exabeam

Product

Exabeam Overview

## Giving your organization the best chance to outsmart the odds

Odds are your organization is the target of a cyberattack. Odds are there is an employee who is compromised. Odds are a rogue insider is quietly siphoning sensitive data out of your environment. When it comes to keeping your organization secure the odds are definitely stacked against you.

All too often security products operate in silos failing to share critical data with other security products making it easy for attackers to evade detection. Even with a SIEM deployed, organizations struggle due to their complexity and are left in a constant state of recovery. Exabeam is dedicated to breaking this never-ending losing cycle by delivering innovative products and services that empower organizations to outsmart attackers and beat the odds.

> Understanding what's going on inside our environment, from the perspective of data movement and data loss gives us a holistic view to make it easier to identify abnormal events.
>
> **Deneen Defiore**
> **VP & Chief Information Security Officer**
> United Airlines
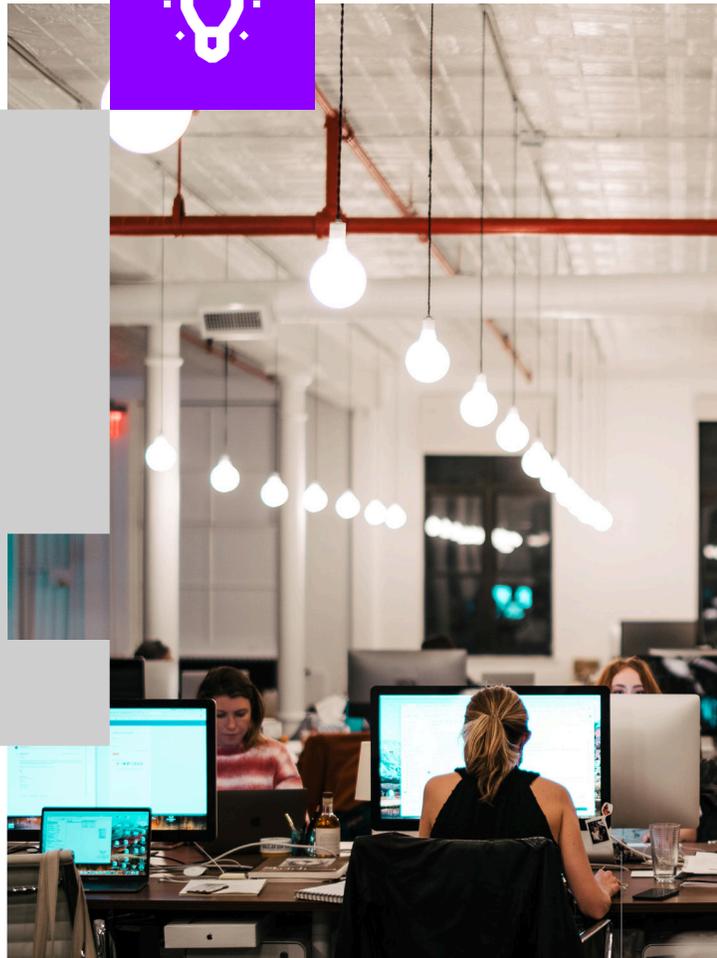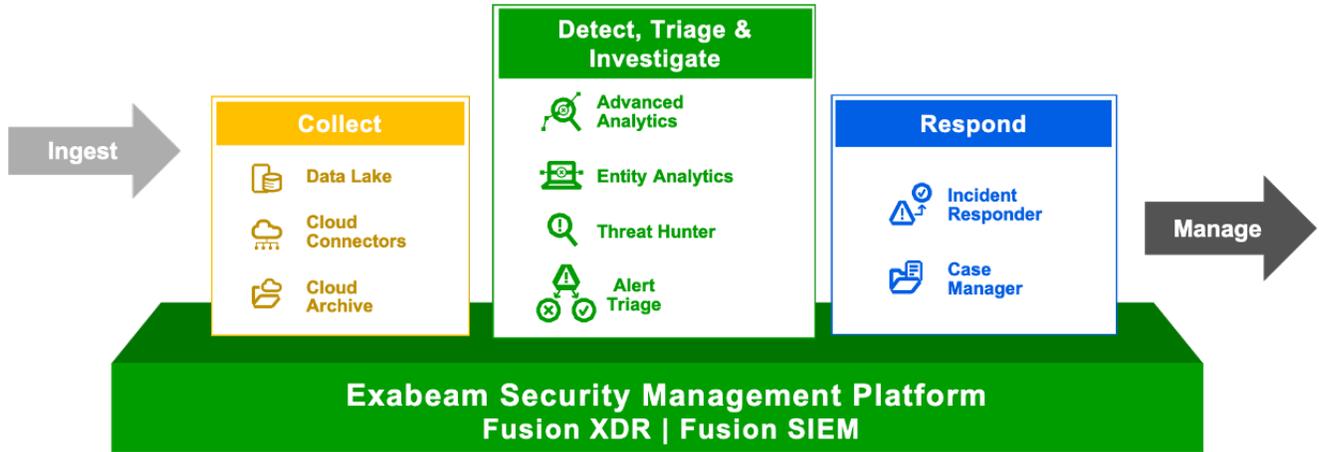
Exabeam delivers industry-leading security analytics coupled with automated threat, detection, investigation, and response (TDIR) purpose-built for today's environments. Unlike other security platforms that rely on experts to complete time-consuming manual processes to reach a conclusion, Exabeam automates every step in the TDIR workflow, from data collection through the "last mile" of the investigation, enabling security analysts of any skill and experience to complete comprehensive investigations.

With Exabeam organizations can:

- Easily collect valuable data from any of the 500+ security, IT, and productivity products with pre-built integrations

- Continuously and automatically analyze collected data, identifying threats that would otherwise go unnoticed

- Standardize SecOps processes using automated TDIR playbooks and field-vetted investigation checklists without replacing your current SIEM

- Remove the need to purchase and maintain expensive hardware, with cloud-delivered solutions accessible from any web browser

- Meet your security compliance needs with ease

Exabeam Security Management Platform

The Exabeam Security Management Platform is modular and delivered as a cloud solution or through a managed security service provider (MSSP).

- **Exabeam Fusion XDR**: Efficiently detect, investigate, and respond to threats without disrupting your existing security stack.

- **Exabeam Fusion SIEM**: Fusion XDR plus advanced SIEM capabilities delivered in a single modern SecOps solution.

Comprehensive threat detection, investigation and response (TDIR) for successful outcomes

Capabilities

- **Alert triage**: Quickly and confidently dismiss or escalate security alerts at scale

- **Behavior analytics**: Advanced user and entity behavior analytics deliver modern threat detection and investigation

- **Case management**: Purpose-built workspace to manage and collaborate on incident resolution

- **Cloud Connectors**: Pre-built, reliable log collection and response orchestration for over 40 cloud services

- **Log management**: Exabeam Data Lake provides a highly scalable data lake for lightning-fast log storage, search, and management

- **Response automation**: Security orchestration, automation, and response (SOAR) enables consistent automated TDIR process across the entire security team, dramatically improving efficiency and outcomes

- **Threat hunting**: Point-and-click search interface enables fast threat identification without writing complex queries or requiring significant security expertise

- **Threat intelligence**: Real-time insight into malicious hosts and other indicators of compromise

Use-case centric approach

Industry analysts, as well as SOC leaders, recognize the need for pre-packaged content as part of a successful security strategy. Exabeam offers:

- **Pre-packaged use case coverage** helps organizations solve specific problems by providing visibility, detection models, investigation checklists, and response playbooks.

- **Use case content and features** for each stage of the analyst workflow, not just detection.

- **Clear guidance on the data sources** needed for security teams to protect against external and internal threats.

Exabeam automates manual, repetitive tasks

Based on a Ponemon research study, SOC teams spend 12% of their time on detection, 36% on triage, 26% on the investigation, and 26% on response. Yet most cybersecurity vendors provide security analytics that only automates the detection and response parts of the workflow. Exabeam automates the entire TDIR process to:

- Improve security teams' productivity at every phase of their workflow

- Assist with detection, triage, and investigation saving significant analyst time

- Enable junior analysts to make decisions, while advanced threat hunters focus their efforts on raw log analysis

Select Awards & Recognition

The Exabeam difference

Both customers and industry analysts recognize Exabeam as a leading security vendor, with the Exabeam solution positioned in the coveted Leaders quadrant of the Gartner Magic Quadrant for the third year in a row. This sort of recognition doesn't happen by accident. Exabeam "cracked the code", delivering best-in-class TDIR support with the following unique capabilities:

- 100% automation across the entire TDIR workflow
- Embedded machine-learning algorithms that continuously learn and enable better, faster, more effective TDIR
- Smart Timelines with risk scores that provide a comprehensive view of user activity that anyone can understand

The Exabeam outcome-based approach to security has helped organizations around the world outsmart attackers and consistently beat the odds. Securing a dynamic organization is always going to be challenging, but with Exabeam security teams of any size and ability finally have a way to stack the deck in their favor.

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 Management 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