Sponsored

LogRhythm®

ON-PREM SIEM VS CLOUD NATIVE SIEM

SIEM: WHICH ONE IS RIGHT FOR YOU?

INTRODUCTION

Determining the "best" SIEM option is not straightforward as it varies based on each organisation's specific needs. Factors such as specific security requirements, compliance obligations, data privacy concerns, and available resources play a significant role in this decision.

Both on-prem and cloud-native SIEM solutions have distinct benefits and drawbacks, and the right choice for a business depends on its overall security strategy and operational needs.

Ultimately, the right choice for a business depends on aligning the SIEM solution with its overall security strategy and operational needs. It requires a holistic view of the organisation are subject to change.

Here we set out the key differences in this simple comparison table.

COMPARISON CHART

Feature	On-Prem SIEM	Cloud-Native SIEM
Control	High control over data and security infrastructure.	Less control due to reliance on third-party providers.
Customisation	High degree of customisation possible.	Limited customisation due to central management by the service provider.
Compliance	Easier to meet industry-specific compliance needs.	May not meet all compliance requirements due to third-party policies.
Data Sovereignty	Data stored within the organisation's environment.	Potential challenges in meeting data sovereignty requirements.
Cost	Higher upfront costs for hardware, software, and maintenance.	Lower upfront costs, but ongoing subscription fees.
Complexity	Complex installation and management may require specialised skills.	Simplified management, often user-friendly and accessible.
Scalability and Flexibility	Limited scalability; requires hardware/software changes for expansion.	High scalability; easy to adapt to changing needs without altering physical infrastructure.
Access	Typically accessible only within the organisation's network.	Accessible from any location with internet connectivity.
Maintenance	Requires in-house maintenance and upgrades.	Maintenance and upgrades handled by the service provider.
Deployment and Updates	Potentially slower deployment; manual updates and configurations.	Faster deployment and automatic updates due to cloud-based automation.
Skills Required	Need for in-house expertise in installation, configuration, and management.	Reduced need for specialised skills for infrastructure management.

LogRhythm Axon, traditionally known for its strong presence in the on-premises SIEM market, has strategically positioned itself in the cloud-native SIEM arena.

This transition marks a significant shift, aligning with the growing demand for flexible, scalable, and maintenance-free security solutions. By leveraging its robust experience in handling complex security data and threat management on-prem, LogRhythm Axon now offers these capabilities through a cloud-based model.

This move not only enhances its appeal to organisations looking for cloud-native efficiencies but also retains the depth and sophistication of its original on-prem solution.

The evolution of LogRhythm Axon into the cloud-native space represents a response to the evolving cybersecurity landscape, aiming to meet the needs of modern organisations that prioritise agility, scalability, and seamless integration with cloud-based operations.

Whichever way your strategy takes you, LogRhythm have the expertise to guide you through.

Why not take them upon their offer of time with their specialist via this SIEM **Cloud Clinic** to discuss your options.

www.thecloudcommunity.net