EXABEAM SECURITY MANAGEMENT PLATFORM

Legacy SIEMs no longer meet the needs of most organizations. While the premise of SIEM—to provide complete visibility into threats unfolding on a network and enable automated, intelligent responses—sounds as attractive as ever, most SIEMs have become outdated and are unable to fulfil that promise. They're built on aging, proprietary log data management technologies that are (over)priced based on data volumes; lack intelligent, machine learning-based analytic capabilities; and require deep technical skills to operate. To highlight the issues, nearly every company that suffered a public breach in recent years had relied on a legacy SIEM at the time of breach. Modern security organizations deserve better.

EXABEAM – THE SMARTER SIEM™

Exabeam Security Management Platform (SMP) empowers enterprises to detect, investigate, and respond to cyberattacks more efficiently so their security operations and insider threat teams can work smarter—not harder. Security organizations no longer have to live with excessive logging fees; missed distributed attacks and unknown threats; or time-consuming manual investigations and remediation. Equipped with the Exabeam Security Management Platform, analysts can collect unlimited log data, use behavioral analytics to detect attacks, and automate incident responses—both on-premises or in the cloud.

PRICED BY USER, NOT BYTES

Unlike Legacy SIEMs, Exabeam isn't priced based on data volumes. Instead, Exabeam Security Management Platform offers unlimited data ingestion using a predictable, user-based pricing model. This means you no longer need to fear that chatty data sources such as firewalls, endpoint detection and response, or web proxies will bloat your SIEM expenditure.

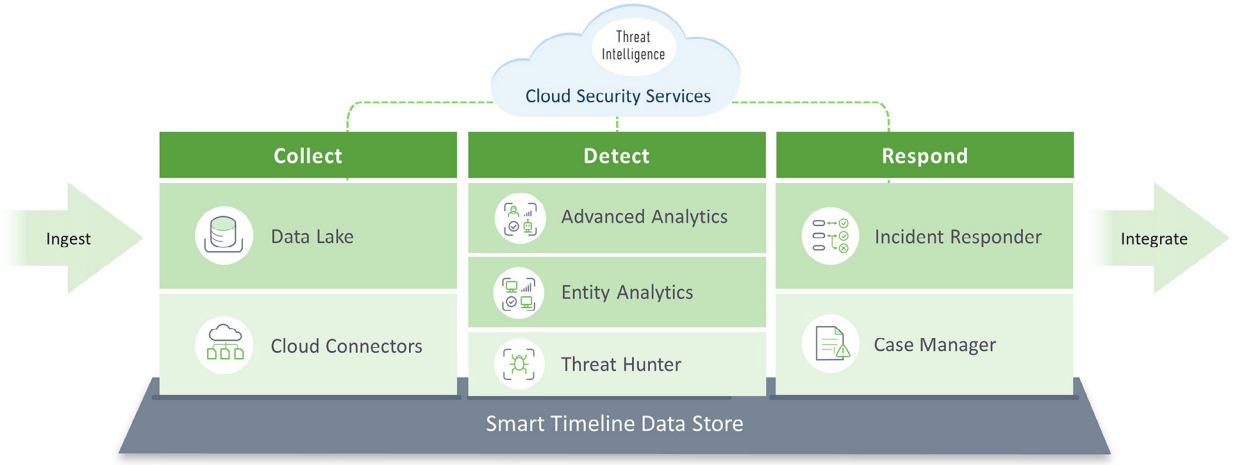
DETECTION USING BEHAVIOR, NOT RULES

Exabeam detects complex insider threats using user and entity behavior analytics (UEBA). This approach to threat detection reduces false positives and eliminates the maintenance overhead that traditionally results from the use of static correlation rules. UEBA not only identifies risky anomalies, it also recreates entire attack chains using Exabeam's Smart Timeline technology. Smart Timelines automate the process of gathering evidence and assembling it into a timeline to assist analysts in understanding the scope of any attack.

INVESTIGATION AND RESPONSE IN MINUTES, NOT DAYS

Exabeam increases the productivity of incident response (IR) and security operations center (SOC) staff by leveraging automated playbooks and API-based orchestration (SOAR). Prebuilt or customized incident playbooks and workflows standardize response procedures from a self- contained case management system. This ensures swift, repeatable incident response that amplifies productivity while minimizing human errors.

EXABEAM SECURITY MANAGEMENT PLATFORM



The Exabeam Security Management Platform encompasses the following solutions, delivered as physical or virtual appliances, or as a cloud service:

- **Exabeam Data Lake** – Unlimited, security data collection and storage, without volume-based pricing
- **Exabeam Cloud Connectors** – Turnkey connectors to extend security monitoring to cloud-based services and infrastructure providers
- **Exabeam Advanced Analytics** – Advanced behavior analytics to detect complex threats and lateral movement
- **Exabeam Entity Analytics** – Behavior analytics for internet-connected devices and user-less machines
- **Exabeam Threat Hunter** – Point-and-click threat hunting that returns machine-built timelines
- **Exabeam Incident Responder** – API-based security orchestration and response playbooks to amplify SOC analyst productivity
- **Exabeam Case Manager** – Feature-rich case management, directly integrated into all detection, investigation, and response workflows

FOR MORE INFORMATION, PLEASE CONTACT EXABEAM AT INFO@EXABEAM.COM