
# Can Your SIEM Do This?

The NetWitness® Platform is more than a SIEM, it is a holistic view of your infrastructure—from the endpoint to the cloud—that allows you to quickly identify and respond to the threats that matter. The NetWitness Platform was designed to be the foundation of your security strategy, the hub that easily connects with your suite of security tools. It reduces dwell time and provides a prioritized view that encompasses the full scope of the threat.

## The power of full visibility

If you can't see it, you can't detect it. Other SIEMs are heavily reliant on logs and are blind to the cloud. The NetWitness Platform consumes disparate data from across your entire network and makes it intelligent in real time. Network packet data sees everything. Deep endpoint data, at the kernel level, identifies if a file is behaving differently on disc vs. in memory. Indexing and correlation capabilities extend across metadata from all these sources, so analysts can detect known and unknown threats, see the complete scope of an attack, and reduce business impact.

## Why good enough isn't good enough

Not all packet capture technology is created equal. Solutions that only start capturing data when an alert triggers only give you partial ability to investigate an attack and have no ability to detect the threats that may be flying under the radar. The NetWitness Platform captures and enriches full network packet data, along with other data sources, and creates a uniform metadata model across all data types, allowing you to find the attacks that logs miss.

## Compliance is the by-product of security done right

Because the NetWitness Platform captures, retains, and archives data to support your security needs, you are already prepared for an audit and enabled to share your out-of-the-box compliance reports with regulatory bodies.

## See the threats that matter

The NetWitness Platform is the only solution that allows you to see everything with point in time identification, real-time analytics, and full historic data from across your entire network. When your team spends less time digging they have more time to look ahead and operate strategically.

## Incident response done right

NetWitness has your back. When an incident happens, you can count on our IR team to respond immediately and comprehensively to close the breach and reestablish security. In fact, organizations around the world use NetWitness for their own internal IR needs. Our IR team is one of the few in the industry certified by the NSA.

## More visibility means better detection and response

The NetWitness Platform provides the deepest and broadest visibility through Logs, Packets, and Endpoint to help you define "how bad is it." Logs identify something has gone wrong. Packets actually tell you what occurred. And Endpoint gives you deep insight into each and every machine on and off your network.

## Find the full scope of the threat

It's about connecting the dots in real time so you don't miss something. And, you can't do that without end-to-end visibility and behavior analytics to find the threats that would normally fly under the radar. Once you understand the full scope of what you are dealing with, you need to take prioritized action to stop an attacker before damage is done.

NETWITNESS

**Visit NetWitness.com to learn more**