The Exabeam Security Operations Platform

Detect the Undetectable™

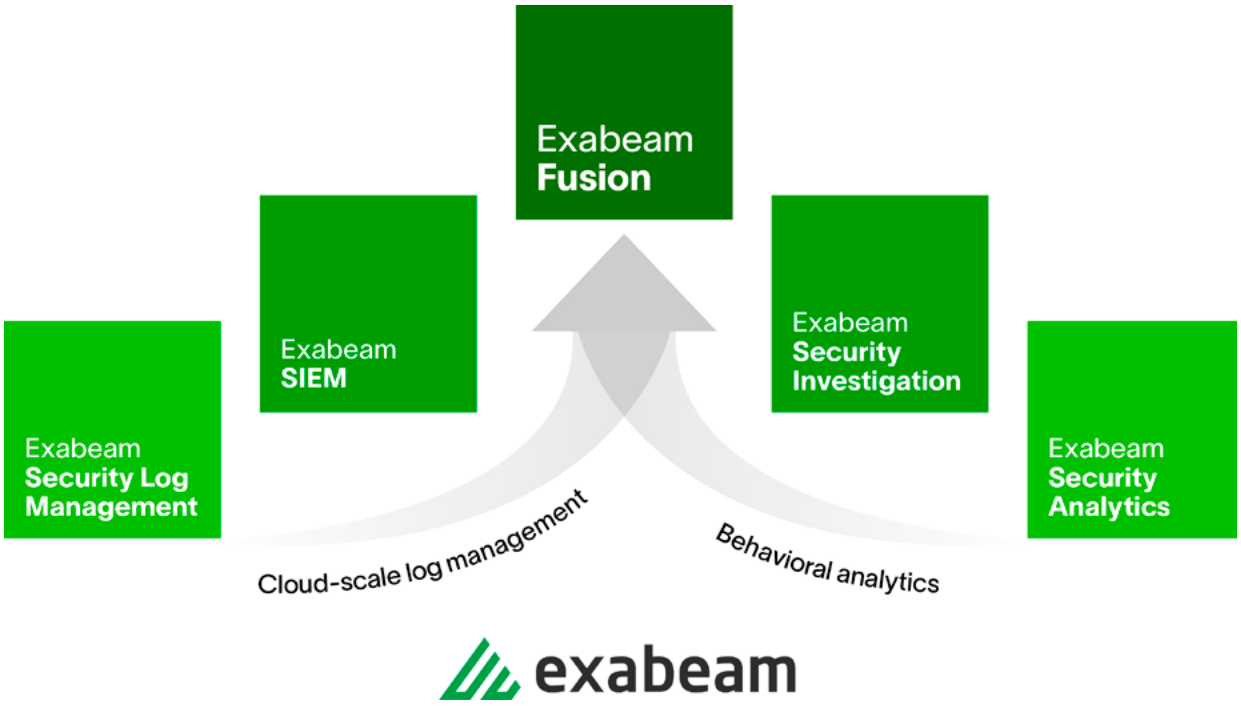
Security operations teams fail due to the limitations of legacy SIEM. The lack of innovation in the market relative to the growth of data, the sophistication of attacks, and a shift to the cloud has created a SIEM effectiveness gap. Security teams are overwhelmed with data and don't even know what data to collect. Legacy tools don't provide a complete picture of a threat; they bury analysts with alerts and compel slow, ineffective, and manual investigations. Meanwhile, attacks are becoming increasingly sophisticated, hard-to-detect, and credential-based attacks are multiplying.

Whether it's phishing, ransomware, malware, or another external threat, valid credentials are now the adversaries' primary target. This demands a shift in investment from legacy on-premises, rule-based detection to cloud-native SIEM platforms designed to identify abnormal behavior and automate the entire threat detection, investigation, and response (TDIR) workflow.

Security operations success requires a new approach: New-Scale SIEM™ from Exabeam. New-Scale SIEM is a breakthrough combination of the capabilities security operations staff need in products they want to use. These capabilities include rapid data ingestion, a cloud-native data lake, hyper-quick query performance, powerful behavioral analytics for next-level insights that other tools miss, and automation that changes the way analysts do their jobs.

The Exabeam Security Operations Platform provides complete coverage. Security log management leverages a cloud-scale architecture to ingest, parse, store, and search data at lightning speed. Behavioral analytics baseline the normal behavior of users and devices with histograms, to detect, prioritize, and respond to anomalies based on risk. An automated investigation experience across the TDIR workflow provides a complete picture of a threat, automating manual routines and simplifying complex work.

Whether you replace a legacy product with a New-Scale SIEM, or complement an ineffective SIEM solution by adding the industry's most powerful user and entity behavior analytics (UEBA) and automation to it, the Exabeam Security Operations Platform can help you achieve security operations success.



Our Products

Exabeam Security Log Management

Cloud-scale log management to ingest, parse, store, and search log data with powerful dashboarding and correlation

Exabeam SIEM

Cloud-native SIEM at hyperscale with fast, modern search, and powerful correlation, reporting, dashboarding, and case management

Exabeam Fusion

New-Scale SIEM™, powered by modern, scalable security log management, powerful behavioral analytics, and automated threat detection, investigation, and response

Exabeam Security Investigation

Threat detection, investigation, and response powered by user and entity behavioral analytics, correlation rules, and threat intelligence, supported by alerting, incident management, automated triage, and response workflows

Exabeam Security Analytics

Automated threat detection powered by user and entity behavioral analytics with correlation and threat intelligence

Exabeam Security Log Management

Built to support security use cases, Exabeam Security Log Management, the industry's most advanced cloud-native solution, is the entry point to ingest, parse, store, and search security data for your organization in one place, providing a lightning fast, modern search and dashboarding experience across multi-year data. Exabeam Security Log Management provides your organization affordable log management at scale without requiring advanced programming or query-building skills.

Key Product Features

Collectors

The Exabeam Security Operations Platform provides extensive data collection capabilities and coverage. A single interface is used to securely configure, manage, and monitor the transport of data into the Exabeam service from on-premises, cloud, and context sources. The Platform provides collection from 200+ on-premises products and supports 30+ cloud-delivered security products, 10+ SaaS productivity applications, and 20+ cloud infrastructure products.

Log Stream

Delivers rapid log ingestion processing at a sustained rate of over 1M EPS. A central console enables you to visualize, create, deploy, and monitor parsers within a unified ingestion pipeline for all Exabeam products and features. As it is ingested, data is parsed using 7,937 pre-built log parsers, and enriched using 3 context collectors from open source and commercial threat intelligence feeds. Live Tail provides self-service, real-time monitoring and management of parser performance, and visibility into the data pipeline.

Common Information Model (CIM)

Exabeam built a Common Information Model (CIM) that provides a schema to simplify the normalization, categorization, and transformation of raw log data into actionable events in support of security use cases. The CIM defines the 10 most important fields and 76 subjects used by security experts and specifies them as core, detection, or informational, and includes 395 activity types and two outcomes (specified as success or fail).

Search

A simplified search experience with faster query and instant results over petabytes (PB) and years of data; search hot and cold data at the same speed.

Reporting and Dashboards

Print, export, or view dashboard data with pre-built compliance reports, customized reports, and dashboards with 14 different chart types.

Correlation Rules

Correlation rules compare incoming events with predefined relationships between entities to identify and escalate anomalies. Write, test, publish, and monitor custom correlation rules for your most critical business entities and assets, including defining higher criticality via Threat Intelligence Service-sourced activity.

Outcomes Navigator

Outcomes Navigator maps the feeds that come into our Security Log Management against the most common security use cases and suggests ways to improve coverage. Outcomes Navigator supports measurable, continuous improvement focusing on outcomes by recommending information, event stream, and parsing configuration changes to close any gaps.

Service Health and Consumption

Visualize your service health for every service and application, as well as data consumption, while monitoring your connections and sources. Service Health and Consumption provides dashboards showing uptime and health of all your log parsers, applications, data flow, and connections, as well as your total license volume consumptions to help with long-term storage and capacity planning.

Threat Intelligence Service

Available in all Exabeam products at no additional cost, the Exabeam Threat Intelligence Service ingests multiple commercial and open source threat intelligence feeds, then aggregates, scrubs, and ranks them, using proprietary machine learning algorithms to produce a highly accurate, up-to-date stream of IoCs. It adds context enrichment such as file, domain, IP, URL reputation, and TOR endpoints to events from multiple external threat intel services and feeds. The threat intelligence data is refreshed every 24 hours.

Context Enrichment

Exabeam supports enrichment using three methods: threat intelligence, geolocation, and user-host-IP mapping. Armed with the most up-to-date IoCs, our threat intelligence service adds enrichments such as file, domain, IP, URL reputation, and TOR endpoint identification to prioritize or update existing correlations and behavioral models. Geolocation enrichment provides location-based context not often present in logs. Exabeam's User-host-IP mapping enrichment adds user details to logs which is critical to building behavioral models for detecting anomalous activity.

Exabeam SIEM

Exabeam extends the cloud-scale capabilities of Exabeam Security Log Management with features for TDIR. Exabeam SIEM includes Case Management, a centralized system of record for investigation and response, 100s of pre-built correlations, integrated threat intelligence for more improved detection, and powerful dashboarding capabilities. The solution delivers analysts new speed, processing at over 1M EPS sustained, and multi-year search capability for query responses across PB of hot, warm, or cold data in seconds. Alert and Case Management improves analyst productivity with a guided incident checklist, and a ticketing system specifically designed for security. If more storage, longer storage time, or additional processing power is needed, Exabeam SIEM easily scales to meet your needs.

Key Features

Collectors

The Exabeam Security Operations Platform provides extensive data collection capabilities and coverage. A single interface is used to securely configure, manage, and monitor the transport of data into the Exabeam service from on-premises, cloud, and context sources. The Platform provides collection from 200+ on-premises products and supports 30+ cloud-delivered security products, 10+ SaaS productivity applications, and 20+ cloud infrastructure products.

Log Stream

Delivers rapid log ingestion processing at a sustained rate of over 1M EPS. A central console enables you to visualize, create, deploy, and monitor parsers within a unified ingestion pipeline for all Exabeam products and features. As it is ingested, data is parsed using 7,937 pre-built log parsers, and enriched using 3 context collectors from open source and commercial threat intelligence feeds. Live Tail provides self-service, real-time monitoring and management of parser performance, and visibility into the data pipeline.

Common Information Model (CIM)

Exabeam built a Common Information Model (CIM) that provides a schema to simplify the normalization, categorization, and transformation of raw log data into actionable events in support of security use cases. The CIM defines the 10 most important fields and 76 subjects used by security experts and specifies them as core, detection, or informational, and includes 395 activity types and two outcomes (specified as success or fail).

Search

A simplified search experience with faster query and instant results over PB and years of data; search hot and cold data at the same speed.

Reporting and Dashboards

Print, export, or view dashboard data with pre-built compliance reports, customized reports, and dashboards with 14 different chart types.

Correlation Rules

Correlation rules compare incoming events with predefined relationships between entities to identify and escalate anomalies. Write, test, publish, and monitor custom correlation rules for your most critical business entities and assets, including defining higher criticality via Threat Intelligence Service-sourced activity.

Pre-built Correlation Rules

Over 100 pre-built fact-based correlation rules and models matching some of the most common use cases of malware and compromised credentials.

Outcomes Navigator

Outcomes Navigator maps the feeds that come into our SIEM against the most common security use cases and suggests ways to improve coverage. Outcomes Navigator supports measurable, continuous improvement focusing on outcomes by recommending information, event stream, and parsing configuration changes to close any gaps.

Service Health and Consumption

Visualize your service health for every service and application, as well as data consumption, while monitoring your connections and sources. Service Health and Consumption provides dashboards showing uptime and health of all your log parsers, applications, data flow, and connections, as well as your total license volume consumptions to help with long-term storage and capacity planning.

Threat Intelligence Service

Available in all Exabeam products at no additional cost, the Exabeam Threat Intelligence Service ingests multiple commercial and open source threat intelligence feeds, then aggregates, scrubs, and ranks them, using proprietary machine learning algorithms to produce a highly accurate, up-to-date stream of IoCs. It adds context enrichment such as file, domain, IP, URL reputation, and TOR endpoints to events from multiple external threat intel services and feeds. The threat intelligence data is refreshed every 24 hours.

Alert and Case Management

A defining feature separating a SIEM from a security data lake is the ability to sort alerts by severity and combine them into cases and incidents to be worked through to resolution by your analysts. Alert and Case Management centralizes events and alerts sourced from Exabeam and/or third-party products, letting an analyst review alerts individually or at volume — or set conditions to automate the alert triage workflow and escalate events and alerts into incidents. Alert and Case Management allows analyst teams to create incidents, add tags and events to the incident, collaborate across groups and timezones, and offers customizable, outcome-driven steps for analysts to guide them through to mitigation or resolution.

Context Enrichment

Exabeam supports enrichment using three methods: threat intelligence, geolocation, and user-host-IP mapping. Armed with the most up-to-date IoCs, our threat intelligence service adds enrichments such as file, domain, IP, URL reputation, and TOR endpoint identification to prioritize or update existing correlations and behavioral models. Geolocation enrichment provides location-based context not often present in logs. Exabeam's User-host-IP mapping enrichment adds user details to logs which is critical to building behavioral models for detecting anomalous activity.

MITRE ATT&CK Coverage

The Exabeam Security Operations Platform uses the MITRE ATT&CK framework as a critical lens to help improve the visibility of your security posture. Support for MITRE ATT&CK spans all 14 categories, including 101 techniques and 180 sub-techniques in the MITRE ATT&CK framework.

Exabeam Fusion

Our most comprehensive offering for TDIR, Exabeam Fusion represents the industry's most powerful and advanced cloud-native SIEM and introduces New-Scale SIEM. It unites Exabeam Security Log Management and Exabeam SIEM with Exabeam Security Analytics and Exabeam Security Investigation. The combined capabilities include a cloud-native data lake, rapid data ingestion, hyper-quick query performance, powerful behavioral analytics to uncover weak signals that other tools miss, and automation that changes the way analysts do their jobs. Pre-built integrations with over 549 third-party security tools, over 1,800 fact-based correlation rules, and over 750 behavioral model histograms automatically baseline normal behavior of users and devices to detect, prioritize, and respond to anomalies based on risk. Exabeam enriches events using three methods: threat intelligence, GEO location, and user-host-IP mapping. Exabeam Fusion enables analysts to run their end-to-end TDIR workflows from a single control pane that performs automation of highly manual tasks such as alert triage and prioritization, incident investigations, and response to accelerate investigations, reduce response times, and ensure consistent, repeatable results.

Key Features

Collectors

The Exabeam Security Operations Platform provides extensive data collection capabilities and coverage. A single interface is used to securely configure, manage, and monitor the transport of data into the Exabeam service from on-premises, cloud, and context sources. The Platform provides collection from 200+ on-premises products and supports 30+ cloud-delivered security products, 10+ SaaS productivity applications, and 20+ cloud infrastructure products.

Log Stream

Delivers rapid log ingestion processing at a sustained rate of over 1M EPS. A central console enables you to visualize, create, deploy, and monitor parsers within a unified ingestion pipeline for all Exabeam products and features. As it is ingested, data is parsed using 7,937 pre-built log parsers, and enriched using 3 context collectors from open source and commercial threat intelligence feeds. Live Tail provides self-service, real-time monitoring and management of parser performance, and visibility into the data pipeline.

Common Information Model (CIM)

Exabeam built a Common Information Model (CIM) that provides a schema to simplify the normalization, categorization, and transformation of raw log data into actionable events in support of security use cases. The CIM defines the 10 most important fields and 76 subjects used by security experts and specifies them as core, detection, or informational, and includes 395 activity types and two outcomes (specified as success or fail).

Search

A simplified search experience with faster query and instant results over PB and years of data; search hot and cold data at the same speed.

Reporting and Dashboards

Print, export, or view dashboard data with pre-built compliance reports, customized reports, and dashboards with 14 different chart types.

Correlation Rules

Correlation rules compare incoming events with predefined relationships between entities to identify and escalate anomalies. Write, test, publish and monitor custom correlation rules for your most critical business entities and assets, including defining higher criticality via Threat Intelligence Service-sourced activity.

Pre-built Correlation Rules

Over 100 pre-built fact-based correlation rules and models matching some of the most common use cases of malware and compromised credentials.

Outcomes Navigator

Outcomes Navigator maps the feeds that come into Fusion against the most common security use cases and suggests ways to improve coverage. Outcomes Navigator supports measurable, continuous improvement focusing on outcomes by recommending information, event stream, and parsing configuration changes to close any gaps.

Service Health and Consumption

Visualize your service health for every service and application, as well as data consumption, while monitoring your connections and sources. Service Health and Consumption provides dashboards showing uptime and health of all your log parsers, applications, data flow and connections, as well as your total license volume consumptions to help with long-term storage and capacity planning.

Threat Intelligence Service

Available in all Exabeam products at no additional cost, the Exabeam Threat Intelligence Service ingests multiple commercial and open source threat intelligence feeds, then aggregates, scrubs, and ranks them, using proprietary machine learning algorithms to produce a highly accurate, up-to-date stream of IoCs. It adds context enrichment such as file, domain, IP, URL reputation, and TOR endpoints to events from multiple external threat intel services and feeds. The threat intelligence data is refreshed every 24 hours.

Advanced Analytics

Offers UEBA with over 1,800 rules, including cloud threat detection, and over 750 behavioral models to automatically baseline normal behavior of users & devices with histograms to detect, prioritize and respond to anomalies based on risk. Advanced Analytics automatically visualizes these events in Smart Timelines™ that show full event flows and activities to inform the next right action.

Alert and Case Management

Alert and Case Management allows analyst teams to create incidents, add tags and events to the incident, collaborate across groups and timezones, and offers customizable, outcome-driven steps for analysts to guide them through to mitigation or resolution.

Turnkey Playbooks

Automate repeated workflows for investigation into compromised credentials, external attacks, or malicious insider use cases with guided checklists for resolution.

Incident Responder

Optional add on to orchestrate and automate repeated workflows to 100 third-party products with 576 response actions, from semi- to fully-automated activity.

Alert Triage

Categorize, aggregate, and enrich third-party and Exabeam-generated security alerts, so analysts can confidently and efficiently dismiss or escalate alerts from a single screen.

Dynamic Alert Prioritization

Applies machine learning to automate third-party alert prioritization. Classifying alerts provides a starting point for the analyst to begin the triage process, focusing time and resources on the alerts of the highest risk to the organization.

Context Enrichment

Exabeam supports enrichment using three methods: threat intelligence, geolocation, and user-host-IP mapping. Armed with the most up-to-date IoCs, our threat intelligence service adds enrichments such as file, domain, IP, URL reputation, and TOR endpoint identification to prioritize or update existing correlations and behavioral models. Geolocation enrichment provides location-based context not often present in logs. Exabeam's User-host-IP mapping enrichment adds user details to logs which is critical to building behavioral models for detecting anomalous activity.

MITRE ATT&CK Coverage

The Exabeam Security Operations Platform uses the MITRE ATT&CK framework as a critical lens to help improve the visibility of your security posture. Support for MITRE ATT&CK spans all 14 categories, including 101 techniques and 180 sub-techniques in the MITRE ATT&CK framework.

Exabeam Security Analytics

For most SIEM products, UEBA and automation is an afterthought. If available at all, most offerings provide either loose integrations, first-generation UEBA, or worse yet, statistical analysis masquerading as machine learning. Exabeam Security Analytics is the only UEBA product in the market that can run on top of an existing legacy SIEM or data lake to upgrade an organization's defenses and contend with sophisticated and credential-based attacks. Security Analytics takes in logs, and upon intake normalizes and parses them via CIM with data enrichment and threat intelligence to build events — offering over 1,800 fact-based correlation rules, including cloud infrastructure security, and over 750 behavioral model histograms that automatically baseline normal behavior of users and devices to detect, prioritize, and respond to anomalies based on risk scores. The Smart Timeline conveys the complete history of an incident, showing full event flows and activities and scores the risk associated with each event. This eliminates the writing of hundreds of queries and changes the way analysts do their jobs.

Key Features

Collectors

The Exabeam Security Operations Platform provides extensive data collection capabilities and coverage. A single interface is used to securely configure, manage, and monitor the transport of data into the Exabeam service from on-premises, cloud, and context sources. The Platform provides collection from 200+ on-premises products and supports 30+ cloud-delivered security products, 10+ SaaS productivity applications, and 20+ cloud infrastructure products.

Log Stream

Delivers rapid log ingestion processing at a sustained rate of over 1M EPS. A central console enables you to visualize, create, deploy, and monitor parsers within a unified ingestion pipeline for all Exabeam products and features. As it is ingested, data is parsed using 7,937 pre-built log parsers, and enriched using 3 context collectors from open source and commercial threat intelligence feeds. Live Tail provides self-service, real-time monitoring and management of parser performance, and visibility into the data pipeline.

Common Information Model (CIM)

Exabeam built a Common Information Model (CIM) that provides a schema to simplify the normalization, categorization, and transformation of raw log data into actionable events in support of security use cases. The CIM defines the 10 most important fields and 76 subjects used by security experts and specifies them as core, detection, or informational, and includes 395 activity types and two outcomes (specified as success or fail).

Anomaly Search

A simplified search experience with faster query and instant results. A single interface allows analysts to search for Exabeam-triggered events across their data repository. Anomaly Search offers a drop-down menu for easy query construction against the list of events to determine and declare incidents. Anomaly Search pairs behavior-based TTP detection with known IoCs to enhance an analyst's threat hunting capability providing a flexible search interface across a variety of different objects such as sessions, rules, users, assets, MITRE TTPs, anomaly identification, and cases.

Reporting and Dashboards

Print, export, or view dashboard data with pre-built compliance reports, customized reports, and dashboards with 14 different chart types.

Correlation Rules

Correlation rules compare incoming events with predefined relationships between entities to identify and escalate anomalies. Write, test, publish and monitor custom correlation rules for your most critical business entities and assets, including defining higher criticality via Threat Intelligence Service-sourced activity.

Pre-built Correlation Rules

Over 100 pre-built fact-based correlation rules and models matching some of the most common use cases of malware and compromised credentials.

Outcomes Navigator

Outcomes Navigator maps the feeds that come into our Security Analytics against the most common security use cases and suggests ways to improve coverage. Outcomes Navigator supports measurable, continuous improvement focusing on outcomes by recommending information, event stream, and parsing configuration changes to close any gaps.

Service Health and Consumption

Visualize your service health for every service and application, as well as data consumption, while monitoring your connections and sources. Service Health and Consumption provides dashboards showing uptime and health of all your log parsers, applications, data flow and connections, as well as your total license volume consumptions to help with long-term storage and capacity planning.

Threat Intelligence Service

Available in all Exabeam products at no additional cost, the Exabeam Threat Intelligence Service ingests multiple commercial and open source threat intelligence feeds, then aggregates, scrubs, and ranks them, using proprietary machine learning algorithms to produce a highly accurate, up-to-date stream of IoCs. It adds context enrichment such as file, domain, IP, URL reputation, and TOR endpoints to events from multiple external threat intel services and feeds. The threat intelligence data is refreshed every 24 hours.

Advanced Analytics

Offers UEBA with over 1,800 rules, including cloud infrastructure security, and over 750 behavioral models to automatically baseline normal behavior of users & devices with histograms to detect, prioritize and respond to anomalies based on risk. Advanced Analytics automatically visualizes these events in Smart Timelines™ that show full event flows and activities to inform the next right action.

Alert Triage

Categorize, aggregate, and enrich third-party and Exabeam-generated security alerts, so analysts can confidently and efficiently dismiss or escalate alerts from a single screen.

Alert and Case Management

Alert and Case Management allows analyst teams to create incidents, add tags and events to the incident, collaborate across groups and timezones, and offers customizable, outcome-driven steps for analysts to guide them through to mitigation or resolution.

Context Enrichment

Exabeam supports enrichment using three methods: threat intelligence, geolocation, and user-host-IP mapping. Armed with the most up-to-date IoCs, our threat intelligence service adds enrichments such as file, domain, IP, URL reputation, and TOR endpoint identification to prioritize or update existing correlations and behavioral models. Geolocation enrichment provides location-based context not often present in logs. Exabeam's User-host-IP mapping enrichment adds user details to logs which is critical to building behavioral models for detecting anomalous activity.

MITRE ATT&CK Coverage

The Exabeam Security Operations Platform uses the MITRE ATT&CK framework as a critical lens to help improve the visibility of your security posture. Support for MITRE ATT&CK spans all 14 categories, including 101 techniques and 180 sub-techniques in the MITRE ATT&CK framework.

Exabeam Security Investigation

Leveraging the UEBA capabilities of Exabeam Security Analytics, and the unique ability to run on top of a third-party legacy SIEM or data lake, Exabeam Security Investigation adds content, workflows, and automation to provide outcome-focused TDIR capabilities. To help standardize around TDIR best practices, Security Investigation includes prescribed workflows for ransomware, phishing, malware, compromised insiders, and malicious insiders and pre-built content (e.g., MITRE ATT&CK framework) that focus on specific threat types and techniques to achieve more repeatable and successful TDIR. Security Investigation takes in logs, and upon intake normalizes and parses them via CIM with data enrichment and threat intelligence to build events — offering over 1,800 fact-based correlation rules including cloud infrastructure security and over 750 behavioral model histograms that automatically baseline normal behavior of users and devices to detect, prioritize, and respond to anomalies based on risk. With Exabeam Security Investigation, analysts are able to run their end-to-end TDIR workflows from a single control plane that performs automation of highly manual tasks such as alert triage with dynamic alert prioritization, detailed incident investigation, and incident response with options to add on hundreds of SOAR integrations. Turnkey Playbooks allow security operations to accelerate investigations, reduce response times, and ensure consistent, repeatable results.

Key Features

Collectors

The Exabeam Security Operations Platform provides extensive data collection capabilities and coverage. A single interface is used to securely configure, manage, and monitor the transport of data into the Exabeam service from on-premises, cloud, and context sources. The Platform provides collection from 200+ on-premises products and supports 30+ cloud-delivered security products, 10+ SaaS productivity applications, and 20+ cloud infrastructure products.

Log Stream

Delivers rapid log ingestion processing at a sustained rate of over 1M EPS. A central console enables you to visualize, create, deploy, and monitor parsers within a unified ingestion pipeline for all Exabeam products and features. As it is ingested, data is parsed using 7,937 pre-built log parsers, and enriched using 3 context collectors from open source and commercial threat intelligence feeds. Live Tail provides self-service, real-time monitoring and management of parser performance, and visibility into the data pipeline.

Common Information Model (CIM)

Exabeam built a Common Information Model (CIM) that provides a schema to simplify the normalization, categorization, and transformation of raw log data into actionable events in support of security use cases. The CIM defines the 10 most important fields and 76 subjects used by security experts and specifies them as core, detection, or informational, and includes 395 activity types and two outcomes (specified as success or fail).

Anomaly Search

A simplified search experience with faster query and instant results. A single interface allows analysts to search for Exabeam-triggered events across their data repository. Anomaly Search offers a drop-down menu for easy query construction against the list of events to determine and declare incidents. Anomaly Search pairs behavior-based TTP detection with known IoCs to enhance an analyst's threat hunting capability providing a flexible search interface across a variety of different objects such as sessions, rules, users, assets, MITRE TTPs, anomaly identification, and cases.

Reporting and Dashboards

Print, export, or view dashboard data with pre-built compliance reports, customized reports, and dashboards with 14 different chart types.

Correlation Rules

Correlation rules compare incoming events with predefined relationships between entities to identify and escalate anomalies. Write, test, publish and monitor custom correlation rules for your most critical business entities and assets, including defining higher criticality via Threat Intelligence Service-sourced activity.

Pre-built Correlation Rules

Over 100 pre-built fact-based correlation rules and models matching some of the most common use cases of malware and compromised credentials.

Outcomes Navigator

Outcomes Navigator maps the feeds that come into our Security Investigation against the most common security use cases and suggests ways to improve coverage. Outcomes Navigator supports measurable, continuous improvement focusing on outcomes by recommending information, event stream, and parsing configuration changes to close any gaps.

Service Health and Consumption

Visualize your service health for every service and application, as well as data consumption, while monitoring your connections and sources. Service Health and Consumption provides dashboards showing uptime and health of all your log parsers, applications, data flow, and connections, as well as your total license volume consumptions to help with long-term storage and capacity planning.

Threat Intelligence Service

Available in all Exabeam products at no additional cost, the Exabeam Threat Intelligence Service ingests multiple commercial and open source threat intelligence feeds, then aggregates, scrubs, and ranks them, using proprietary machine learning algorithms to produce a highly accurate, up-to-date stream of IoCs. It adds context enrichment such as file, domain, IP, URL reputation, and TOR endpoints to events from multiple external threat intel services and feeds. The threat intelligence data is refreshed every 24 hours.

Advanced Analytics

Offers UEBA with over 1,800 rules, including cloud threat detection, and over 750 behavioral models to automatically baseline normal behavior of users & devices with histograms to detect, prioritize and respond to anomalies based on risk. Advanced Analytics automatically visualizes these events in Smart Timelines™ that show full event flows and activities to inform the next right action.

Alert Triage

Categorize, aggregate, and enrich third-party and Exabeam-generated security alerts, so analysts can confidently and efficiently dismiss or escalate alerts from a single screen.

Alert and Case Management

Alert and Case Management allows analyst teams to create incidents, add tags and events to the incident, collaborate across groups and timezones, and offers customizable, outcome-driven steps for analysts to guide them through to mitigation or resolution.

Turnkey Playbooks

Automate repeated workflows for investigation into compromised credentials, external attacks, or malicious insider use cases with guided checklists for resolution.

Incident Responder

Optional add on to orchestrate and automate repeated workflows to 100 third-party products with 576 response actions, from semi- to fully-automated activity.

Dynamic Alert Prioritization

Apply machine learning to automate third-party alert prioritization. Classifying alerts provides a starting point for the analyst to begin the triage process, focusing time and resources on the alerts of the highest risk to the organization.

Context Enrichment

Exabeam supports enrichment using three methods: threat intelligence, geolocation, and user-host-IP mapping. Armed with the most up-to-date IoCs, our threat intelligence service adds enrichments such as file, domain, IP, URL reputation, and TOR endpoint identification to prioritize or update existing correlations and behavioral models. Geolocation enrichment provides location-based context not often present in logs. Exabeam's User-host-IP mapping enrichment adds user details to logs which is critical to building behavioral models for detecting anomalous activity.

MITRE ATT&CK Coverage

The Exabeam Security Operations Platform uses the MITRE ATT&CK framework as a critical lens to help improve the visibility of your security posture. Support for MITRE ATT&CK spans all 14 categories, including 101 techniques and 180 sub-techniques in the MITRE ATT&CK framework.

	Exabeam Security Log Management	Exabeam SIEM	Exabeam Fusion	Exabeam Security Investigation	Exabeam Security Analytics
Collectors	●	●	●	●	●
Threat Intelligence Service	●	●	●	●	●
Log Stream	●	●	●	●	●
Search	Search	Search	Search	Anomaly Search	Anomaly Search
Pre-built Reports	Compliance	Compliance Case management	Compliance Case management Anomalies and detections	Case management Anomalies and detections	Case management Anomalies and detections
Dashboards	Security Log Manager Dashboard	SIEM Dashboard	Fusion Dashboard	Security Analytics Dashboard	Security Analytics Dashboard
Correlation Rules	●	●	●	●	●
Service Health and Consumption	●	●	●	●	●
100+ Pre-built Correlation Rules		●	●	●	●
Alert and Case Manager			●	●	●
Advanced Analytics			●	●	●
Outcomes Navigator			●	●	●
Dynamic Alert Prioritization			●	●	●
Turkey Playbooks			●	●	
Optional Add-ons			●	●	
Incident Reponder - playbook customization action editor			Sold by Seat	●	
Long-term Search and Storage subscription add-ons	●	●	●	●	●

Exabeam Customer Success Services

At Exabeam, customer success means more than just deploying and maintaining software. For us, it means helping you achieve your desired business goals and security outcomes. To that end, Exabeam Customer Success provides around-the-clock access to an experienced team of support professionals with the technical expertise to ensure your Exabeam environment is running optimally.

Exabeam Support Services

Exabeam offers three levels of support options which include operational assessments, reporting, and ongoing adoption tuning services.

Standard Support

Standard Support is available through the Exabeam Community. You get access to the support portal, self-help Knowledge Base, documentation, webinars, videos, and guidance on deploying Exabeam products. The Exabeam Community also provides customers a forum to directly interact with each other and is included as part of the Exabeam annual subscription license.

Premier Support

Premier Support provides all of the benefits of our Standard Support offering plus a point of contact for support escalation for faster, more personalized response and resolution. You'll also get monthly performance reports to ensure your team is maximizing system performance and a bi-annual security coverage assessment.

Premier Plus Support

Premier Plus Support is our highest level of support and provides all of the benefits of Premier Support, plus a named Customer Success Manager (CSM) and a Technical Account Manager (TAM) who provide a tailored customer adoption experience post deployment. The TAM works with you to ensure execution on defined operational outcomes to achieve your security goals.

Exabeam Customer Success Management

Customer Success Managers (CSMs) are your strategic partners to help you achieve your business goals with Exabeam. CSMs will:

- **Guide and advocate for customers** throughout the Exabeam customer journey
- **Coordinate and align resources** to meet customer needs
- **Collaborate with the Technical Adoption Manager** (TAM) to share best practices to maximize the value-add from Exabeam

Exabeam Customer Success: delivering around-the-clock access to an experienced team of support professionals with the technical expertise to ensure your Exabeam environment is running optimally.

Exabeam Professional Services

Exabeam Professional Services provide a well-defined framework of fixed delivery packages or customized services to accelerate deployment, integration, and platform management while maximizing your success. Exabeam Professional Services are designed to allow you to accelerate your deployment and time to value.

Exabeam Professional Services include Deployment Services and Staff Augmentation Services.

- Deployment Services support the implementation and roll out of the Exabeam Security Operations Platform
- Staff Augmentation Services extend your reach and supplement your resources with experienced Dedicated and/or Partial Resident Engineers

Exabeam Education

Exabeam Education provides remote and hands-on courses to up-level your security analysts or engineers with instructor-led training or self-paced online classes. Your team will learn to maximize the features and functionalities of Exabeam products to get the most value out of the platform. Our Education team is constantly working to create new courseware for all learning types.

Classes include topics like:

- Administering Advanced Analytics
- Introducing Common Information Model
- Fundamentals of Log Stream
- Introducing Search
- Behavioral Analytics and Investigation in the Exabeam Security Operations Platform
- Security Search and Dashboards in the Exabeam Security Operations Platform

About Exabeam

Exabeam is a global cybersecurity leader that created the New-Scale SIEM™ for advancing security operations. We Detect the Undetectable™ by understanding normal behavior, even as normal keeps changing – giving security operations teams a holistic view of incidents for faster, more complete response.

CYBERSEER

Official MSSP Partner - **To request more information, please visit:** https://www.cyberseer.net/technologies/**exabeam/**
Book a call | info@cyberseer.net

Learn more about Exabeam today

Get a Demo Now →