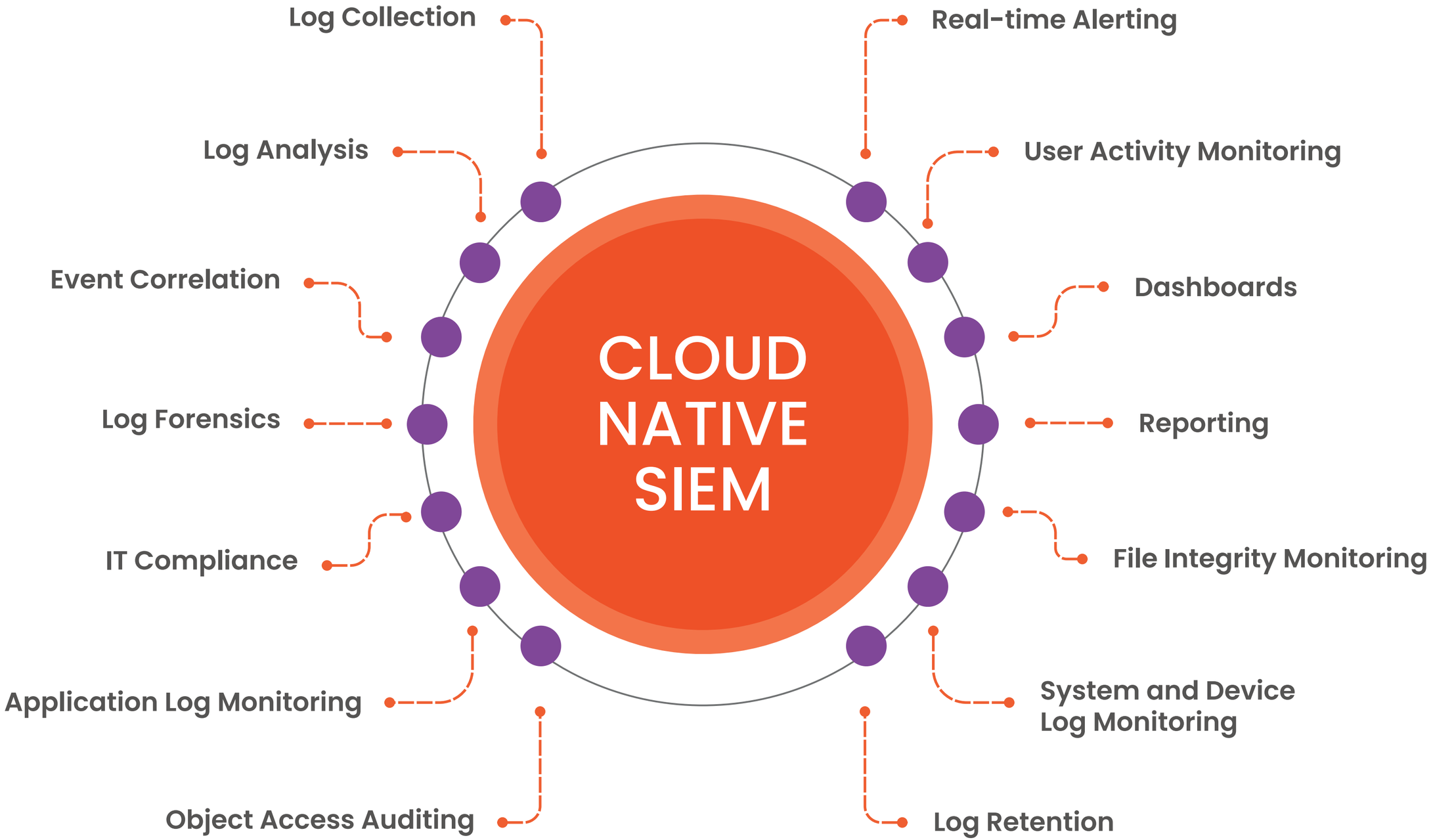
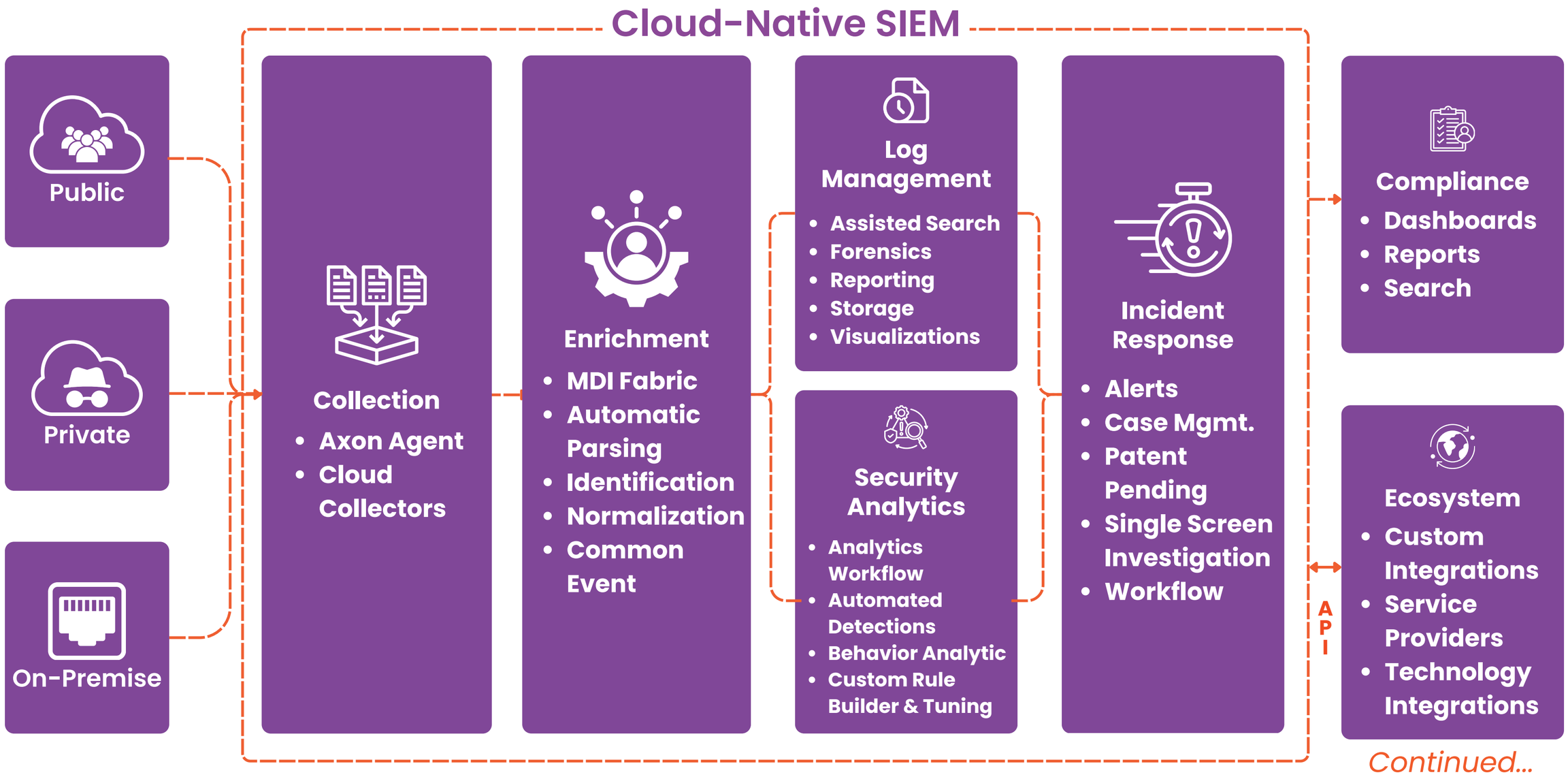
# DEMYSTIFYING CLOUD NATIVE SIEM

LMACS


Log Collection
Log Analysis
Event Correlation
Log Forensics
IT Compliance
Application Log Monitoring
Object Access Auditing
Real-time Alerting
User Activity Monitoring
Dashboards
Reporting
File Integrity Monitoring
System and Device
Log Monitoring
Log Retention
CLOUD
NATIVE
SIEM

# Quick overview Cloud Native SIEM




LMACS

*Continued...*

# Quick overview Cloud Native SIEM

Cloud-native SIEM solutions centralize data from various sources into a single cloud-based location

This approach offers faster and more cost-efficient deployment, automatic scalability, and the ability to leverage the cloud's speed and economies of scale

Cloud-native SIEM solutions integrate seamlessly with various cloud platforms and services, providing a centralized Security Operations Center (SOC) with dashboards that focus on security monitoring and management across cloud environments

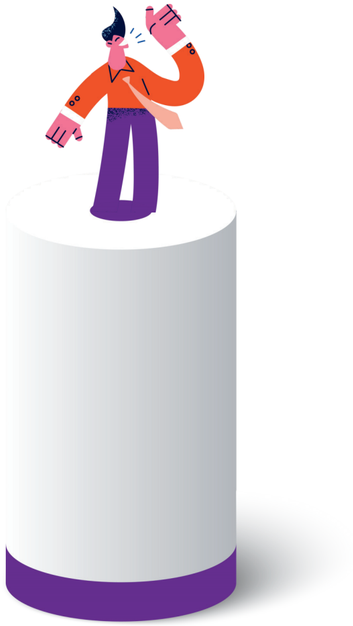
With cloud-native SIEM, organizations gain better visibility into distributed workloads, including servers, devices, infrastructure components, and users connected to the network

A unified dashboard provides real-time visibility into security events, allowing security teams to quickly identify, investigate, and respond to threats

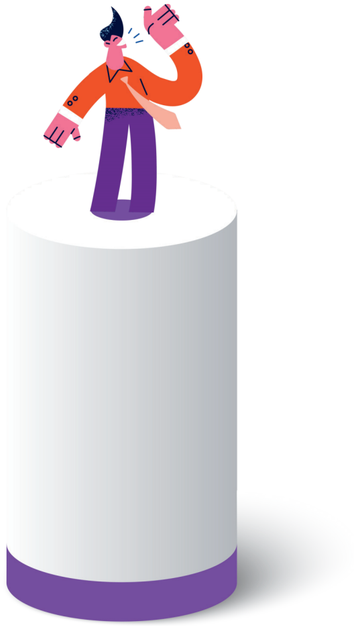
LMACS

# Here are some important features of a SIEM installation that is independent of any specific cloud service provider

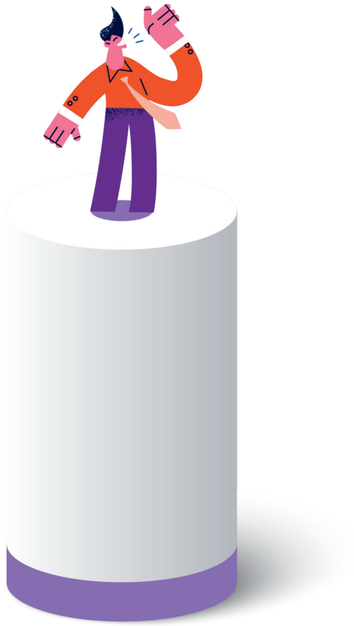
SIEM should support standardized data formats and protocols for easy data transfer.



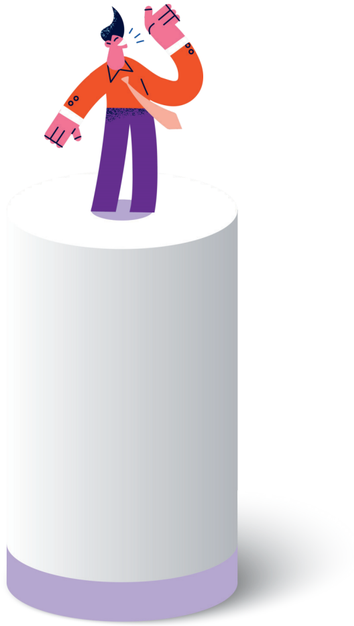
It should be compatible with multiple cloud providers for collecting and analyzing security data.



SIEM should be cloud-agnostic and not tied to any specific vendor's proprietary technologies.



There should be mechanisms in place to ensure data availability and resilience during cloud provider transitions or outages.



# Architecting for Detection
# Building a Solid Foundation – Cloud SIEM

Consolidate data from each central cloud account into an organization-wide, cloud-agnostic SIEM.

Combining cloud telemetry with SIEM helps security teams quickly identify hybrid attacks. Consider these architectural suggestions for effective execution.

Enhance your security team's ability to proactively combat emerging threats by integrating centralized cloud telemetry with your existing SIEM solution.

It is advisable to extend existing SIEM system capabilities to cover cloud environments.

Architect your detection strategy to enhance security posture and streamline operations.

Forwarding cloud telemetry into your established SIEM platform optimizes existing investments and ensures consistent approach to threat detection.

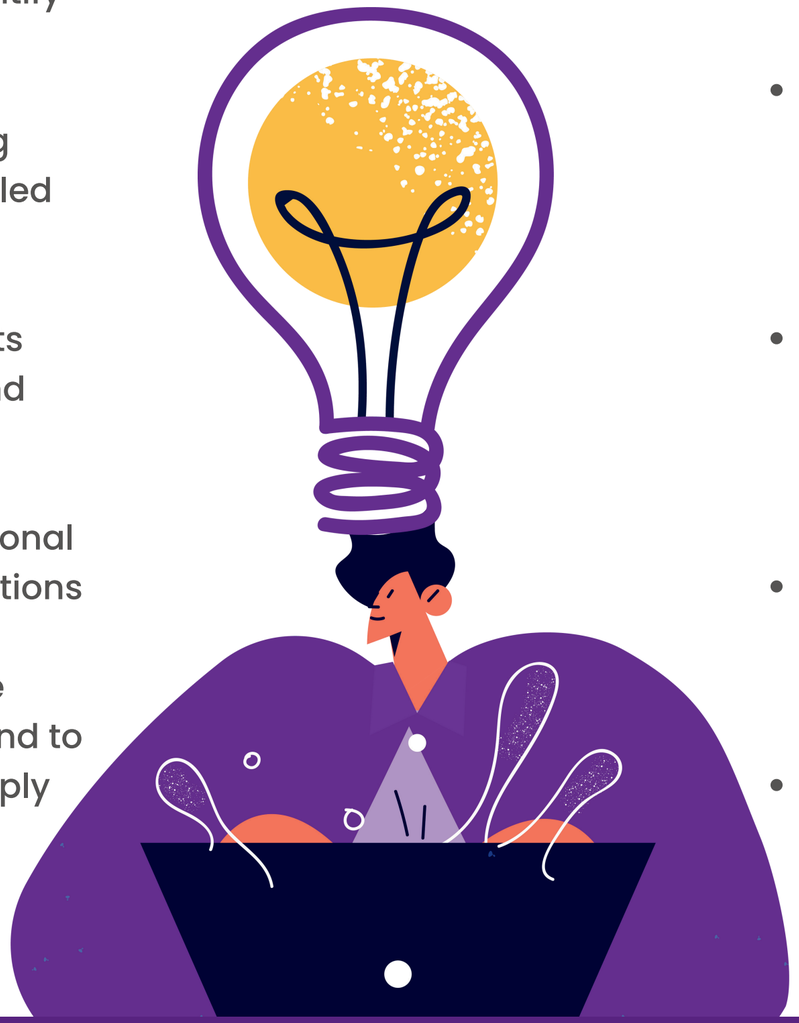
Establish a central account per cloud provider for multi-cloud environments.

Configure all telemetry sources in a central cloud account for a single source of truth.

A robust detection strategy requires a well-thought-out architecture for cloud infrastructure and detection platform.

# What are the benefits of using Cloud SIEM?

- Cloud-native SIEM employs advanced analytics, Artificial Intelligence (AI), and Machine Learning (ML) technologies to identify potential security threats
- Cloud SIEM assists organizations in meeting regulatory requirements by providing detailed security audit logs and reports
- Real-time monitoring of cloud environments with Cloud SIEM enables quick detection and response to security threats
- Cloud-based solutions help reduce operational costs compared with on-premise SIEM solutions
- Cloud SIEM enables organizations to secure their cloud infrastructure, detect and respond to security threats in near real-time, and comply with regulatory requirement



- Cloud SIEM enables centralized security management across multiple cloud platforms and services
- Cloud SIEM provides real-time alerts, actionable insights, and detailed reports to help IT teams quickly respond to security incidents and mitigate risks
- Organizations can handle more data with scalable cloud architecture, ensuring robust security, easy access, and optimal performance regardless of size
- Proactive threat detection allows IT administrators to stay ahead of malicious actors
- Automated tools manage the entire process of collecting security data, reducing manual work for administrators

# On-Premise SIEM vs Cloud-Native SIEM

| | |
|---|---|
| When the SIEM exceeded its EPS limit, the tool's performance for querying and data correlation was impacted | Cloud SIEM performance should not be impacted by log collection as it sits on a scalable cloud platform. |
| Nowadays, on-premise vendors can scale, but this may require additional investment or effort | In a cloud environment, scalability is not limited and generally occurs without any effort from the customer. |
| Operating system patches are usually neglected, and updating applications often disrupts log collection | The vendor will handle all network, operating system, and application updates while minimizing disruption to the collection process. |

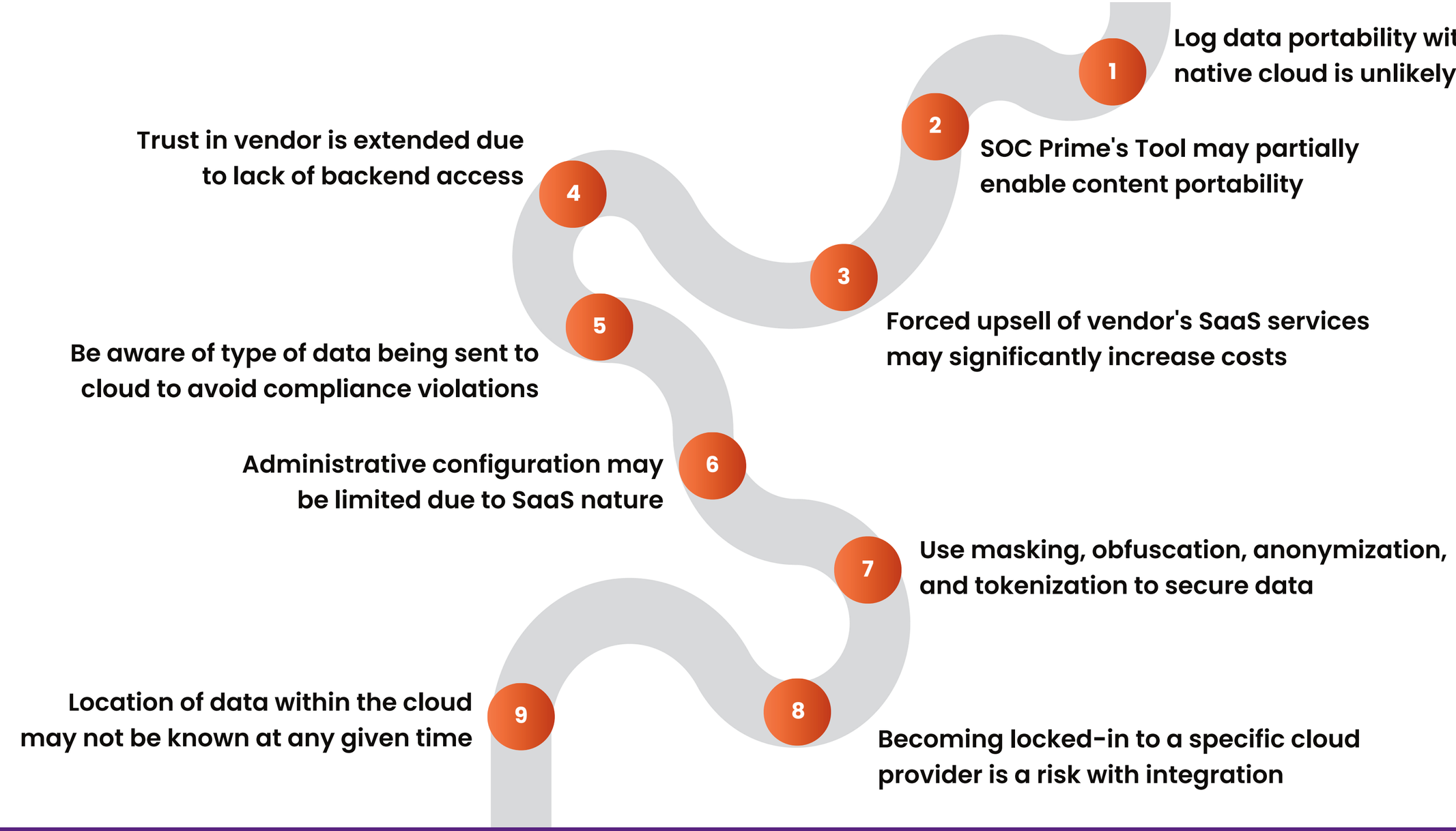
*Continued...*

*Continued...*

# On-Premise SIEM vs Cloud-Native SIEM

| On-Premise SIEM | Cloud-Native SIEM |
| --- | --- |
| It is difficult to provide a general statement about usability in on-premise SIEM solutions as it depends on the specific solution. | Simplicity is a key feature of cloud native SIEM solutions, making them easy to use. |
| Vendor quality of on-premise SIEM High Availability (HA) capabilities varies and some still experience log collection interruptions with fail-over unless a complex HA setup is considered. | Due to SaaS design, high availability is inherent and high SLA rates are typically guaranteed. |
| Most SIEM vendors include encryption in transmission, log obfuscation, and encryption at rest for confidentiality. | It is generally not recommended to send sensitive log information to the cloud. If data encoding is necessary, it should be performed on the data before it is sent. |
| Most SIEM vendors have comprehensive audit records on their SIEM applications, which provide detailed information and insights. | Every action on the system is logged in an API record, enabling detailed auditing of the solution's activities. |

# Critical highlights when using cloud native SIEM



# Use cases of Cloud Native SIEM

- SIEM helps detect potential security threats such as phishing attacks and endpoint threats
- It provides data to improve security operations and detect threats within a network
- Logs help identify how attackers penetrate a network and who attacked the organization
- Some endpoint security providers use the cloud for detection and response capabilities
- Cloud-based SIEMs can help meet security and compliance requirements for virtual workloads and distributed applications
- Some cloud-native SIEMs allow users to write, test, publish, and monitor custom correlation rules for assets and business entities

*Continued...*

*Continued...*

# Use cases of Cloud Native SIEM

- **Built-in AI in some cloud-native SIEMs can perform threat response, threat visibility, alert detection, and proactive hunting**
- **SIEM solutions can aid in detecting and preventing privileged access abuse, trusted entity compromise, and insider threats**
- **Cloud-native SIEM can monitor unwanted activity, third-party violations, departed employee activity, human errors, and overexposure of sensitive data**
- **Cloud-native SIEM can identify potential misuse of privileged access by correlating events across multiple data sources and applying advanced analytics, enabling security teams to mitigate risks quickly**
- **Cloud-based SIEM can monitor user accounts, servers, network devices, and antivirus monitoring for signs of compromise or malicious behavior**
- **Cloud-native SIEM with UEBA and ML identifies insider threat patterns**

# Here are some best practices for cloud SIEM

**Adjust correlation rules:**
Set thresholds for each customer you work with.

**Assign a SIEM administrator:**
This can help detect threats like targeted attacks, insecure configurations, and threat intel listed IPs.

**Establish security policies:**
Create policies for each application and use them when choosing a cloud provider.

**Implement a response plan:**
Outline roles and responsibilities, steps to take in case of an incident, and communication channels.

**It is important to provide training to staff on security practices and how to use cloud SIEM.**

**Use intrusion detection and prevention:**
These techniques can help identify threats in the cloud.

**Build automation:**
Respond to events and changes in your environment.

**Collect security log data efficiently:**
This can help improve security.

Article by

**Praveen Singh**

Infographics by

**Netpoleon India**

Techtalk Series-An initiative by

**Mohan Kumar T L**