TECHNOLOGY PARTNER BRIEF

Symantec Technology Partner: Exabeam

Intelligently prioritize and automatically investigate suspicious DLP alerts with Exabeam and Symantec

Symantec

exabeam

Partner Product: Risk Fabric / Information Centric Analytics (ICA)

Symantec Product: DLP

Tackling data loss can be overwhelming to security teams

The threat of unauthorized exfiltration of sensitive data shows no signs of abatement. In fact, preventing or mitigating data loss is becoming more difficult as data is increasingly stored and accessed on local networks, in cloud services, and on mobile devices. Thus data loss prevention (DLP) solutions are essential tools for detecting organizational data that may be at risk from external bad actors, malicious insiders and even well-meaning but negligent employees. And, while DLP solutions alert security teams to suspicious activities, they also generate high volumes of alerts – many of which may be false positives. Responding to this deluge can overwhelm even the highest performing security teams. To understand the true scope of an attack, teams need to quickly parse through these alerts and identify anomalous activity in order to collect, detect, investigate and respond to suspicious activity.

Exabeam's user and entity behavior analytics (UEBA) solution uses behavioral modelling of users, peer groups, and other tools to automatically baseline normal activity, assign a risk score to suspicious events and intelligently prioritize them for further evaluation – across all your security solutions of choice. The powerful combination of Exabeam and Symantec Data Loss Prevention uses behavior to bridge the gap between DLP and other security and IT infrastructure tools as part of a modern security management strategy.

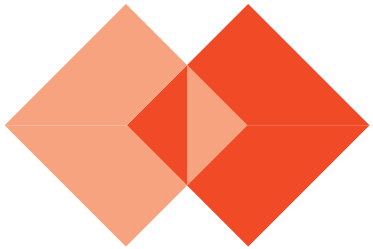
Quickly and efficiently analyze massive amounts of DLP data

Exabeam and Symantec allow security professionals to monitor DLP events and quickly identify anomalous activities, like excessive downloads, that could indicate compromised credentials, privileged account abuse or sensitive data loss. By creating a baseline for normalized behavior of users, peer groups and other t ools, and parsing through massive amounts of DLP data, Exabeam identifies DLP alerts associated with high-risk users and machines to aid security teams in successfully detecting anomalous behavior and prioritizing incident response. Exabeam behavioral modelling also makes it possible to recognize legitimate business events or abnormalities that many not be malicious such as a misconfiguration that might otherwise be flagged for investigation, relieving staff of the time-consuming task of following up on unnecessary events. Machine-built incident timelines create greater efficiencies, allowing SOC analysts to quickly and efficiently analyze and respond to threats using incident response playbooks that ensure timely and consistent action.

“

The combination of Symantec DLP and Exabeam provides joint customers a powerful tool to effectively detect, prioritize, and investigate data loss and data exfiltration at scale.”

Chris Stewart
Sr. Director of Business Development
Exabeam



Integration benefits

Collect
Collect unlimited Symantec DLP data for threat detection and eliminate unpredictable volume-based expenses with Exabeam’s flat pricing model. Free security teams to remove exclusions that may have been put in place to save time and budget and make all of their Symantec DLP data available for ingestion and analysis. Quickly collect and search on the broader set of data sources needed to find insider threats, like data exfiltration, without making compromises due to lack of scalability or budget.

Detect
Exabeam UEBA uses DLP alert data, alongside data from a wide assortment of third-party security and infrastructure tools to establish a baseline behavior and pattern set for entities and users and prioritize DLP alerts involving users or machines that are exhibiting a high degree of anomalous activity.

Investigate
Dramatically reduce the time analysts spend investigating incidents, including DLP alerts, with intelligent alert prioritization, even for attacks not seen before. Exabeam Smart Timelines - automate the manual assembly of evidence from multiple, disparate systems into machine-built incident timelines that accurately pinpoint anomalous events and improve productivity while significantly reducing response time.

Respond
Reduce human error and boost response productivity with pre-built, out-of-the-box playbooks that automate and standardize incident response actions including threat containment, mitigation and response.

Top use cases

- Protect against theft and accidental data disclosure by trusted insiders
- Reduce mean time to identify data breaches
- Maintain compliance with corporate and governmental data regulations/ Identify non-compliant data migration
- Protect from data loss associated with BYOD and IoT

How it works

- Exabeam ingests Symantec DLP alerts, as well as data from third party security solutions, and contextual sources of information like Active Directory and change management databases (CMDBs). Exabeam parses, normalizes and enriches the data with context from your environment.
- Exabeam creates a behavioral baseline for all users, entities, and devices in your environment. Identifies DLP alerts associated with users and machines exhibiting high degrees of anomalous activity and automatically prioritizes them based on risk scores. Exabeam Smart Timelines stitch all user activity into a machine-built incident timeline for rapid investigation.

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.

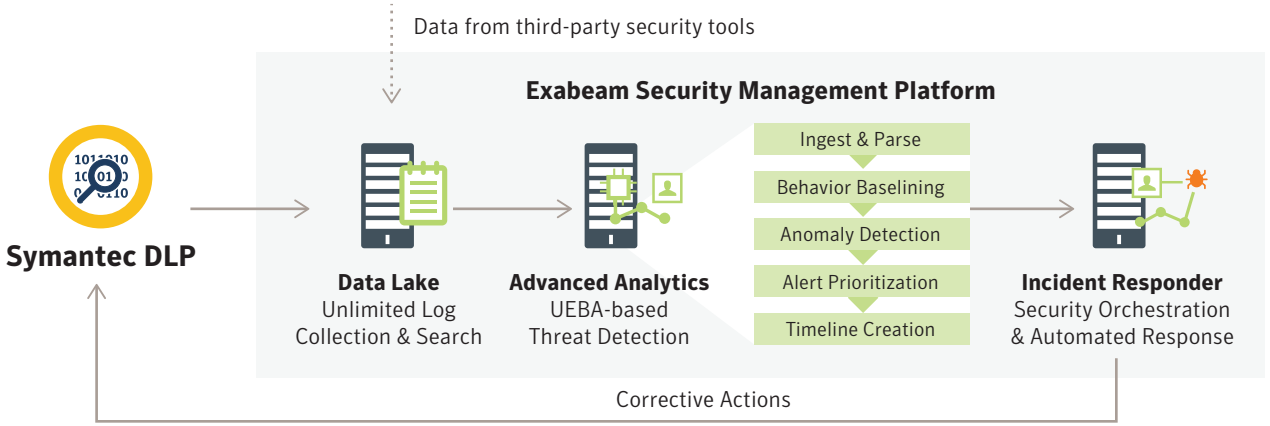
To learn more about how exabeam can help you, visit exabeam.com today.

- Once a risk threshold has been reached for a particular user, entity or device, it is pushed into the Exabeam dashboard on a watch list with an attached timeline.
- A case is opened in the Exabeam case management system, and all data from the Exabeam analytics engine is added to the ticket.
- Response playbooks can be used to take corrective actions in Symantec DLP to prevent data loss.

About Symantec DLP

Symantec Data Loss Prevention (DLP) solution delivers the levels of protection organizations need to prevent data breaches and safeguard their reputation. With Symantec industry-leading technology, customers get comprehensive discovery, monitoring and protection capabilities that give visibility and control over their confidential data.

Symantec DLP alerts are ingested into exabeam for analytics-based alert prioritization, rapid alert triage, and response automation.



About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com, subscribe to our blogs, or connect with us on Facebook, Twitter, and LinkedIn.

Symantec

350 Ellis St., Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com

20B273682_SB_TIPP_EXABEAM_EN