LogRhythm®

What To Look for When Purchasing a Cloud-Native SIEM

10 Factors That Will Make or Break Your SecOps Success in the Cloud

Contents

The Advantages of a Cloud-Native SIEM Approach

While some security teams continue to favor self-hosted security information and event management (SIEM), a growing number of organizations are making a strategic shift to cloud-native SIEM platforms.

Embracing a cloud-native SIEM unlocks many advantages, including:

- Faster and simpler initial deployment with a quicker time to insight
- Greater ability for analysts and engineers to focus on finding and responding to cyberthreats
- Reduced ongoing operational complexity
- Access to advanced security techniques that harness cloud computing resources
- Frequent access to new features without complex upgrade cycles

But for most organizations, the difference between success and failure with a cloud-native SIEM comes down to the characteristics, capabilities, and cultural fit of the vendor they choose. The following are ten success factors that are critical to consider when evaluating cloud-native SIEM vendors.

Success Factor 1

Ease of Data Ingestion and Integrations

Your SIEM approach depends on extensive access to logs and other security data from all of your on-premises and cloud environments. It’s important to evaluate how robust and user-friendly your prospective cloud-native SIEM’s data ingestion capabilities are. This should start with the number of formal partnerships and out-of-the-box integrations the vendor has with your existing security tool. You should also ensure that the vendor supports a diverse set of data ingestion techniques, including cloud collectors, agents, and API and webhooks integrations, along with user-friendly mechanisms for creating custom data parsing policies when necessary.

> “Coming from an on-premises Splunk implementation, we were shocked by how quick and easy it was to integrate all of our security data sources, including some that are quite specialized. We had our data flowing to the cloud and were accessing meaningful dashboards and analytics in about a month.”
>
> **Commercial Director, Healthcare**

Success Factor 2

Threat Detection Completeness, Accuracy, and Flexibility

The principal function of a cloud-native SIEM is to enable comprehensive, accurate, and efficient detection of security threats. It's critical to challenge the SIEM vendors you are considering to demonstrate the efficacy of the techniques they use to surface the threats that matter most to your organization. Take the time to understand how the vendor prevents visibility gaps, minimizes false positive alerts, and avoids false negatives. Pay particular attention to how well the solution links disparate data points in useful and intelligent ways. Sophisticated out-of-the-box detection methods should be complemented by the flexibility to customize detection rules to your organization's unique needs.

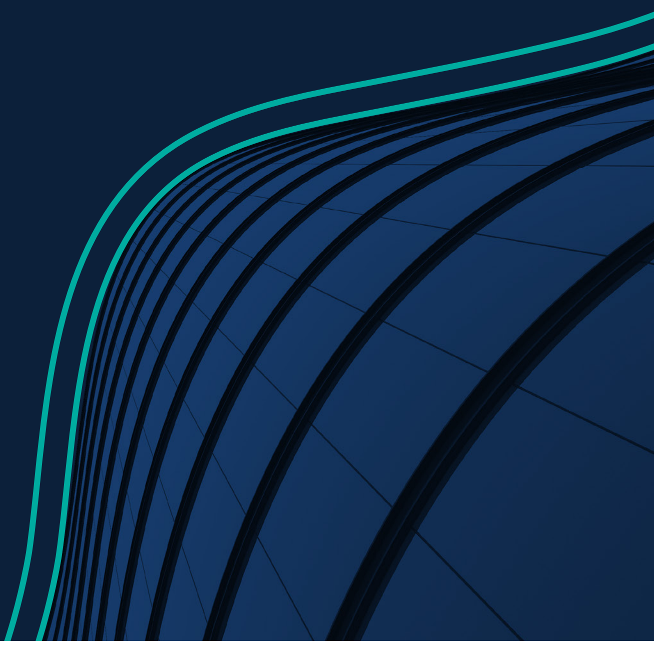
Success Factor 3

Analytics and Reporting Capabilities

In addition to its criticality when an active security incident is unfolding, the data and insights derived from your cloud-native SIEM platform can also play an important role in your overall security strategy and ongoing threat hunting activities. But effectiveness in these areas requires powerful and user-friendly analytics and reporting capabilities. Ideally, your cloud-native SIEM platform will include dashboards that provide a top-level view of your security posture and flexible and intuitive interfaces that integrate with search functionality. When evaluating these capabilities, assess the flexibility and customizability of dashboards, along with the data visualization techniques available to use for individual dashboard widgets.

Success Factor 4

Integrated Incident Response Workflows



When looking for a cloud-native SIEM, combining threat detection with integrated tools for managing the response process is ideal. This will enable an advanced security operations model where security analysts and incident responders can move swiftly to respond, contain, and recover from incidents using a systematic approach with clear prioritization and communication among stakeholders. Effective and user-friendly capabilities in this area will also make it faster and easier to onboard new security personnel and avoid analyst frustration and burnout.

Success Factor 5

Data Normalization, Enrichment, and Searchability

Much of the effectiveness of a cloud-native SIEM hinges on how it can extract meaningful insights from large volumes of raw security event data. For this reason, it's essential to evaluate the techniques that your prospective SIEM vendor uses to normalize and enrich the data they ingest. Closely scrutinize how effectively the vendor uses automation to bring varying data types into a consistent format, extracts and organizes meaningful metadata, and enables searchability. Search capabilities should include support for basic search operators, as well as more sophisticated queries that include compound search operators, separators, and regular expression operators. When evaluating search capabilities, you should also look for analyst convenience features such as assisted search wizards, saved searches, search history views, and auto-refresh capabilities.

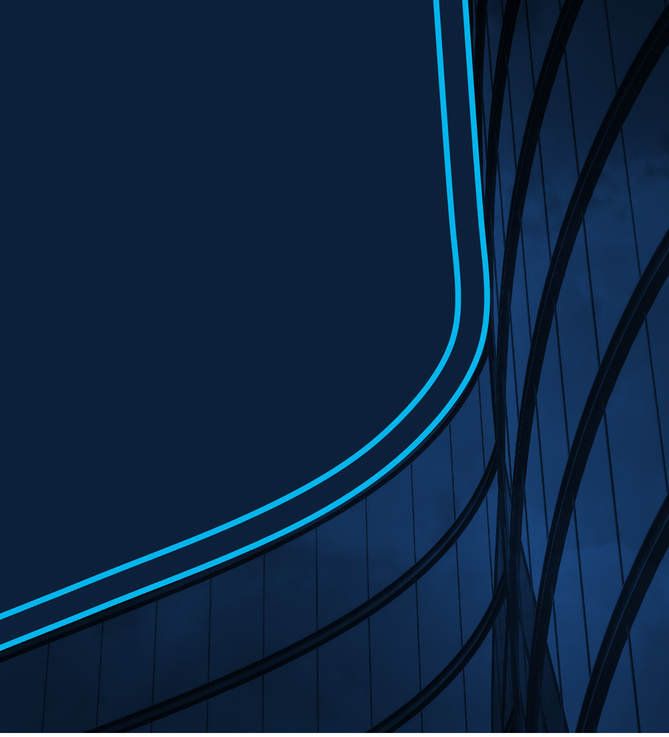
Success Factor 6

Security Framework Mappings

Mapping security operations practices to specific industry frameworks like MITRE ATT&CK® can be a complex and time-consuming process. A cloud-native SIEM vendor may be able to simplify and accelerate this process by providing out-of-the-box modules for specific cybersecurity frameworks and best practices. Explore your prospective cloud-native SIEM vendor's capabilities in this area and look for relevant case studies in your organization's industry for proof points of real-world success.

Success Factor 7

Access to Specialized Support and Services Expertise



One of the key advantages of a cloud-based SIEM platform is that it puts significantly less burden on in-house teams to deploy, customize, and operate than traditional on-premises software; however, this does not eliminate the need for effective support and services from your vendor of choice. The difference is that rather than relying on your SIEM vendor for administrative functions like on-premises platform deployments, maintenance, and upgrades, you can instead engage your vendor's specialized expertise for higher-value activities. While your goal should always be to operate as self-sufficiently as possible, a cloud-native SIEM vendor with strong support and professional services capabilities can help you accelerate your time to value and work with you on an ongoing basis to maximize the value of your investment.

> "We're a small team that is pulled in many directions, so we needed to see value quickly and avoid putting unnecessary burden on our security resources. Having product experts by our side for the first three months executing a systematic ramp-up process helped us make an impact with our cloud-based SIEM much faster than we expected."
>
> **Chief Information Security Officer**
> Regional Family Medicine Practice Group

Success Factor 8

Vendor Track Record, Focus, and Future Outlook

Security leaders are often forced to make difficult trade-offs when making strategic vendor selections. Larger security vendors offer stability and one-stop shopping but generally lag behind startups when it comes to innovation. Startups bring fresh ideas and new technologies, but this can come at the expense of uncertainty. Startup products are often less mature, and factors like acquisitions and access to venture capital can affect long-term corporate viability. An ideal cloud-native SIEM vendor will reside in the sweet spot between these two extremes: well-established enough to have mature product capabilities and financial independence but nimble enough to innovate rapidly. Similarly, it's also important to weigh the trade-offs between working with a pure-play security vendor versus a company that provides SIEM capabilities as part of a broader product portfolio. In general, vendors with a core focus on SIEM will have more incentive to invest in product usability and feature innovation.

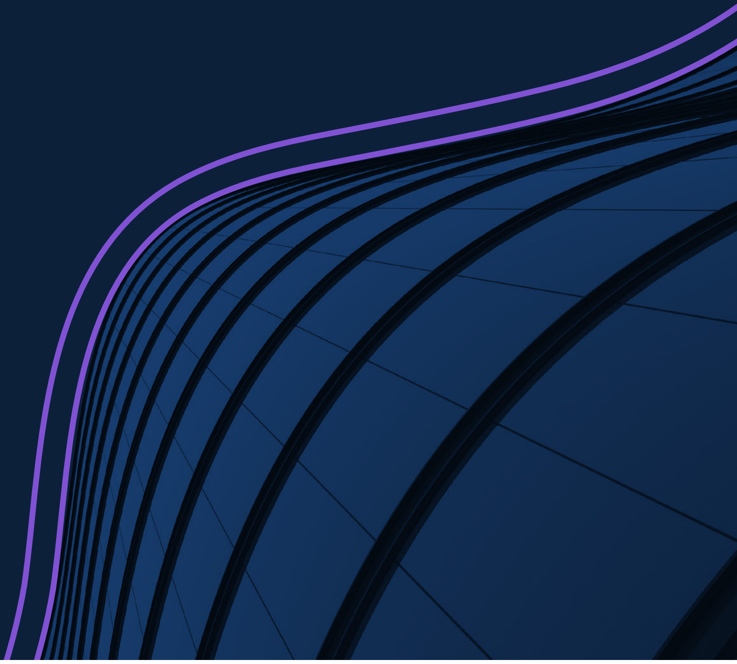
Success Factor 9

Data Storage Locations, Policies, and Practices

One potential obstacle for many organizations considering a cloud-native SIEM is uncertainty about data storage and security. A primary concern is, of course, how effectively your sensitive security data will be segmented and secured in a shared cloud environment. But there are other factors to consider as well. For example, some organizations are subject to data residency requirements that specify where certain types of data may be stored. Similarly, data collected by your cloud-native SIEM may be subject to data retention policies based on your industry or geography. It’s critical to challenge prospective vendors to demonstrate that they have the infrastructure, policies, and flexibility to meet your organization’s needs across these areas.

Success Factor 10

Architecture, Resilience, and Scalability



One of the biggest challenges in the security operations domain is the sheer volume of data that must be collected and analyzed continuously. SIEM platform functionality that shows well in a product demo may have substantially different performance and scalability characteristics when deployed at an enterprise scale. It’s critical to assess your cloud-native SIEM vendor’s architectural design and operational practices and ensure that they have a track record of scaling to meet the needs of organizations with similar size and characteristics as yours. This evaluation should include factors like platform uptime and performance considerations such as security event data processing throughput.

Bringing It All Together

Deploying a cloud-native SIEM can have a transformational impact on your risk posture by simplifying your security tool footprint while also providing ongoing access to the latest innovations. However, operating a critical component of your security stack in the cloud requires a great deal of trust in your vendor. Considering the factors above — and ideally partnering with a vendor who brings these elements together cohesively — will ensure that you:

- Respond efficiently and effectively to emerging security threats
- Gain meaningful insights from your SIEM quickly
- Address your unique requirements and regulatory needs
- Meet critical scalability needs as your organization grows and evolves

Buyer’s Checklist for Cloud-Native SIEM

Success Factors	What to Look For	Questions to Ask
Ease of Data Ingestion and Integrations	□ Out-of-the-box data integrations □ Multiple methods of data ingestion, such as cloud collectors, agent, and integrations via APIs and webhooks □ Flexible and intuitive approach for custom parsers	□ How many of my existing data sources can you support out-of-the-box? □ What is the full list of techniques you use to ingest customer data? □ Can you walk me though the process for creating a custom parsing rule?
Threat Detection Completeness, Accuracy, and Flexibility	□ Systematic approach for avoiding visibility gaps □ Well-defined techniques for minimizing false positives □ User-friendly approach for custom detection rules	□ How do you ensure that critical security events are not missed? □ What techniques and tuning are used to avoid false positive alerts? □ Can you walk me though your approach for creating custom detection rules?
Analytics and Reporting Capabilities	□ Information-rich dashboards □ Customizable dashboard widgets □ Direct integration between dashboards and search	□ Can you show me some examples of dashboards to provide a top-level view of risk posture? □ What types of data visualizations are supported? □ How can I drill down and search if something in a dashboard interests me?
Integrated Incident Response Workflows	□ Incident prioritization and tracking integrated with SIEM functionality □ Customizable response workflows	□ Does your platform include incident prioritization and tracking capabilities? □ Can you demonstrate the process for tracking and reporting on incidents?
Data Normalization, Enrichment, and Searchability	□ Capability to bring disparate data sources into a common format □ Metadata generation □ Sophisticated search capabilities	□ What types of processing do you do to raw log data that you collect? □ Can I perform complex searches on my data using compound search operations, separators, and regular expressions? □ Is the data normalized to make searching easy across various log sources? □ Is it easy to search across days, weeks or months of logs? □ What features do you offer to guide users through complex searches?

Success Factors	What to Look For	Questions to Ask
Security Framework Mappings	□ Out-of-the-box frameworks for MITRE ATT&CK® and/or other security best practice frameworks □ Success stories in your industry	□ Do your detection techniques map to any industry frameworks or best practices? □ How much effort will it take for me to configure your product to support my compliance needs? □ What other companies are you working with in my industry?
Access to Specialized Support and Services Expertise	□ Well-defined onboarding services to accelerate time to value □ Ongoing support and customer success functions	□ How long does it take a typical customer to be up and running with your product? □ What support can I expect from your team with integrating data sources and configuring dashboards? □ How does support engagement work after the initial deployment?
Vendor Track Record and Future Outlook	□ Financial independence without dependence on venture capital □ Level of focus on cybersecurity or SIEM □ Track record of delivering updates and innovations	□ Is your company profitable? □ Are you dependent on future venture capital rounds to fund ongoing operations? □ What percentage of your revenue comes from your SIEM offerings? □ What updates have you released for your products over the last 12 months?
Data Storage Locations, Policies, and Practices	□ Data retention policies that match your organization's requirements □ Ability to meet data residency requirements	□ How long do you store customer data? □ Where is your customer data stored? □ Can data storage be limited to specific regions if necessary?
Architecture, Resilience, and Scalability	□ Deployments of similar size or larger □ Mature capacity planning processes □ Strong historical uptime track record	□ How many locations and users does your biggest deployment have? □ Does the cloud SIEM have high availability and disaster recovery capabilities built in? □ How do you ensure that performance isn't degraded as usage and data volumes grow? □ What is your infrastructure uptime percentage?

How LogRhythm Axon Can Help

LogRhythm Axon is a cloud-native SIEM platform built for security teams that are overwhelmed by immense amounts of data and an ever-evolving threat landscape. Optimized for the analyst experience, LogRhythm Axon's powerful security analytics, intuitive workflow, and simplified incident response give analysts contextual insight into cybersecurity threats so they can reduce noise and quickly secure the environment. LogRhythm Axon reduces the burden of managing threats and the operating infrastructure, helping security teams prioritize and focus on the work that matters.

Learn More

About LogRhythm

LogRhythm helps security teams stop breaches by turning disconnected data and signals into trustworthy insights. From connecting the dots across diverse log and threat intelligence sources to using sophisticated machine learning that spots suspicious anomalies in network traffic and user behavior, LogRhythm accurately pinpoints cyberthreats and empowers professionals to respond with speed and efficiency.

With cloud-native and self-hosted deployment flexibility, out-of-the-box integrations, and advisory services, LogRhythm makes it easy to realize value quickly and adapt to an ever-evolving threat landscape. Together, LogRhythm and our customers confidently monitor, detect, investigate, and respond to cyberattacks.

Learn more at logrhythm.com.

www.logrhythm.com // info@logrhythm.com

United States: 1.866.384.0713 // United Kingdom: +44 (0)1628 918 300
Singapore: +65 6222 8110 // Australia: +61 2 8019 7185
Middle East: +97155 642 2224