NETWITNESS

PRODUCT BRIEF

NetWitness Cloud SIEM

Enterprise Security and Compliance as a Service

NetWitness is the tool of choice for some of the world's biggest and most security-sensitive organizations. For nearly 25 years, NetWitness has enabled professional threat hunters to detect and respond to threats, even as the cyber environment has grown ever more impactful and sophisticated.

SIEM logs are a key data source for any cyber-defense efforts, and also serve an important role in a strong compliance program. A large, complete, centralized repository for log data is essential to ensuring quality threat detection and regulatory reporting and compliance functions. That's why, for most organizations, SIEM is core technology like firewalls and intrusion prevention systems (IPSs).

However, SIEM deployment and management can impose significant demands on IT staff. Data volumes can be very large, requiring careful planning for storage, as well as the deployment of high-end hardware for the ingestion and investigation components. Like any server-based solution, SIEM requires IT support for patches and version upgrades, and procurement support for both hardware acquisition and software licenses.

With IT resources stretched in many organizations, there's a growing desire to outsource functions where possible. NetWitness Cloud SIEM is an ideal solution for this requirement because it delivers world-class SIEM capabilities in a single, usage-based license, rapidly deployable, and without IT involvement.

You might say, "There are lots of cloud SIEM offerings out there. What makes NetWitness Cloud SIEM different?" The answer is in the SIEM component, not the cloud component.

NetWitness Cloud SIEM is part of the NetWitness Platform, a leader in enterprise-grade threat detection and response. Corporations and government agencies around the globe use NetWitness to address demanding security requirements. Skilled threat hunters choose NetWitness as their go-to solution, due to its abilities to rapidly analyze and process huge volumes of information from many different sources. And exacting compliance teams have long depended on NetWitness to store vast amounts of data while providing fast access in supporting compliance activities.

Other cloud SIEMs have taken a different approach. There are advantages to cloud, as noted above, but to leverage them completely, you need SIEM technology that

has already been hardened and battle-tested through years of real-world use in the most challenging environments. Many cloud SIEM vendors started with the cloud component and are still working out SIEM feature/function and scalability.

NetWitness Cloud SIEM provides the opportunity to build your security and compliance capabilities through integration with other parts of the NetWitness Platform, including the growing number of cloud components. NetWitness Detect AI provides large-scale analytics, and RSA IoT Security Monitor adds Internet of Things devices into your cybersecurity and compliance processes.

Easy to Acquire, Easy to Deploy

NetWitness Cloud SIEM is packaged as a single subscription license, including software, infrastructure, support, and upgrades. Setup is a simple web-based process that can be performed by internal staff or procured as a service from RSA. Support is provided by NetWitness and all patches and upgrades are provided automatically.

Licenses are tiered based on the 90-day retention volume of data ingested by the SIEM, with longer retention periods available as an add-on purchase. Licenses start as small as 50 GB/day and are tiered in 10 GB increments, while discounts grow with volume. Like its on-premises counterpart, NetWitness Cloud SIEM scales to support the largest SIEM data sets in the world.

NetWitness Cloud SIEM is a worldwide offering. For details and a quote, please contact your NetWitness seller or authorized NetWitness partner.

About NetWitness

NetWitness, an RSA® Business, provides comprehensive and highly scalable threat detection and response capabilities for organizations around the world. The NetWitness Platform delivers complete visibility combined with applied threat intelligence and user behavior analytics to detect, prioritize, investigate threats, and automate response. This empowers security analysts to be more efficient and stay ahead of business-impacting threats. For more information, go to netwitness.com.

NETWITNESS
An RSA Business