exabeam

EXABEAM SAAS CLOUD ENTERPRISE

Security operations without the operational overhead

Deploying, maintaining, and upgrading a legacy SIEM can require significant resources. This adds to the myriad of responsibilities today's already strained security operations center (SOC) teams face. And they can be enough to derail the adoption of newer SIEM technology that might otherwise improve security analyst productivity.

Burdensome operational overhead and maintenance isn't unique to SIEM—it's a prime value proposition driving the adoption of cloud-based services. When applications move to the cloud, the security data they generate moves with them. This creates challenges for the teams tasked with monitoring, securing, and proving compliance for such systems. Thus a need exists for new tools capable of efficiently ingesting and analyzing cloud activity data so as to identify threats.

As a software as a service (SaaS) deployment, Exabeam SaaS Cloud Enterprise solves these problems by transferring ownership of SIEM operations from your SOC staff to Exabeam. Additionally, its cloud-to-cloud data integrations easily ingest log data and detect threats and a predictable, user-based pricing model enables teams to store security data in the cloud without the fear of large, unpredictable bills.

MINIMIZE SIEM OPERATIONAL OVERHEAD

Exabeam SaaS Cloud Enterprise dramatically reduces deployment time and the operational overhead of managing a SIEM. Software upgrades, capacity management, and content updates are automatically handled. 24×7 health monitoring gives SOC managers the peace of mind that the system is functioning at peak performance. With SaaS Cloud, security analysts are freed from the responsibility of managing infrastructure to focus on higher value security tasks such as incident response and threat hunting.

KEEP SECURITY MANAGEMENT IN THE CLOUD

SaaS Cloud Enterprise keeps security management in the cloud by providing the full breadth of Exabeam's collection, detection, investigation, and response capabilities as a cloud-based service. Prebuilt connectors facilitate direct ingestion of data from cloud services. They help extend security visibility into SaaS application activity for threat detection and investigation, without the need to route data to on-premise data centers.

Data is aggregated and analyzed via user and entity behavior analytics (UEBA) to detect complex threats. Improving SOC productivity, playbooks reduce response times by automating incident investigation, containment, and mitigation using prebuilt connectors to other on-premise and cloud IT and security infrastructure.

KEY FEATURES

SaaS Cloud Enterprise reduces the operational overhead of SIEM by delivering the Exabeam Security Management Platform as a hosted cloud service.

Key SaaS Cloud Enterprise features include:

- Rapid deployment and quick return on investment (ROI)

- Predictable, user-based pricing that doesn't grow over time

- No operational overhead (e.g., maintenance, upgrades, capacity expansion)

- 24×7 health monitoring to ensure peak system performance

- Prebuilt integrations easily ingest data from popular cloud-based services and infrastructure providers

- Behavioral analytics to analyze data from any cloud or on-premise data source for threats

- Integration with Exabeam Threat Intelligence Service further improves threat detection based on a daily updated stream of indicators of compromise (IoCs)

- Response playbooks automate incident investigation, containment, and mitigation

- Enterprise security controls ensure data is handled according to best practices, including data encryption, third-party pen testing, and SOC type 2 compliance

EXABEAM SECURITY MANAGEMENT PLATFORM

Providing all of the Exabeam Security Management Platform solutions as a cloud service, SaaS Cloud includes:

- Exabeam Data Lake
- Exabeam Cloud Connectors
- Exabeam Advanced Analytics
- Exabeam Entity Analytics
- Exabeam Threat Hunter
- Exabeam Case Manager
- Exabeam Incident Responder
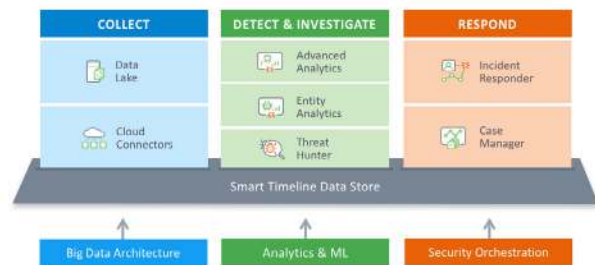
VISIT WWW.EXABEAM.COM/FREE-TRIAL TO GET STARTED.