NETWITNESS

DATA SHEET

NetWitness® Platform XDR

Accelerated Threat Detection and Response

Overview

Cyber-defense has never been so challenging, nor more important. Sophisticated and well-funded adversaries are capable of breaching even the most hardened environments, rendering a generation of single-purpose defenses ineffective. Existing security skills fall far short of demand, leading to high costs and retention issues – even as burnout causes talent to leave the industry every day.

Clearly ours is an industry in need of breakthrough thinking, and eXtended Detection & Response (XDR) promises to both strengthen and simplify the tools and methodologies used to defend against cyber threats. Collapsing disparate tools and controls into a single, unified, highly automated platform increases effectiveness, lowers costs, and helps security experts to succeed with less stress.

NetWitness® Platform XDR empowers security teams to detect and understand the full scope of a compromise by analyzing data and behavior across all an organization's technology assets, using a unified data architecture. Network packets, logs, endpoint, and internet of things (IoT) information, whether on-premises or in the cloud, are enriched with business and security context. Coordinated, real time intelligence from a broad variety of sources is applied. And the platform automatically identifies threats and anomalies to accelerate the remediation and elimination of both known and unknown threats.

NetWitness® Platform XDR accelerates the effectiveness of the security analysts and responders who are responsible for protecting valuable assets and networks. It empowers them with important capabilities including:

- A unified solution that integrates all security, and relevant business and technical context, in one application
- Visibility across all data sources and deployment types, with the ability to correlate seamlessly among them
- Advanced analytics and detection of even stealthy threats that increases accuracy and productivity
- Intuitive and efficient workflows to help alleviate the pressures of security skills shortage
- Strong response and forensics capabilities to stop attackers, understand what happened and remove them completely

Key Features

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

Key Benefits

- Gain complete visibility across your entire infrastructure
- Alleviate pressures from security staff shortages with intuitive workflows
- Focus on the threats that really matter with relevant context
- Faster root cause analysis reduces time and cost of incident response and investigation
- Drastically reduce dwell time by rapidly detecting and investigating threats
- Increase resolution rate with reduced time-to-remediation for incidents
- Completely understand the full scope of attacks across logs, packets, endpoints and IoT in your entire infrastructure with the NetWitness Platform XDR

Flexible and Scalable Platform

NetWitness Platform XDR is a modular threat detection and response solution that is the centerpiece of an evolved security operation. It enriches data at capture time, adding full metadata to dramatically accelerate alerting and analysis and quickly understand the full scope of an attack. Core NetWitness Platform XDR capabilities include a unified data architecture, radical scalability and flexible deployment options, as well as its sophisticated analyst toolset, forensic capabilities and reporting engine. XDR product modules are available for network, logs, endpoints, IoT devices, and security orchestration.

NetWitness Platform XDR for Network

Network Detection and Response (NDR). Collect and analyze network data in real time to turbocharge 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 Platform XDR for 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 Platform XDR for Logs

Security Incident and Event Management (SIEM). Achieve 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 Platform XDR for 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 Platform XDR for Endpoint

Endpoint Detection and Response (EDR). Continuously monitor and respond on endpoint devices – such as laptops, desktops, servers, and virtual machines – to provide deep visibility and powerful threat analysis. NetWitness Platform XDR for 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 Platform XDR for IoT

Internet of Things Detection and Response (IoTDR). Integrate IoT data into the threat detection and response process to defend against new types of attacks. NetWitness Platform XDR for IoT delivers lightweight, cloud-based alerting on its own for IoT operations staff, as well as the SOC.

NetWitness Orchestrator

Security Orchestration, Automation and Response (SOAR). Centralize, grade, and apply your threat intelligence wisely. 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 Professional Services

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

NETWITNESS