NETWITNESS

DATA SHEET

# NetWitness® Detect AI

## Cloud-native Analytics for Rapid Threat Detection of Sophisticated Threats

## Overview

The digital attack surface continues to expand rapidly and grow increasingly complex. This makes it harder for security teams to protect every asset from every threat vector, from commodity malware to state sponsored exploits and zero-day threats. Existing security monitoring technologies still produce too much data, too much noise, too many false alerts for overburdened security teams to sift through, and they often miss unknown threats.

NetWitness Detect AI is a cloud-native SaaS offering that uses advanced behavior analytics and machine learning to quickly reveal unknown threats and provide high-fidelity threat detection. It frees security teams to focus on actionable alerts by automatically flagging suspicious behaviors and anomalies that can signal the highest risk threats.

## Advanced analytics and high-fidelity threat detection using the power and scale of the cloud

NetWitness Detect AI applies advanced analytics and machine learning to data captured by NetWitness Platform XDR to deliver actionable threat detection.

### High-fidelity threat detection

NetWitness Detect AI's machine learning algorithms automatically and continually get smarter about your organization's user and entity behaviors. NetWitness data scientists tune and update the algorithms regularly so that it always provides accurate threat monitoring without requiring rules, signatures or manual analysis.

### Relief for security analysts

NetWitness Detect AI uses an innovative risk scoring model to alleviate analysts' alert fatigue by zeroing in on the highest risk indicators within noisy data environments.

### Quick, easy deployment

NetWitness Detect AI requires no additional hardware, which dramatically simplifies installation and ongoing management. Administrators and analysts don't need to manually tune algorithms, and with native SaaS benefits, stability is never an issue.

### Fast time-to-value

NetWitness Detect AI begins processing data the moment you turn it on. Within hours, it shows baseline behaviors so analysts can quickly understand anomalies. Within days, the system generates meaningful, high-fidelity, and actionable alerts.

## Key Features

- Innovative, dynamic statistical risk scoring model produces high-fidelity alerts with meaningful insights
- Intelligent peer grouping of anomalies provides additional context for understanding suspicious behavioral activity
- Massively scalable native SaaS application is capable of processing billions of daily events
- Patented unsupervised machine learning and behavioral analytics drives advanced and highly automated threat detection

## Key Benefits

- Reduces mean time to detect and respond with advanced analytics and machine learning that work right out of the boxs
- Frees up valuable time that analysts can spend investigating real business threats based on precisely tuned alerts
- Reduces your reliance on expensive hardware and data scientists
- Lowers your organization's risk profile by addressing a wide range of analytics use cases important to business leaders, including insider threats, employee misuse, sophisticated external attacks and more

## Flexible and Scalable Platform

NetWitness Detect AI is a cloud-native, big-data driven advanced analytics and machine learning solution that is an integral 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) and Log Detection and Response (LDR). 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