



# Seize the Breach<sup>TM</sup>

Eliminate your blindspots and respond to threats faster and more accurately with Exabeam.



**Exabeam can help you  
detect, investigate, and  
respond more quickly and  
accurately to threats to  
Seize the Breach™ and  
mitigate damage.**

# Analytics. Automation. Outcomes.

## About Exabeam

Exabeam is a global cybersecurity leader that adds intelligence to every IT and security stack. The leader in Next-gen SIEM and XDR, Exabeam is 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.

Exabeam offers a comprehensive cloud-delivered solution that leverages machine learning and automation using a prescriptive, outcomes-based approach to TDIR. We design and build products to help security teams detect external threats, compromised users and malicious adversaries, minimize false positives, and best protect their organizations.

For more information,  
visit [www.exabeam.com](http://www.exabeam.com) →

## Products

### Exabeam Fusion XDR

Efficiently detect, investigate, and respond to threats without disrupting your existing security stack.

### Exabeam Fusion SIEM

Fuse SIEM and open XDR into a modern SecOps solution.

## Capabilities

### Alert Triage

Exabeam Alert Triage enables analysts to quickly and confidently dismiss or escalate security alerts at scale.

### Behavioral Analytics

Together, Exabeam Advanced Analytics and Exabeam Entity Analytics form a UEBA solution that leverages behavioral analytics for modern threat detection and investigation.

### Case Management

Exabeam Case Manager provides a security-specific workspace to manage and collaborate on incident resolution.

### Cloud Connectors

Exabeam Cloud Connectors provide 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 and search.

### Response Automation

Security orchestration, automation and response (SOAR) to make your incident response team more productive.

### Threat Hunting

Exabeam Threat Hunter leverages a point-and-click search for behavioral threat hunting.

### Threat Intelligence

Exabeam Threat Intelligence Service provides real-time insight into malicious hosts and other indicators of compromise.



# Comprehensive Threat Detection, Investigation and Response (TDIR) for Successful Outcomes

## Automation

### Exabeam automates manual and repetitive tasks

Based on a Ponemon research study, SOC teams spend 12% of their time on detection, 36% on triage, 26% on 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 everything that the SOC needs from detection to triage to investigation and response.

- Automation helps improve security teams' productivity at every phase of their workflow, not just response.
- Automation assists with detection, triage, and investigation where analysts spend 74% of their time.
- With automation, even junior analysts can make decisions. Advanced hunters can still query raw logs.






## Use Cases

### Use case-based content for successful outcomes

Industry analysts such as Gartner and Forrester have recognized the need for pre-packaged content as part of a successful security strategy.

Exabeam offers:

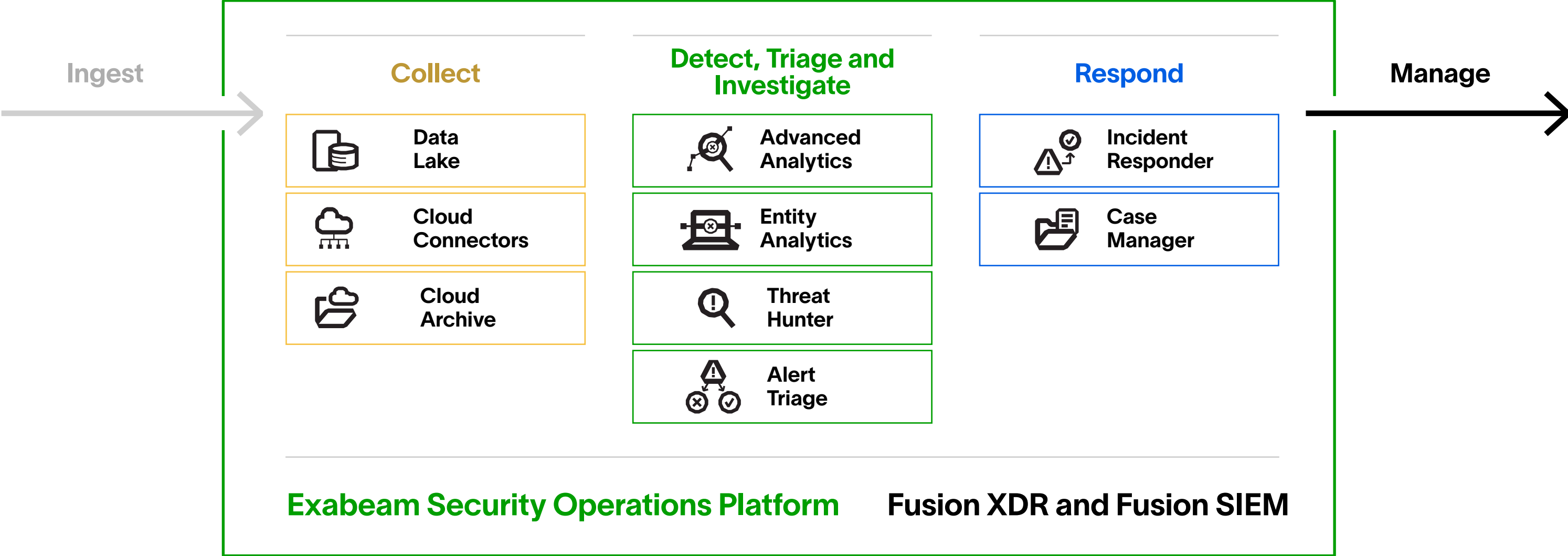
- Pre-packaged use case coverage that helps organizations solve specific problems by providing visibility, detection models, investigation checklists, and response playbooks.
- Use case content and features for each stage of the analyst workflow, not just detection.
- Clear guidance on the data sources needed for security teams to protect against external and internal threats.

SOC STEPS	TIME SPENT	EXABEAM AUTOMATION SOLUTION	VALUE
 Collection		Cloud Connectors	<ul style="list-style-type: none"><li>• Predefined data sources</li><li>• 500+ integrations</li><li>• Cloud connectors</li></ul>
 Detection	12%	User and Entity Behavior Analytics (UEBA)	<ul style="list-style-type: none"><li>• Behavior-based threat detection</li><li>• Watchlists</li><li>• MITRE mapping</li></ul>
 Triage	36%	Alert Prioritization	<ul style="list-style-type: none"><li>• Dynamic alert prioritization</li><li>• Context gathering and enrichment</li><li>• Auto case creation</li></ul>
 Investigation	26%	Automated Incident Timeline Creation	<ul style="list-style-type: none"><li>• Pre-built incident timelines for all entities</li><li>• Automated Q&amp;A</li></ul>
 Response	26%	Security Orchestration, Automation, and Response (SOAR)	<ul style="list-style-type: none"><li>• Turnkey playbooks</li><li>• Custom incident types</li><li>• Case management with incident checklists</li></ul>

# Improve SecOps with the Exabeam Security Operations Platform

Modular and cloud-delivered, to augment existing security tools or update your SIEM.

The Exabeam Security Operations Platform is modular and delivered as a cloud solution or through a managed security service provider (MSSP). It can be used to augment your existing security tools, or you can deploy it to replace your SIEM. Security teams migrating to Exabeam can do so all at once, or in phases.



# Why Exabeam

Successfully used by customers across the globe.



Directly mapping common security use cases to response workflows is **critical for SecOps success.**"

Marc Crudgington

CISO, SVP Information Security



**Technologically advanced companies like Exabeam allow us to better understand the truly anomalous user behavior that matters to our business.** The value is in being able to maximize our efficiency at analyzing events that could pose a threat to our clients' businesses."

Jorge Castañeda

Corporate General Manager



We were able to quickly turn on the **'out of the box' use cases** and integrate with our systems and processes, **improving our detect and response capabilities.**"

Jennifer Shields

VP of Information Technology



**Our Exabeam partnership helped to make our team more efficient** and has been a core building block within our cybersecurity program."

Colin Anderson

Chief Information Security Officer





# Analysts & Recognition

## Recognized for leadership and innovation

### 2021 Gartner® Magic Quadrant™: **Leader**

Our vision to build a cloud platform that improves threat detection, incident investigation, and response for security ops and insider threat teams is making a real-world impact. Gartner agreed and named Exabeam a Leader in the 2021 Magic Quadrant for SIEM.

### 2020 Forrester Wave for Security Analytics Platforms: **Leader**

Exabeam was named a leader based on a 27-criterion evaluation for 11 of the most significant security analytics platform providers. "Exabeam excels on user experience," according to the report. "Midmarket companies and enterprises seeking a modular yet integrated Security Analytics platform with a focus on user behavior should consider Exabeam.



### 2021 Gartner Peer Insights™: **Customers' Choice for SIEM**

The Gartner Peer Insights Customers' Choice distinction is based on feedback and ratings from end-user professionals who have experience purchasing, implementing, and/or using Exabeam Fusion SIEM.



### Forrester TEI Study

Exabeam commissioned Forrester Consulting to perform a Total Economic Impact (TEI) study on the potential financial impact of deploying Exabeam Fusion SIEM. Based on their findings, a typical customer could see:



**ROI**  
**245%**



**Benefits PV**  
**\$3.73M**



**NPV**  
**\$2.65M**



**Payback**  
**<6 months**

## Select Awards & Recognition



For more information, visit [www.exabeam.com](https://www.exabeam.com) →

Gartner does not endorse any vendor, product or service depicted in its research publications and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's Research & Advisory organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose. GARTNER and MAGIC QUADRANT are trademarks and service marks of Gartner, Inc. and/or its affiliates and are used herein with permission. All rights reserved.

