Exabeam Fusion

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

Security operations success needs to be redefined, and it starts with the SIEM. As the IT infrastructure shifts into the cloud, the entire security portfolio needs to scale and follow suit. Legacy approaches force security operations teams to manage massive amounts of data across billions of events, but they don't show the complete picture of complex and hard to detect, credential-based attacks. Whether it's phishing, ransomware, malware, or lateral movement, accessing valid credentials is the adversaries' primary objective. This demands a shift in investment from legacy on-premises detection approaches to massively scalable, cloud-native platforms designed to detect abnormal behavior. Security operations success requires a new approach: New-Scale SIEM.

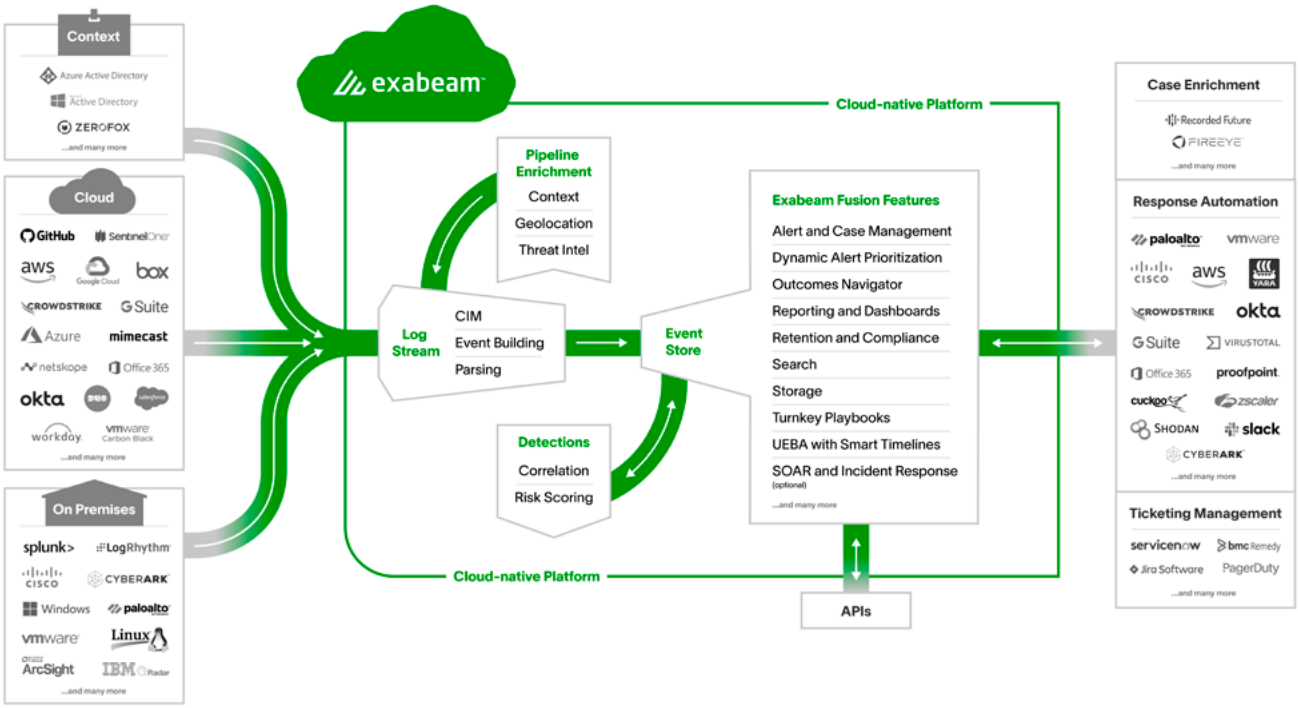
Our most comprehensive offering for threat detection, investigation, and response (TDIR), Exabeam Fusion, represents the industry's most powerful and advanced cloud-native SIEM and introduces New-Scale SIEM. Exabeam Fusion unites the capabilities of Exabeam Security Log Management, and Exabeam SIEM with Exabeam Security Analytics and Exabeam Security Investigation.

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. Security log management leverages a cloud-scale architecture to ingest, parse, store, and search data at lightning speed. Behavioral analytics leverages over 1,800 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. Smart Timelines™ convey the complete history of an incident and highlight the risk associated with each event. Automated investigations in Exabeam Fusion reduce highly manual tasks, such as alert triage, with dynamic alert prioritization, incident investigation, and incident response. This boosts analyst productivity and allows security operations to accelerate investigations, reduce response times, and ensure consistent, repeatable results with hundreds of security orchestration, automation, and response (SOAR) integrations.

Key Features

- Collectors
- Log Stream
- Common Information Model (CIM)
- Search
- Reporting and Dashboards
- Correlation Rules
- Pre-built Correlation Rules
- Outcomes Navigator
- Threat Intelligence Service
- Service Health and Consumption
- Advanced Analytics
- Alert and Case Management
- Turnkey Playbooks
- Incident Responder
- Dynamic Alert Prioritization
- Context Enrichment
- MITRE ATT&CK® Coverage

How it works



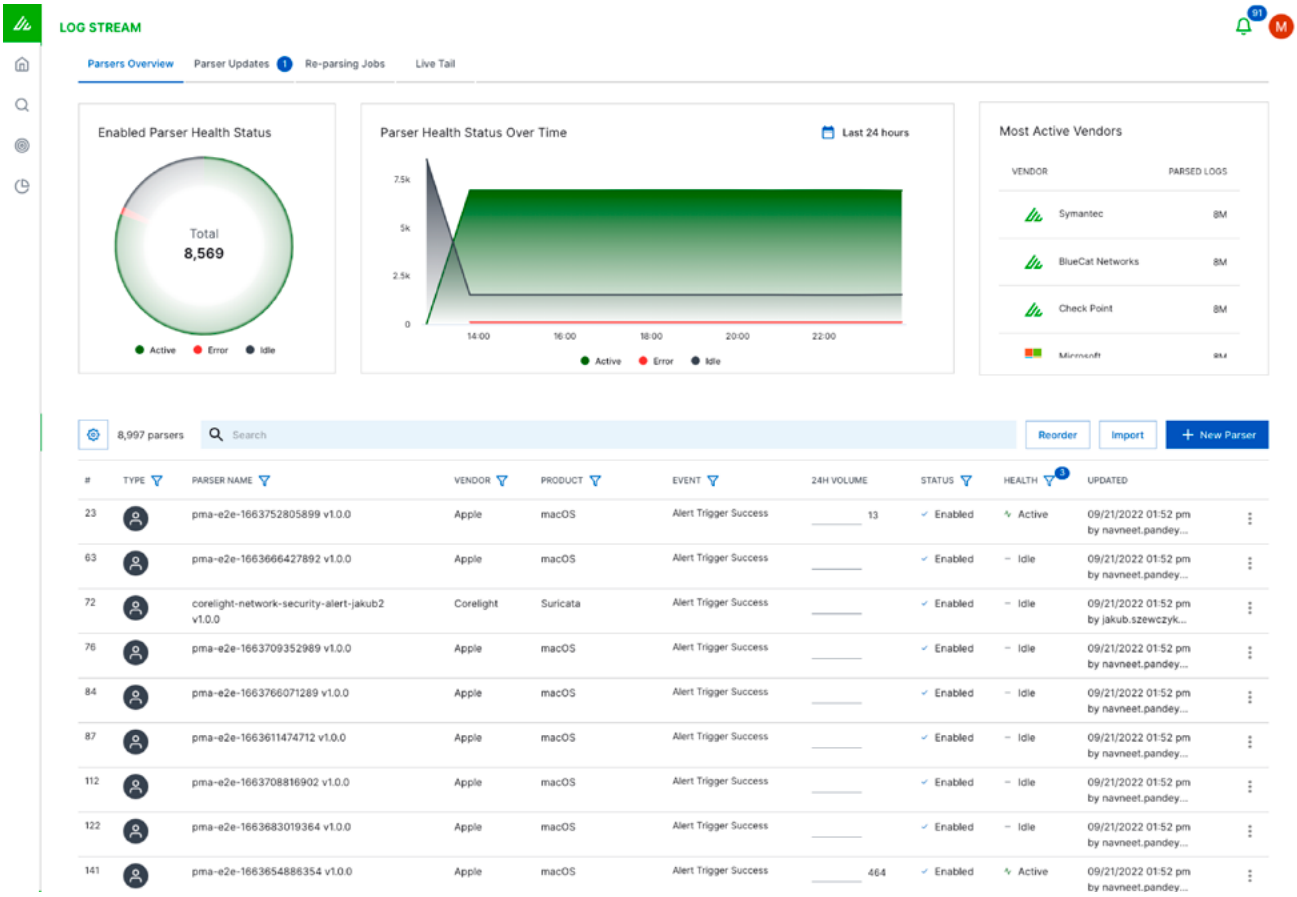
Key Features

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 at scale from on-premises, cloud, and context sources. The platform provides collection from 200+ on-premises products, through a variety of transport methods including APIs, collectors, syslog, and log aggregators such as SIEM or log management products. To meet the increasing need for cloud security and cloud data collection, Exabeam supports 30+ cloud-delivered security products, 10+ SaaS productivity applications, and 20+ cloud infrastructure products from the three leading cloud infrastructure providers. For context, the platform supports the collection of threat intelligence feeds, geolocation data, user, and asset details.

Inbound Data Source Categories for Log Ingestion Include:

- Authentication and Access Management
- Applications Security and Monitoring
- Cloud Access Security Broker (CASB)
- Cloud Security and Infrastructure
- Data Loss Prevention (DLP)
- Database Activity Monitoring (DAM)
- Email Security and Management
- Endpoint Security (EPP/EDR)
- Firewalls
- Forensics and Malware Analysis
- Information Technology Service Management (ITSM)
- IoT/OT Security
- Network Access, Analysis, and Monitoring
- Physical Access and Monitoring
- Privileged Access Management (PAM)
- Security Analytics
- Security Information and Event Management (SIEM)
- Threat Intelligence Platform
- Utilities/Others
- VPN Servers
- Vulnerability Management (VM)
- Web Security and Monitoring



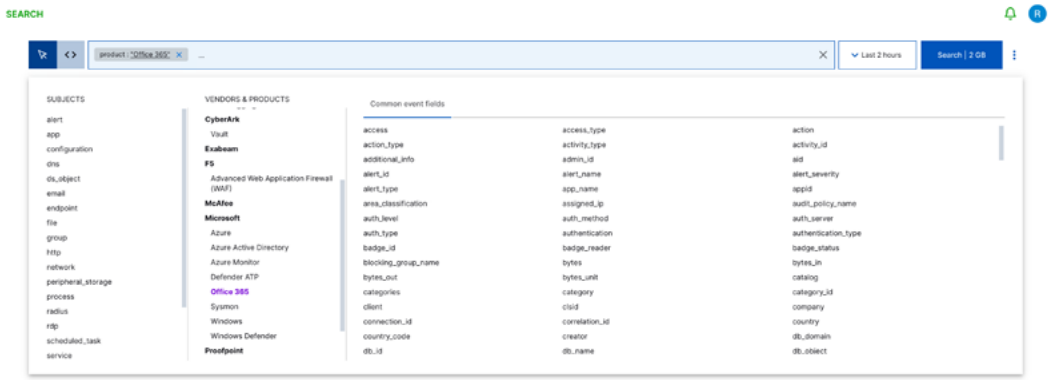
Log Stream

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.

Enriched, parsed data is available as security-relevant events for faster performance in search, correlations, and dashboards. Live Tail provides self-service, real-time monitoring of parser performance, and visibility into the data pipeline, allowing organizations the ability to take immediate action to improve the quality of data ingestion.

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). This process allows organizations to more quickly detect and respond to threats, visualize and report on data, and supports lightning-fast search performance. A robust CIM also establishes a standard process for customers and partners to efficiently create and modify log parsers that are easier to maintain and less prone to misconfiguration.

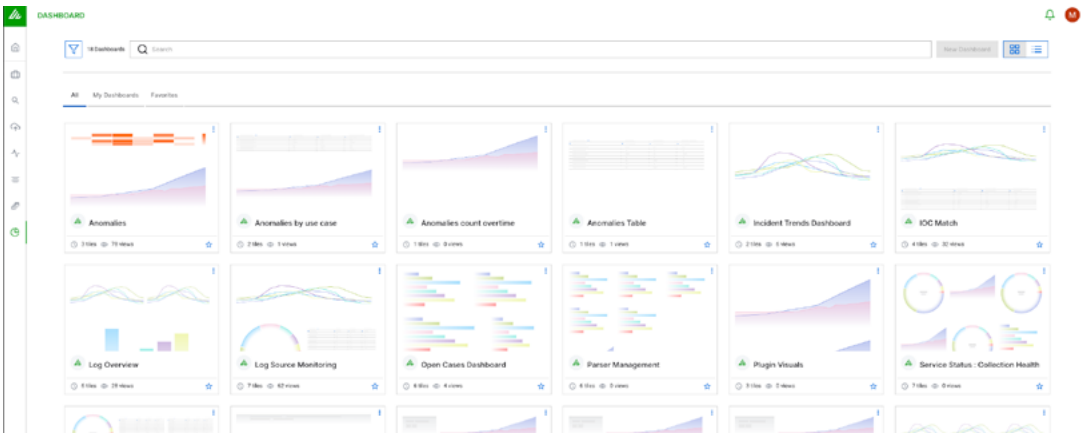


Search

A simplified search experience with faster query and instant results over petabyte-scale and/or years of data; search hot and cold data at the same speed.

Search is an essential feature of Exabeam Fusion. Search is a single interface that allows analysts to search for events, IoCs, or Exabeam-generated anomalies. The time savings is particularly valuable as investigations usually entail multiple queries and require that search terms be refined over multiple iterations to obtain the desired results. Analysts no longer have to wait hours to get search results from NAS or other offline storage. Searching across real-time or historical data is no longer a barrier — security operations center (SOC) teams do not have to import and wait for historical data to be restored and processed.

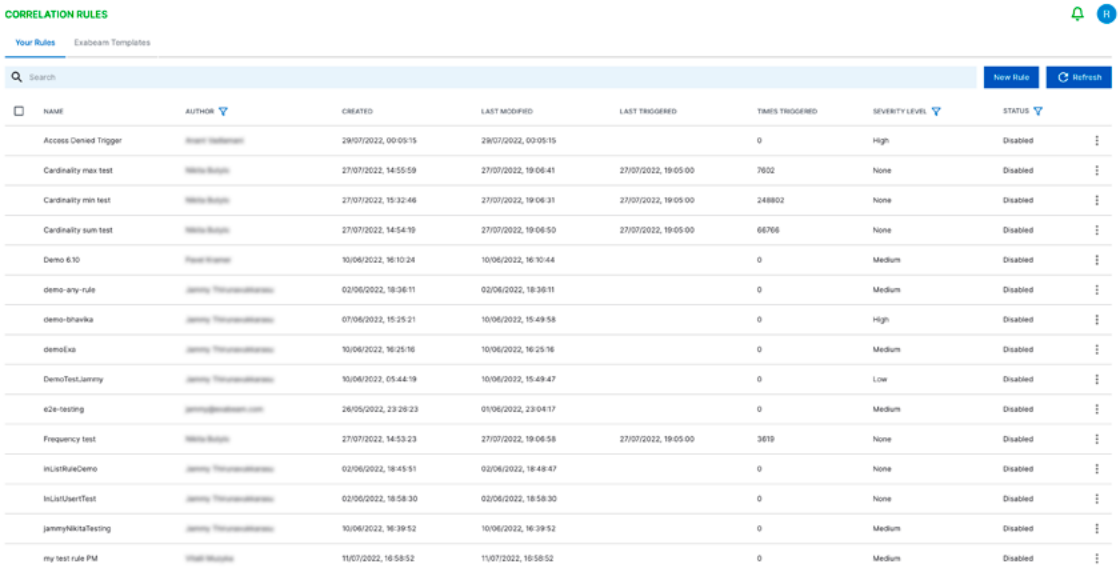
Moreover, there's no learning curve, meaning analysts aren't required to learn a proprietary query language. Search delivers a query builder wizard to point and click from a list of intelligent fields to help build effective search queries quickly and easily.



Reporting and Dashboards

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

Build a dashboard in a minute from 14 different pre-built chart types as if you were using a leading BI tool. The Exabeam dashboard app is fully integrated within Exabeam Fusion, allowing you to create powerful visualizations from your parsed log data quickly. Customers can choose one or more visuals to meet their business needs. These include bar chart, column chart, line graph, area chart, pie chart, donut chart, bubble chart, funnel, single value, sankey map, word cloud, heat map, table, and a Coverage Map.



Correlation Rules

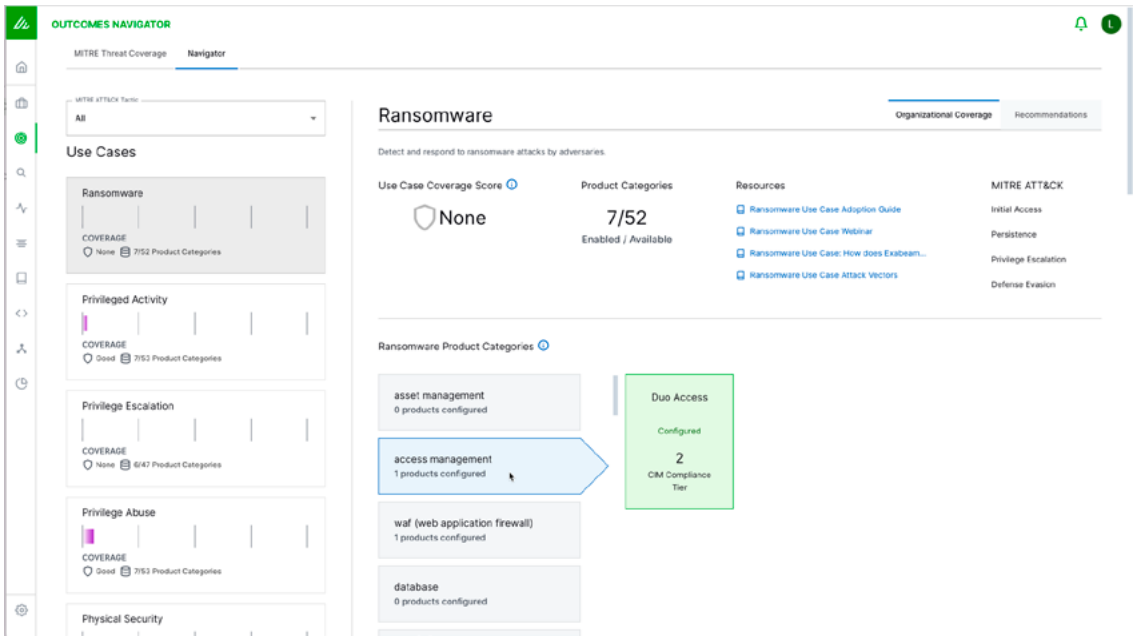
Correlation rules compare incoming events with predefined relationships between entities to identify and escalate anomalies. A single interface lets you write, test, publish, and monitor hundreds of custom correlation rules for your most critical business entities and assets, including defining higher criticality rules for advanced threats sourced from the Exabeam Threat Intelligence Service (available at no additional cost).

Properly designed correlation rules enable enterprises to surface a broad range of abnormal behavior and events. Correlation builder provides analysts with an easy application to create custom correlation rules suited to their organization's security and use case requirements.

Correlation rules monitor for well-known threats, identify compliance violations, and detect signature-based threats using context from the Exabeam Threat Intelligence Service or other third-party threat intelligence.

Pre-built Correlation Rules

Exabeam Fusion offers over 100 pre-built correlation rules and models matching some of the most common use cases of malware and compromised credentials.

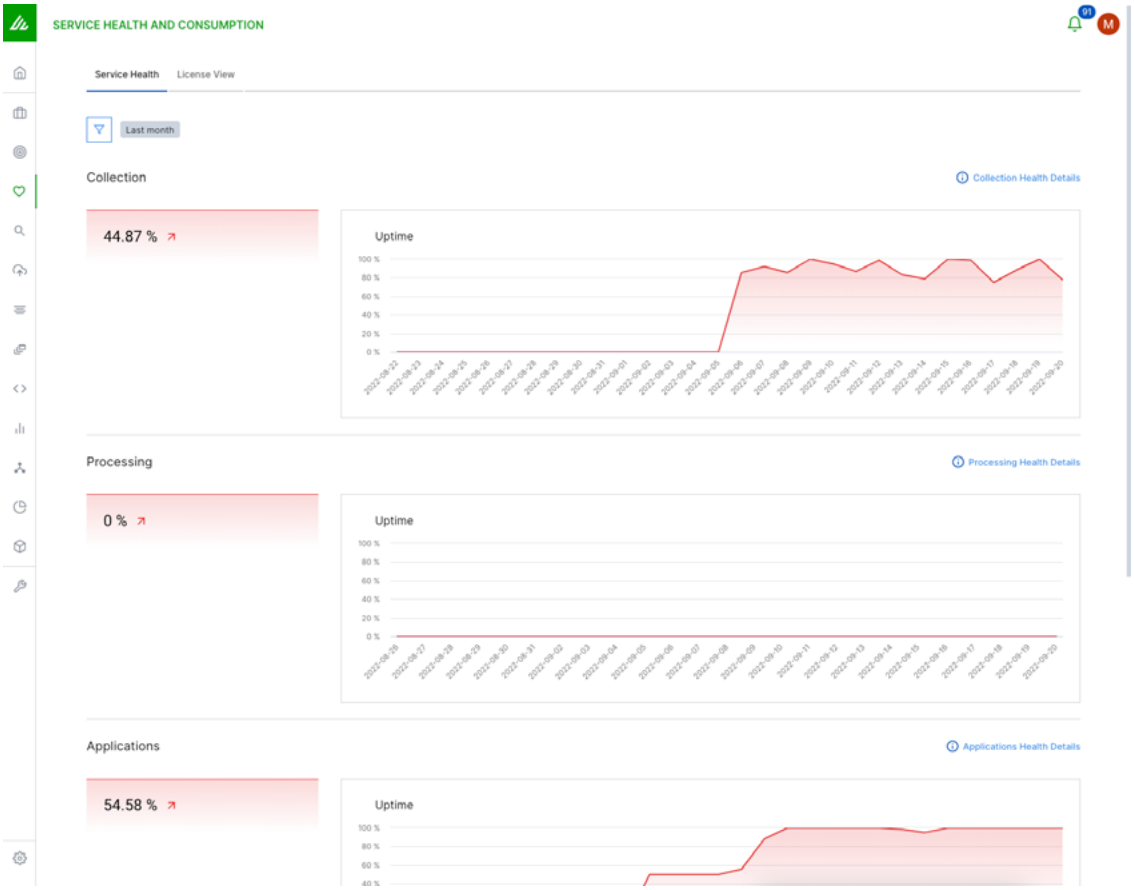


Outcomes Navigator

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.

Threat Intelligence Service

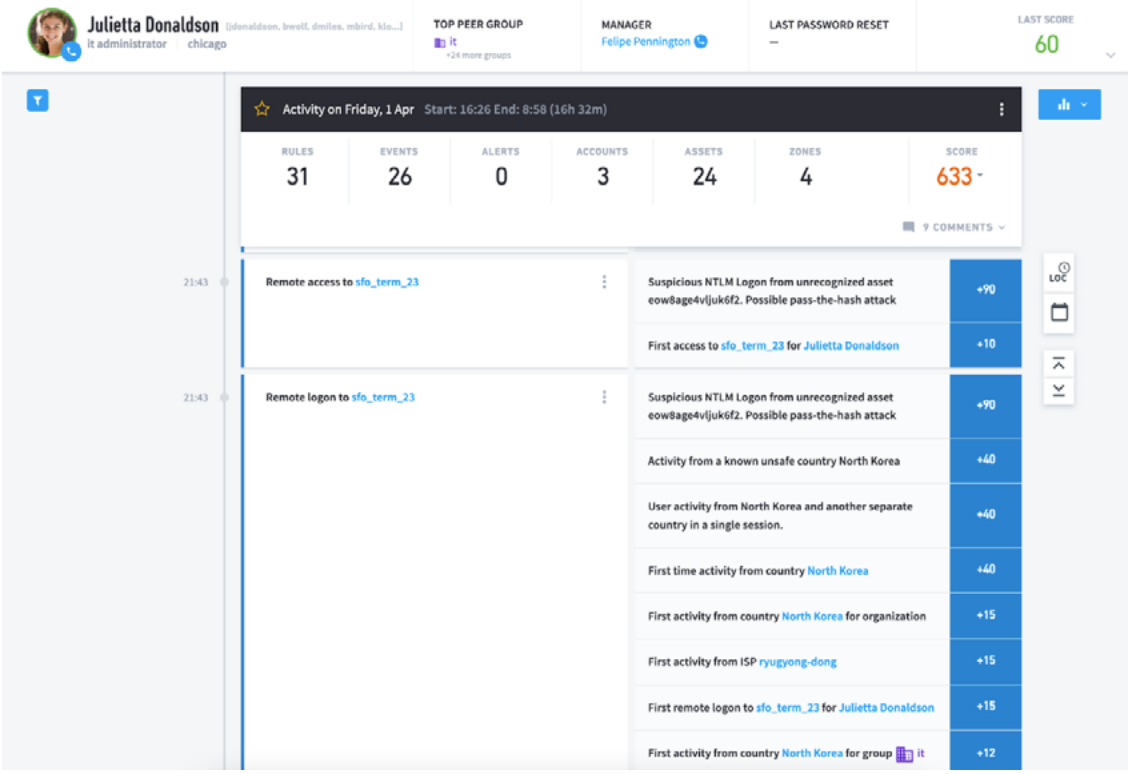
Available in all Exabeam products at no additional cost, the Exabeam Threat Intelligence Service (TIS) adds context enrichment to events from multiple commercial and open source threat intelligence feeds, then aggregates, scrubs, and ranks them, using proprietary machine learning algorithms to produce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



Service Health and Consumption

Provide high-level and detailed views of the health and data consumption performance of your cloud-delivered service. Visualize your service health and data consumption while monitoring your connections and sources. Monitoring visualizations makes it easy to understand the current state of your Exabeam implementation. The performance component illustrates how your data contributes to overall license consumption and highlights significant changes.

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.

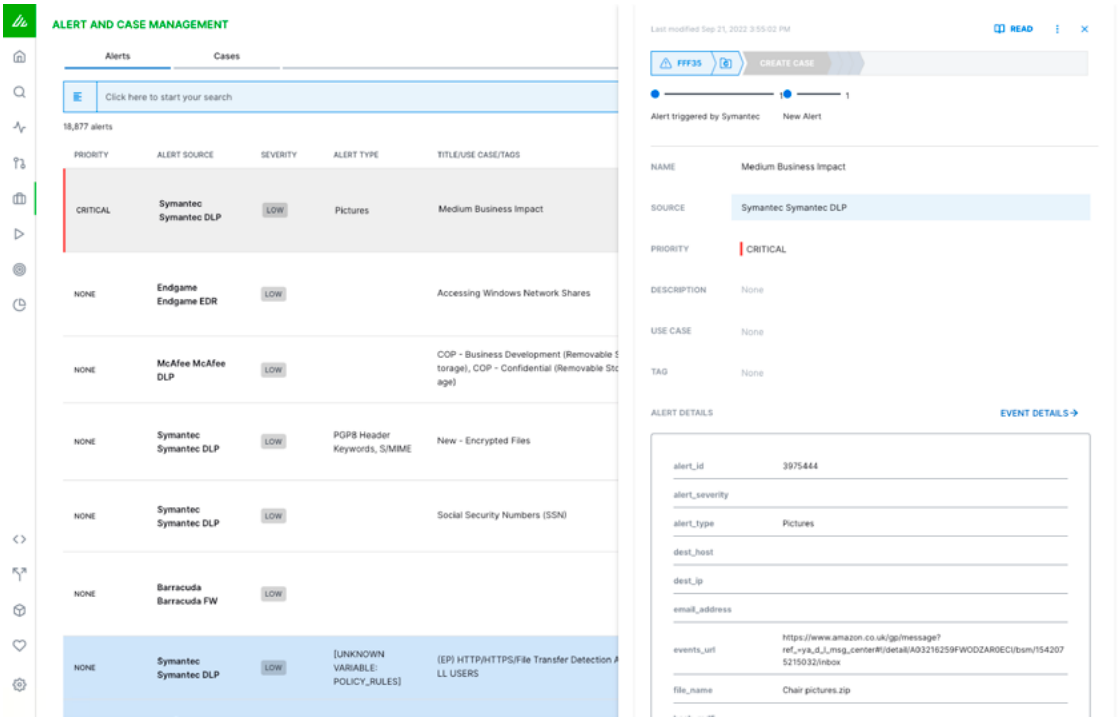


Advanced Analytics

Advanced Analytics offers UEBA with over 1,800 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. Advanced Analytics automatically visualizes these events in Smart Timelines™ that show full event flows and activities to inform the next right action.

To understand normal and detect anomalies as normal keeps changing, all user and device activities get baselined. Risk-based prioritization uses machine learning to automatically assign risk scores to all events, prioritizing triage, investigation, and response for key incidents, and automatically visualizing these events within Smart Timelines that show full event flows and activities to inform the next right action. Smart Timelines detect lateral movement by organizing incidents to follow attack activity, credential use, or permission changes within your environment. The results: find and stop the threats other tools miss, uplevel your security team speed and performance, and stay ahead of your adversaries.

- Machine learning classifies entities, such as workstation versus server, and service account versus user, identifies personal email addresses, and more.
- Extensive rule mapping enables analysts to do behavior-based threat hunting on abnormal TTPs, and use Outcomes Navigator to map coverage against the MITRE ATT&CK® Framework.
- Bringing in existing SIEM, XDR, and logs from other data lakes or resources, such as CASB, SaaS event APIs, and Web gateways, adds depth, helps establish normal, and creates correlation potential to see end-to-end attack event strings.



Alert and Case Management

Centralize incidents sourced from Exabeam or third-party products for an analyst with manual review or automate the alert triage workflow. Alert Triage lets analysts 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. Case Management lets analysts organize alerts from Exabeam and other security tools into incidents requiring further investigation or response.

Alert and Case Management helps the analyst sort incoming events at volume, making it easy to see the most crucial events that correspond to anomalies or high-value signatures. Analysts can manually or automatically sort events into incidents for focused investigation and/or escalation — or export into other third-party workflow solutions. Auto attribution of alerts to users and assets, nearby anomalies, and user and host context provides additional context for more effective triage and investigations.

Turnkey Playbooks

Turnkey Playbooks automate repeated workflows for investigation into compromised credentials, external attacks, or malicious insider use cases. Turnkey playbooks use Exabeam automation to offer pre-built playbooks that work without requiring configuration or investment in additional third-party products, so analysts can respond to common security scenarios such as phishing with a single product.

Incident Responder

Incident Responder is an option that allows analysts to orchestrate and automate repeated workflows with APIs to 65 different vendors and 100 products with 576 response actions, from semi to fully-automated activity. With Incident Responder, analysts can automate gathering key pieces of information about incidents via integrations with popular security and IT infrastructure, and run response playbooks to programmatically perform investigation, containment, or mitigation. Responding to threats faster means organizations better utilize their existing processes and tools, and drastically improve analyst productivity.

Dynamic Alert Prioritization

Dynamic Alert Prioritization applies machine learning to automate third-party alert prioritization by infusing third-party security alerts with context from UEBA to dynamically identify, prioritize, and escalate the alerts which require the most attention. 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

Context enrichment provides powerful benefits across several areas of the platform. 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. Outside of authentication sources, user information is rarely 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 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.

Learn more about Exabeam today

Get a Demo Now →