exabeam

SOLUTION BRIEF

EXABEAM AND AMAZON S3

Thwart Attacks on Cloud Storage Objects

ELASTICITY AT A COST:

Organizations are storing their data in the cloud to leverage the scalability, security, and performance of an object storage service. Cloud storage provides organizations the flexibility to scale resources up and down to meet their business' fluctuating demands. It also allows for data and access controls to be easily managed remotely, eliminating the need for costly data centers. As organizations look to transform their business, many turn to the cloud to drive their digital transformation.

Despite maintaining compliance programs like PCI-DSS, HIPAA, FedRAMP, and EU Data Protection Directive, cloud data storage has been at the root of many breaches these past few years. That is because configuration blunders can easily expose sensitive data, and go undetected by the organization. In fact, the number of breaches as a result of configuration errors are on the rise. Organizations need visibility into their cloud storage object activity to prevent exposed databases from compromising sensitive data like personal information, customer data or API data.

Amazon S3 AWS CloudTrail

> "Exabeam enables us to extend security to our cloud-based data," commented Richard Clark, VP, global technical security at cxLoyalty. "By understanding normal activity for cloud storage objects, we can identify anomalies based on deviations from typical behavior and detect potential threats. This level of visibility will empower our security analysts to take the necessary steps to secure our cloud-based data."

RICHARD CLARK, VP, GLOBAL TECHNICAL SECURITY, CXLOYALTY

CLOUD STORAGE MONITORING

The Exabeam Security Management Platform and Amazon S3 integration allows for a single platform to monitor the activity of users and entities, including cloud storage buckets. Leveraging the visibility from CloudTrail logs, Exabeam helps identify anomalies and enable security teams to more efficiently detect, prioritize, and investigate threats to cloud storage objects.

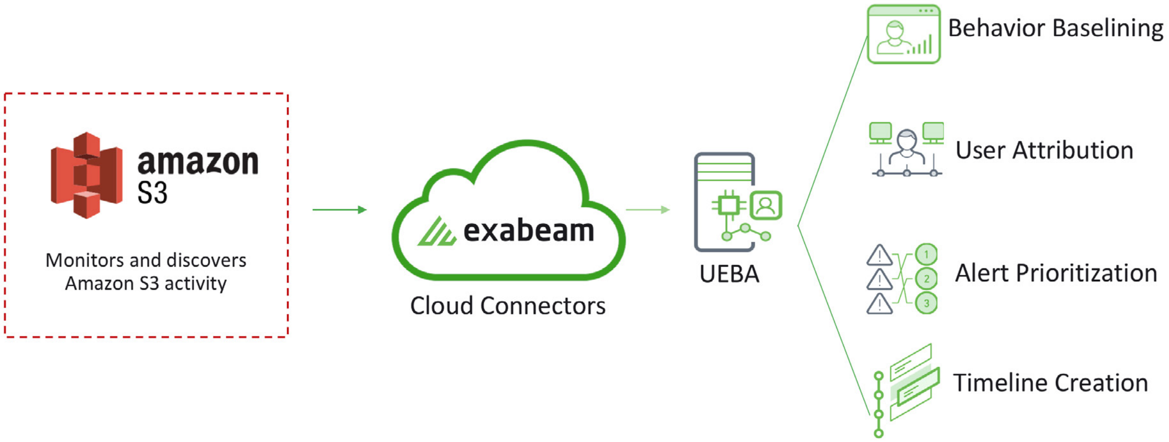
Exabeam's behavior analytics solution detects threats by identifying high-risk, anomalous activity. This happens by using machine learning to baseline normal activity for all users and entities in an environment. Once a baseline is available, Exabeam can automatically detect deviations compared to that baseline and assign that activity a risk score. Exabeam's machine-built incident timelines (Exabeam Smart Timelines™), stitch together both the normal and abnormal behavior for users and machines. These timelines include all information an analyst needs to perform a rapid investigation, including normal and abnormal behavior, as well as the surrounding context, like what happened before and after an alert, or whether the alert maps to a MITRE ATT&CK tactic or technique. With this joint solution, security analysts can easily follow attacks to cloud storage objects, helping security analysts identify attacks before they lead to exfiltration.

Key Integration Benefits:

- Enhance visibility of cloud storage objects through monitoring and identifying malicious activity and anomalies from a single platform
- Augments native audit data from AWS CloudTrail, Amazon S3 server access logs and AWS VPC netflow logs, with context to confidently identify malicious activity from normal behavior
- Integrates and enhances security alerts from GuardDuty, Amazon's native security monitoring solution
- Prioritize alerts confidently by associating security alerts to users and entities and sorting them by risk
- Expedite investigations with automated, machine-built timelines that follow attacks as they move between users, devices, and storage objects

TOP USE CASES

USE CASE / CHALLENGES	SOLUTION DESCRIPTION	BENEFITS
Identify Object Activity - Many organizations are unaware of activity occurring on their cloud storage objects.	Amazon S3 CloudTrail logs discover activity on cloud storage objects, identifying unauthorized access, threats, and anomalies. Exabeam then consolidates device data from Amazon S3 with security information events and logs from all security, identity, and contextual data sources in an environment.	Extended visibility into malicious and anomalous activity on cloud storage objects.
User attribution - Without the ability to discover and classify assets in an environment, security analysts are unable to easily associate an asset to users and can miss a key part of an attack.	Exabeam ingests Amazon S3 CloudTrail logs to automatically identify users associated with cloud storage.	Enhanced detection and visibility of advanced threats as security analysts can follow attacks that span between devices and users.
Alert prioritization - Analysts deal with an overwhelming volume of alerts from the numerous attacks happening across all devices and assets like cloud storage objects.	Exabeam aggregates alerts and activity by user, entity or cloud storage objects, prioritizes them by risk score, and focuses analysts in the highest risk threats.	Increase SOC efficiency and effectiveness by focusing analyst efforts on the highest risk threats.
Advanced threat detection - Limiting visibility of user or entity behavior to a single security vendor for all systems, makes it difficult to detect advanced threats.	Exabeam uses machine learning to distinguish normal and abnormal behavior for a user or cloud storage object, helping to identify risky activity—like that associated with credential compromise, exfiltration, and privilege abuse— even if it has never been seen before.	Improve security posture and detect modern threats with UEBA.
Lateral movement detection - Threats using lateral movement become difficult to detect due to changes in IP address, device, or credentials.	Patented host-to-IP-to-user mapping allows Exabeam to automatically follow attacks and attribute device activity back to the related user or cloud storage object, regardless of how an attacker moves through the network.	Ensure sophisticated attacks involving lateral movement don't go undetected.
Incident investigation - Analysts must spend too much time investigating an attack to ensure effective post-incident remediation.	Exabeam Smart Timelines enable analysts to dramatically reduce time spent on incident investigations by automatically stitching together events before and after an alert to give the full picture of an attack.	Enhance analyst productivity by automating tedious investigations with machine-built timelines.



AWS CLOUDTRAIL LOGS FOR S3 AND IAM ACTIVITY ARE INGESTED INTO EXABEAM THROUGH CLOUD CONNECTORS FOR UEBA-BASED THREAT DETECTION, PRIORITIZATION, AND RAPID INVESTIGATION.

HOW IT WORKS

- Collecting AWS CloudTrail audit logs for S3 and IAM activity, as well as AWS GuardDuty security alerts, from cloud storage objects whether it's access to objects, admin activity or enumeration of objects.
- Amazon S3 activity data is sent to Exabeam to be aggregated and analyzed alongside data from other security products
- Exabeam baselines normal user and device activity using UEBA and then automatically detects deviations from those behavioral baselines.
- Risk is added to the relevant user or entity for each anomalous activity detected
- Threats are automatically prioritized by risk score to focus analyst efforts on high-risk anomalies
- Exabeam stitches together Amazon S3 activity with third party security solutions' data to create machine-built incident timelines, for rapid threat investigation

ABOUT AMAZON S3

Amazon Simple Storage Service (Amazon S3) is an object storage service that offers scalability, data availability, security, and performance. This means customers of all sizes and industries can use it to store and protect any amount of data for a range of use cases, such as data lakes, websites, mobile applications, backup and restore, archive, enterprise applications, IoT devices, and big data analytics.

ABOUT EXABEAM

Exabeam is the Smarter SIEM™ company. We help security operations and insider threat teams work smarter, allowing them to detect, investigate and respond to cyberattacks in 51 percent less time. Security organizations no longer have to live with excessive logging fees, missed distributed attacks and unknown threats, or manual investigations and remediation. With the modular Exabeam Security Management Platform, analysts can collect unlimited log data, use behavioral analytics to detect attacks, and automate incident response, both on-premises or in the cloud. Exabeam Smart Timelines, sequences of user and device behavior created using machine learning, further reduce the time and specialization required to detect attacker tactics, techniques and procedures.

Exabeam is continuously adding new integrations with best of breed security vendors to its offering. These integrations are included as part of the solution at no additional cost, supporting organizations as they expand their security ecosystem, and providing peace of mind that Exabeam integrations will support your unique environment as it evolves over time. For more information, visit www.exabeam.com.

TO LEARN MORE ABOUT HOW EXABEAM CAN HELP YOU, VISIT EXABEAM.COM TODAY.