Exabeam Security Log Management

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

Log management is a foundational component of every enterprise security program. Critical to every log management solution is the flexibility to capture and manage diverse data on a massive scale, whether generated by on-premises tools, cloud data sources, or context feeds. The pace and complexity of attacks are unrelenting, data volumes are exploding, and teams are bogged down with unreliable alerts. And to top it all off, costs have reached unsustainable rates. All of this translates into a need for hyperscale, cloud-native security log management that can thrive within today's cybersecurity challenges.

Ingesting, parsing, storing, and searching log data at scale must be easier to accomplish and not require advanced programming or query-building skills. Exabeam Security Log Management changes all of this. Finally, there is a powerful and affordable log management solution, purpose-built for security, that your teams will want to use, without the need for extensive training. **Deploy quickly and easily, and scale as you need with Exabeam Security Log Management.**

Key Features

- Collectors
- Context Enrichment
- Log Stream
- Common Information Model (CIM)
- Search
- Dashboards
- Correlation Rules
- Outcomes Navigator
- Threat Intelligence Service
- Service Health and Consumption

How it works

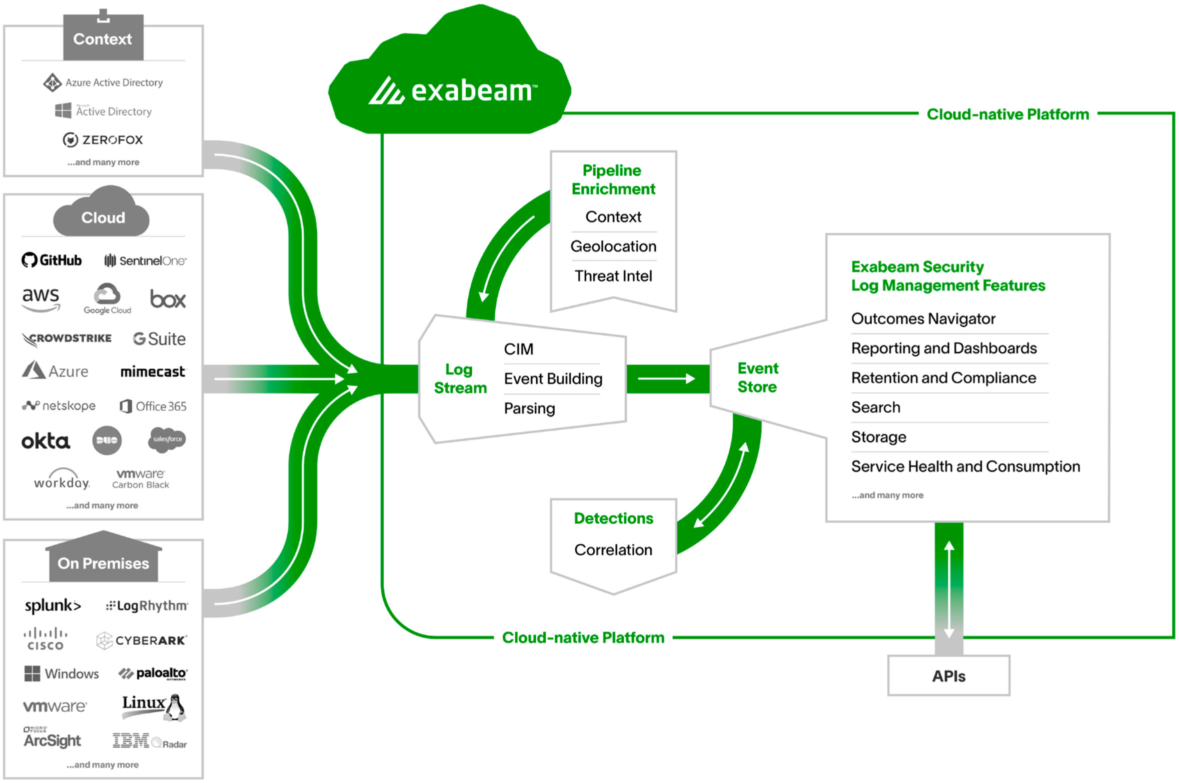


Figure 1.

Architecture flow from data sources through parsing and search to long-term storage

Key Features

Collectors

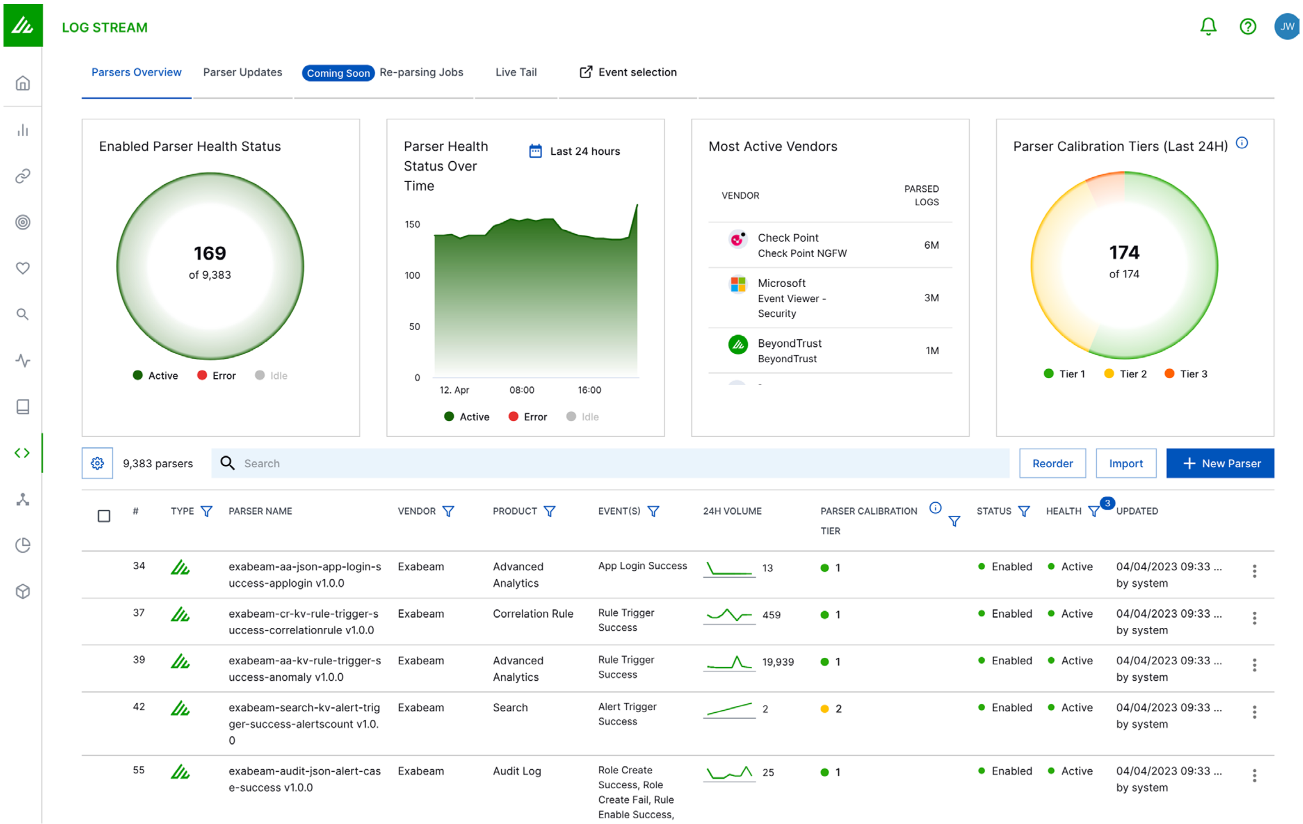
The Exabeam Security Operations Platform provides extensive data collection capabilities and coverage. A single interface is used to securely configure, manage, and monitor the transport of data into the Exabeam service at scale from on-premises, cloud, and context sources. The platform collects logs and events from 471 products under 56 categories, from more than 250 different vendors, through a variety of transport methods including APIs, collectors, syslog, and log aggregators. 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, and 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 (CWP)
- Data Loss Prevention (DLP)
- Database Activity Monitoring (DAM)
- Email Security and Management
- Endpoint Security (EPP/EDR)
- Firewalls (WAF, SWG, Proxy)
- Forensics and Malware Analysis
- Information Technology Service Management (ITSM)
- IoT/OT Security
- Network Access, Analysis, and Monitoring (NDR, IDS, IPS)
- Physical Access and Monitoring
- Privileged Access Management (PAM)
- Risk Management Software
- Security Analytics
- Security Information and Event Management (SIEM)
- Threat Intelligence Platforms
- Utilities/Others
- VPN, ZTNA Servers
- Vulnerability Management (VM)
- Web Security and Monitoring (CWP)

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 indicators of compromise (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 enrichment adds user details and relationships to event logs, which is critical to building correlation rules and dashboards to detect and report on potentially suspicious activity.



Most Active Vendors

VENDOR	PARSED LOGS
Check Point Check Point NGFW	6M
Microsoft Event Viewer - Security	3M
BeyondTrust BeyondTrust	1M
-	

9,383 parsers

Search

#	TYPE	PARSER NAME	VENDOR	PRODUCT	EVENT(S)	24H VOLUME	PARSER CALIBRATION TIER	STATUS	HEALTH	UPDATED
34		exabeam-aa-json-app-login-success-applogin v1.0.0	Exabeam	Advanced Analytics	App Login Success	13	● 1	● Enabled	● Active	04/04/2023 09:33 ... by system
37		exabeam-cr-kv-rule-trigger-success-correlationrule v1.0.0	Exabeam	Correlation Rule	Rule Trigger Success	459	● 1	● Enabled	● Active	04/04/2023 09:33 ... by system
39		exabeam-aa-kv-rule-trigger-success-anomaly v1.0.0	Exabeam	Advanced Analytics	Rule Trigger Success	19,939	● 1	● Enabled	● Active	04/04/2023 09:33 ... by system
42		exabeam-search-kv-alert-trigger-success-alertscount v1.0.0	Exabeam	Search	Alert Trigger Success	2	● 2	● Enabled	● Active	04/04/2023 09:33 ... by system
55		exabeam-audit-json-alert-case-success v1.0.0	Exabeam	Audit Log	Role Create Success, Role Create Fail, Rule Enable Success,	25	● 1	● Enabled	● Active	04/04/2023 09:33 ... by system

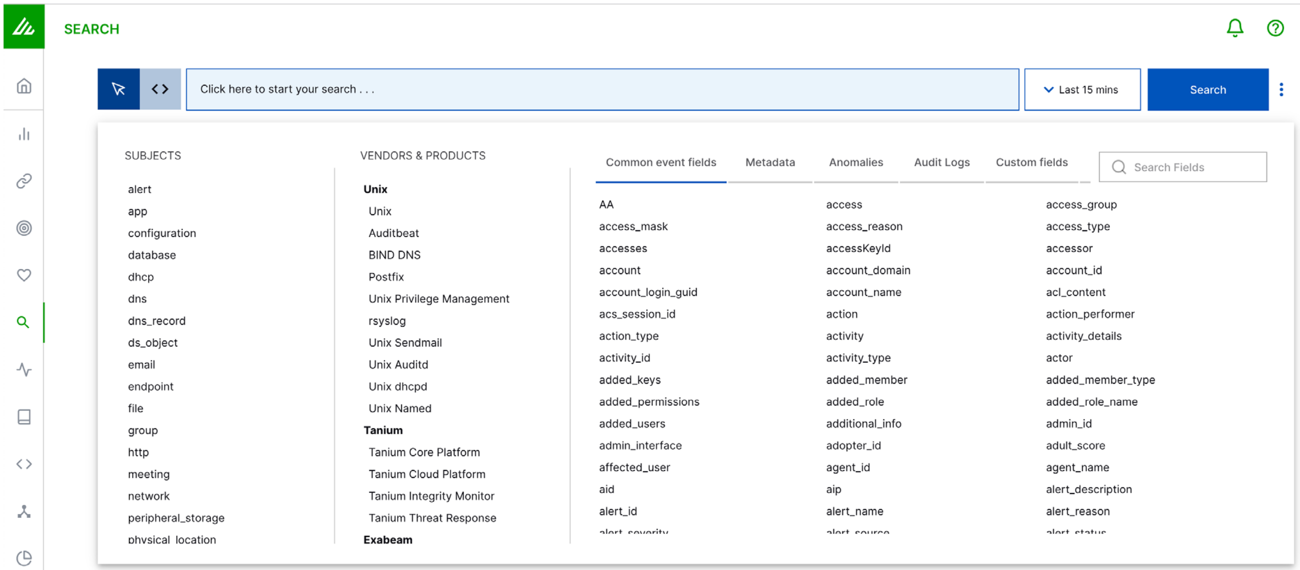
Log Stream

Log Stream delivers rapid log ingestion processing at a sustained rate of more than 1M events per second (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 more than 9,000 pre-built log parsers, and enriched using three 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.



SUBJECTS

alert
app
configuration
database
dhcp
dns
dns_record
ds_object
email
endpoint
file
group
http
meeting
network
peripheral_storage
physical_location

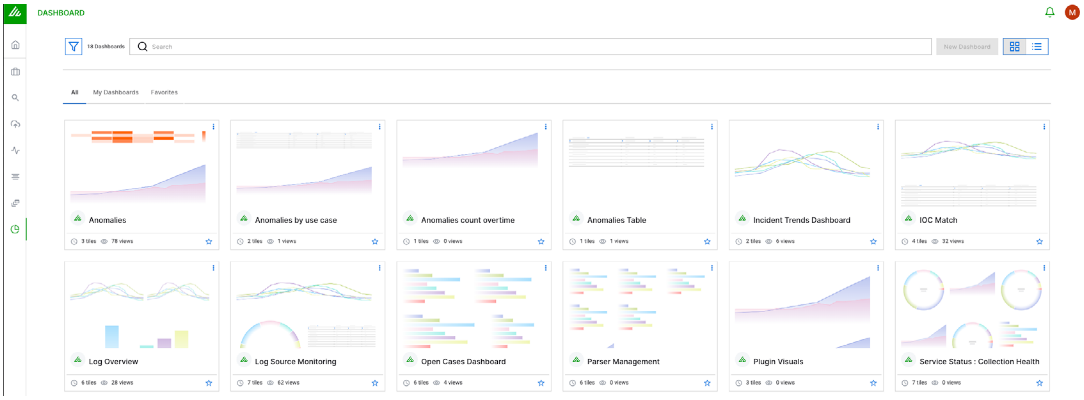
VENDORS & PRODUCTS

Unix
Unix
Auditbeat
BIND DNS
Postfix
Unix Privilege Management
rsyslog
Unix Sendmail
Unix Auditd
Unix dhcpd
Unix Named
Tanium
Tanium Core Platform
Tanium Cloud Platform
Tanium Integrity Monitor
Tanium Threat Response
Exabeam

AA	access	access_group
access_mask	access_reason	access_type
accesses	accessKeyId	accessor
account	account_domain	account_id
account_login_guid	account_name	acl_content
acs_session_id	action	action_performer
action_type	activity	activity_details
activity_id	activity_type	actor
added_keys	added_member	added_member_type
added_permissions	added_role	added_role_name
added_users	additional_info	admin_id
admin_interface	adopter_id	adult_score
affected_user	agent_id	agent_name
aid	aip	alert_description
alert_id	alert_name	alert_reason
alert_severity	alert_source	alert_status

Search

Search offers a simplified search experience with faster query and instant results over petabytes and years of data; search hot and cold data at the same speed. Search is a single interface that allows analysts to search for events, alerts, strings, or IoCs. 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. 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.

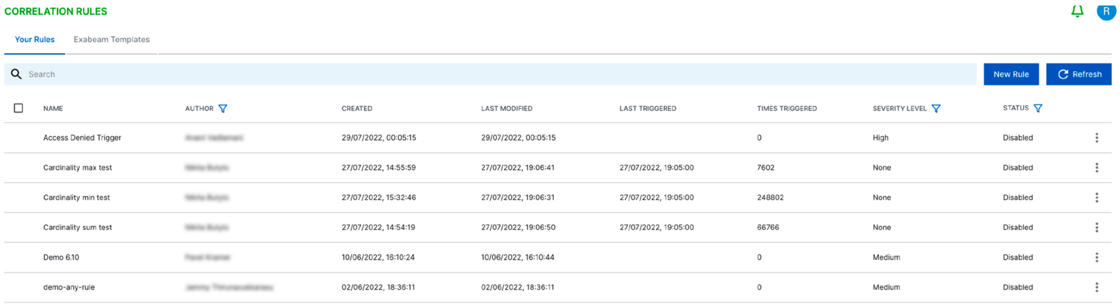


Anomalies — 3 tiles, 78 views
Anomalies by use case — 2 tiles, 1 views
Anomalies count overtime — 1 tiles, 0 views
Anomalies Table — 1 tiles, 1 views
Incident Trends Dashboard — 2 tiles, 6 views
IOC Match — 4 tiles, 32 views
Log Overview — 6 tiles, 28 views
Log Source Monitoring — 7 tiles, 62 views
Open Cases Dashboard — 6 tiles, 4 views
Parser Management — 6 tiles, 0 views
Plugin Visuals — 3 tiles, 0 views
Service Status : Collection Health — 7 tiles, 0 views

Dashboards

Print, export, or view security event data with 13 pre-built dashboards covering most compliance needs, complete with pre-built compliance visualizations, exportable reports, and the option to create your own dashboards in only a minute. With 14 different chart types, you can easily analyze your data as if you were using a leading BI tool.

The Dashboards app is fully integrated within Exabeam Fusion, allowing you to quickly create powerful visualizations from your parsed log data. Choose from a variety of options, including bar charts, column charts, line graphs, area charts, pie charts, donut charts, bubble charts, funnels, single values, sankey maps, word clouds, heat maps, tables, and coverage maps. Customize your visualizations to highlight the metrics that matter most for your business needs.



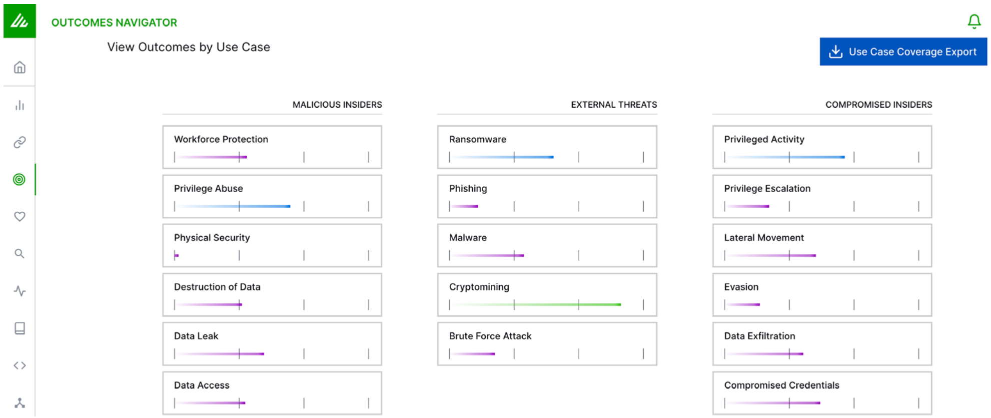
☐	NAME	AUTHOR	CREATED	LAST MODIFIED	LAST TRIGGERED	TIMES TRIGGERED	SEVERITY LEVEL	STATUS
	Access Denied Trigger	[redacted]	29/07/2022, 00:05:15	29/07/2022, 00:05:15		0	High	Disabled
	Cardinality max test	[redacted]	27/07/2022, 14:55:59	27/07/2022, 19:06:41	27/07/2022, 19:05:00	7602	None	Disabled
	Cardinality min test	[redacted]	27/07/2022, 15:32:46	27/07/2022, 19:06:31	27/07/2022, 19:05:00	248802	None	Disabled
	Cardinality sum test	[redacted]	27/07/2022, 14:54:19	27/07/2022, 19:06:50	27/07/2022, 19:05:00	66766	None	Disabled
	Demo 6.10	[redacted]	10/06/2022, 16:10:24	10/06/2022, 16:10:44		0	Medium	Disabled
	demo-any-rule	[redacted]	02/06/2022, 18:36:11	02/06/2022, 18:36:11		0	Medium	Disabled

Correlation Rules

Correlation rules define conditions that function as triggers by comparing 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 assets. Define higher-priority entities, or add specific Threat Intelligence Service-sourced conditions and assign specific MITRE ATT&CK® tactics, techniques, and procedures (TTPs).

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 monitors for well-known threats, identifies compliance violations, and detects signature-based threats using context from the Exabeam Threat Intelligence Service or other third-party threat intelligence.



OUTCOMES NAVIGATOR

View Outcomes by Use Case

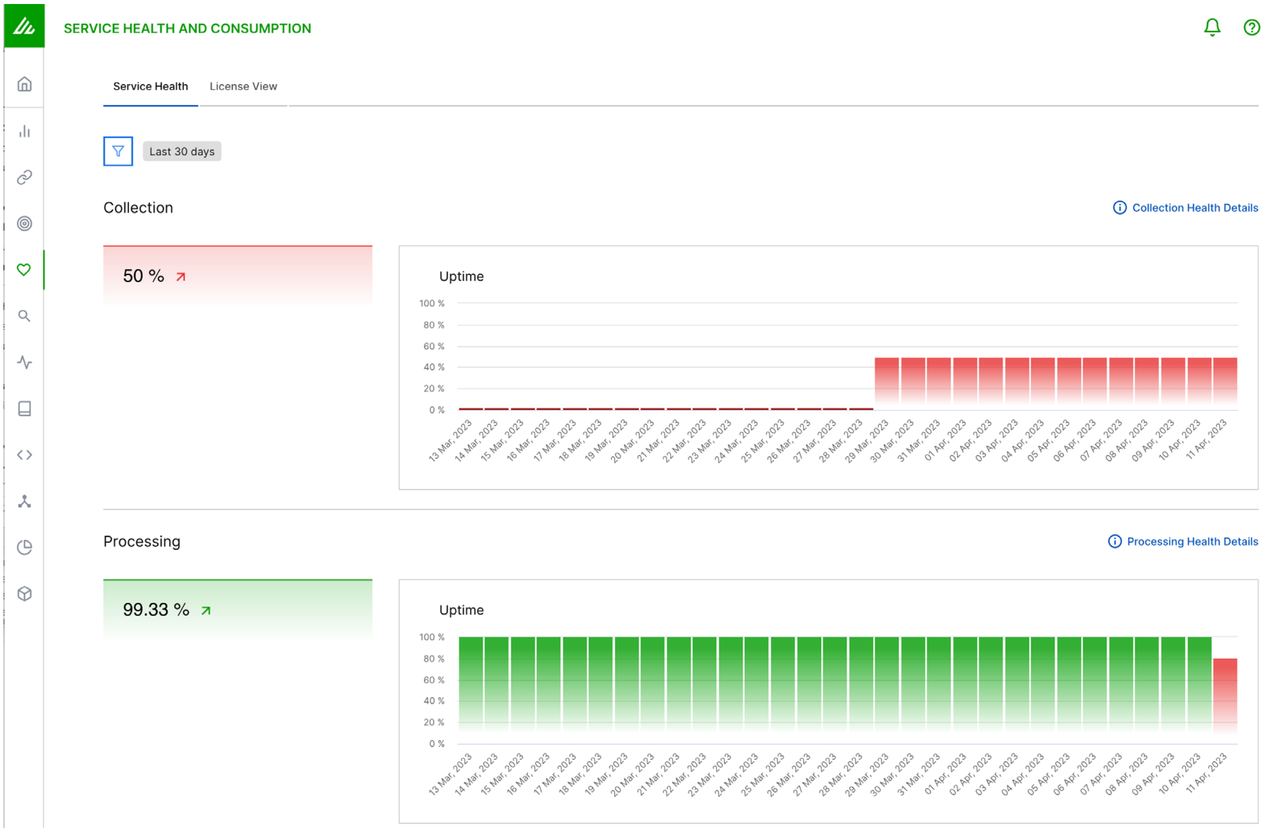
MALICIOUS INSIDERS	EXTERNAL THREATS	COMPROMISED INSIDERS
Workforce Protection	Ransomware	Privileged Activity
Privilege Abuse	Phishing	Privilege Escalation
Physical Security	Malware	Lateral Movement
Destruction of Data	Cryptomining	Evasion
Data Leak	Brute Force Attack	Data Exfiltration
Data Access		Compromised Credentials

Outcomes Navigator

Outcomes Navigator maps the security log feeds that come into the Exabeam Event Store against the most common security use cases and suggests ways to improve coverage. It examines the completeness of the logs parsed and the Dashboards and Correlation Rules associated with those use cases, identifies gaps in log parsing or sources, and suggests ways to improve coverage. Outcomes Navigator supports measurable, continuous improvement by recommending information, event stream, and parsing configuration changes needed to close any gaps.

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 highly accurate 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.



Service Health and Consumption

Visualize the health of 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.

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

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

Standard Support

Standard Support is 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

To maximize your Exabeam investment, our Education team has created a series of classes to get you up and running as quickly and efficiently as possible. Whether you are a security analyst, engineer, or just interested in understanding more about the functionality of Exabeam, we have training for you in a variety of modalities: eLearning, Virtual Instructor-led, and Onsite.

About Exabeam

Exabeam is a global cybersecurity leader that created New-Scale SIEM™ for advancing security operations. We help organizations detect threats, defend against cyberattacks, and defeat adversaries. The powerful combination of our cloud-scale security log management, behavioral analytics, and automated investigation experience results in an unprecedented advantage over insider threats, nation states, and other cyber criminals. We understand normal behavior, even as normal keeps changing — giving security operations teams a holistic view of incidents for faster, more complete response.

exabeam®

Detect
Defend
Defeat™

Learn how at
Exabeam.com →