exabeam

# Outsmart the Odds

Improve SecOps with the
Exabeam Security Management Platform

**Exabeam is leading** the disruption of security analytics by automating threat **detection, investigation, and response** with continuous innovation that empowers organizations **to outsmart the odds.**

exabeam

# Analytics. Automation. Outcomes.

## 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 →**

## Products

### Fusion XDR

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

### Fusion SIEM

Fuse SIEM and 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.

### Log Management

Exabeam Data Lake provides a highly scalable data lake for lightning fast log storage and search.

### Behavior Analytics

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

### Response Automation

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

### Case Management

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

### Threat Hunting

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

### Cloud Connectors

Exabeam Cloud Connectors provide pre-built, reliable log collection and response orchestration for over 40 cloud services.

### Threat Intelligence

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

exabeam

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

## Automation

### 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 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. And 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.

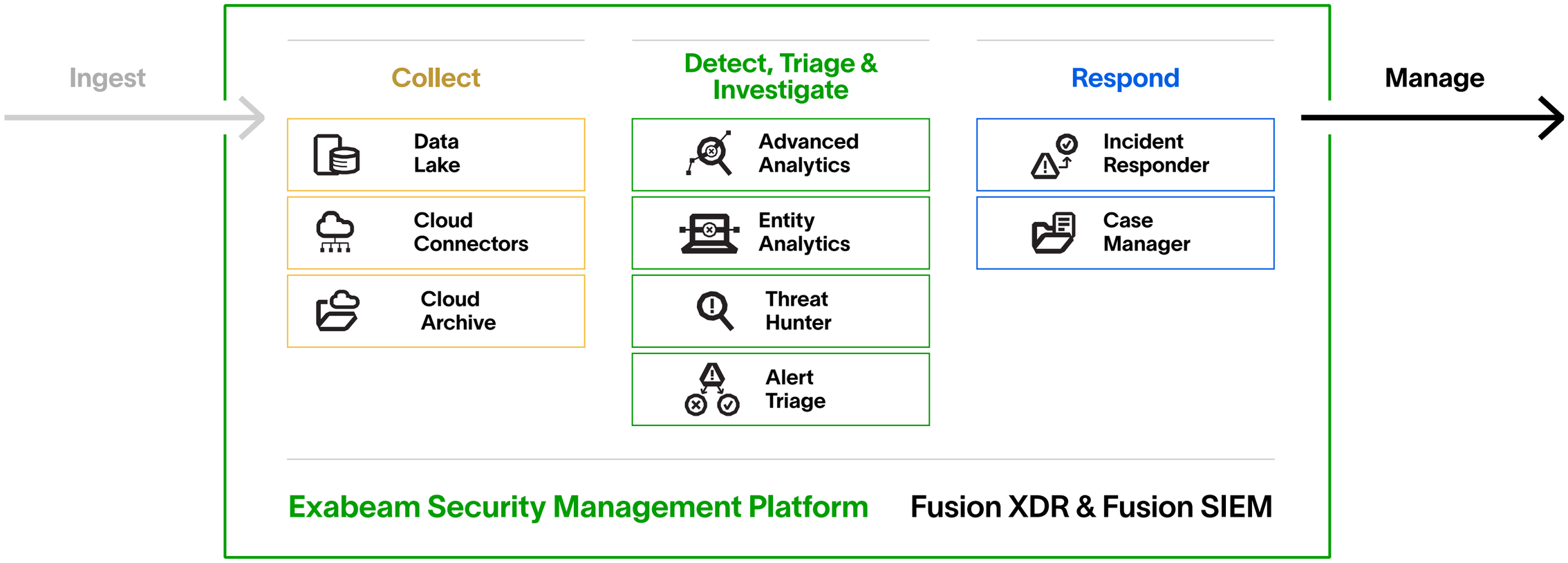
| SOC STEPS | TIME SPENT | EXABEAM AUTOMATION SOLUTION | VALUE |
|---|---|---|---|
| Collection | | Cloud Connectors | • Predefined data sources<br>• 500+ integrations<br>• Cloud connectors |
| Detection | 12% | User & Entity Behavioral Analytic (UEBA) | • Behavior based threat detection<br>• Watchlists<br>• MITRE mapping |
| Triage | 36% | Alert Prioritization | • Alert prioritization<br>• Context gathering and enrichment<br>• Auto case creation |
| Investigation | 26% | Automated Incident Timeline Creation | • Prebuild incident timelines for all entities<br>• Automated Q&A |
| Response | 26% | Security Orchestration, Automation, & Response (SOAR) | • Turnkey playbooks<br>• Custom incident types<br>• Incident checklists |

exabeam

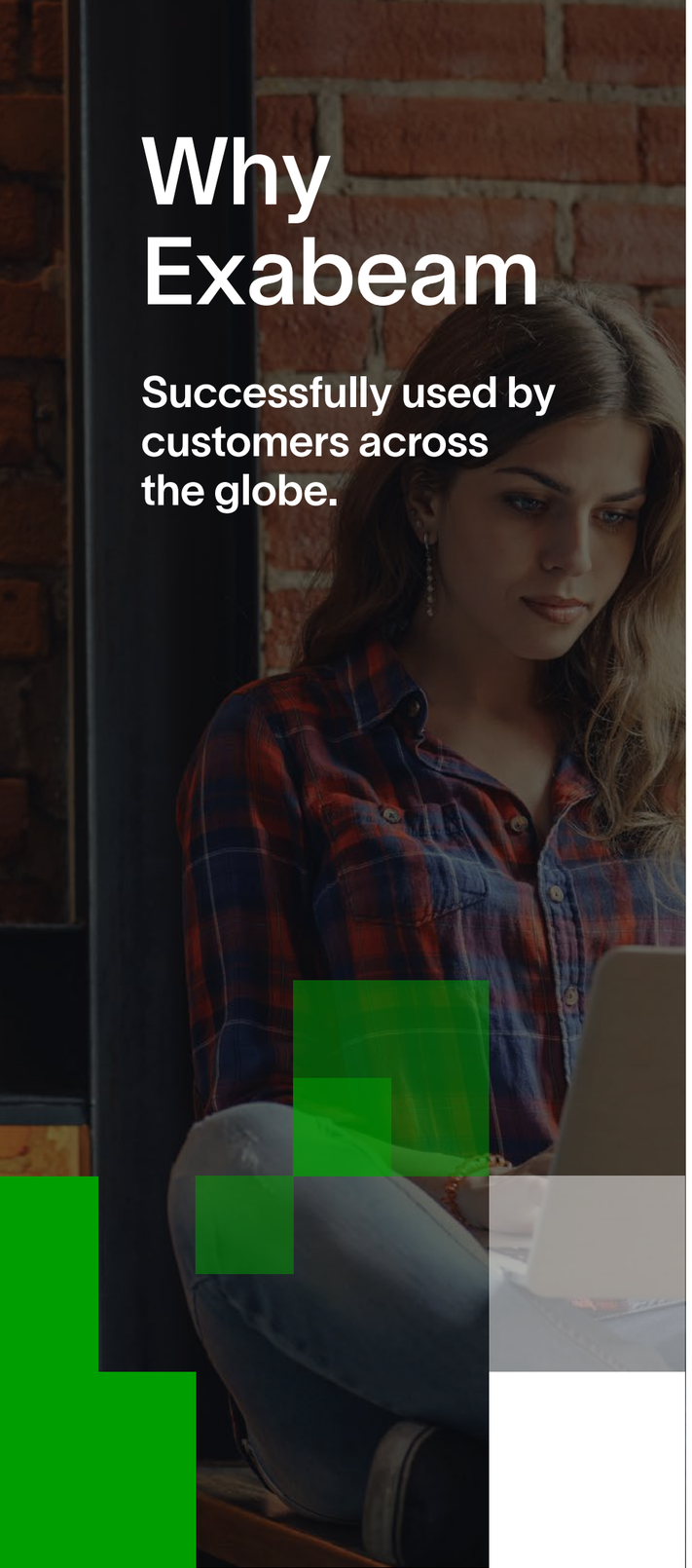
# Improve SecOps with the Exabeam Security Management Platform

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

The Exabeam Security Management 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.




exabeam



# Why Exabeam

**Successfully used by customers across the globe.**

> 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

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

**Marc Crudgington**

**CISO, SVP Information Security**

WOODFOREST NATIONAL BANK℠

> 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**

P&G

exabeam

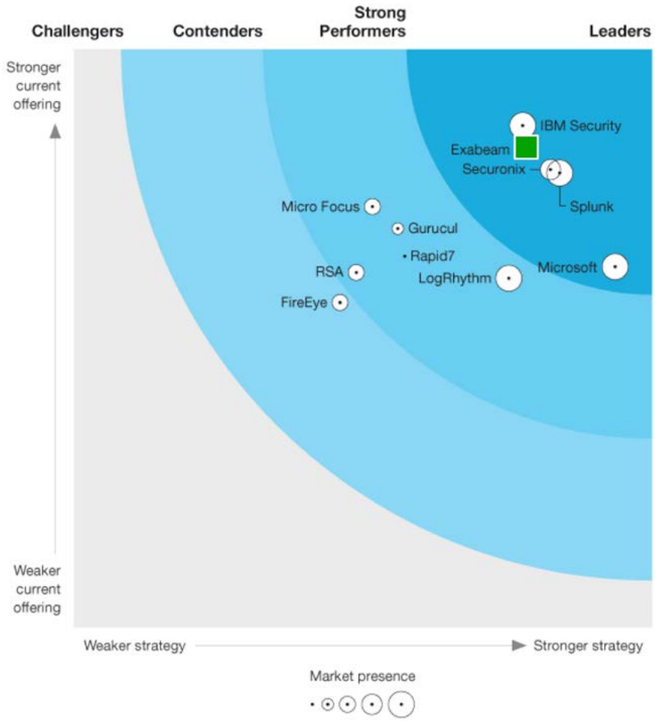
# Analysts & Awards

## Recognized for leadership and innovation

### Gartner Magic Quadrant for SIEM


Source: Gartner (February 2020)

### Forrester Wave for Security Analytics




### Select Awards & Recognition

500™ Technology Fast 500 2020 NORTH AMERICA Deloitte.

SC 2020 Awards Winner Best SIEM Solution

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2021

America's Fastest-Growing Private Companies Inc. 500

Forbes THE 2019 Cloud 100 THE WORLD'S BEST CLOUD COMPANIES Bessemer Venture Partners salesforce ventures

BPTW BEST PLACES TO WORK 2021

For more information, visit **www.exabeam.com** →

exabeam