

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 (EDR) 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 zero-day, 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

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.

