NETWITNESS

NetWitness® SASE Integration

Unparalleled Full Network Visibility

The rise in distributed workforces requires the need for new technologies to support the trend. Secure Access Service Edge (SASE) and cloud migration offer cost savings and efficiencies, but present new security challenges, like visibility into encrypted traffic, remote users, and cloud workloads. Complete visibility across the entire attack surface is critical.

Eliminate blind spots. Strengthen your SASE security.

NetWitness addresses this problem by partnering with major SASE vendors on technical integrations that open up visibility, even for encrypted data, if desired. This supports not only SASE use cases, but critical hybrid use cases that look across on-premises and cloud data. Customers receive the best of both worlds: SASE flexibility and inherent security advantages, and full threat detection and response visibility.

Scalable, high performance cloud security

- Gain complete network visibility and threat detection across the entire enterprise, even portions you no longer control
- Detect and analyze all remote user network traffic with familiar on-prem mechanisms such as rules, parsers, feeds, and machine learning
- Log into a single user interface to perform a search or other interaction and quickly receive the results of network communications no matter where they originated
- Perform forensic examinations on a triggered detection and do threat hunting for unknown threats against retained network communications

Key Features

- **All remote user network traffic captured in near real-time**
- **Components can be hybrid, on-premises and/or in the cloud**
- **All data collected from anywhere is accessible to the detection engine and available for analyst interactions**
- **Customizable deployment limits risk of storing Personally Identifiable Information (PII)**

Working Together as a Single Solution

NetWitness' SASE integrations enable organizations to retain full visibility into their cloud security stack, cost-effectively eliminating blind spots in their cloud traffic and maximizing the effectiveness of their security infrastructure investments. Organizations have the visibility and control they need over encrypted traffic to ensure compliance with their privacy, regulatory, and acceptable use policies, whether on-premises or in the cloud.

Single User Interface	The NetWitness SASE integration structure supports a hybrid scenario, where some elements are on-premises and others in the cloud, enabling analysis of data no matter where it is collected. Analysts can log in to a single user interface to perform index searches, pivoting through metadata, and reconstructing network sessions to quickly receive results.
Retention of Raw Network Communications	Empower analysts to perform forensic examination on a triggered detection and threat hunt for unknown threats against retained network communications. All original network packets for remote user connections are retained.
Correlation of Disparate Data Sets	Analysts enrich the context of their investigations by correlating detections from the actual network traffic of remote access users with other access by that same user to receive a complete the end-to-end story of what transpired.
Storage Optimization	NetWitness strives to minimize customers' operating costs by using new compression algorithms, selective retention, and splitting network decoder components to limit what must run in the cloud.

NetWitness Professional Services — Committed to Your Success

NetWitness offers the services to support the ongoing success of security operations teams. These range from SOC design, implementation, and training, to managed detection and response (MDR) and major incident response (IR). IR Retainer Services ensure rapid response in the event of a major attack or breach.

NetWitness SASE integrations give customers the best of both worlds: SASE flexibility and security advantages, with full threat detection and response visibility.

Ready to learn more? Visit www.netwitness.com

NETWITNESS