

# NetGain Log Analytics Datasheet

Logs are files that capture the events and activities within the operating system or application. Such event information could include file requests, login requests, error messages and the like.

Log management is the practice of gathering, storing and processing the logs data. Log management is an important IT function. The benefits of an effective log management include:

- Improved observability across the enterprise
- Improved audit and compliance requirements
- Enhanced security especially when used with an SIEM to find hidden cyber threats
- Ability to conduct forensics after a security event

## NetGain Log Analytics

NetGain Log Analytics is an easy-to-use centralized log management system. It first collects and ingests logs from the different systems in the infrastructure. The logs are then normalized and stored in one unified database.

NetGain Log Analytics provide a powerful search and query functionality, so that the operator can perform log data analysis and predictive modeling intuitively. The logs also feed into NetGain's observability solutions and also Security Analytics, to allow the enterprise full-stack visibility and security.

NetGain Log Analytics is available as both an on-premise software or as a SaaS offering.

## Key Features

### Log Analytics

Log Analytics is designed to collect systems logs from a variety of IT devices, including security devices, servers, network devices and more, whether they are on-prem or in the cloud. The logs are mapped using a common schema, that will allow intelligent search and correlation. The user can then generate custom dashboards and compliance reports from the logs.

- **Comprehensive log sources supported**

A variety of log sources are supported, including syslogs from network, security devices, servers, on-prem and cloud.

Instructions are provided in the software on how to configure the devices to send logs to NetGain.

Log sources
Syslogs
Audit logs
Windows event logs
Other logs
Sample logs

Configure your network devices to forward to NetGain EM IP addresss, at port 514  
See below for some examples

**Cisco devices Syslog forwarding**

Take the following steps to configure your Cisco device

```

conf terminal
logging <ip address>
logging source-interface <interface>
logging trap warning
logging console warning
logging facility syslog
copy running-config startup-config

```

- **Efficient log mapping using Filebeat and GROK**

Log mapping is the process of putting different log data into standard fields so that logs can be treated intelligently, can be manipulated, and logs from different systems can be correlated.

The solution comes out-of-the-box with support for vendors and device types. For any other brands which are not currently supported, the user can use GROK function to map the logs.

The following are the out-of-the-box supported vendors:

activemq	apache	auditd	aws	awsfargate	azure	barracuda	bluecoat
cef	checkpoint	cisco	citrix	coredns	crowdstrike	cyberark	cyberarkpas
cylance	elasticsearch	envoyproxy	f5	fortinet	gcp	google_workspace	googlecloud
gsuite	haproxy	ibmmq	icinga	iis	imperva	infoblox	iptables
juniper	kafka	logstash	microsoft	misp	mongodb	mssql	mysql
mysqlenterprise	nats	netscout	nginx	o365	okta	oracle	osquery
panw	pensando	postgresql	proofpoint	rabbitmq	radware	redis	santa
snort	snyk	sonicwall	sophos	squid	suricata	symantec	system
threatintel	tomcat	traefik	zeek	zookeeper	zoom	zscaler	






- **Mapping to the Elastic Common Schema (ECS)**

NetGain uses Elasticsearch as the underlying database, and Filebeat as the primary tool to collect and map the logs. Filebeat is community-created to support the latest devices. The logs are mapped to Elastic Common Schema.

- Intelligent search, query and correlation

The module comes with an intelligent search capability that provides search suggestions as you type. The query is lightning fast even with a large data set. The search allows correlation of the data and the results are shown on screen or can be downloaded as a report.

The GUI also allows the user to select and zoom into the time period as needed.

Log Analytics		Security Analytics	Reports	Watcher
Search		Sources	Filters	Mapping
 	time			
 	@timestamp <i>search this log field</i>			
	azure-eventhub.enqueue_time <i>search this log field</i>			
<b>Frequently</b>				
Today	Last 5 minutes	Last 3 hours	Last 7 days	
This week	Last 15 minutes	Last 6 hours	Last 1 month	
This month	Last 30 minutes	Last 12 hours	Last 3 months	
This year	Last 1 hour	Last 24 hours	Last 1 year	

## Watcher

The Watcher feature allows the user to set a query based on key words or phrases, and the system will alert the operation staff once the query is triggered.

Log Analytics

Security Analytics

Reports

Watcher

NetGain ITM & SM Trial Edition (Demo) v11.1.299

Watcher

☆

↺

↻

🔍

📷

Logs Watcher

+ Add rule

1-2 of 2

Show

100

View columns

Export

Search table...

<

>

Rule name	Enabled	Run Interval	Time Window	Alarm Message	Last Run	Last Triggered
detect account creation in windows AD	<input checked="" type="checkbox"/>	1 mins	15 mins	account created in Windows AD	Jul 01, 10:40:54	
traffic from source.ip: source.ip : 10.88.102*	<input checked="" type="checkbox"/>	1 mins	3600 mins	two more traffic is captured from source.ip source.ip : 10.88.102.*	Jul 01, 10:40:54	

## Reports

There are hundreds of standard reports that are configurable so the user can always get the report that he or she needs. Compliance reports for standard compliance such as HIPAA, are also available out-of-the-box. Adhoc reports can also be created by the user.

Standard compliance reports include:

CCPA	COCO	CYBER ESSENTIALS	FERPA	FISMA
GDPR	GLBA	GPG	HIPAA	ISLP
ISO 27001 2013	NERC	NIST	NRC	PCI DSS
PDPA	SOX			

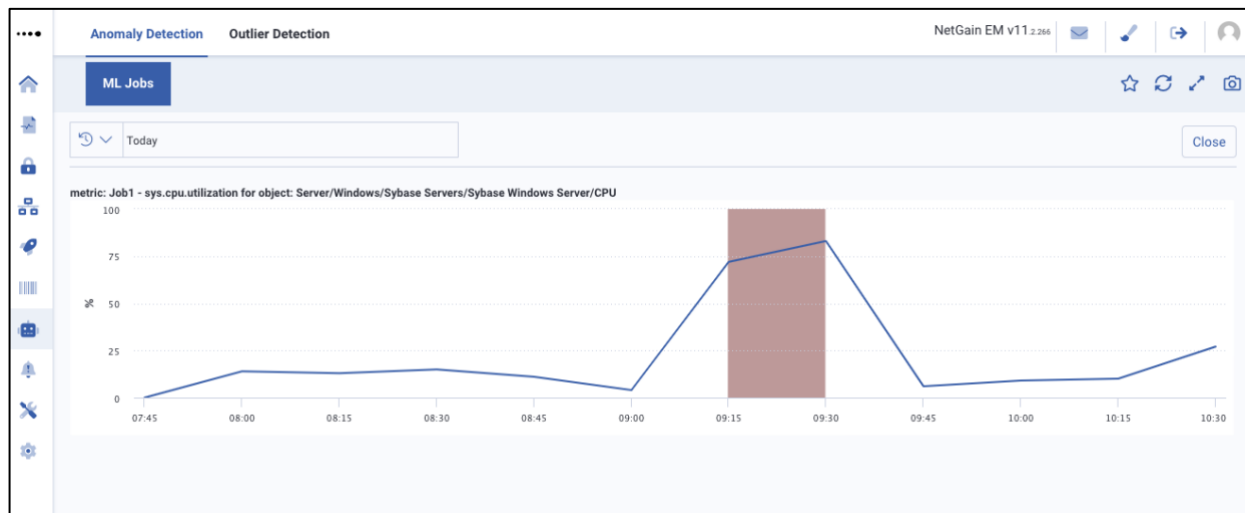
## AI Ops

Artificial Intelligence-assisted Operations (AI Ops) is a separate module that uses the logs ingested to perform the following functions:

- **Anomaly detection**

Anomaly detection is the identification of the behavior of IT components that deviate from its normal behavior. An example would be a source IP which sends traffic to a specific server only during office hours. However, if it starts to send traffic to the same server at midnight, this is an anomaly. By using historical data, the AI determines the baseline behavior, and identifies deviation from baseline behavior as it happens. IT ops may also set the sensitivity of the AI detection.

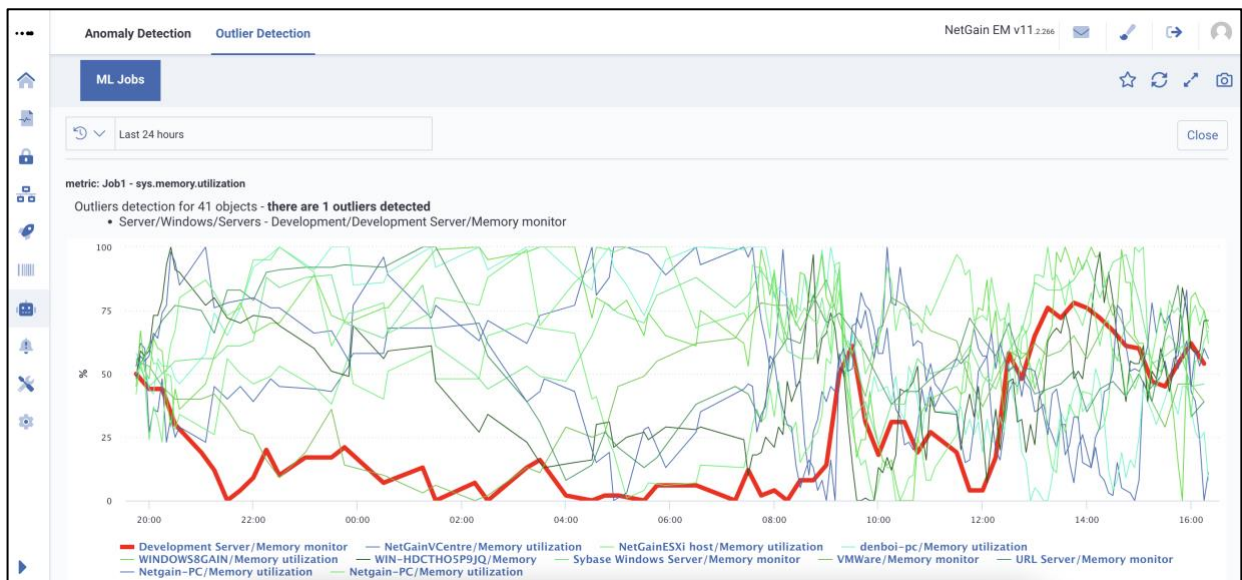
With anomaly detection, IT ops do not need to set static thresholds, and instead rely on the AI to find the thresholds automatically, and then alert the ops team when the anomaly occurs.



- **Outlier detection**

An outlier is an IT component that deviates drastically from the given norm or average of the data set. An example would be if a set of 20 servers are all sending logs to the system, and one server is sending more logs than the others, then this server would be deemed an outlier. AI is used to identify the outlier in the given data set. IT ops may also set the sensitivity of the AI detection

With outlier detection, the AI is able to find potential issues even if the fault does not exceed the threshold, and is able to alert the IT ops team automatically.



## **How It Works**

Logs are collected and ingested into the NetGain platform. Logs typically come from a variety of IT devices, including security devices, servers and networking devices.

Logs data are normalized using the Elastic Common Schema. This allows the data from different devices to be correlated for analysis.

The user can start to do intelligent search and correlation through user-friendly query interface.

## **Deploying NetGain Log Analytics**

NetGain Log Analytics can be deployed in a single server or distributed over multiple VMs, appliances or cloud instances. Its highly flexible and scalable architecture lets it fit easily into any existing environment while having the capacity to meet any future growth and expansion.

NetGain Log Analytics can manage devices in your IT infrastructure spanning multiple geographies, in the cloud and in hybrid physical / cloud networks by leveraging on NetGain Cloud Vista Suite, allowing you to remotely monitor and manage threats to your IT infrastructure from virtually anywhere.



## System Requirements

The requirements for running and operating NetGain **Log Analytics** will depend on the number of devices and the size of the network it is deployed in. The following gives an indication of the hardware requirements for a given IT environment. Please contact NetGain on the requirements for your environment.

<b>Managed Log Analytics environment:</b> Up to 100 devices, consisting of 1-10 firewalls, 10-40 switches/routers, and 20-40 Windows or Linux servers/containers  <b>Data Retention period:</b> 6 months	
Hard disk	2TB
CPU	Quad Core
RAM	16GB
Operating System	CentOS 7, RHEL 8 or equivalent
Browsers Supported	Firefox, Google Chrome, Safari, Microsoft Edge.

## About NetGain Systems

Founded in 2002, NetGain Systems is a pioneer in the IT monitoring business, and continues to develop its business as it evolves from IT monitoring to IT observability. It has established local teams throughout the Asia Pacific Region, including Australia, China and Singapore.

Regardless of location, type, size, or complexity, our solutions give our customers the power to observe their IT infrastructure, services, applications and devices with ease, all from a single management dashboard, to achieve operational excellence with reduced complexity and gain useful insights to improve business outcomes.

By understanding that every organization's IT environment is different, NetGain's dynamic solutions are designed to be highly adaptable, fitting the unique demands of your operating environment and evolving with your growing organization.

Elasticsearch and Filebeats are trademarks of Elasticsearch B.V., registered in the U.S. and in other countries.

Apache, Apache Lucene, Apache Hadoop, Hadoop, HDFS and the yellow elephant logo are trademarks of the Apache Software Foundation in the United States and/or other countries.