exabeam

SOLUTION BRIEF

EXABEAM AND NETSKOPE

Proactively Detect and Respond to Suspicious Cloud Activity with Exabeam and Netskope

MODERN CYBER THREATS OFTEN SPAN CLOUD AND ON-PREMISE SYSTEMS

As businesses embrace software as a service delivery, much of the day-to-day business activity of their users is moving from on premise systems to the cloud. Thus, cloud access security broker (CASB) solutions are increasingly valuable tools for detecting numerous risks to those systems, including compromised credentials and insider threats. And, while CASB solutions collect rich insights into the activity of end users accessing cloud services and websites, they do not offer a complete picture for security teams tasked with assessing risks. To understand the scope of an attack, these teams must also identify and block threats by collecting and analyzing a broader set of data from other security tools, servers, endpoints, badge readers and cloud services in order to collect, detect, investigate and respond to suspicious activity.

Exabeam's user and entity behavior analytics (UEBA) solution uses behavioral modelling to automatically baseline normal activity and detect anomalous behaviors indicative of a threat – across all your security solutions of choice. The powerful combination of Exabeam and Netskope uses behavior to bridge the gap between CASB and other security and IT infrastructure tools, as part of a modern security management strategy. The integration between Exabeam and Netskope also helps ensure cloud services are scrutinized similarly to on-premise solutions for consistent security monitoring and adherence to compliance regulations.

netskope

MONITOR CLOUD-ACCESS EVENTS AND IDENTIFY UNUSUAL ACTIVITY

Using Netskope CASB data, Exabeam enables rapid detection of threats by monitoring cloud-access events and identifying anomalous activities, such as excessive downloads, that could indicate compromised credentials, privileged account abuse or sensitive data loss. Machine-built incident timelines automatically

bring together normal and abnormal behaviors for users and devices, allowing SOC analysts to quickly and efficiently analyze and respond to threats using incident response playbooks that ensure timely and consistent action.

INTEGRATION BENEFITS

COLLECT

Collect unlimited Netskope CASB data for threat detection and eliminate unpredictable volume-based expenses with Exabeam's flat pricing model. Quickly collect and search all your data sources for analysis and centralized compliance reporting, without making compromises due to lack of scalability or budget.

DETECT

Analyze data from cloud-based services, like email, CRM and file sharing, in conjunction with other security and infrastructure solutions to detect anomalous activity. Generate behavioral baselines unique to your organization, employees, and team, and automatically identify risky behavior that may be indicative of security incidents or threats – even attacks that have never been seen before. Eliminate manual gathering and assembly of data from multiple, disparate systems into incident timelines.

INVESTIGATE

Improve productivity by dramatically reducing the time analysts spend investigating incidents with intelligent risk scoring and Exabeam Smart Timelines that automate the manual process of gathering evidence and assembling incident timelines.

> "The joint Netskope/Exabeam solution helps security teams track threats no matter where they spread. By combining best of class CASB data with security, context, and infrastructure data from other tools for analysis, the solution easily detects and investigates advanced threats even if they move laterally through both cloud and on-premise systems."
>
> **CHRIS STEWART, SR. DIRECTOR OF BUSINESS DEVELOPMENT, EXABEAM**

RESPOND

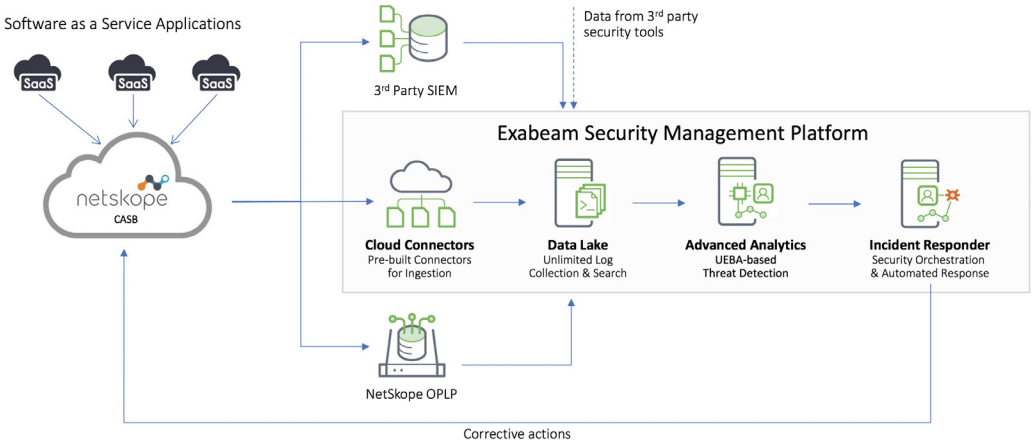
Reduce human error and boost response productivity with response playbooks that automate and standardize actions including containment, mitigation and response using pre-built security orchestration, automation, and response (SOAR) actions specific to the Exabeam-Netskope integration.

TOP USE CASES

- Compromised and malicious user activity detection
- Data exfiltration via SaaS applications and file sharing services
- IaaS and PaaS Visibility and Monitoring
- Anomalous web activity monitoring

Analysts can run three actions in Netskope directly from Exabeam including:

- Update File Hash List
- Update URL List
- Update Group



UNLIMITED NETSKOPE CASB DATA IS INGESTED INTO EXABEAM FOR CENTRALIZED LOGGING, UEBA-BASED THREAT DETECTION, AND AUTOMATED INCIDENT RESPONSE.

HOW IT WORKS

- Netskope monitors user activities across thousands of cloud services and millions of websites using its CASB solution.
- Exabeam ingests this cloud service and website telemetry via Netskope's API, Exabeam Cloud Connectors, or a 3rd Party SIEM. Exabeam parses, normalizes and enriches the data with context from your environment.
- Logs are sent to Exabeam Data Lake for unlimited log collection and search, and ingested into Advanced Analytics for analysis and threat detection.
- Exabeam baselines normal cloud service and website access activity for your organization using UEBA and then automatically detects deviations from those behavioral baselines.
- Risk is added to the relevant user, entity or device for each anomalous activity detected.
- Concurrently, Exabeam stitches together Netskope data with third party security solutions' data to create machine-built incident timelines for rapid threat investigation.
- When user risk scores surpass a pre-defined risk threshold, an incident is opened in Exabeam's case management system.
- Response playbooks in Exabeam Incident Responder — a SOAR solution with pre-built integration points with the Netskope platform— take corrective actions in the relevant systems using NetSkope

exabeam

ABOUT NETSKOPE

Netskope helps the world's largest organizations take full advantage of the cloud and web without sacrificing security. Their Cloud XD technology helps eliminate blind spots by quickly targeting and controlling activities across thousands of cloud services and millions of websites. Netskope customers benefit from 360-degree data protection that guards data everywhere and advanced threat protection that stops elusive attacks.

ABOUT EXABEAM

Exabeam empowers enterprises to detect, investigate and respond to cyberattacks more efficiently so their security operations and insider threat teams can work smarter. With Exabeam, 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 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.

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