on deep endpoint process data to rapidly detect anomalies in user and machine behaviors—all in a single, complete platform. NetWitness Endpoint and NetWitness Detect AI, core product offerings within the NetWitness Platform, offer deep and broad visibility that boosts detection and response capabilities for security analysts, regardless of the terrain attackers are operating in. PowerShell mis/ab-use, malicious scripting, process and kernel hooks, registry decencies, memory exfiltration, fileless attacks, and more are quickly detected by NetWitness Platform's ability to correlate millions of events without the need of manual analysis or customization of rules and signatures.
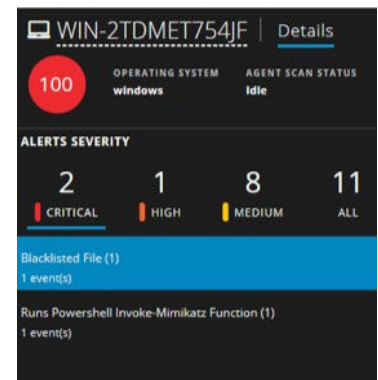
Improve response time. Reduce breach impact.

A critical aspect of effective remediation is understanding how far a targeted attack has spread across your network. NetWitness Endpoint provides this broad and deep threat visibility, empowering security teams with targeted response capabilities to swiftly remediate incidents across all endpoints in the enterprise. NetWitness Endpoint quickly gathers all of the most critical data needed for an effective forensic investigation and instantly identifies all infected endpoints, for immediate understanding of the scope and breadth of an attack.

Security teams can isolate an endpoint on the network, preventing attacker communication and threat lateral movement, and can block and quarantine threats across all infected endpoints. Deep investigation and metadata integrations with the NetWitness Platform allow organizations to see and understand the full scope of an attack across network and endpoint telemetry, optimizing security operations response.

The NetWitness Platform

With over 30 years of security expertise, RSA continues to lead the market with innovative solutions that address the biggest challenges of security operations across the globe. NetWitness Endpoint extends the NetWitness Platform and its evolved SIEM and XDR offerings, leveraging its pervasive visibility across logs, network and endpoints.

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