Cloud SIEM: Assessing Your Readiness to Move Your SIEM to the Cloud

Published 30 June 2020 - ID G00720719 - 35 min read

By Analysts Eric Ahlm, Augusto Barros

Initiatives: Security Operations for Technical Professionals

Security and risk management technical professionals are often tasked with doing more on their SIEM platform, while at the same time managing cost and operational impact. This assessment gives them the analysis framework to decide if a cloud SIEM platform can improve the monitoring operations.

Overview

Key Findings

- Cloud security information and event management (SIEM) offers more protection against initial missizing of storage or compute that often plagues SIEM deployments.
- Cloud SIEM doesn't eliminate all platform operations, such as rules tuning or alert monitoring, but it can offer measurable operational time savings for SIEM platform health and upkeep.
- A move to cloud SIEM can cause loss of architectural flexibility, as the provider controls most underlying components of the SIEM solution.
- Justifying the move to cloud SIEM isn't always based on cost or cost savings. Often, it's other reasons, such as supporting your company's move to the cloud, time to value or high availability.

Recommendations

Security and risk management technical professionals focused on security monitoring and operations should:

- Build cloud SIEM justification on more than just a simple cost analysis by employing operational agility, readiness for scale, level of cloud services adoption and other qualitative factors.
- Adopt cloud SIEM to reduce the time to implement and scale an SIEM solution.
- Determine if a move to cloud SIEM would also require a reevaluation of your existing security services provider's ability to support a switch to SIEM solutions.

Analysis
A cloud SIEM is, in fact, a SIEM like any other that just happens to have different handling of its software platform and underlying architecture than a normal SIEM.

A cloud SIEM is possibly better labeled a SIEM as a service or SaaS SIEM. A cloud SIEM is a SIEM platform maintained at some level by the provider that exists in a data center also chosen by the provider.

What can get confusing is that the term cloud SIEM is used universally but can mean very different things, each with their own reasons for selection. See, for example, Figure 1. Notice there are three parties involved in this deployment: the customer, or the SIEM end user, the cloud SIEM provider, such as Splunk or IBM, and the infrastructure as a service (IaaS) provider, such as Amazon Web Services (AWS) or Microsoft Azure.

All three cloud SIEM models shown in Figure 1 share the same components: customer-specific rules and data, the SIEM software or platform and the underlying cloud infrastructure that support the deployment. What changes in each model is how these components are grouped and the responsibilities of each party involved.

**Figure 1: Types of Cloud SIEM Offerings**

**Types of Cloud SIEM Offerings**

<table>
<thead>
<tr>
<th>Cloud-Native SIEM</th>
<th>Cloud-Hosted SIEM</th>
<th>Customer-Deployed SIEM in the Cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer-Specific Event Data</td>
<td>The SIEM Software and Connections</td>
<td>The SIEM Software and Connections</td>
</tr>
<tr>
<td>Customer-Specific SIEM Policy/Configuration</td>
<td>SIEM Architectural Dependencies</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Customer &quot;A&quot; Ownership</td>
</tr>
</tbody>
</table>

Source: Gartner
Customer-Deployed SIEM in the Cloud

You don’t need a cloud SIEM provider to run a SIEM in the cloud. Most SIEM platforms are software that can be normally deployed in the infrastructure-as-a-service cloud of your choice. This do-it-yourself (DIY) cloud SIEM benefits from the cloud-scale compute, storage and data center facilities provided by the IaaS vendor. This could offer much of the same benefits as commercial cloud SIEMs, such as more resources for rules processing and queries, and easily expandable storage based on services, such as Amazon S3. 

The main difference between this configuration and a cloud-hosted SIEM is ownership and responsibility of the underlying architecture and SIEM software itself. In this model, the customer (you) owns it all except for the development of the SIEM software. Operational responsibilities, such as patching and updating the SIEM software and all other platform design and support functions, remain the customer’s job.

Vendor-Hosted Cloud SIEM

A cloud-hosted SIEM is often not labeled as such from a vendor, but would rather be called just a cloud SIEM. To many buyers, cloud-hosted SIEM looks like any other cloud SIEM solution, whether native or hosted. The vendor cloud-hosted SIEM shares the same components as other configurations, but the roles and responsibilities are different.

From a design standpoint, this configuration is much the same as the customer-deployed SIEM in the cloud. The SIEM provider handles the architecture and deployment of the SIEM is the main difference, and is responsible for the operations and management of the SIEM infrastructure, including the SIEM software and underlying architectural dependencies.

Cloud-hosted SIEMs may lack some scale or benefits that come from multitenant platforms. The cost can often be somewhat higher, as these models are less efficient to operate for the cloud SIEM vendor.

Cloud-Native SIEM

This cloud-native SIEM shares the same components as the other configurations. The ownership and responsibilities are much the same as cloud-hosted SIEM. The cloud SIEM provider is responsible for SIEM software deployment, updating and upkeep of the underlying architectural components.

The architecture is multitenant, built to maximize typical SaaS characteristics, such as elasticity and a common codebase, which is the main difference for this configuration as compared to cloud-hosted SIEM. This architecture also benefits the vendor, since the shared platform is more efficient, and therefore, more profitable to operate. Most vendors do pass along some of these efficiency gains to the customer (you), and can offer some additional security benefits as well, such as shared rules knowledge.
The Role of SIEM Hasn't Changed

The shift of any technology to the cloud can be transformational. The most visible SIEM providers are already offering or actively developing a cloud-based solution.

Even if the ticket price of the cloud SIEM is nearly free, thanks to enterprise licensing agreements from your cloud or software vendor, you may not be able to afford to run it correctly.

A move to the cloud does not change the role a SIEM plays in your security operations. The justification for your organization to use or not use a SIEM hasn't changed, nor has the bulk of the operational responsibility required to get useful outcomes out of a SIEM. If you are considering a SIEM for the first time because of the attractive nature of a cloud-based offering, you should start by understanding more about the role of a SIEM and your organization's readiness to operate one correctly. More on these topics can be found in “How to Develop and Maintain Security Monitoring Use Cases” and “How to Operate and Evolve a SIEM Solution.”

Once you've decided a SIEM is right for your organization, you can move to choose which SIEM platform is best for your needs.

Contrasting SIEM Responsibilities and Services

It's quite common for customers to use a mix of service partners around the various tasks associated with SIEM operations. The role of a security services partner can be diverse, as seen in “The Managed Security Services Landscape Is Changing.” What role the partner plays can vary based on deployment strategies.

The use of service providers for SIEM operations doesn't change with cloud SIEM either; however, some responsibilities may change. There are three major areas involved in SIEM operations — adapting, running and watching. These areas can be further broken into separate processes:

- **Architectural design**: In a cloud SIEM deployment, the underlying architecture is solely the cloud SIEM provider's responsibility. The provider chooses how the SIEM software is configured, how much compute is available for analytics and how event storage is done. While this does have its benefits of specialized knowledge and cloud-up scale, it comes at a loss of flexibility. If your SIEM design requires specialization, such as data storage locations for compliance requirements, you might be out of luck with cloud SIEM.

- **Deployment**: In cloud SIEM, the underlying architecture and SIEM software itself is predeployed. Deployment time for cloud SIEM is often significantly reduced, as it is limited to setting up the
log collection, rules creation and general usage setup tasks that remain the customer's responsibility.

- **Storage maintenance**: A cloud SIEM provider can also take the responsibility of maintaining cloud storage systems. This can include general storage systems upkeep and also options for a longer-term event storage archive. Although this task is somewhat trivial, it's a regularly occurring job that shifts away from your operations team to the cloud SIEM provider.

- **Data center facilities**: This one is obvious, but worth mentioning that all responsibilities and costs associated with maintaining the facilities that house the SIEM deployment shift completely to the cloud SIEM provider. Calculating your own facilities cost and operational impact, as it relates to a noncloud SIEM, can help in building cost justification for a cloud SIEM.

- **SIEM adapt/tune content**: This critical job for a SIEM doesn't go away with cloud SIEM. Analytics, integrations, custom parsers, threat feeds and other content must be created and tuned to generate meaningful alerts and produce the reports required by your organization. The cloud SIEM provides the platform, but the work of managing and adapting the content remains the customer's responsibility or their partner's.

- **SIEM software updates/maintenance**: This SIEM software version level and regular SIEM software maintenance are solely the cloud-SIEM provider's responsibility. This eliminates these tasks and time spent on these tasks from your team. It can also have some security value in that the SIEM platform itself is always up to date and ready to run the latest rules.

- **Log collection**: SIEM requires input data to provide its value. The integration of log sources to the cloud SIEM remains with the customer, although the exact point where the responsibilities are split can vary from vendor to vendor. Setting up systems to generate and send logs is certainly on the customer side, but setting up and managing the log collection infrastructure, such as on-premises log collectors, may have split responsibilities. Organizations adopting cloud SIEM must understand what pieces of the solution they'll still need to manage and what resources will have to be available to deploy them. Those planning to use a services provider to operate their cloud SIEM must ensure the responsibilities over these components are clearly defined.

- **Alert monitoring and incident response**: Acting on the output of the cloud SIEM is also the customer's responsibility. This also includes any reporting, threat hunting or response actions. This is essentially where the value from a SIEM is realized, so it's critical to secure the appropriate resources for it. Security services providers providing co-managed SIEM services can run a great part of these processes for the customer, but there are limitations on how much of incident response can be outsourced to a service provider.

Figure 2 shows the three key tasks involved in operating a SIEM — adapting, running and watching. Where cloud SIEM can help is shown in more detail in Table 1.
Cloud SIEM mainly helps with the running responsibilities of SIEM. Tuning and watching remain unchanged.

Some of the responsibilities of running a SIEM normally done by the customer have moved to the provider.

The other parts of SIEM operations, adapting and watching still require attention; and how you use a service provider to help for these tasks may change based on what platform type you use. Table 2 shows how a security service provider’s role may change for adapting and watching for your SIEM.

Figure 2: The SIEM Operations Responsibility Triade

The SIEM Operations Responsibility Triade

Source: Gartner
720719_C

Table 1: Responsibility Matrix in a Cloud SIEM Deployment

<table>
<thead>
<tr>
<th>Duty/Task</th>
<th>Cloud SIEM Provider (SaaS SIEM)</th>
<th>Customer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Architectural Design</td>
<td>Primary</td>
<td>N/R</td>
</tr>
</tbody>
</table>
### Table 2: Responsibility Matrix in a Cloud SIEM Deployment Including Security Services Provider

<table>
<thead>
<tr>
<th>Duty/Task</th>
<th>Cloud SIEM Provider (SaaS SIEM)</th>
<th>Security Service Provider</th>
<th>Customer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deployment</td>
<td>Primary</td>
<td>N/R</td>
<td>N/R</td>
</tr>
<tr>
<td>Storage Maintenance</td>
<td>Primary</td>
<td>N/R</td>
<td>N/R</td>
</tr>
<tr>
<td>Data Center Facilities</td>
<td>Primary</td>
<td>N/R</td>
<td>N/R</td>
</tr>
<tr>
<td>Adapt/Tune Content</td>
<td>N/R</td>
<td>Primary</td>
<td>Supportive</td>
</tr>
<tr>
<td>Software Updates and</td>
<td>Primary</td>
<td>N/R</td>
<td>N/R</td>
</tr>
<tr>
<td>Maintenance</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Log Collection</td>
<td>Supportive</td>
<td></td>
<td>Primary</td>
</tr>
<tr>
<td>Alert Monitoring and Incident Response</td>
<td>N/R</td>
<td>Primary</td>
<td>N/R</td>
</tr>
</tbody>
</table>

N/R: no responsibility.

Source: Gartner
Deciding if Cloud SIEM Is Right for You

Here in 2020, it’s safe to say cloud SIEM is mainstream and here to stay. All major providers have some sort of cloud SIEM offering now, as compared to only a handful of vendors a few years back. It’s also clear from speaking with SIEM vendors that the bulk of their innovation and R&D spending going forward will be cloud-first. In short, the risk of moving to a cloud SIEM is relatively low.

Is cloud SIEM better? For most organizations, yes, just like many other technologies offered as cloud services. However, there are still cases where it may not be the most appropriate solution.

Justifying a move to a cloud SIEM solution can be tricky. After all, the role of the SIEM hasn’t changed, and from a capabilities standpoint, both cloud and noncloud SIEM are offering much of the same. Costing or total cost of ownership (TCO) can come up, but the difference can be in degrees and isn’t always a clear advantage. Often, the reasons for justification can be more qualitative or supportive in nature and are usually based on these reasons:

**Reasons to Move to Cloud SIEM**

**Operational Time Savings**

In any cloud SIEM model, the provider owns the maintenance for the platform. This leads to direct time savings since functions like storage maintenance, SIEM software updates, underlying server
updates, backup functions and other platform-related tasks are handled by the provider. However, this does not include tasks related to the use of the SIEM, like creating and tuning use cases.

Based on the size of your SIEM deployment, this time saved may be large, or may be a very small part of your team’s time. Either way, the time saved is measurable and accounting for how much of your team’s time is spent on these tasks can help in your justification for a move to cloud SIEM.

**Time to Value**

Shelfware is a real risk of first-time SIEM deployment. The dependencies required to deploy and operate a SIEM are nontrivial and can hold up a SIEM deployment, or even bring it to a full stop. Time to value, in this context, is about having the SIEM ready to go for creating monitoring use cases on Day 1. There is no delay for planning and deploying a SIEM platform with cloud SIEM.

The same time to value can apply to running a proof of concept or avoiding monitoring delays due to missing updates.

Measuring the time to value for justification is a harder task, as it surely is a more qualitative metric. Some organizations, however, can be so bureaucratic that any work eliminated from the implementation project can greatly affect the time to value. Adding new servers to a data center may require weeks of paperwork and planning in some cases. If your organization has had bad experiences with large-scale project rollouts before, this could be enough to warrant justification.

**Cost or TCO**

If you are trying to build cloud SIEM justification solely on cost, be careful. A quality cost analysis between in-house and cloud SIEM can be complex, and simply looking at the cost of event volume cost or devices monitored won’t do you justice.

The biggest measurable factor for cloud TCO is the operations time saved for platform maintenance. Although there is generally some time or money saved there, it might not be enough by itself to justify the move. A good TCO will also include the infrastructure management cost savings, up to and including data center power, cooling, rack space and other such factors. For larger SIEM deployments using multiple servers, this can start to add up. For single-server SIEM deployments, it’s a TCO rounding error and won’t matter much.

Another less-tangible factor to put into a cost analysis is avoiding a redesign due to missizing. Often, Gartner will hear from clients at the 18-month point of their SIEM deployment, talking about scalability issues for compute or storage. Unplanned scaling can be costly, causing unexpected changes to the budget model. Cloud SIEM, on the other hand, has nearly unlimited scale, keeping the cost of scaling predictable and aligned to the original budget.

The price of data movement can also factor into a cloud SIEM, as data transport isn’t free. Some cloud SIEM providers are quick to point out that moving data within a cloud provider is cheaper than moving data from the AWS cloud to your on-premises SIEM or to another cloud provider. This is true; however, the cost savings might be so small it’s not even worth measuring.
From a wide-area network cost point of view, your monitoring should be as close to the largest density of assets being monitored as possible. The reality is that not all of your reporting devices for monitoring will live in one cloud. For justification, if you are moving around a very high volume of log data, it could be worth your time to build a cost justification model and understand the data transport costs involved.

**Sandbox SIEM**

Having a second SIEM for testing or training was a luxury out of reach for most organizations. Cloud SIEM allows for a second R&D or training SIEM to be set up quickly and cost-effectively. This can be ideal for testing new policies or letting junior members learn without harm to production systems.

As a justification factor, this one again is more qualitative in nature. If, however, you have a regular need for training new team members, your staff size for SIEM operations is larger, or you like to experiment on new monitoring use cases, this factor could help sway justification.

**High Availability and Resilience**

All high availability and resiliency for your cloud SIEM is handled by your provider. Likely, their high availability assurances are built on the underlying cloud provider, such as Amazon Web Services, Microsoft Azure or similar infrastructure providers. In addition to the high availability of the infrastructure, the cloud SIEM providers help strengthen resiliencies by managing SIEM software outages due to updates or misconfigurations.

This can be an important justification factor if your organization has high availability (HA) or resilience concerns for security monitoring. However, keep in mind that increased back-end availability may not offset the addition of new points of failure such as WAN connections.

**Security Capabilities**

A cloud SIEM can offer some security advantages for monitoring over its noncloud counterpart. Although each of these factors may be a bit of a stretch, they do offer some justification value for cloud SIEM. Cloud SIEM security advantages include:

- A cloud SIEM software is more likely to be up to date, sooner. This means the SIEM platform is more ready to support any new or advanced security rules dealing with new threats.
- Some cloud SIEM providers can leverage threat detection content development and tuning across clients. This adds to better efficacy through group tuning.
- During an outbreak or emergency, the load of monitoring and query can break due to lack of system resources. There are many horror stories of organizations finding about their SIEM capacity bottlenecks due to increased activity caused by a major incident. Cloud SIEM allows for greater scale in emergency situations, thus ensuring continuity of monitoring and investigations exactly when they are needed most.
High availability also adds to security capabilities. Ensuring the SIEM is online as much as possible increases the time allotted to monitoring.

More computational performance can allow for analytics or secondary detection functions that may otherwise be deprioritized due to system constraints.

Proximity to Data
As organizations move to the cloud, a decision point usually happens when deploying a SIEM — do I hybridize, and if so, where does the main data and log collection occur, on-premises or in the cloud?

Data Retention Capabilities
Some cloud SIEM providers are offering new data retention offerings built on new cloud object storage methods, such as Amazon S3 and Amazon S3 Glacier from Amazon.¹ These new models can help eliminate the complex design of mixed frozen or offline storage options found in noncloud SIEMs. This is a new concept, and the usage and value of having all logging data hot is in the experimentation stage.

Certainly, for organizations that do hunting, or want to do data modeling on long-term trends, this is an invaluable feature. For other organizations, it might just be nice to know it’s an option for cheaper long-term retention.

Support Your Business's Cloud Goals
One justification for cloud SIEM that comes up often is the desire from security operations to match or pace with the corporate cloud policy. For example, if your organization is standardizing on Microsoft (MS) Office 365, and planning to move even more applications to Azure in the next few years, it helps justify a move to a cloud SIEM with native support for that environment.

Considering that SIEM refresh cycles are long, typically five or more years, it’s a good idea to check the current and likely future cloud posture from your business when making your next SIEM refresh decision.

Reasons to Not Move to Cloud SIEM
Although the prevailing trend for security stack and monitoring solutions is a shift to the cloud, there are certainly reasons why your SIEM should stay noncloud-based. These reasons include:

Regulatory Issues
If you are in a highly regulated industry or geography, check with your audit team about the move to cloud SIEM. One issue, especially in European and Middle Eastern countries, might be data residency. Your cloud SIEM provider might not have the same restriction on data crossing out of certain geographical regions than you do. There might also be issues concerning data sovereignty, depending on how your SIEM vendor and the underlying IaaS provider spell out your terms and conditions of who owns your event data.
A No-Cloud IT/Security Culture

Whether it’s an irrational fear of cloud, or a quite fact-based, data-driven fear of cloud, if your company is cloud avoidant, then cloud SIEM isn’t right for you. A virtualized SIEM platform in your data center design of choice can accomplish most of the same goals, so the fighting lines for cloud SIEM as the first cloud security solution aren’t very strong. This also holds true if your culture is more pro capital spending than operational spending.

Given that many SIEM refresh windows are between three and five years, it is good now to check if your culture might change in that time frame before locking into a noncloud SIEM.

Internet Speed Limitation

Data transport alone might be the reason not to consider cloud SIEM. A good rule of thumb is to have the monitoring close to the assets they monitor, especially one that can generate high alert volumes. If the bulk of your high alert volume assets aren’t in the cloud, but you plan on moving your SIEM to the cloud, check the impact on your internet links. Latency or general lack of available bandwidth can also limit or stop a move to cloud SIEM.

Complex or Specialized Architectural Needs

Considering SIEM has been around since before 2000, some deployments could be entering their second decade in operation! Even if your deployment isn’t that “tested,” many SIEM deployments have seen many years or operations, and as such developed specialized configurations or methods of platform operation.

If you are willing and able to shed these specialized architectural needs for what the cloud SIEM vendor offers, then it’s a nonissue. If, however, your specialized configurations are more entrenched in your operations, it might be worth considering postponing a move to cloud SIEM.

Managing the Move to Cloud SIEM

It’s not the intent of this research note to cover all aspects of how to migrate from a noncloud SIEM to a cloud SIEM. However, there are a few key considerations about the transition that may be helpful in justifying, or not justifying, your choice of SIEM platform.

If your cloud SIEM is your first SIEM deployment, then this section can be skipped. If, however, you have an existing SIEM, this information is for you.

Plan on a Full Migration Project

Making this switch to cloud SIEM unfortunately isn’t as easy as just adding a cloud component as a hybrid to what you’ve already built. Even if your move to cloud remains with the same vendor, a hybrid SIEM model may not work well.

The main reason is the inconsistency of SIEM platform versioning and configuration between your SIEM instance and the vendor’s cloud instance. Since the vendor owns and maintains software
upkeep with cloud SIEM, there’s a good chance their upgrade schedule and preferences won’t match yours exactly. Those inconsistencies will cause break points and must be avoided.

Some vendors can offer workarounds for a semihybrid configuration; however, the clearly preferred option is an outright migration of the SIEM platform from your existing instance to the cloud instance.

Specific Considerations for Microsoft Azure Sentinel

Gartner is seeing a growing interest in the role of Microsoft’s Azure Sentinel SIEM. Sometimes, this interest is about an organizational shift to Microsoft Azure, such as a move to Microsoft Office 365. Other times, it’s about leveraging E5 licensing agreements that include Azure Sentinel. Or other times, it’s both.

This can force a decision point for what role Azure Sentinel should play, and what role your existing SIEM should play. This decision point usually falls within one of these three options:

- Should we do all MS-specific monitoring on our existing SIEM?
- Should we move all monitoring (Azure and all other) to the Azure Sentinel Platform?
- Can we do split monitoring using Sentinel for Azure assets, and our existing SIEM for all others?

Use Existing SIEM for All Monitoring

Pros:

- More simple SIEM operations, single system.
- Advanced feature set of mature SIEM product.
- Team training and operations remain the same.

Cons:

- Data export cost from Azure.
- Additional SIEM platform cost and upkeep.
- Not cloud-forward or embracing company’s move to cloud.

Move All Monitoring to Azure Sentinel

Pros:

- May save money due to existing licensing agreements (retire some/all former SIEM license).
- Cloud security monitoring to match company cloud culture.
- Better support for monitoring Azure-specific resources.

Cons:
- Less mature SIEM may lack required features for your operations.
- Team training and migration cost for platform switch.
- Vendor/cloud lock-in.

Split Monitoring Between Sentinel and Existing SIEM

Pros:
- Balancing of cloud culture and mature product monitoring.
- Some licensing cost reduction by moving some load to Azure Sentinel.
- Best-of-breed thinking keeps vendor lock-in risk reduced.

Cons:
- Available Azure Sentinel to existing SIEM integration may lack full centralized monitoring goals.
- Some operational redundancies from running two platforms will impact operations.

Strengths

SaaS SIEM advantages include:
- Simplicity of deployment and operation.
- Always-current capabilities.
- Close vendor support and monitoring.

Easier managed service enablement includes:
- Easier use-case expansion due to lack of hardware limits.
- Faster product improvements, stemming from the vendor’s access to data.
- Superior model for centralized log management (CLM).

Simplicity of Deployment and Operation
Many of the tasks related to deploying servers or appliances, configuring complex storage systems and installing software are not required because they are completely managed by the service provider. Cloud SIEM implementation is instead primarily focused on installing data collectors, configuring data sources and configuring network controls to allow the required data flows. This provides the opportunity for a much faster initial deployment time — days versus months compared with traditional SIEM. In fact, for one client we interviewed, the cloud SIEM was operational within a single afternoon.

Operation is also simplified, because most management and administration tasks, such as updating software and hardware, are handled by the provider. Hardware maintenance and refresh challenges are also eliminated, and there is no need for any large-scale hardware purchases. Cloud SIEM also enables clients to simplify process dependencies because all maintenance and updates of the underlying SIEM infrastructure are no longer subject to internal change management requirements. With traditional SIEM, adding a new storage component may require months of advanced planning for some organizations. By contrast, with cloud SIEM, this activity happens automatically and completely behind the scenes.

**Always-Current Capabilities**

Users of traditional SIEM must contend with complex deployment and update procedures, often making migration to newer product versions a slow process. Users of SaaS SIEM, however, will always be running the latest product version with the most recent functionality and detection logic. The out-of-the-box (i.e., vendor-provided) content is also solid and always up to date.

**Close Vendor Support and Monitoring**

Running the detection logic in the cloud allows vendors to provide closer support for content-tuning needs. Traditional SIEM users often have to struggle with rules that cause performance issues. By contrast, SaaS SIEM vendors must stay close enough to clients to avoid such issues since the impact on multitenant environments could have bigger implications. Support processes are often streamlined. It is easier to identify when the issue is with the vendor versus with the client.

**Easier Managed Service Enablement**

Many cloud SIEM vendors are also providers of managed detection and response (MDR) or managed security service (MSS), usually leveraging the same technology platform — the cloud SIEM. Clients of such vendors can easily transition from cloud SIEM to those other service offerings. This flexibility is a key benefit for organizations that are still determining the type and amount of services they need to meet their security operations requirements. However, your existing security service provider may not offer services on a cloud platform, so it’s good to check their readiness.

**Easier Use-Case Expansion Due to Lack of Hardware Limits**

Many organizations have ambitious plans to apply their SIEM to new use cases, but hit capacity limitations before they can implement those plans. With traditional SIEM, the work of aligning use-
case expansion with capacity planning is complex and many organizations end up not expanding their usage of the tool due to capacity constraints. Cloud SIEM makes expanding SIEM function linear. More capacity comes at a predictable pace and cost. Compared to noncloud SIEM, some scale barriers may require costly and unplanned hardware or storage architectural changes.

Faster Product Improvements, Stemming From the Vendor’s Access to Data

With cloud SIEM, vendors can see in near real time how their product improvements or new policies are working on actual client data. This is because all clients using the cloud SIEM have their data on the cloud platform itself. This real-time feedback to product changes in cloud SIEM can allow vendors to do:

- Perform deeper analysis to identify new threats.
- Test the utilization of new detection methods and the performance of newly developed content.

More data may lead to more effective threat detection when certain machine learning algorithms are in use. This may not be the case for current tools. However, the centralization of data provides vendors with more possibilities to offer services that require broad data access or that improve in quality as the volume of data grows, as is typically the case with machine learning algorithms.

Parsing and normalization of events can also be better supported by the vendor in a SaaS SIEM model. The vendor can see all log data and develop or update parsers more efficiently. Finally, the vendor can monitor the utilization of the system by its clients more efficiently, providing additional support and guidance on the creation of more effective detection rules.

Superior Model for Centralized Log Management

One of the most complex areas for SIEM architecture and planning is CLM at large scale, with many distributed log sources and with long retention times. As one client stated, “petabytes make everything hard” — and also costly. Any organization planning to expand collection or retention of logs on a traditional SIEM needs to consider the following:

- How to expand storage and indexing capabilities.
- How such expansion will affect search performance and online monitoring.

In fact, many organizations have been opting to keep CLM separate from SIEM to avoid the challenges of architecting a solution that can handle the disparate requirements. Such requirements include providing effective online monitoring and providing fast search capabilities over longer data retention periods. A cloud-based solution, with its inherent elasticity and capacity, can help clients implement CLM as part of SIEM, without the scalability, performance and architecture concerns that usually come with this task. A cloud-based solution can also store logs for longer periods of time and at lower prices, while keeping them accessible for reports or investigations as needed.
Weaknesses

SaaS SIEM disadvantages include:

- Internet and connectivity dependencies.
- Compliance and trust issues related to data in the cloud.

Internet and Connectivity Dependencies

Naturally, cloud SIEM's No. 1 weakness is its inherent reliance on internet connectivity. The exposure to connectivity issues is a well-known risk for cloud-based solutions. For cloud SIEM, loss of an internet connection leads to an interruption, loss of log flow to the SIEM and loss of console access by the users. Bandwidth limitations can also affect the ability to collect logs. Moreover, if log collection consumes excessive bandwidth, it can negatively impact connections used by other processes and systems.

Cloud SIEM collectors will, of course, buffer data. However, buffering will only enable you to access the data later; it will not make your SIEM function during the period of connectivity interruption. Note that such locally buffered data needs to be protected from any attackers that may have gained access to your environment.

Compliance and Trust Issues Related to Data in the Cloud

Acceptance of cloud-based solutions has been growing consistently, but there are still many concerns related to sending data to cloud-based providers. Cloud SIEM will always be unpalatable to organizations that cannot use public cloud solutions. Organizations may have specific regulatory requirements that prevent them from sending logs to the cloud. Moreover, in some jurisdictions, users’ internet-browsing data, or even the IP addresses of their home PCs used for work, may be considered private and protected. On top of this, data sovereignty concerns create additional challenges for organizations that want to collect logs with browser history, such as secure web gateway (SWG) and some endpoint logs, via their cloud SIEMs. These concerns revolve around the need to store data within a particular country, and hence, inside provider systems residing in that same locale. In fact, even if a cloud SIEM vendor is based in a particular country but uses a data center in another country, concerns of this type are not laid to rest.

When remote system polling and API access are used to collect logs, credentials for the source systems also need to be stored in the cloud SIEM, presenting a potentially greater concern than the logs themselves. Vendors alleviate this risk by storing credentials on the local collectors only and not in the cloud.

In fact, all general cloud risks are present for cloud SIEM implementations. These include third-party control, remote access and tenancy. For more on general cloud security risks, see “Security Risks in Cloud Computing.”
Cloud SIEM also means that all collected data is in the hands of the service provider, requiring organizations to consider the challenges of creating an exit strategy for the service. If an organization decides to move its data to another tool (or service provider), a method to download and migrate that data needs to be defined. Some service providers may not have the tooling to do this in an efficient manner.

Finally, if your organization is subject to data residency or data sovereignty requirements, you may be limited when using, or even prevented from using, a SaaS SIEM, as would be the case with any other SaaS tool.

**Risks From Pay-per-Use Pricing and Subscription Models**

Some cloud SIEM offerings are charged in a “pay-per-log” manner, which links the cost of the service directly to the amount of data being sent to the system. Organizations that experience high and fast growth may incur unexpected increases in the overall cost of the solution, essentially creating an economic denial of service (DoS) risk.

Subscription-based pricing can also amplify the effect of budget cuts to security. For example, if the budget for the cloud SIEM is cut, access to logs stored in the solution could be affected.

**Guidance**

Review the questions below to determine whether your organization is close to the cloud SIEM “sweet spot.” Assess the drivers for adopting cloud SIEM, such as being a heavy cloud user, possessing a highly distributed environment or having trouble with the upkeep of a traditional SIEM. Include cloud SIEM on your shortlist if you meet these criteria. Prioritize cloud SIEM if your organization is actively migrating to the public cloud. In this scenario, cloud SIEM provides better cloud log support, covers more cloud use cases and offers easier/cheaper cloud log collection and storage.

Every answer of “yes” indicates a readiness or reason to justify a move to cloud SIEM.

1. Does your organization lack either the resources to run its own SIEM or the desire to allocate its resources to this task (perhaps it failed with legacy SIEM due to infrastructure management challenges)?

2. Has your organization decided “not” to use a MDR offering, but build your own SIEM deployment?

3. Is your organization looking to move more security purchases to operating expenditure (opex) instead of capital expenditure (capex)?

4. Is your organization able and willing to accept cloud storage of log data (i.e., no compliance restriction based on storage location)?
5. Is management pushing your organization to adopt more “security from the cloud” (e.g., via cloud-first or cloud-only initiatives)?

6. Is your organization widely distributed over many locations, with a broad scope of monitored assets and many teams tasked with monitoring responsibilities? In other words, would an on-premises SIEM require a complex, federated approach with numerous components?

7. Does your organization have both on-premises and cloud assets to monitor? (See “Security Monitoring and Threat Detection in Public Cloud Environments.”)

8. Do your locations needing to send logs have the bandwidth and capabilities to send to a cloud provider?

Naturally, you don’t need to match all of the above criteria. However, matching more of the criteria increases the likelihood that cloud SIEM will be a good fit for your organization. Note also that some of the criteria above are unrelated and point at different adoption scenarios. For example, one organization may choose SaaS SIEM to gain flexibility in regard to MSS/MDR, while another may do so to facilitate cloud asset monitoring.

Evaluate Cloud SIEM Tools

Evaluating a cloud SIEM solution is much easier than evaluating noncloud SIEMs. The SIEM platform is live and ready to monitor on Day 1, and only needs log data sent and a basic use case for monitoring configured to get a feel for the platform’s capabilities.

Even if your organization isn’t due for a SIEM refresh for some time, it might be worth setting up a basic cloud SIEM evaluation. This is especially true if your organization is in the process of moving a major application, such as email or collaboration to the cloud.

Another reason to do a cloud SIEM evaluation is if your organization has a push to better use enterprise buying agreements from companies such as Microsoft, IBM or Google.

Prepare to Deploy Cloud SIEM

Fortunately, deployment of cloud SIEM is expected to be much easier than deployment of traditional software or appliance SIEM. Before deployment, work with the vendor to establish the bandwidth requirements for log upload. Make sure you have connections for both log transfer and platform access to keep the SIEM working when under attack. Check your resiliency and continuity plans to ensure that you can continue using your SIEM under high traffic load, such as that brought on by DoS and distributed denial of service (DDoS) attacks. Note that you cannot control what happens when your SIEM vendor is hit by a DDoS attack. Therefore, you need to query the vendor about its DDoS resiliency, in addition to focusing on your own.

To compensate for cloud-related issues, design the architecture and associated processes to include additional resilience factors. Connectivity is a sensitive point and compensating controls should be in place to handle any issues that could cut the connection between the monitored

Gartner, Inc. | 720719
systems and the SIEM. Store-and-forward mechanisms, redundant connections and alternative access methods are typical approaches that organizations use to mitigate risk from cloud-based solutions.

Cloud SIEM vendors always recommend using a set of central forwarders deployed on-premises or inside your IaaS environment. These forwarders encrypt, compress and buffer data at the last spot before the internet and then deliver that data to the vendor’s cloud. Note that these forwarders may both listen for logs (syslog-based log sources) and poll for logs (Microsoft Windows logs and some others).

Although most compute and storage resources will reside at the vendor, you will still need on-premises resources to handle the performance-tuning, management and update tasks for the collectors and forwarders. Those systems will also have their standard requirements, such as rack space, network connectivity, password management and other IT operations needs. Before deployment, review the SaaS SIEM requirements in relation to your current network architecture realities and requirements. For example, ensure that the on-premises forwarders can collect logs and deliver them to the SIEM platform by confirming that the necessary access control lists (ACLs), network routes, bandwidth and gateways are in place. Some organizations have strict network zoning requirements, such as rules that ban network zones from accessing internal systems and the internet simultaneously. Such organizations may need to design a multilevel collector architecture to comply with those requirements.

Build an Effective Cloud SIEM Operation

Clearly define the expected roles and responsibilities of a SIEM service provider before selecting cloud SIEM. If you expect the vendor to actively participate in the security monitoring process, you should focus on MSS or MDR offerings instead.

As your cloud SIEM enters production, you will need to carefully manage retention costs. The cloud scale of cloud SIEM might enable technical achievements that are economically infeasible. If your cloud SIEM is volume-priced, watch for spikes in log volume due to a DDoS attack — being hit by economic DoS is a real risk.

During the steady-state operation of your cloud SIEM, monitor the collectors. Make sure that logs flow to the correlation engine in real time to confirm that rules are working correctly.

Cloud SIEM vendors are in a better position to execute on advanced analytics your team develops, so plan to use analytics functions that leverage the platform’s strengths. In other technology domains, the cloud can clearly enable better cross-customer data analysis, better model learning and other advantages relevant to advanced analytics functions.

In regard to use-case content, do not deviate from standard SIEM and security use-case practices. For example, make sure security processes, such as incident response, are in place, because you will still need to act on cloud SIEM alerts (see “How to Implement a Computer Security Incident
Response Program”). Also, review “How to Develop and Maintain Security Monitoring Use Cases” for details on developing use cases for SIEM.

Evidence

1. “Amazon Simple Storage Service (Amazon S3),” Amazon.

Recommended by the Authors

How to Operate and Evolve a SIEM Solution
How to Develop and Maintain Security Monitoring Use Cases
Use Central Log Management for Security Operations Use Cases
Solution Path for Implementing Threat Detection and Incident Response
SOAR: Assessing Readiness Through Use-Case Analysis

Recommended For You

Learning Sprints (Bose Corporation)
Magic Quadrant for Data Center and Cloud Networking
Critical Capabilities for Data Center and Cloud Networking
Forecast: Unified Communications, Worldwide, 2017-2024, 2Q20
Forecast: Mobile Phones, Worldwide, 2018-2024, 2Q20 Update