NETWITNESS

DATA SHEET

NetWitness® MDR

Managed Detection and Response Service

Overview

Organizations around the globe value NetWitness Platform XDR for its broad and effective threat detection and response capabilities and its ability to address the never-ending and increasingly sophisticated attacks they face. Yet, tools are only part of the solution.

Ultimately, the success of cybersecurity depends on the availability of skilled security analysts and threat hunters, a major challenge due to an ongoing skills shortage. According to the (ISC)[2] Cybersecurity Workforce Study[1], there's a worldwide gap of over 2.7 million cybersecurity professionals.

In response, organizations are turning to Managed Detection and Response (MDR), a specialized security service designed to augment in-house staff and tools. Smaller organizations may use MDR to outsource the Threat Detection and Response function completely. While larger and more highly security-conscious organizations may choose to offload day-to-day triage, response, and system administration to free in-house staff for strategic activities like threat hunting, planning, and systems hardening, as well as ongoing skills enhancement that is difficult when security analysts are bogged down with repetitive, lower-level tasks.

There are other advantages to an MDR approach. Vendors who offer MDR typically operate across a number and variety of customers, so they're able to see attacks in real time against one customer, and immediately apply that knowledge to protect other customers before they're even attacked.

For all these reasons, customers seek an MDR service that works closely with NetWitness XDR. This delivers the best of both worlds: a sophisticated, and comprehensive XDR platform that is operated and maintained by dedicated, highly skilled staff.

In this focused model, NetWitness MDR provides customized offerings that deliver whatever organizations need: skilled security analysts who connect directly to a NetWitness Platform XDR infrastructure to perform critical functions including threat hunting, incident management, even system administration and upgrades.

The NetWitness MDR service is an ideal solution for organizations that seek trusted analysts and threat hunters using a proven XDR platform.

Key Features

- Managed Detection and Response services based on the industry's most mature and powerful XDR platform
- Security analysts with deep skills and knowledge of the constantly evolving threat landscape, and the NetWitness Platform XDR security solution
- A direct relationship with NetWitness XDR Professional Services, eliminating the traditional gap between software manufacturer and its service practitioners
- Deployment, administration, patching, and upgrade services to free internal staff for other strategic security activities

Key Benefits

- High-quality staff augmentation
- Ability to use industrial-strength tooling without the need to acquire, train, and retain dedicated staff
- 24/7 coverage available
- Comprehensive threat intelligence across or within industries and verticals
- Flexible and customized services allow organizations to address specific requirements
- Ongoing partnership promotes knowledge sharing, skills growth, and collaborative incident management

(ISC)[2], Cybersecurity Workforce Study, 2021, https://www.isc2.org/Research/Workforce-Study

Flexible and Scalable Platform

The NetWitness® MDR Service enables companies to leverage NetWitness®XDR in a fully outsourced model, combining technology, planning, training, and managed detection into a single, complete offering. NetWitness® XDR delivers modular threat detection and response to advanced SOCs with modules available for network, logs, endpoints and IoT devices.

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