Six Reasons Why SIEM May Remain On-Premises to Power Security Operations

As threats evolve, many organizations are reassessing where and how they run their security operations. Cloud-based security information and event management (SIEM) platforms, including New-Scale SIEM, are an attractive option for many enterprises. However, for organizations in regulated sectors, those operating mission-critical or air-gapped networks, or teams that need maximum control over their data and costs, an on-premises SIEM remains a strategic choice.

This guide is for security leaders evaluating a move to a cloud SIEM who want to weigh the advantages of remaining on-premises. It highlights the top reasons organizations continue to rely on on-premises SIEM deployments like LogRhythm SIEM: full control of data and infrastructure, predictable costs, flexible integrations, compliance alignment, and consistent performance. By understanding these drivers, you can make an informed decision about the right SIEM architecture for your organization.

Introduction

Security operations are under more pressure than ever. Cybercrime costs are estimated to be in the tens of trillions of dollars annually, and the average cost of insider threats has climbed to $17.4 million. Security teams are struggling to keep up with the surge in attack volume and complexity. Analyst burnout is common, with 84% of cyber security professionals reporting it and over half quitting for that reason. SOC teams are suffering from alert fatigue to the point that 62% of SOC alerts are being ignored as teams struggle to separate real threats from noise.

This combination of rising threats, limited staff, and complex compliance requirements is pushing CISOs to rethink their SIEM platforms. The question is no longer "should we modernize our SIEM?" but "where should it live?"

Cloud-based SIEM platforms offer compelling advantages like managed infrastructure and elastic scalability. Yet many enterprises, particularly in regulated industries, are choosing to stay with on-premises SIEM deployments. Their reasons are pragmatic: maintaining direct control over sensitive data, avoiding unpredictable cloud costs, and ensuring compliance with strict data residency mandates.

The right deployment choice is critical. A SIEM is the hub of a security operations center (SOC), and the wrong decision can create visibility gaps, runaway costs, and operational disruptions. This guide explores six key drivers for keeping your SIEM on-premises, helping you make a strategic decision that fits your organization's needs.

1. Complete Control Over Data, Deployment, and Performance

For many security leaders, control over data and infrastructure is non-negotiable. An on-premises SIEM allows your organization to own every aspect of its security environment, from where log data resides to how the system is tuned. This is critical for industries that handle highly sensitive information, including financial services, government, and healthcare, where a single misstep in data handling can cause regulatory risk or reputational damage.

You can deploy an on-premises SIEM as a preconfigured appliance for rapid installation or as self-hosted software on existing hardware for maximum customization. Both approaches let you define retention policies, manage encryption keys, and govern user access according to your internal policies rather than a cloud vendor's shared responsibility model. This is particularly important for meeting strict data residency mandates.

This control extends to operational performance. Your teams can fine-tune the SIEM's architecture, allocate resources based on log ingestion patterns, and optimize for peak workloads. Because the system is under your control, performance is not impacted by external connectivity issues or multi-tenant cloud noise. This autonomy is essential in mission-critical environments, including air-gapped or partially connected networks, where any loss of visibility creates unacceptable risk. This level of ownership means you know exactly where data lives, who can access it, and how it is processed.

2. Predictable Costs and Transparent Licensing

Cost predictability a compelling reason to maintain an on-premises SIEM. Cloud-based SIEMs often have usage-based pricing that can result in unpredictable monthly bills as log sources grow or incident volumes spike. This variability makes it difficult to forecast security budgets and justify ongoing investment.

An on-premises SIEM provides a stable, transparent pricing model. Whether delivered as a dedicated appliance or self-hosted software, you can plan for capital expenditures and avoid surprise costs related to data egress or long-term retention. This approach lets you scale coverage and add new data sources without worrying about escalating monthly fees.

In addition, an on-premises SIEM consolidates multiple functions, including log management, compliance reporting, and automated response into a single platform. This reduces the need for separate point solutions and lowers overall operational spend. When combined with unlimited or high-capacity data ingestion models, you can achieve a lower total cost of ownership while maintaining deep visibility. For executive stakeholders, predictable costs also mean a clearer return on investment, positioning the SOC as a value-driving function rather than a cost center.

3. Simplified Compliance and Audit Readiness

Meeting compliance requirements is a constant priority. Regulations such as PCI DSS, HIPAA, SOX, GDPR, and CMMC continue to evolve, and failure to comply can result in steep fines, reputational damage, or operational disruption. An on-premises SIEM helps you stay ahead of these mandates by providing full control over data handling, retention policies, and reporting processes.

Most modern on-premises SIEMs include content that simplifies compliance efforts. Built-in rules, dashboards, and reports aligned to common regulatory frameworks reduce the manual work required from SOC teams. By centralizing log collection and correlation, the SIEM creates a single, reliable audit trail for regulators, helping teams prove compliance more quickly.

Audit readiness also improves when you control the infrastructure directly. Your security teams can ensure that evidence is stored according to internal policies, that retention periods meet regulatory timelines, and that access to sensitive data is limited to authorized personnel. This assurance makes compliance reporting faster and lowers the risk of audit findings that require costly remediation. For CISOs, this transforms compliance from a burdensome exercise into a strategic advantage, strengthening trust with executives, boards, customers, and regulators.

4. Greater Security Operations Efficiency

While cloud SIEMs can reduce infrastructure management overhead, an on-premises SIEM offers efficiency through control and customization. When tuned correctly, it can dramatically reduce noise and speed investigations.

Because your organization owns and operates the system, teams can adjust correlation rules, detection thresholds, and analytics models to match the environment. This fine-tuning allows teams to suppress irrelevant alerts, enrich events with local context, and surface only the most meaningful incidents. The result is fewer false positives and a clearer signal for analysts.

Performance consistency is another advantage. Query speed, dashboard responsiveness, and correlation times are not dependent on shared cloud resources or external connectivity. With an on-premises SIEM, investigations run at full speed even during peak usage periods or in partially disconnected networks. Finally, local control of automation means playbooks and response actions can execute instantly. Actions like blocking an IP or disabling an account do not depend on external API calls, reducing delays during a critical event. These advantages improve mean time to detect and respond (MTTD/MTTR) without requiring additional headcount.

5. Full Integration and Ecosystem Control

Modern security environments rely on a broad mix of tools, from EDR and NDR to SOAR and threat intelligence feeds. An on-premises SIEM lets you control how these tools integrate and exchange data. This flexibility is critical for building a best-of-breed security stack rather than rely on a single vendor's proprietary ecosystem.

Because the SIEM is deployed inside your infrastructure, you can choose which data sources to collect, how to normalize them, and how to enrich events with local context. Open APIs and broad log source support ensure the SIEM can keep pace with legacy systems and modern cloud workloads.

Local control also reduces latency when integrating with other security tools. If an investigation requires pulling additional context from an EDR solution, the request does not need to traverse the public internet. By maintaining control of the security ecosystem, your SIEM can work in harmony with your unique workflows and risk priorities. This creates a security operations environment that is more efficient an resilient to vendor lock-in.

6. Long-Term ROI and Stability

When evaluating SIEM strategies, cost over time is just as important as initial purchase price. An on-premises SIEM offers financial predictability and stability that can be difficult to achieve with usage-based cloud models. Because infrastructure is owned or leased upfront and licensing is typically fixed tiers, you can plan budgets years in advance.

Over the life of the platform, this predictability often translates into a lower total cost of ownership (TCO). High-capacity ingestion models allow security teams to collect more data without worrying about overage charges. Consolidating multiple security functions into a single SIEM also eliminates the need for separate point tools, which reduces licensing, maintenance, and training costs.

Return on investment is not just measured in dollars. A well-tuned on-premises SIEM delivers measurable improvements in security outcomes, including faster detection, fewer false positives, and shorter investigation cycles. These outcomes help prevent costly breaches and reduce the business impact of security incidents. Finally, an on-premises SIEM provides long-term operational stability. You are not dependent on a vendor's cloud roadmap, service uptime, or pricing changes. You control when upgrades occur and how the system scales, allowing your SIEM to adapt to new threats on your own timeline.

Category	On-Premises SIEM	Cloud-Based SIEM
Data Control	Full ownership of data; full control over retention, encryption, and access policies	Shared responsibility model; data stored in provider infrastructure
Deployment and Performance	Choice of appliance or self-hosted software; consistent performance for all environments	Faster to deploy, but may introduce latency; performance depends on connectivity
Cost Predictability	Stable, predictable costs with upfront CapEx and transparent licensing	Variable costs based on data ingestion, storage, and usage
Compliance Alignment	Direct control over evidence storage and retention to meet strict mandates	Provider may offer compliance certifications, but less control over residency
Integration Flexibility	Freedom to integrate with best-of-breed tools, no vendor lock-in	Easy integration with cloud-native tools, may favor vendor ecosystem
Maintenance	Requires internal resources for scaling, upgrades, and patching	Infrastructure management handled by provider

Table 1: A comparison of on-premises and cloud SIEM

Conclusion

Cloud SIEM platforms have brought important innovations to the security operations space. They offer managed infrastructure, elastic scalability, and the convenience of a solution that can be accessed from anywhere. For many organizations, especially those with limited IT staff or rapidly changing environments, these benefits make cloud SIEM an appealing option.

However, as this guide has outlined, there are significant advantages to maintaining an on-premises SIEM. Total control over data and performance, predictable costs, simplified compliance, and ecosystem flexibility are all compelling reasons why many organizations continue to operate on-premises.

The decision is not about which approach is better, but which aligns most closely with your organization's risk tolerance, compliance requirements, and budget. The goal is to build a security operations environment that enables you to detect and respond to threats effectively, maintain compliance, and demonstrate value. For many enterprises, an on-premises SIEM continues to deliver those outcomes with a level of control and assurance that cannot be easily replicated elsewhere.

Next Steps

- **Compare the LogRhythm SIEM and New-Scale SIEM data sheets.**
- **Schedule a demo to see how an on-premises SIEM can meet your security goals.**

About Exabeam

Exabeam is a leader in intelligence and automation that powers security operations for the world's smartest companies. As a global cybersecurity innovator, Exabeam provides industry-proven, security-focused, and flexible solutions for faster, more accurate threat detection, investigation, and response (TDIR).

exabeam

Learn more at www.exabeam.com →