NETWITNESS®

WHITE PAPER

# NetWitness® XDR

## NetWitness IS eXtended Detection and Response

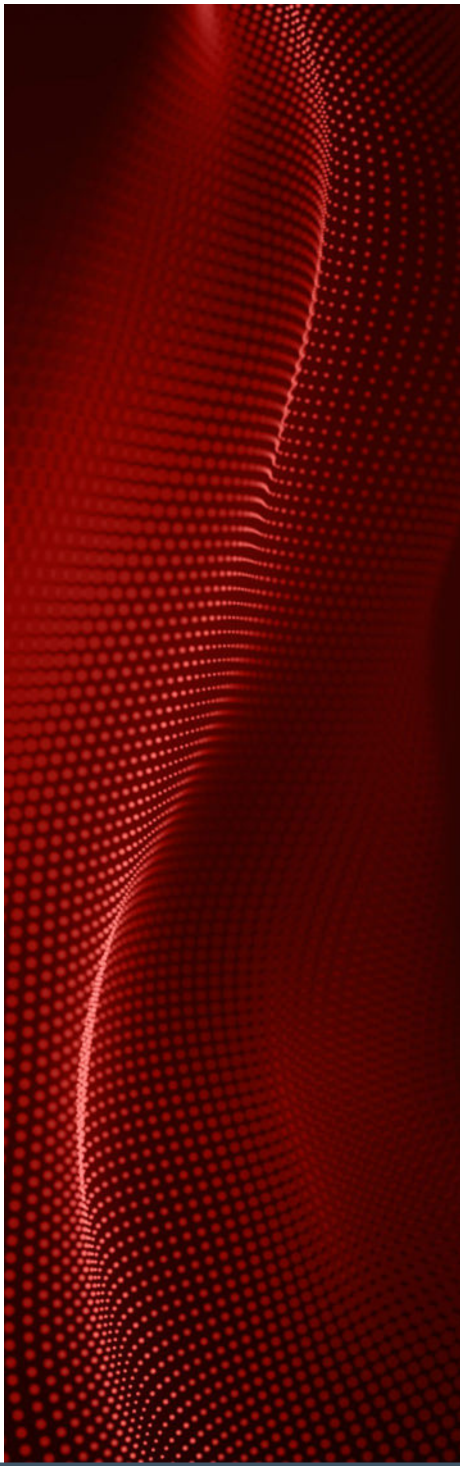
## The XDR Revolution

If you zoom out to the entire history of cyberthreats, and cyber defense, you can see how we got to where we are today, and where we are going in the future. At the global scale, organizations have invested untold amounts of money, yet still are attacked every day, often successfully. The increasing sophistication of threats is one big part of the problem, but so is the equivalent complexity in staging an effective cyber defense.

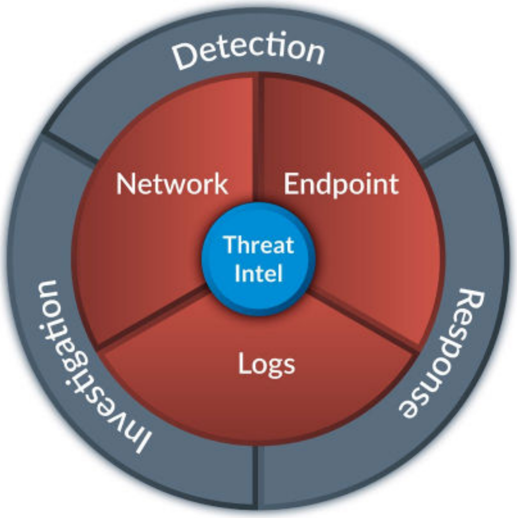
To get past this dilemma, we are going to need a solution that is comprehensive, effective, and simple. Over the past few years, a vision of this solution has emerged under the term eXtended Detection & Response, or XDR. Its basic principles are:

- A unified solution that integrates all security and IT (Information Technology) controls in one application
- Visibility across all data sources and deployment types, with the ability to correlate seamlessly among them
- Advanced analytics – AI (Artificial Intelligence) and machine learning – to detect sophisticated, stealthy threats
- Incident automation and orchestration capabilities, to increase efficiency and address the worldwide security skills gap
- Strong response and forensics capabilities to stop attackers when they strike, understand what happened, and remove them completely

XDR in fact describes capabilities and activities that SOCs (Security Operations Centers) provide today, but in often disjointed ways, across disparate tools and solutions. The promise of XDR is in simplifying the spectrum of processes – administratively and operationally – to the point where a security-conscious organization, on its own or through a service provider, can effectively protect against cyberthreats and suppress the risks imposed by these attacks.



## NetWitness XDR – Past, Present, Future



While the vision of XDR is forward-looking, it describes an architecture that NetWitness has been building for literally decades. Starting in 1996, when NetWitness began as a government-sponsored research project to inspect network packets for cyberthreats, and tools to detect and respond to them, NetWitness has iterated and innovated to keep up with the ever-increasing sophistication and velocity of attacks. Adding the ability to ingest logs and endpoint, along with a unified data model and automated analytics, NetWitness created the precursor to XDR called "Evolved SIEM." With the inclusion of security orchestration automation and response (SOAR), NetWitness now delivers all the integrated capabilities of XDR – while others are still assembling piece parts.

To reflect this leadership in the emerging XDR market, NetWitness has re-branded as NetWitness XDR with a new version that showcases its uniquely powerful support for all XDR use cases.

NetWitness Platform XDR 12 is the newest release of the venerable NetWitness security solution. Typically deployed as customer-managed software or hosted by MSSPs (Managed Security Service Providers), NetWitness Platform XDR is updated with a focus on unrivaled detection capabilities, to find threats before they can make a negative impact. With a tagline of "See Everything. Fear Nothing.", NetWitness Platform XDR is already protecting iconic organizations around the globe, empowering the most sophisticated SOCs with tools for visibility, insight, and action. The industry's best threat hunters rely on NetWitness Platform XDR to defend against threats and keep their organizations running.

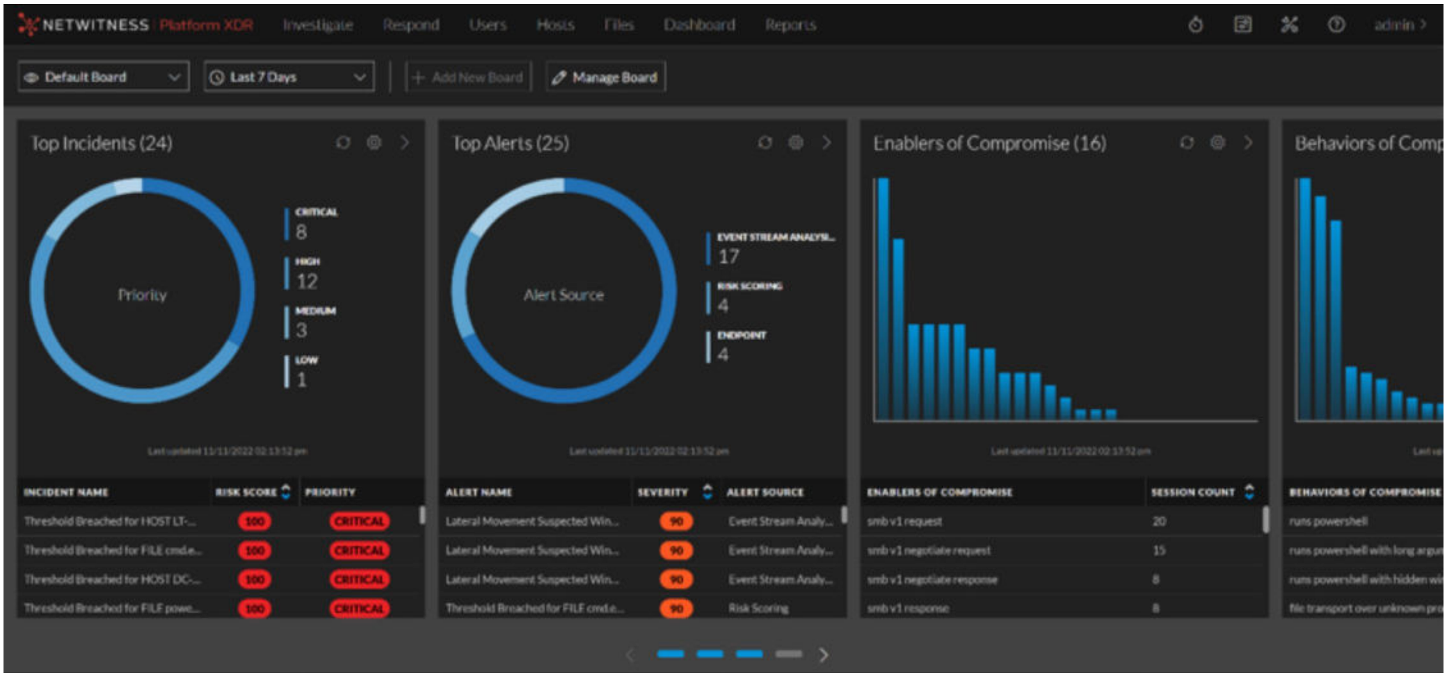
NetWitness XDR Cloud Services is a set of native SaaS applications that can be used with NetWitness Platform XDR. They add focused capabilities such as behavior analytics, threat intelligence, orchestration and automation, and characterization and risk ranking for assets connected to a network.

## The NetWitness XDR Difference

As the cybersecurity industry coalesces around the concept of XDR, NetWitness XDR has important differentiators beyond its radical visibility, advanced analytics, and incident response automation. With its heritage as a network-centric tool, NetWitness XDR is instrumented to take advantage of the fact that network traffic is the place that everything must touch. Endpoint and logs sensors are important for detecting changes and processes, correlating anomalies, and conducting investigations, but only work where they can be installed – an ongoing challenge with the explosion of systems and IP-based devices.

The "network-forward" approach makes NetWitness more powerful than other XDR solutions, particularly ones that are being built out by endpoint-focused vendors. Because NetWitness was designed from the start to handle massive volumes of data – many times more than SIEM or endpoints generate – it has evolved rich tools to search, correlate, and analyze the ever-increasing volumes generated by modern organizations. More data means more places for attacks to hide, and NetWitness XDR sees them all.

For threat hunters and security analysts, the NetWitness XDR interface is a single pane of glass for all the data in an infrastructure, across data center, virtualized, or cloud sources. It works well with all types of applications including Secure Access Service Edge (SASE), Cloud Access Security Broker (CASB), SaaS applications (e.g., Microsoft Office 365, Salesforce), identity systems, and the diverse security controls you see in all modern organizations.



| INCIDENT NAME | RISK SCORE | PRIORITY |
|---|---|---|
| Threshold Breached for HOST LT-... | 100 | CRITICAL |
| Threshold Breached for FILE cmd.e... | 100 | CRITICAL |
| Threshold Breached for HOST DC-... | 100 | CRITICAL |
| Threshold Breached for FILE powe... | 100 | CRITICAL |

| ALERT NAME | SEVERITY | ALERT SOURCE |
|---|---|---|
| Lateral Movement Suspected Win... | 90 | Event Stream Analy... |
| Lateral Movement Suspected Win... | 90 | Event Stream Analy... |
| Lateral Movement Suspected Win... | 90 | Event Stream Analy... |
| Threshold Breached for FILE cmd.e... | 90 | Risk Scoring |

| ENABLERS OF COMPROMISE | SESSION COUNT |
|---|---|
| smb v1 request | 20 |
| smb v1 negotiate request | 15 |
| smb v1 negotiate response | 8 |
| smb v1 response | 8 |

| BEHAVIORS OF COMPROMISE |
|---|
| runs powershell |
| runs powershell with long argu |
| runs powershell with hidden wi |
| file transport over unknown pro |

Other important NetWitness XDR benefits include:

- Unified Data Architecture (UDA) that converts and enhances data at the time of ingestion, for faster, more accurate machine analysis and human investigation
- Threat Intelligence Platform (TIP) to integrate and correlate multiple intelligence sources and optimize for specific environments
- Flexible deployment options, from on-premises to cloud-native, and everything in-between
- Advanced incident investigation and response tooling, with visualization, automation, and playbooks that enable fast, accurate action in addressing threats
- Access to relevant and timely content, with rich customizations that build value over time
- Real-world continuous testing by NetWitness Professional Services and Incident Response, working shoulder-to-shoulder with customers to combat attackers

## Open XDR for Today and Tomorrow

With its long history and global footprint, NetWitness XDR integrates directly with the world's most critical and widely deployed tools, and many specialized or industry-specific ones as well. Built and maintained by NetWitness and its partners, these integrations are open and customizable for any environment, and new ones are released continuously. Even new or unrecognized systems are supported by the capability to auto-parse feeds according to various standards and conventions, enabling security until specific integrations are developed – or even if they're not.

Nor is it required to adopt every NetWitness offering to gain its XDR benefits. Since each NetWitness Platform XDR offering contains the full back-end engine, organizations can start with any data source and add whenever they're ready. Similarly, it is straightforward to swap in an alternative SIEM, endpoint, or network system, and to use the NetWitness XDR engine as intended. This flexibility has always been part of the solution design and is valued by customers who wish to use other security tools on a temporary or even long-term basis.

Lastly, the industry is beginning to develop an "Open XDR" framework that automates the process of integration between components. While still in its infancy – and just an XDR-specific application of the "composable security" model that's been underway for a while – the idea of openness is baked into the NetWitness XDR architecture, and we are committed to supporting, and contributing to, open XDR standards that will emerge in the next few years.

## XDR for Everyone

NetWitness Platform XDR has always satisfied the most demanding SOC use cases and is the foundation of many of the world's most sophisticated SOCs. With the release of NetWitness XDR version 12, the power of NetWitness XDR is available to a wider range of organizations. Simplified and flexible deployment options, new content and visualization features, and SaaS and managed service capabilities make NetWitness XDR the choice for organizations of all sizes and types, delivering – for the first time for many – the ability to finally get ahead of the attackers and contain the risks that are keeping CISOs and CEOs awake these days. For SOCs that are seeking best-in-class XDR today and want to future-proof their systems going forward, NetWitness XDR is the clear choice.

For more information and a demo, contact **NetWitness XDR Sales** or your local NetWitness XDR partner.

## About the NetWitness Platform

NetWitness 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