graylog

API Security

— Getting Started Guide —

What is Graylog API Security?

Graylog API Security captures real API traffic to detect attacks, leaks, and other threats to your APIs. Graylog API Security discovers your APIs and the risks from their use by legitimate customers, malicious attackers, partners, and insiders. This protection is accomplished with built-in automated and custom signatures and alerts.

Why You Need To Monitor Your APIs

Web application development can be hard to monitor in today's ever-growing world of data integrations and seamless data sharing. Many organizations have no idea how many APIs they have and how to manage them. These data points are crucial for application architecture and their usage in business-critical applications. As every year passes, the scaling of APIs is exponential. Without the proper oversight, this can leave you vulnerable to exposing personally identifiable information (PII), making them easy targets for attackers.

As APIs are developed, many enterprises need a way of monitoring their own APIs and how to identify threats. Not knowing your APIs and their use can create a very tricky situation for your security teams. When security teams are unaware of what APIs are in use, they can't protect what they don't know they have.

Limitations and Cautions

A few notes to ensure a successful and compliant implementation of the free version of API Security:

- The free license is good for 1 year, unlimited renewals for as long as this program is available
- 1 free license per organization

- Storage capacity is limited to a local 16GB rolling buffer, meaning once the limit is reached, the oldest data will roll off as new data comes in. This roll-off includes all alerts associated with that data.
- Data can be manually exported for retention purposes but will consume the local storage if imported back in.
- API Security is a cloud-native architecture. It can be run on-prem or in a Private Cloud but requires a **minimum of 6 vCPU and 18GB RAM**. Due to the sensitive nature of what is captured, Graylog does not offer a Cloud Hosted option.
- The free license does not include Iceberg storage.

Deployment and Installation Options

Graylog API Security is deployed on Kubernetes Clusters using Helm. The supported deployments are AWS, Azure, GCP, and IBM Cloud. The supported chipsets are 64-bit X86, ARM, Xeon, AMD, Amazon Graviton, and Apple Silicon.

Graylog API Security Free Edition is a single node deployment requiring 6 Cores and 18GB of RAM. Storage capacity is 16GB, with the oldest stored data aged out over time.

Using helm

Helm is the standard package manager for Kubernetes. Think apt or brew but for your Kubernetes cluster. After installing Helm, you can install and upgrade Kubernetes applications (called **charts**) onto your Kubernetes cluster. The main helm commands are shown below, and the rest of this documentation gives all the specific examples needed to administer your installation.

Installing on AWS

When installing API Security on an existing EKS cluster, you'll need 6 vCPU and 18 GB of memory for each API Security node deployed. If your existing EKS cluster cannot meet these requirements, create a new node group using **m7g.2xlarge** (ARM), **m7i.2xlarge** (x86), or larger VMs. In addition, the **Amazon EBS CSI Driver** add-on must be enabled in your cluster to provision persistent volumes. The Amazon EBS CSI plugin requires IAM permissions to call AWS APIs on your behalf. Create the corresponding IAM Role or attach the *AmazonEBSCSIDriverPolicy* to your existing role.

Installing on Azure

When installing API Security on an existing AKS cluster, you'll need 6 vCPU and 18 GiB of memory for each API Security node deployed. If your existing AKS cluster cannot meet these requirements, create a new node pool using **Standard_D8ps_v5** (ARM), **Standard_D8as_v5** (x86), or larger VMs.

Installing on GCP

When installing API Security on an existing GKE cluster, you'll need 6 vCPU and 18 GiB of memory for each API Security node deployed. If your existing GKE cluster cannot meet these requirements, create a new node pool using **c3d-standard-8** (x86) or larger VMs. We do not recommend deploying on ARM at this time.

Installing on IBM Cloud

When installing API Security on Red Hat OpenShift on IBM Cloud, you'll need 6 vCPU and 18 GiB of memory for each API Security node deployed. If your existing OpenShift cluster cannot meet these requirements, create a node pool using **bx2-8x32** (x86) or larger VMs. We do not recommend deploying on ARM at this time.

Installing on microk8s

Microk8s is a lightweight Kubernetes distribution that runs on your hardware. To start, you'll need a Linux machine or VM with at least 8 vCPU and 24GB of memory. Each API Security node requires 6 vCPU and 18 GB of memory, and resources must be left over for microk8s, Minio (if enabled), and the operating system.

Microk8s requires `snap`, which is enabled by default on Ubuntu and its derivatives. For other Linux distributions, enable snap support before installing microk8s.

Methods to Capture API Calls

Each Graylog API Security cluster has a capture URL used to receive incoming API Calls. This is different from the URL used to connect to the database. This capture URL is acquired by running a script on your Kubernetes Cluster. Once this is acquired, you have multiple ways to receive API calls. These sources include:

- Submitting JSON
- Sniffer DaemonSet
- Sniffer sidecar
- VPC Traffic Mirroring
- Tyk API Gateway
- AWS API Gateway
- Kong API Gateway
- Logger Libraries

Submitting JSON

Graylog API Security accepts API calls in JSON format from practically any source, including `curl`. This makes for an easy “hello world” test to verify that your database can receive API calls over the network before configuring any sniffers or other data sources.

Sniffer DaemonSet

Graylog API Security can deploy a network sniffer to every node in your Kubernetes cluster using a DaemonSet. This allows API calls to be captured without having to modify each pod. Our sniffer discovery feature automatically captures all API traffic as services start and stop within the cluster.

Sniffer sidecar

Graylog API Security provides a containerized network-level packet-capture sniffer that can run alongside your applications as a sidecar. This allows API calls to be captured directly from their shared network interface. Our sniffer sidecar works for AWS ECS, Azure ACI, Docker compose, stand-alone Kubernetes manifests, and anywhere you can run multi-container applications.

VPC traffic mirroring

Traffic mirroring (supported by Amazon VPC) copies network traffic from EC2 instances to monitoring platforms like Graylog API Security. This allows a high volume of API traffic to be delivered to a Graylog API Security network sniffer that captures the API calls. Traffic monitoring doesn't require changes to existing APIs and doesn't negatively impact API performance.

Tyk API Gateway

For APIs fronted by a Tyk gateway, API calls can be easily captured to Graylog API Security through the Tyk pump. The Tyk pump does not slow down calls made through the Tyk gateway. All code related to Tyk pump integration is open-source (and packaged/distributed by Tyk) but is independently tested and supported by Graylog. We're proud to be part of the Tyk community! Resurface Labs and Graylog API Security won a Tyk Community Award in 2021 and announced a formal partnership with Tyk in 2023.

AWS API Gateway

For APIs fronted by Amazon API Gateway, API calls can be captured to your API Security database through Kinesis data streams. This doesn't require changes to existing APIs and doesn't negatively impact API performance. This open-source integration module is shared on GitHub under the Apache2 license and is fully supported by Graylog API Security.

Kong API Gateway

For APIs fronted by a Kong gateway, API calls can be captured to Graylog API Security by adding a Kong plugin. Our open-source plugin is hosted on GitHub, shared under the Apache2 license, and is fully supported by Graylog.

Logger libraries

Our open-source logging libraries are easy to integrate, with friendly Apache2 licensing and minimal dependencies. These include prebuilt middleware for many popular frameworks so you can log API calls in just a few minutes. There are many options for logger libraries, and these include the following:

- logger-go
- logger-java
- logger-nodejs
- logger-python
- Logger-ruby

How to Get Your Free License

You can get your free license by filling out this online form here:
https://go2.graylog.org/api-security-free

Installation Documentation and Links

For installation commands and detailed documentation, please follow this link.
For an AWS Tutorial Install, see this link.
Contact Graylog: Contact Us
Support: api-support@graylog.com