EXABEAM CLOUD CONNECTORS

Reliably collect logs from over 30 cloud services

Cloud services and infrastructure are commonplace in today's modern network. Your business doesn't stop at the firewall, and neither should your security program. Ensuring you security team have visibility into activities within your cloud services requires the right information being sent to your SIEM. But, collecting logs from cloud services isn't always as easy as collecting them from on-premise solutions - coding is often required, and if you don't have the skills in-house to do this, you will likely need to involve a consultant. When your cloud services vendors make changes to their API, communications can break, resulting in blind spots for your security team.

Exabeam Cloud Connectors allow you to reliably collect logs from over 30 cloud services into Exabeam Data Lake or Exabeam Advanced Analytics. Updates are made automatically whenever there are API changes, so you don't need coding skills or costly professional service engagements to ensure the right data is being collected.

ENHANCE YOUR VISIBILITY

Prebuilt, turnkey Cloud Connectors are available for a broad range of cloud services, such as AWS, GitHub, Google, Microsoft Office 365, Salesforce, and many other cloud security, identity and access management, infrastructure and business applications.

EXTEND BEHAVIORAL ANALYTICS TO THE CLOUD

Cloud security solutions typically offer limited detection of malicious insiders, compromised credentials and other unknown threats. For example, imagine a disgruntled employee downloading your customer list from Salesforce or stealing source code from Github. Pairing Cloud Connectors with Exabeam Advanced Analytics allow you to combine cloud services activities with data from on-premises applications, to improve detection of attacker tactics, techniques and procedures using behavior-based threat detection.

ENSURE CONTINUOUS COMMUNICATION

Cloud service providers frequently change their APIs, which could lead to unexpected breakdowns in your cloud security and your ability to collect cloud logs if you aren't paying attention. With Cloud Connectors, updates are made automatically whenever there are API changes.

MODERNIZE ANY SIEM

Traditional SIEMs cannot natively ingest and analyze all the cloud logs — creating security and compliance blind spots. Cloud Connectors and Advanced Analytics allow you to collect cloud service logs to modernize your SIEMs or log management tools, including Alert Logic, Alien Vault, ArcSight, Elastic, IBM Qradar, Logpoint, LogRhythm, McAfee, RSA Netwitness, and Splunk.

MAINTAIN REGULATORY COMPLIANCE

As organizations like yours move their business into the cloud, there's often a need to audit and report on risk and regulatory compliance regarding cloud services. Using Cloud Collectors, cloud logs can be reliability collected into Exabeam Data Lake, or any other SIEM or log management tool, to provide the visibility needed to meet your regulatory requirements.

KEY FEATURES

Reliably collect logs from over 30 cloud services:

SECURITY PRODUCTS

- Carbon Black CB Defense
- Centrify
- Cisco Advanced Malware Protection (AMP)
- Crowdstrike Falcon
- CylancePROTECT
- Netskope
- Palo Alto Aperture
- Proofpoint Advanced Threat Protection (ATP)
- Rapid7 InsightVM
- Sophos Central
- Symantec Email Security.cloud
- Symantec Endpoint Protection (SEP) Mobile
- Symantec Web Security Service (WSS)
- Tenable.io

IDENTITY / ACCESS MANAGEMENT

- Centrify
- Duo Security
- Lastpass Enterprise

- Okta
- OneLogin

INFRASTRUCTURE

- Amazon Web Services (AWS)
- AWS Multi-Tenant
- Google Cloud Platform (GCP)
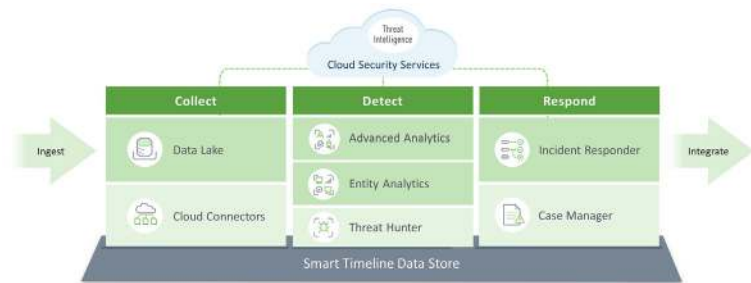- Microsoft Azure

BUSINESS APPLICATIONS

- Box
- Citrix ShareFile
- Dropbox Business
- Egnyte
- GitHub
- Google G-suite
- Microsoft Office 365
- Salesforce Sales Cloud
- ServiceNow
- Slack Enterprise Grid

EXABEAM SECURITY MANAGEMENT PLATFORM

Cloud Connectors is a key component of the Exabeam Security Management Platform. Exabeam's modular offerings can be mix-and-matched according to your organization's specific needs. Whether you're looking for a full SIEM replacement, or to enhance your current setup incrementally by augmenting it with improved threat detection, more cost effective logging, and improved productivity, we can help.

The platform includes:

- Exabeam Data Lake
- Exabeam Cloud Connectors
- Exabeam Advanced Analytics
- Exabeam Entity Analytics
- Exabeam Threat Hunter
- Exabeam Case Manager
- Exabeam Incident Responder