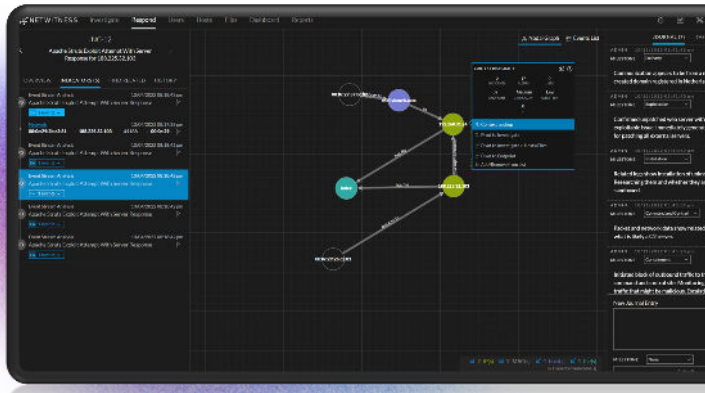
NETWITNESS

NetWitness® XDR

Accelerated Threat Detection and Response



Challenges with data visibility, analyst burnout, tight budgets, and compliance demands lead to a vulnerable SOC. Meanwhile, sophisticated breaches of even the most hardened environments make single-purpose defenses ineffective. The world is in dire need of the deep experience and breakthrough thinking that only NetWitness can provide.

Unify and strengthen your security operations to meet today's threats

NetWitness XDR empowers security teams to rapidly detect, understand, and automatically respond to sophisticated threats and compromises before business damage is done.

By combining logs, network traffic, and endpoint analysis, along with AI/ML-enabled business and security context, behavioral analytics, and cutting-edge threat intelligence, NetWitness XDR delivers total visibility across data planes to deliver unmatched data protection and peace of mind.

Rapidly detect and respond to any threat, anywhere

- Gain complete visibility across your entire technology infrastructure, whether on-premises, in the cloud, or a hybrid combination.
- Focus on the threats that matter most with relevant context.
- Reduce time and cost of incident investigation and response with faster root cause analysis.
- Drastically shrink dwell time.
- Alleviate pressure from security staff shortages with intuitive workflows.
- Increase resolution rate with shortened time-to-remediation.

Key Features

- Highly scalable collection and visibility of network, log, and endpoint data
- Seamless correlation between data types
- Continuously updated threat intelligence
- Real-time data enrichment from security and business sources
- Automatic asset discovery and classification
- Multifaceted analytics including behavior analysis and asset discovery
- Graphical incident investigation and management
- Complete session replay and reconstruction across data types

NetWitness XDR for Extended Visibility, Insight, and Action

NetWitness XDR is a flexible and scalable modular threat detection and response solution that provides complete visibility across your entire technology infrastructure. Data is enriched at capture time to dramatically accelerate alerting and analysis. Get a unified data architecture, radical scalability and flexible deployment options, a sophisticated analyst toolset, forensic capabilities, and robust reporting engine.

NetWitness Network Network Detection and Response (NDR)	Quickly collect and analyze real-time network data on-premises, in the cloud, and across virtual infrastructures for immediate deep visibility. Patented parsing and indexing technology enrich log data at time of full packet capture, dramatically accelerating alerting and analysis of known and unknown threats. Reconstruct entire sessions to reveal threats in ways that preventive solutions can't.
NetWitness Logs Security Incident and Event Management (SIEM)	Get views into all relevant log sources, including industry-leading network and security devices, popular applications, and operating systems. Centralized log management, monitoring for logs generated by public clouds and SaaS applications, and identification of suspicious activity that evades signature-based security tools provide instant visibility.
NetWitness Endpoint Endpoint Detection and Response (EDR)	Cut the cost, time, and scope of incident response with unique, continuous monitoring of endpoint devices and rich response components. Reduce dwell time by rapidly detecting new and nonmalware attacks that other EDR solutions miss. Dive deeper and more accurately to rapidly identify new, targeted, unknown, and even file-less attacks.
NetWitness Analytics User Entity Behavioral Analytics (UEBA) and Insight (Attack Surfaces)	Leverage network, endpoint, and log data to tap a cloud-native SaaS offering that creates a baseline of your organization's behaviors and IT usage. Advanced behavioral analytics and machine learning help you easily identify deviations that indicate suspicious behavior and sophisticated threats. Discover and rank all your network assets and detect changes over time to understand your true network footprint and know where to focus your investigation and response to anomalies.
NetWitness Orchestrator Security Orchestration, Automation and Response (SOAR)	Collaborate, streamline, and automate incident response. Centralize, grade, and apply threat intelligence to address incidents quickly and consistently. Easily communicate risk with relevant insight gleaned from centralized threat intelligence, ensuring security teams immediately understand all of the indicators on which to base their decisions.

NetWitness Professional Services — Committed to Your Success

NetWitness offers services to support the ongoing success of security operations teams. These range from SOC design, implementation, and training, to managed detection and response (MDR) and major incident response (IR). IR Retainer Services ensure rapid response in the event of a major attack or breach.

Ready to learn more? Visit www.netwitness.com

NETWITNESS