NetWitness® Network

Complete network threat visibility for your IT infrastructure

Today's cyber attacks are unparalleled in sophistication, and organizations are failing to keep up. Businesses struggle to identify and prioritize threats as dwell time continues to increase. What options are available? Many depend on perimeter-based security solutions, but a modern approach means capturing all data that provides visibility into the actions, movements and tactics of threat actors in order to increase the ability to defend against attacks.

NetWitness® Network exposes network data to enhance a security team's capabilities to detect and respond to today's advanced threats with immediate deep visibility and efficient investigation and forensics. The NetWitness Platform's patented technology has unparalleled speed for real-time network data processing and behavior analytics to accelerate detection and investigation of threats as they traverse your network.

Visibility into all network data from the cloud to on-premises

NetWitness Network provides real-time visibility into network traffic in the cloud, on-premises and across virtual environments. It enables detection and threat hunting with streamlined workflows and automated investigation tools used to monitor the timing and movements of threat actors. NetWitness Network utilizes behavioral analytics, data science and threat intelligence to detect known and unknown attacks and speed response.

Advanced threat defense
Gain greater visibility, detect threats sooner and focus response more effectively

Intuitive investigation and forensics
Comprehensive investigation toolkit for forensic analysis

Accurate hunting with context and threat analytics
Real-time capture and enrichment of full network data or metadata

Deeper understanding of the full scope of an incident
See what happened with session reconstruction capabilities leveraging network visibility

Empower your analysts to be powerful threat hunters

Provide insight or angle about how the product/solution works and what makes it unique as it relates to its grander value proposition and range of capabilities and integration.

Key features

- Greater visibility to threats that traverse the network with advanced threat detection and streamlined investigation

- Comprehensive investigation toolkit for forensic analysis and a consolidated and comprehensive view to quickly investigate incidents

- Real-time capture and enrichment of network data guides threat hunters to quickly get to the root cause of an incident

- Gain a deep understand of incidents by leveraging comprehensive and continuous network monitoring and visibility

- Scale to meet your needs with flexible full-network packet or network metadata license models for forensics and detection use cases

- Can be deployed on premise on in the cloud, e.g., AWS, Azure or Google Cloud Platform

Key benefits

- Gain unparalleled speed for realtime behavior analytics through NetWitness patented technology that accelerates the detection and investigation of threats

- Enrich network data with business and identity context in addition to threat intelligence, which reveals the insights needed to follow the trail left by threat actors

- Enable accurate hunting with context and threat analytics that makes sense of large amounts of data and information

- Facilitate rapid analysis of all data with pervasive visibility across cloud and on-premises environments, enabling rapid detection, investigation, reporting and management of all network data

- Adheres to Common Criteria Certification for product security and is certified for the U.S. Department of Defense Information Network UC APL

NetWitness Network is an integral part of the NetWitness Platform, an enterprise grade, modular and flexible platform that meets the needs of customers as they evolve their security strategies. Together, the solution delivers the industry's most complete visibility across logs, network and endpoint data, helping to expose the full scope of attacks.

NetWitness Network allows analysts to hunt for threats without ever having to look at a raw packet again. It offers intuitive data visualizations and nodal diagrams—in addition to a complete set of automated detection, investigation and forensics tools—to transform every analyst into an experienced threat hunter. Pervasive visibility facilitates administration and analysis of data across distributed and virtual environments, enabling rapid detection, investigation, reporting and management of all network data. From the intuitive nodal views to the extensive and robust tools available for investigation, the tasks that an analyst must perform are all available within one platform so that an organization can understand the full scope of attacks and the risks they pose.
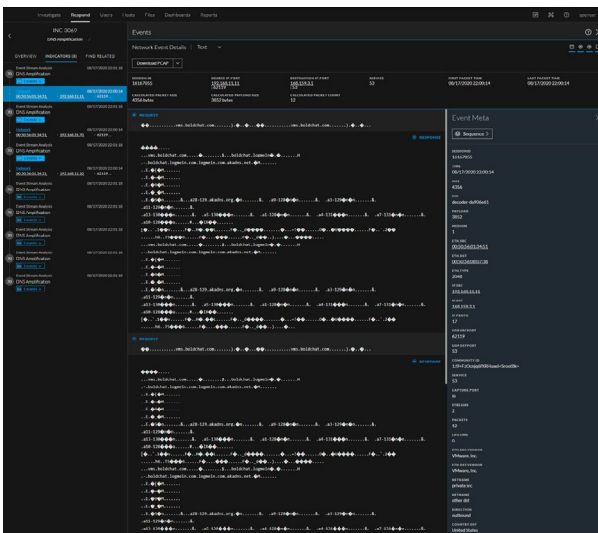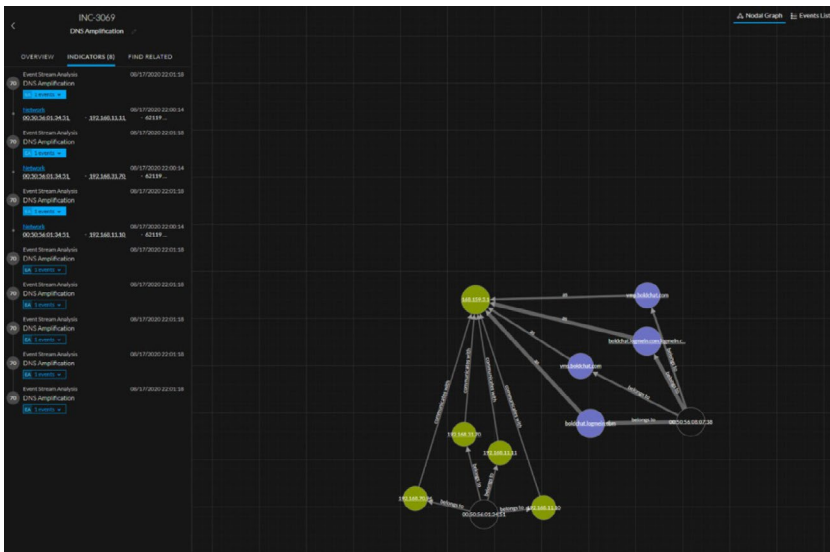
With a single click, dive deep into network details that inform an alert or incident

Quickly gain a visual understanding of an incident with nodal layouts and pivot into event details in a single click to fully understand network threats and digest event details in human-readable metadata

To learn more, visit the NetWitness Network webpage here.