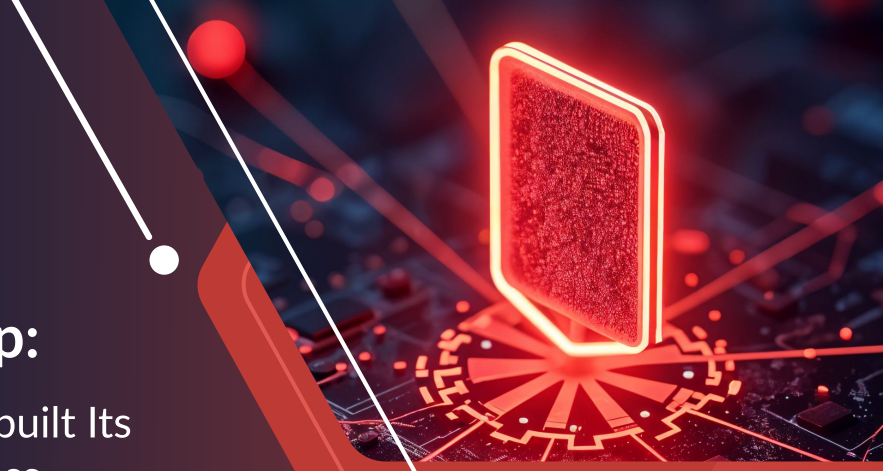
NETWITNESS

See Everything. Fear Nothing.



Closing the Evidence Gap:

How a Global Security Alliance Rebuilt Its Forensic Backbone with NetWitness

Case Study

Customer
Multinational security alliance

Environment
Highly sensitive, mission-critical networks

Solution
NetWitness NDR with full packet forensics

The Customer's Challenge

Blind spots in forensic visibility threatened mission-critical investigations.

The organization's mission depends on strong, resilient cyber defenses to support deterrence, crisis prevention, and collective security across its affiliates. However, within its most sensitive network environments, the organization faced a growing risk: insufficient network evidence to fully investigate and reconstruct sophisticated cyber incidents.

Adoption of deep packet visibility capabilities among analysts remained limited, while encrypted traffic volumes continued to grow. As a result, investigation teams increasingly relied on metadata and flow data rather than comprehensive network evidence - increasing the risk of incomplete investigations and limiting their ability to reconstruct sophisticated attacks. At the same time, the client needed to strengthen its overall security posture and ensure its network forensic capabilities were aligned with the demands of its mission-critical environment.

The risk was significant. Without access to comprehensive network evidence, security teams could miss ongoing malicious activity or critical indicators of compromise, face prolonged or incomplete investigations, and lose the ability to fully reconstruct attacker activity when responding to advanced threats.

The organization needed complete network visibility to reduce investigative blind spots and strengthen cyber resilience across critical operations.

Copyright © 2026 NetWitness Security LLC. All rights reserved

The Solution

When Stakes are This High, Metadata is Not Enough

In an environment where the consequences of incomplete investigations could be significant, relying on flow data alone was insufficient to establish the full sequence and nature of suspicious network activity. While flow data provides information about network connections, including communicating systems, timestamps, and traffic volumes, packet-level evidence allows analysts to examine the underlying network exchanges.

NetWitness remained the organization's strategic platform for deep packet visibility and advanced network forensics. Its capabilities enable investigators to analyze captured network sessions, reconstruct activity, and validate findings beyond aggregated telemetry, providing the investigative depth required in highly sensitive environments.

The decision was driven by the need to strengthen the organization's network forensics capabilities and ensure investigators had access to comprehensive packet-level evidence.

By expanding its NetWitness infrastructure, the organization increased its ability to capture, retain, and analyze full packet data across mission-critical environments. Unlike metadata alone, full packet capture gives the security team the complete context to investigate suspicious activity, detect anomalous behavior, reconstruct exactly what happened, and meet forensic and compliance requirements.

01 Go Beyond Flows (Access packet-level evidence)

02 Analyze Sessions (Examine network exchanges)

03 Reconstruct Activity (Trace suspicious behavior)

04 Validate Findings (Support evidence-based conclusions)

The Result

Expanded Full-Packet Forensic Capability for Mission-Critical Investigations

By enhancing its NetWitness deployment, the organization strengthened full-packet forensic coverage across its most sensitive network environments, giving investigation teams broader access to packet-level evidence for analyzing and reconstructing sophisticated network activity.

The expanded capability enables analysts to examine captured network sessions, reconstruct suspicious activity and validate findings against underlying packet evidence rather than relying primarily on metadata and flow data.

The engagement also establishes a foundation for the next phase of improvement, focused on analyst enablement, encrypted traffic analysis and platform performance optimization.

Do you want to know what NetWitness Platform can do for your complex environment?

Scan to Schedule a Demo

About NetWitness

Built for organizations where certainty matters most, NetWitness detects threats as they happen and gives security teams definitive answers when incident occurs. A pioneer in network forensics since 1997, NetWitness reconstructs attacks from full packets, endpoint and log data across IT, OT and cloud. Through AI reasoning and automation, every finding can be quickly verified. Governments, critical infrastructure operators and enterprises worldwide rely on NetWitness.

See Everything. Fear Nothing. Learn more at www.netwitness.com.

Follow us for regular updates

Website
www.netwitness.com

Copyright © 2026 NetWitness Security LLC. All rights reserved