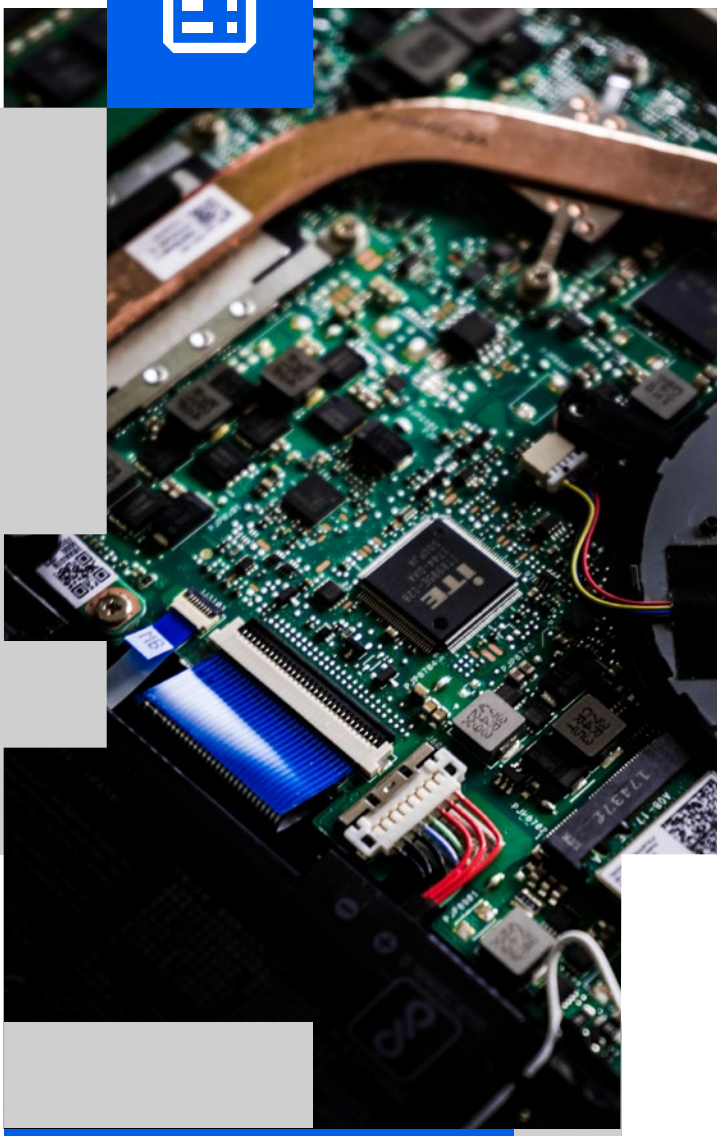
exabeam



Data Sheet

Exabeam + Google Cloud IDS

Incorporate alert and log data for improved behavioral analytics

Google Cloud Platform (GCP) provides the cloud foundation you rely on to build, run and scale your business. However, trusting all your data and critical applications in one place – even one as intrinsically secure as GCP – significantly increases your risk should you suffer a cyberattack. With Exabeam and Google Cloud Intrusion Detection System (IDS), you can dramatically increase your threat visibility across your Google Cloud workload traffic so that you can detect and respond to threats at cloud scale.

The security dilemma: Are your workloads safe from modern cyberthreats?

These days, most workloads are performed in the cloud. However, security operations teams rarely have the same visibility and detection capabilities for cloud-native workloads as they do for on-premises workloads. Attackers know this; that's why they're focusing more and more on targeting cloud workloads using intrusions, malware, spyware, and command-and-control attacks that can spread across a corporate network.

Key capabilities

- Use behavioral analytics to detect anomalous Google Cloud workload activity that may indicate a threat.
- Risk-prioritized analytics and pre-built playbooks help SOCs standardize response.

Thanks to Google Cloud's recent launch of Cloud IDS, security teams can now deploy a cloud-native network threat detection solution built for scale and availability. Using Palo Alto Networks' threat detection technology as a foundation, Cloud IDS delivers industry-leading network threat detection capabilities that are easy to share with any third-party SIEM/SOAR solution.

Exabeam and Cloud IDS: increasing Google Cloud threat visibility

Exabeam makes it simple to use your Cloud IDS log data to dramatically increase your threat visibility across your Google Cloud workload traffic, no matter if it comes from Google Compute Engines (GCE) or containers Google Kubernetes Engine (GKE).

By combining Exabeam and Cloud IDS, you can leverage user and entity behavior analytics (UEBA) based modeling to create a baseline for normal behavior to easily detect and remedy anomalous behaviors that may indicate a cloud-based attack, regardless of its origin.

Exabeam and Cloud IDS benefits

- **Total insight:** Utilize pre-built integrations to easily collect data from 500+ IT and Security products including Google Cloud.
- **Complete coverage:** By automatically building out user- and asset-specific behavior models across all your data and workloads in GCP, Exabeam creates a baseline for normal user behavior so you can detect unusual behavior that can indicate a threat.
- **Effective, automated response:** Pre-built playbooks help SOCs standardize triage, detection, investigation and response actions to any security event across Google Cloud Platform so you can maintain a consistent security posture across all your services.
- **Secure all your clouds and applications:** In addition to running natively on Google Cloud, Exabeam Cloud Connectors make it simple to collect logs from over 40 cloud services into Exabeam Data Lake, Exabeam Advanced Analytics, and any other security information and event management (SIEM) solution.

How Exabeam + Cloud IDS work together

Exabeam collects GCP-specific behavioral data like admin activities, data access, application activity, storage access and other services to build a baseline of normal behavior. Once it detects a deviation, it automatically flags and assigns a risk score to the abnormal activity.

Machine-built Exabeam Smart Timelines stitch together all activity before, during and after the deviation so that your SOC team can easily identify the attack and track it as it moves across Google Cloud and your network. You can then use pre-built playbooks to standardize your triage, detection, investigation, and response actions to any security incident.

Exabeam + Cloud IDS Use Cases

- **Compromised Credentials:** Detect and respond to credential theft, abnormal authentication, and interactions by users that indicate external compromise.
- **Lateral Movement:** Utilize user attribution to follow attacks even as they switch IP addresses, devices or credentials.
- **Privilege Escalation:** Prevent attackers from increasing the privileges of a compromised account.
- **Privileged Activity:** Identify and respond to unusual behavior by privileged accounts and assets, as well as privileged activity by non-privileged users.
- **Account Manipulation:** Prevent persistence techniques such as the creation or manipulation of a user or group that would allow an attacker to maintain access to a network.
- **Data Exfiltration and Leaks:** Gain visibility to data that has been illicitly transferred outside your organization by outside attackers or insiders like employees, partners or contractors.
- **Evasion:** Understand what actions attackers are taking to evade detection.
- **Abnormal Authentication and Access:** Identify abnormal authentication and interactions outside of typical usage or behavior patterns.
- **Data Access Abuse:** Identify data leakage by detecting users who access sensitive corporate data or resources that they shouldn't.

About Google Cloud

Google Cloud accelerates organizations' ability to digitally transform their business with the best infrastructure, platform, industry solutions and expertise. We deliver enterprise-grade solutions that leverage Google's cutting-edge technology – all on the cleanest cloud in the industry. Customers in more than 200 countries and territories turn to Google Cloud as their trusted partner to enable growth and solve their most critical business problems.

Find out how Exabeam can help secure your organization's Google Cloud environment by requesting a private demonstration: **sales@exabeam.com**

About Exabeam

Exabeam is a global cybersecurity leader that adds intelligence to every IT and security stack. We are reinventing the way security teams use analytics and automation to solve threat detection, investigation, and response (TDIR), from common security threats to the most critical that are difficult to identify. The Exabeam Security Operations Platform is a comprehensive cloud-delivered solution that leverages machine learning and automation using a prescriptive, outcomes-based approach to TDIR. It is designed and built to help security teams detect external threats, compromised users and malicious adversaries, minimize false positives, and make security success the norm. For more information, visit www.exabeam.com.

To learn more about how Exabeam can help you visit exabeam.com today.

exabeam