exabeam

Data Sheet

Deployment Services

Delivering a top-notch experience

A great customer experience means more than just well-developed software. It means also turning users into champions by ensuring their projects are successful. To do this, Exabeam offers a wealth of services designed to provide end-users the deployment and configuration necessary to ensure they are taking advantage of everything the Exabeam Security Management Platform has to offer.

Deployment packages

To provide exceptional delivery to our customers, Exabeam offers pre-defined, deployment services packages to assist with the deployment of Exabeam solutions. All deployment packages are outcome-based and include an Exabeam deployment services engineer. Deployment packages will include, but are not limited to:

- Planning and prep work
- Review of customer architecture, requirements and use cases
- Data source onboarding
- Use case configuration and rule tuning
- Deployment review

Exabeam is dedicated to the success of our customers and the deployment of Exabeam products within our customer's environments. As such, we strive to provide our customers with access to the best deployment service engineers and project managers to ensure successful deployments and adoption of Exabeam's solutions.

Deployment services benefits

Customers who utilize Exabeam's deployment services receive the following benefits:

- Faster deployments
- Quicker time to value
- Expert validation of architecture, requirements, use case implementation, and data source parsing and ingestion
- Assistance from Exabeam project managers that may include:
  - Guidance throughout the deployment
  - Progress tracking to keep tasks on schedule
  - Project status meetings

Deployment services engagement methodology

Plan

- Scoping call
- Project kickoff

Deploy

- Installation and configuration
- Data source onboarding
- Use case configuration

Complete

- Deployment review
- Project close out
- Customer success handoff

Deployment services overview

Exabeam offers the following deployment services packages for net new deployments of Exabeam Fusion XDR and Exabeam Fusion SIEM. Each package includes creation and validation of:

1. User and asset timelines
2. Context table
3. Watchlists
4. Threat hunter searches
5. Case management flow
6. Data Lake reports (Fusion SIEM only)

Deployment services packages	Fusion edition	Number of data sources onboarded	Use Case Packages		
			Malicious Insiders	Compromised Insiders	External Threats
Standard	Core	5	Any 2		
	Enterprise	15	Any 3		
Premium	Core	10	Any 2		
	Enterprise	30	Any 3		

A la carte service offerings:

Exabeam offers the following a la carte service offerings:

A la carte service offerings	Description	Outcome
Initial installation and configuration	User interface configuration for Fusion environment.	UI configuration installation of Exabeam Fusion and configuration of one site collector.
Use case configuration	Deployment service to configure use case-specific content for malicious insiders, compromised insiders or external threats.	Setup use case-specific content within Fusion UI, including: • Context tables • User and asset watchlists • Saved Threat Hunter searches • Case Management workflows • Data Lake reports *(Fusion SIEM only)*
Data source onboarding	Onboard and review implementation of one data source.	Parsing and field extractions for data source will be reviewed, along with event type creation.
Rule tuning	Rule tuning to ensure Fusion environment is operating optimally.	Rule tuning for up to 20 Exabeam Rules including: • Reducing risk score • Increasing risk score • Disabling rule

Additional services

Exabeam offers the following deployment migration and assessment services

Additional services	Description	Outcome
On-prem to cloud migration	Cloud deployment services for customers that want to move existing Exabeam configuration to a Fusion environment.	Migration of customer's existing environment configuration into new Fusion environment.
Use Case health check	Comprehensive analysis of existing use case content mappings.	Understanding the existing use case coverage, based upon data source to Exabeam content mappings. This includes data source to event, timeline, model, and rule analysis and recommendations on how to expand coverage.

Custom deployment services

In addition to the deployment services packages, Exabeam also provides outcome-based and time and materials (T&M) custom deployment services to fit the specific needs of our customer's environments. For scoping and quoting custom deployment services engagements, please work with your Exabeam Sales team.

Supported data sources

Data sources are the building blocks for a successful Exabeam deployment. Exabeam provides support for an exhaustive list of data sources which can be found **here**.

Use case packages

TDIR Use Case Packages are prescriptive, threat-centric solutions that allow security teams to automate detection, investigation and response to repeatedly deliver successful outcomes. Exabeam offers three use case packages: compromised insiders, malicious insiders and external threats.

Compromised Insiders

Compromised Insiders include attacks when credentials are exploited by someone outside the organization for the purpose of data theft and/or sabotage. The Exabeam compromised insider use case supports detection, investigation and response of compromised credentials, lateral movement, privilege escalation, privileged activity, account manipulation, data exfiltration, and evasion.

Malicious Insiders

Malicious Insiders are employees, partners, or contractors that commit intentional sabotage or data theft for either personal reasons or financial gain. The Exabeam malicious insider use case supports detection, investigation and response of data leak, privilege abuse, data access abuse, destruction of data, audit tampering, workforce protection, physical access, and abnormal authentication and access.

External Threats

External Threats refer to techniques commonly employed by adversaries to deceive users, gain access to valid credentials, or exploit corporate assets. The Exabeam compromised insider use case supports detection, investigation and response of phishing, malware, ransomware, brute force, and cryptomining.

*Exabeam deployment packages are exclusive of the following services: third-party SIEM migrations, Exabeam to Exabeam data migrations, hardware racking and stacking on-site services.

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**.

exabeam

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