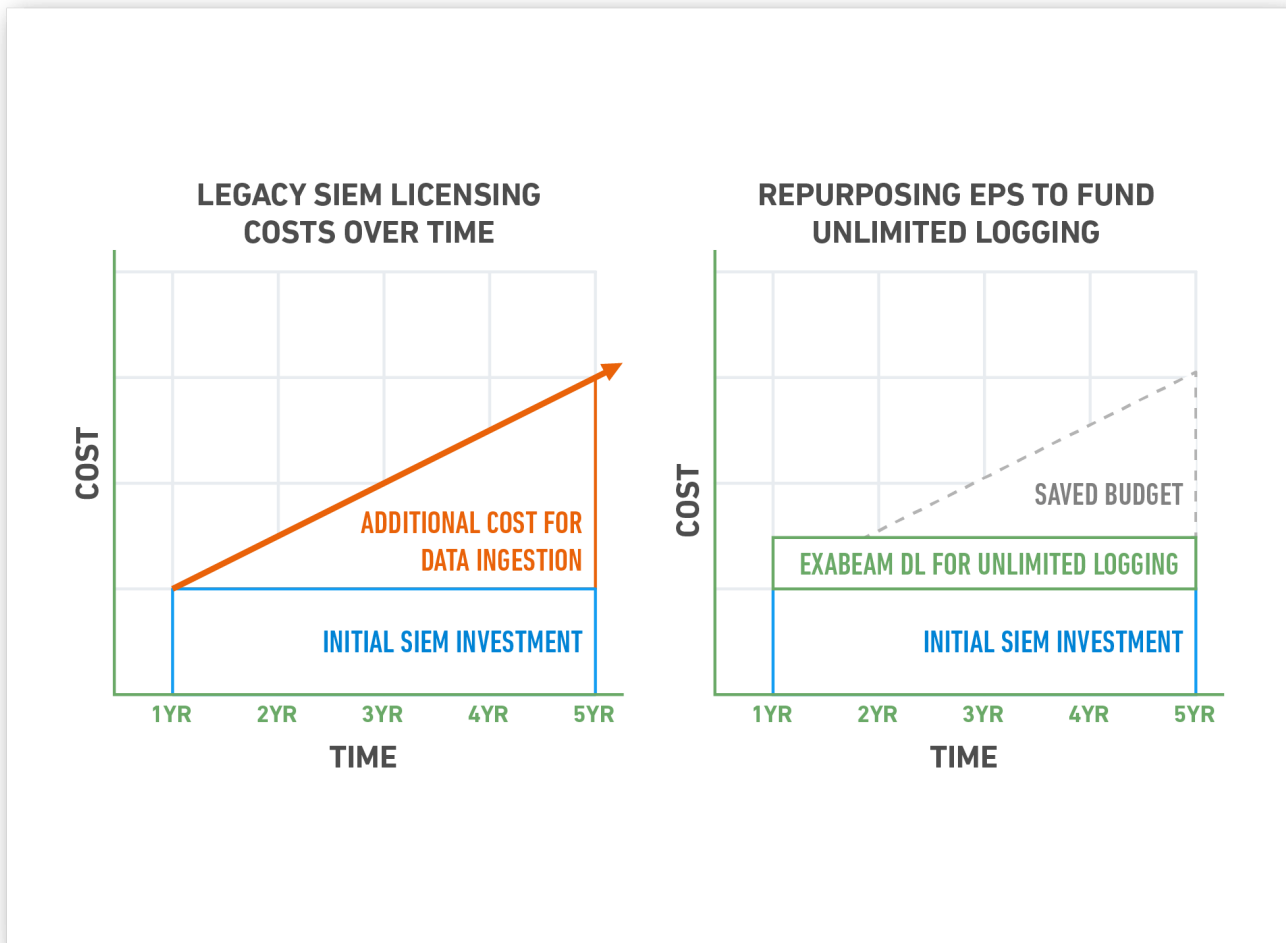


Exabeam Data Lake

Unlimited collection and secure data storage without volume-based pricing



Limitless Scale with Flat, Predictable Pricing

Every log and every security event matters. Not retaining your log data can create security blind spots that prevent compliance or leave your organization vulnerable to attack. Data Lake is designed to scale without complexity or ever-growing costs providing secure data storage at a reasonable price. Simply add nodes to provide additional storage and processing power. Our flat pricing model is based on the number of users in your environment, without the escalating “by-the-byte” licensing fees.

Apr 11th 2018, 15:10:04.000

ENDPOINT

user **grojas** process_name **gresult.exe** dest_host **10.10.3.161** command_line **expand** host -

```

exa_adjustedEventTime: Apr 11th 2018, 15:10:04.000 is_privileged: false pid: 10 exa_category: Endpoint title: Public Relations Officer
directory: C:\Windows\SysWOW64\ path: C:\Windows\SysWOW64\gresult.exe process_guid: b053aeaf-9530-4524-85ae-61e0e85206eb
process_name: gresult.exe exa_rawEventTime: Apr 11th 2018, 15:10:04.000 activity_type: ingress.event.procstart arg: 10:10:04
@version: 1 exa_parser_name: s-process-created-windows indexTime: Apr 11th 2018, 15:10:04.878 process: C:\Windows\SysWOW64\gresult.exe
message: <14>{"win_server":"winserver","command_line":"expand","computer_name":"10.10.3.161","event_type":"process","md5":"27e097f0656ed514aec8e54057f65145","parent_process_guid":"390b6f0d-bb50-4fa2-8747-39fb473f680e","path":"C:\Windows\SysWOW64\gresult.exe","pid":10,"process_guid":"b053aeaf-9530-4524-85ae-61e0e85206eb","sensor_id":72,"timestamp":"04/11/2018 10:10:04 PM","type":"ingress.event.procstart","username":"192.168.2.128\grojas"} @timestamp: Apr 11th 2018, 15:10:04.849
domain: 192.168.2.128 forwarder: 172.18.0.1 data_type: process-created dest_host: 10.10.3.161 parent_process_guid: 390b6f0d-bb50-4fa2-8747-39fb473f680e
time: Apr 11th 2018, 15:10:04.000 fullname: Garrett Rojas user: grojas command_line: expand md5: 27e097f0656ed514aec8e54057f65145
_id: AWK2wjn0nrz1i94M4ded _type: logs _index: exabeam-2018.04.11 _score: -

```

Apr 11th 2018, 15:10:02.108

```

indexTime: Apr 11th 2018, 15:10:02.108 @timestamp: Apr 11th 2018, 15:10:02.051 exa_rawEventTime: Apr 11th 2018, 15:10:02.108
@version: 1 forwarder: 172.18.0.1 message: _id: AWK2wi78nrz1i94M4deY _type: logs _index: exabeam-2018.04.11 _score: -

```

Apr 11th 2018, 15:10:02.000

NETWORK

subtype - event_name - protocol **TCP** rule - network_app - user - src_user - src_ip **10.10.3.17** src_port **6,767** src_country -

dest_user - dest_ip **10.10.3.40** dest_port **7,811** dest_country - bytes - bytes_out - bytes_in - host **192.168.2.100**

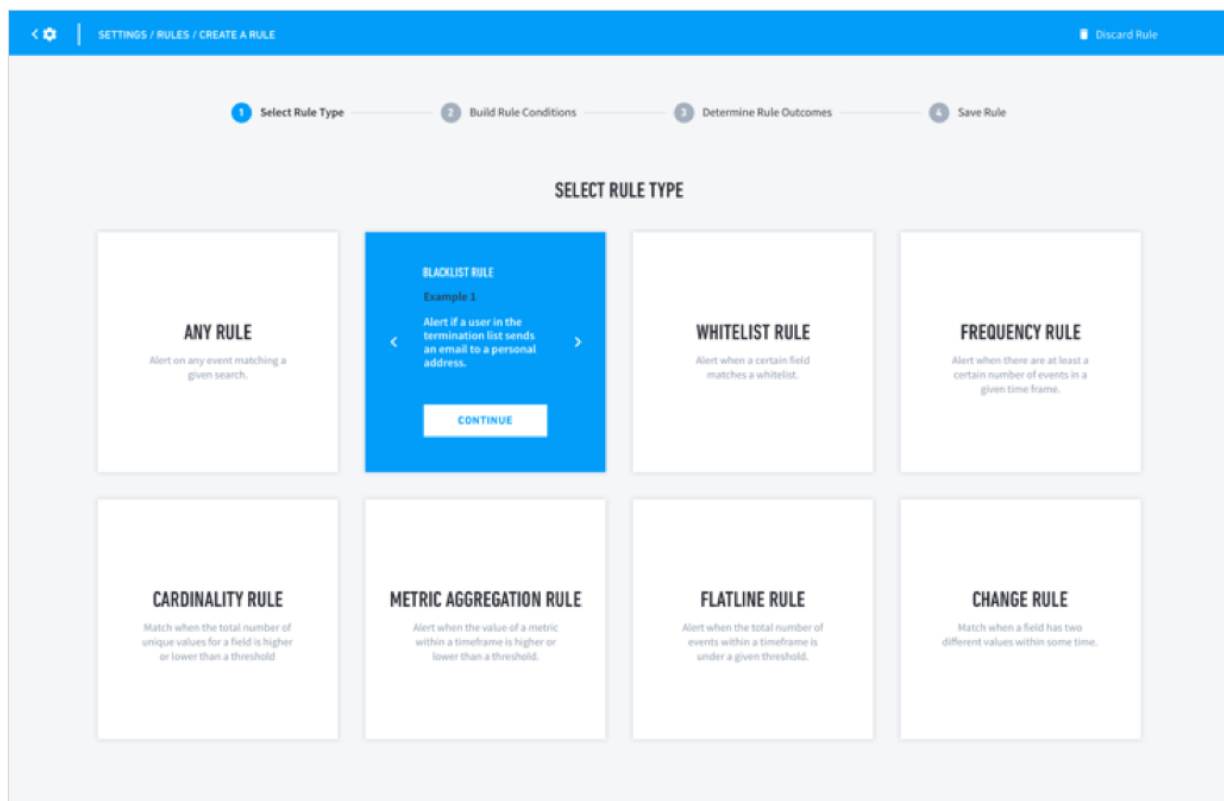
```

indexTime: Apr 11th 2018, 15:10:02.126 exa_adjustedEventTime: Apr 11th 2018, 15:10:02.000 exa_category: Network message: <14>04/11/2018 10:10:02 PM: %ASA-6-302001: Built outbound TCP connection 9389674363 for faddr 192.168.2.100/968 gaddr 10.10.3.40/7811 laddr 10.10.3.17/6767 () src_ip: 10.10.3.17 src_port: 6,767 protocol: TCP @timestamp: Apr 11th 2018, 15:10:02.093 port: 968
exa_rawEventTime: Apr 11th 2018, 15:10:02.000 dest_ip: 10.10.3.40 @version: 1 forwarder: 172.18.0.1 data_type: fw-allow host: 192.168.2.100
connection: 9389674363 time: Apr 11th 2018, 15:10:02.000 exa_parser_name: firewall5 dest_port: 7,811 _id: AWK2wi80nrz1i94M4dea
_type: logs _index: exabeam-2018.04.11 _score: -

```

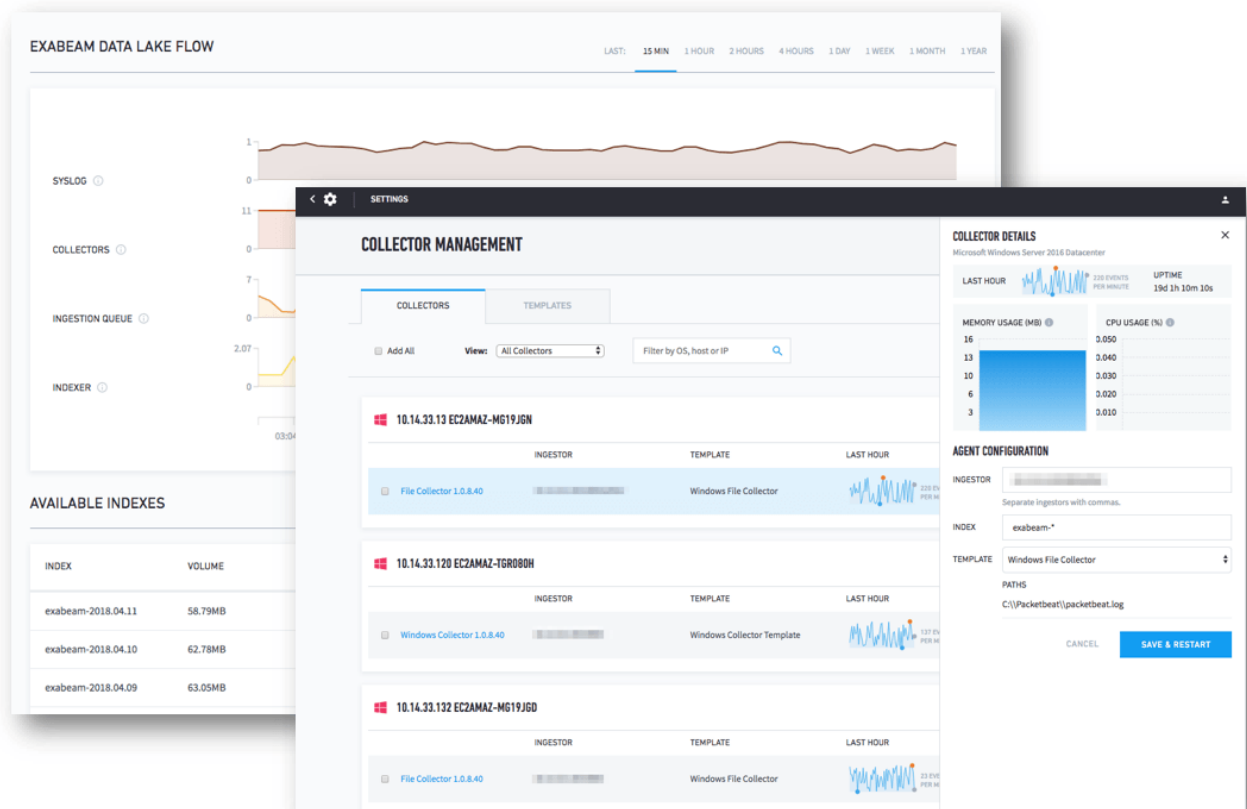
Context-Aware Log Parsing and Presentation

Data lake provides contextual log parsing to help your team quickly find the information they need, without combing through a sea of raw logs. The enhanced log view highlights the security relevant information of specific log types such as user and source IPs from VPN logs to easily view security risks instead of combing through raw logs. Guided search assists analysts by auto completing their search requests.



Natural Language-Based Rule Builder

In next gen SIEMs, threat detection is often performed through a combination of machine learning and behavioral analysis. However, high-value correlation rules may still prove useful for certain tasks, like detecting policy non-compliance. Data Lake leverages a rule building wizard, capable of converting natural language syntax into effective correlation rules. This enables even the most junior analyst to craft complex and effective rules.



Centralized Collector and Health Management

SIEMs must gather data from many sources and are as effective as the data they collect. Thousands of log collectors must be managed — a very time-consuming task. Data Lake’s secure data storage enables SOCs to centrally manage log collectors by configuring, updating, starting, and stopping collectors in bulk through templates. The console makes it easy to monitor the health of your entire deployment, so analysts can spend time on identifying security threats.



Prebuilt Compliance Reports

Data Lake utilizes hundreds of prebuilt reports for common compliance regulations, including PCI-DSS, Sarbanes Oxley, GDPR, NERC CIP, and others — all which help your organization demonstrate adherence. Out of the box security content helps ensure the correct security controls are implemented and operating as expected, so that you can easily demonstrate compliance to your auditors.