Forbes

NetWitness Brings Enterprise Level Security to Remote Workforces

Tod Ewasko, CPO

Wayne Rash / Contributor
Wayne Rash is a technology and science writer based in Washington.

Forbes

April 6, 2023

The remote workforce that accompanied the recent Covid-19 pandemic resulted in a number of compromises in how companies work, especially in some critical areas such as security. Because employees were now working from areas that were not secure, such as their homes, this meant that security needed a new approach that would encompass the new environments.

One such approach is NetWitness, which delivers an extended detection and response suite of products that use Secure Access Service Edge (SASE) integrations with leading vendors of enterprise products. This results in a secure platform that is location independent, so data can reside in the cloud, on the computer of a remote employee or in a data center. This also means that manual data log inspections, usually required for enterprise level security, may no longer be necessary.

"Packet-level information has always been known as the truth serum in the security operations center," said chief product officer Tod Ewasko. "No matter what or how, if you parsed and stored the packets, you know what happened in real time. To fully appreciate this, it's important to understand that prior to this technology, data packets would need to be manually inspected from a log after that data had already utilized the network. Now, those inspections happen in real time; data is relayed to point of presence for inspection, then forwarded through the network."

By using the point of presence, NetWitness also provides improved visibility of the data as it passes through the network. "It's truly unsurpassed visibility that supports the full range of data types and sources, including logs, packets, NetFlow and endpoints, hosted in on-premises, virtualized, or cloud environments," Ewasko said.

> **"Our incident response focuses on the clues that attackers leave behind - and they all leave clues"**
>
> Tod Ewasko, CPO

The Rise of Ransomware

The rise of ransomware and the increasing sophistication of malware in general fostered by organized crime and adversarial nation states has added to the risks. NetWitness says it can detect and fight these risks by watching activity through logs, full packet telemetry and endpoint telemetry. The company says it uses advanced threat intelligence and security operations to create what Ewasko calls "end to end" security.

NetWitness accomplishes this by browsing packet level information. If that produces evidence of a potential threat, then the company takes action while minimizing the opportunity for an attack.

"Our incident response focuses on the clues that attackers leave behind - and they all leave clues," Ewasko explained. He said that experts at NetWitness watch for anomalies, analyze the tools and procedures of the potential threats and use that to identify what assets are being targeted.

NetWitness uses cloud based analytics and machine learning to detect unknown threats, and to provide anomaly detection for analysts to use, and it can use behavioral analysis and threat intelligence over time to expose the full scope of an attack.

Wayne Rash is a science and technology writer based in Washington, DC. He's a columnist for eWEEK and writes for PC Magazine.