NETWITNESS

DATA SHEET

NetWitness® Orchestrator

Security Orchestration, Automation and Response

Overview

A security operations center is under constant pressure to reduce the time to respond to and remediate threats, while at the same time, increasing accuracy. To achieve this, an organization needs to optimize and orchestrate the people, process and technology that make up threat detection and response.

NetWitness® Orchestrator is a comprehensive security operation and automation technology that combines full case management, intelligent automation and orchestration, collaborative investigation, and tightly integrated threat intelligence. It brings consistency and efficiency to threat investigation, hunting and response.

By leveraging playbooks and integrated threat intelligence, NetWitness® Orchestrator not only enriches but also automates analyst workflow, collaboration, and response. By doing so, it can transform SOC operations into a repeatable, measurable and predictable business process.

NetWitness Orchestrator also integrates and coordinates NetWitness Platform XDR and a security operations team's entire security arsenal. It enables automated, bi-directional data flow to any security or business tool that is important to security analysts, vastly streamlining previously chaotic and inconsistent processes. In addition to harmonizing tools, data and technology, it coordinates the people and departments involved in security operations.

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

- Process-based case management that integrates all security, and relevant business and technical resources, in one application
- Automation of repetitive manual tasks to ease staff workload and let analysts focus on higher value activities
- Customizable workflows that assure all required investigative steps are executed and results are accurately documented
- Guided investigation that helps even junior personnel to successfully respond to threats
- Integrated Threat Intelligence management so that investigators are always well informed as they respond to incidents and conduct remediation
- Customizable response actions that can integrate with all of an organization's security controls and systems

Key Features

- End-to-end case management that supports repeatable, scalable, predictable and well documented security processes
- Highly scalable automation of repetitive manual tasks to free valuable human resources
- Increased response accuracy and reduced security impact
- Easily managed and applied threat intelligence that helps drive incident response
- Streamlined collaboration across teams and tools
- Automatic measurement and documentation of all response tasks and processes

Key Benefits

- Lower-level tasks no longer consume valuable resources
- Increased accuracy, repeatability and measurability of manual functions
- Always available and automatically applied threat intelligence
- Constant improvement of recurring processes
- Ability to empower junior analysts quickly
- Speedier response times and reduced errors, improving analyst productivity and minimizing mean time to remediation (MTTR)
- Automation that empowers software to do frequent, common tasks
- Orchestration and automation that can systematize decision-making
- Dashboard and reporting to visualize threat intelligence-driven metrics
- Incident management and collaboration that provides end-to-end investigation, response and improvement

Flexible and Scalable Platform

NetWitness® Orchestrator provides the security orchestration, automation and response required by modern security operations. It is offered as a standalone solution or an optional component of NetWitness XDR, which delivers modular threat detection and response to advanced SOCs. XDR product modules are 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