NETWITNESS

SOLUTION BRIEF

NetWitness® Platform for XDR

See every move intruders make, from when they cross preventative controls to when they attempt to steal data, and stop them in their path

You know how it happens.

The malware enters through a phishing email and slips past both the anti-virus software and the intrusion prevention system, neither of which recognize the malware's unique signature. Once on the network, the malware stretches out and makes itself comfortable. It moves laterally, performs reconnaissance, connects to a command-and-control server, identifies its target, then boom: credit card information on 127 million consumers disappears, a hospital's EMR system locks up or an entire city loses power.

You know why it happens: overwhelmed security operations teams, lack of visibility, siloed data, disparate security technologies, too many screens, too many alerts. The list goes on.

The question, then, is how do we stop it?

XDR: Extended Detection and Response

The NetWitness Platform for XDR enables organizations to more accurately and rapidly analyze, detect and respond to intrusions that have bypassed preventative controls as they cross the network and attempt to infect endpoints. Through a centralized and unique combination of network traffic analysis, behavioral analysis, endpoint analysis, data science techniques, and threat intelligence, NetWitness Platform for XDR detects known and unknown attacks and automates response. It utilizes intelligent metadata from across your network and endpoints to identify anomalies that may signal hidden and unknown attacker behaviors, such as the use of remote access tools, hidden tunnels and backdoors, as well as credential abuse and lateral movement. And it exposes the full scope of an attack by providing unparalleled network and endpoint visibility, connecting incidents over time, and delivering deeper insights through automated evidence abstraction and machine learning.

Analysts can now detect, investigate and truly understand the full scope of sophisticated attacks by leveraging an advanced analytics engine that applies NetWitness's unique combination of behavioral analysis, data science techniques and threat intelligence to discover both known and unknown attacks. The NetWitness Platform for XDR enables enterprises to connect incidents in real-time and over time, making it easier for security analysts to identify and stop attacks in progress, before they impact the business.

Capabilities and benefits

A single, unified platform for all your data. NetWitness Platform for XDR is the only XDR solution that normalizes data by combining threat detection analytics with network and endpoint telemetry, investigation and threat intelligence capabilities to defend against threats.

Integrated threat and business context. By adding business context to analysis, NetWitness Platform for XDR enables organizations to prioritize threats based on their potential impact. In addition, intelligence gathered from industry research, the organization's own data, and crowdsourced from NetWitness customers is fully aggregated and operationalized at ingestion to better detect the unknowns that are prime indicators of compromise.

Automated user behavior analytics. Our unique advanced analytics engine looks for potentially malicious issues across disparate data sets and correlates data across full network packets and endpoints, with a focus on all prime attack vectors for today's advanced threats. By analyzing all these data sources at the same time and searching for attack behaviors, NetWitness Platform can dramatically speed threat detection and response.

Rapid investigations. The NetWitness Platform for XDR provides an advanced analyst workbench where analysts can triage alerts and incidents, and it features an interface designed specifically for security investigations. The deep insight that the NetWitness Platform provides into data from across an organization's infrastructure allows analysts to natively and visually reconstruct a network attack or data exfiltration in its entirety. Moreover, it empowers analysts to connect incidents over time in order to expose the full scope of an attack.

Automation and orchestration. The NetWitness Platform for XDR facilitates both threat hunting and consistent, transparent and documented threat investigations by leveraging NetWitness Orchestrator's vast threat intelligence to automate detection of potential incidents, automatically collect pertinent evidence, and automatically complete tasks for quicker resolution and better efficiency.

Flexible, scalable architecture. You can deploy NetWitness Platform for XDR in the cloud, on premises or virtually. It scales to meet your organization's unique needs and security priorities, making it a good fit for SMBs and large enterprises alike.

End-to-end security operations. The NetWitness Platform for XDR fully operationalizes security end to end by unifying network and endpoint telemetry, advanced threat intelligence, and orchestration and automation.

About NetWitness

NetWitness, an RSA® Business, provides comprehensive and highly scalable threat detection and response capabilities for organizations around the world. The NetWitness Platform delivers complete visibility combined with applied threat intelligence and user behavior analytics to detect, prioritize, investigate threats, and automate response. This empowers security analysts to be more efficient and stay ahead of business-impacting threats. For more information, go to **netwitness.com**.

NetWitness Platform for XDR:

- Offers unparalleled visibility across user, endpoint and network data enriched with behavioral analytics and threat intelligence.
- Identifies new, targeted and unknown threats with real-time, data science and machine learning analytics so analysts can stop attacks in progress.
- Empowers security teams to accelerate investigations by monitoring in real time all traffic and endpoint processes.
- Empowers analysts to understand the full scope of an attack and be three times more efficient and effective at detection and response.
- Scales to meet the needs of SMBs and large enterprises.

NETWITNESS
An RSA Business