securonix

7 Things to Consider When Migrating to the Cloud

Migrating to the cloud gives you scalability and growth. How can you ensure your migration goes smoothly? Here are factors to consider before your cloud migration.

What is a modern cloud SIEM?

A modern cloud SIEM is by definition cloud-native, developed for and running in the cloud.

- Modern SIEM offers full visibility over the environment.
- UEBA identifies deviations in normal that indicate threats.
- Unifies security data silos and incident response.

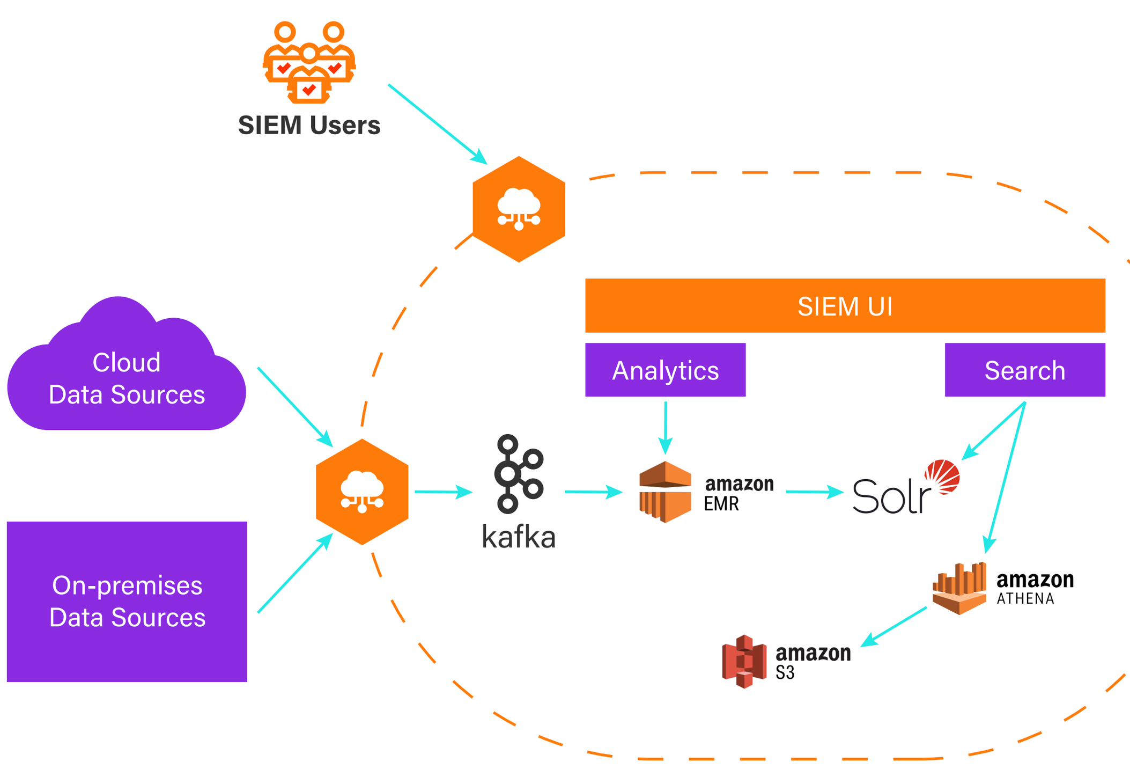
Understanding why you need the cloud

Compared to a traditional on-premises application, a cloud enterprise security software system always wins. Every aspect of the modern SIEM is best delivered by a cloud computing model.

SCALABILITY:
cloud SIEM manages and processes terabytes of data in near real time.

ELASTICITY:
resources are dynamically adjusted to meet application demands.

RESILIENCY:
applications run in redundant and secure environments and are not vulnerable to hardware failure.



A cloud-based SIEM architecture

Which cloud SIEM model should you choose?

When selecting a cloud SIEM solution, you can choose from three types of clouds according to how the responsibility is shared (single-tenant or multi-tenant, and the scalability range):

Customer Deployed in the Cloud
- Single tenant
- Customer responsible for hardware
- Customer responsible for software
- Scalability limited by complexity and architecture

Cloud-Hosted
- Single tenant
- Provider responsible for hardware
- Provider responsible for software
- Scalability possible but expensive

Cloud-Native
- Multi-tenant
- Cloud provider responsible for hardware
- Provider responsible for software
- Dynamically scalable

The three cloud SIEM models

What Types of Constraints Are There?

If you are planning to migrate to cloud-native SIEM, consider these software as a service (SaaS) constraints:

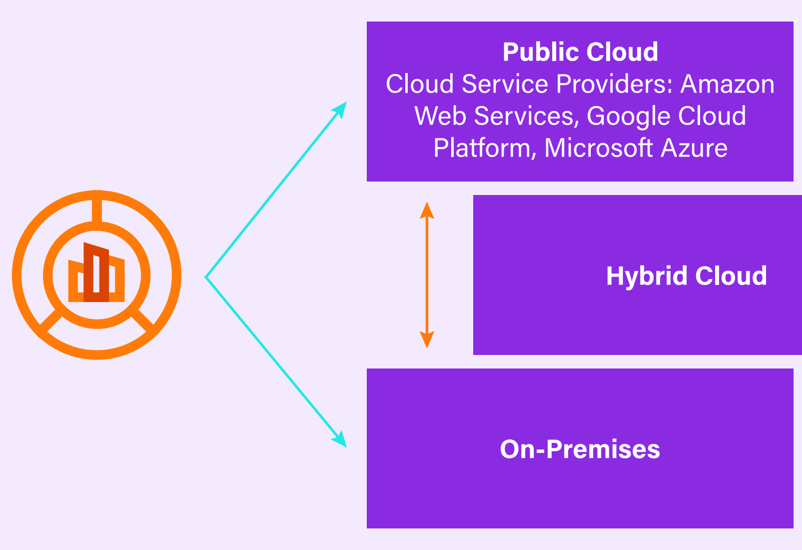
1. **REGULATORY CONSTRAINTS:**
there could be regulatory and legal constraints, like data privacy and sovereignty laws when choosing a cloud SIEM solution.
2. **BANDWIDTH:**
cloud-native SIEM requires enough bandwidth to ingest data and access the user interface.
3. **NETWORK RELIABILITY:**
applications run in redundant and secure environments and are not vulnerable to hardware failure.

How compatible is the system with your cloud?

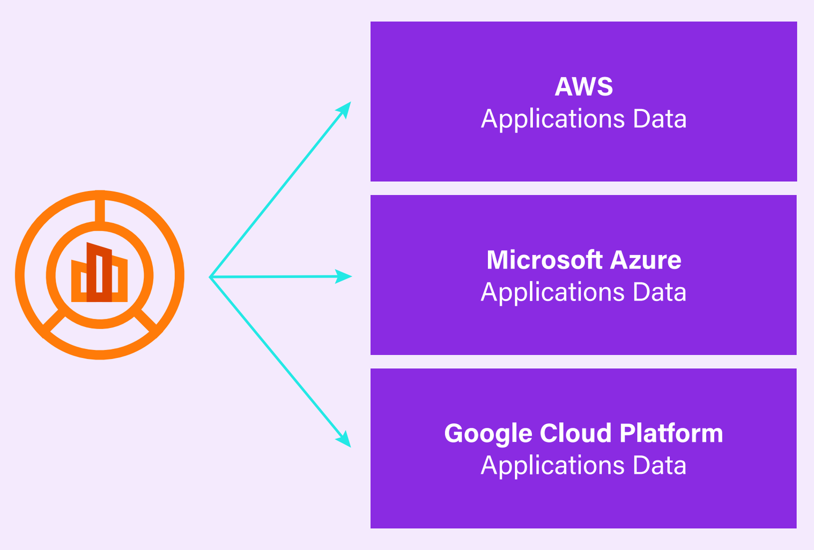
Different public clouds offer different capabilities and pricing models. Evaluate which fits better with your system:

HYBRID CLOUD:
a hybrid cloud integrates on-premises computing, storage, and services with those in the public cloud. This model can make SaaS SIEM viable for organizations that cannot leave their on-premises infrastructure.

MULTI-CLOUD:
uses multiple public cloud providers, delivering more reliability and lower latency.

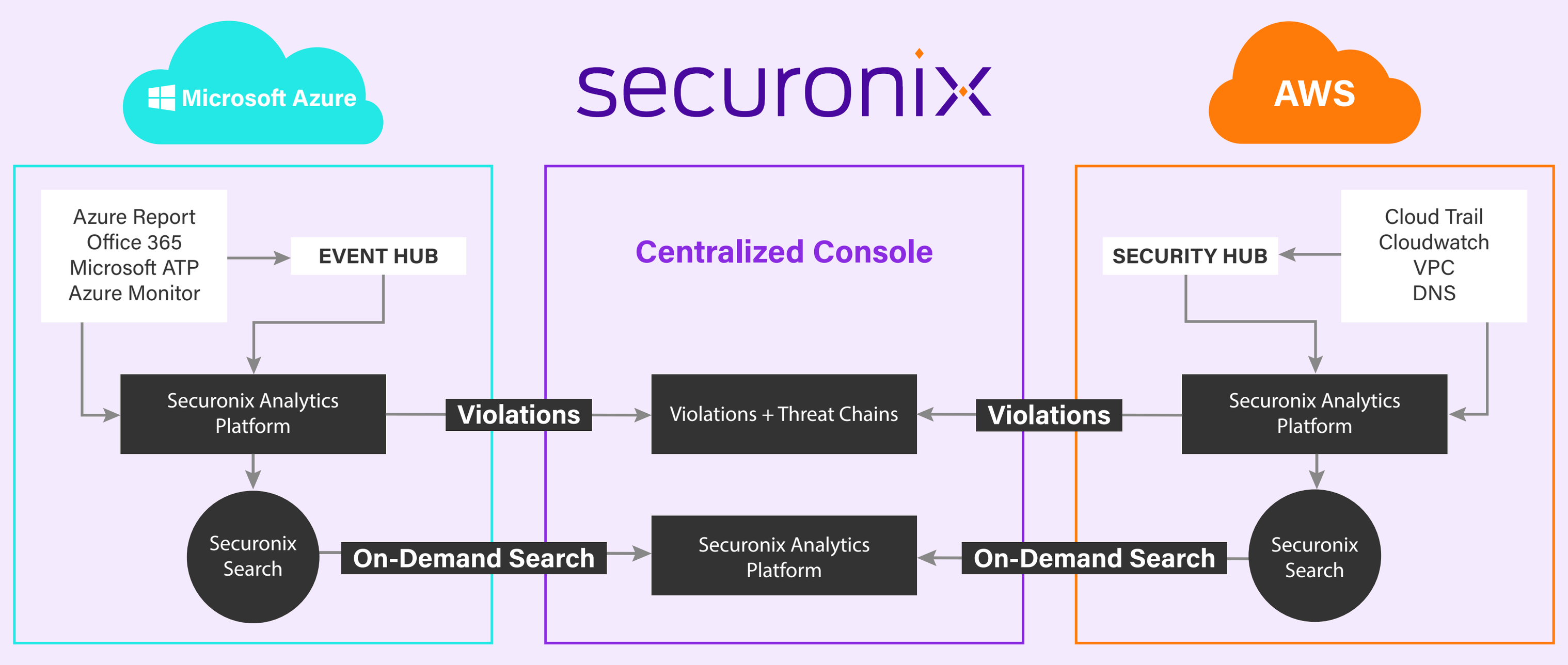


Hybrid cloud design



The multi-cloud strategy

FEDERATED SIEM DEPLOYMENT:
multiple SIEM instances can be deployed on multiple clouds and locations, adding another SIEM layer. This centralized console enables visibility and control over policies.



The federated cloud SIEM model

Evaluate integrations support

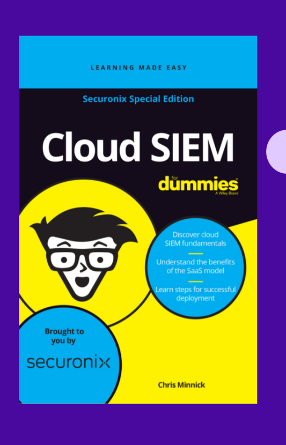
- The SIEM must integrate with the organization's existing data sources and devices.
- The higher the quality of your data, the better the results.
- Know the volume, velocity, and variety of your data.

Should you use a managed security service provider?

1. All cloud SIEM models reduce the investment and resources needed to operate a SIEM, but don't prevent you from managing them.
2. If you don't want the extra responsibility, managed security service providers (MSSPs) and managed detection and response (MDR) are additional options.
3. Using an MSSP eliminates the need for an onsite SOC, but it will require trust and partnership with your provider.

Ready to learn more? Click to read the Cloud SIEM for Dummies, Securonix Special Edition e-book:

GET e-BOOK



securonix

Sources and Footnotes

https://www.securonix.com/resources/cloud-siem-for-dummies/
https://swisscyberinstitute.com/blog/21-cloud-security-statistics-you-probably-didnt-know/