

# Gain Visibility & Control Over Your Exposure to Sensitive Data Leakage

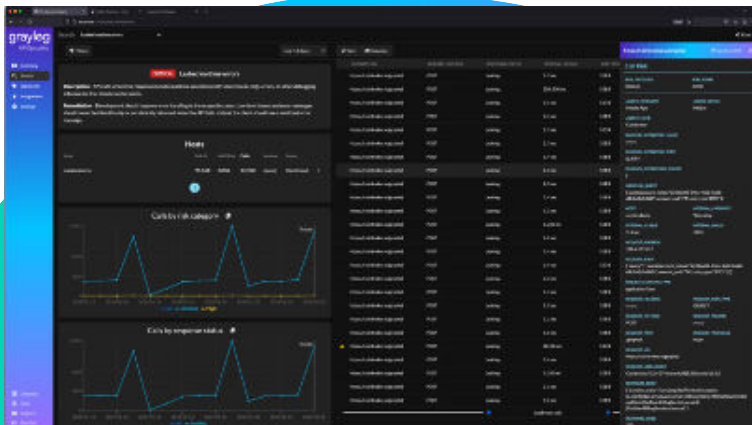
with complete API and PII discovery, automatic risk scoring, and TDIR

**Graylog API Security** is the first API security solution that is purpose-built to provide security teams with full observability into runtime API activity inside the perimeter. Unlike traditional security tools that see only part of the picture, Graylog API Security continuously discovers APIs and the sensitive data they could potentially expose. This helps your security team know exactly which APIs are handling PII (Personally Identifiable Information), what types of PII are present, and how data moves through your ecosystem. With full API request and response payload analysis, you gain the insights needed to detect data leaks, insider threats, and compliance risks before damage occurs.



## Ask Our Experts and See Graylog API Security in Action

Seeing is believing. At Graylog, we want you to get all your questions answered before you buy. We offer scheduled product demos that demonstrate product functionality and allow time for Q&A. [Schedule your Graylog API Security demo today](#) and see our powerful cybersecurity platform in action.



### Graylog API Security Benefits

- **Continuous API & PII Discovery** — Automatically discover and categorise all APIs, ensuring none stay under the radar
- **Guided Threat Detection & Response** — Get alerts with clear, actionable steps to deal with threats immediately
- **Full Request AND Response Payload** — Go beyond header data for precise alerts, retroactive threat hunting, and API-specific remediation
- **Secure Self-Managed Solution** — Keep sensitive data in-house, avoid 3rd-party disruptions, PII concerns, and the red tape of SaaS security reviews

## POWERFUL FEATURE SET



### API CAPTURE

Gain complete visibility into your API attack surface through network, gateway, and in-application capture options.



### ASSET CLASSIFICATION

Save development time by automatically classifying the data that flows through any API.



### CONTINUOUS API & PII DISCOVERY

Eliminate the burden on development and security teams to manually identify the APIs in use by your organization.



### NO-CODE RULES

Easily build your own custom threat detection and alerting rules.



### OWASP TOP 10+

Utilize Graylog's threat signatures that go beyond OWASP for immediate risk reduction.



### REAL-TIME THREAT DETECTION

Monitor for security issues at runtime, generating well-tuned alerts with full context and customized remediation guidance.



### REMEDiation

Alerts include detailed, targeted, and customizable instructions to address risks immediately.



### REQUEST & RESPONSE CAPTURE

Automatically capture the header and body data of all requests and responses for REST APIs and GraphQL queries.



### RISK SCORING

Prioritize threats based on potential data leakage and focus on securing high-risk APIs first.



### SIMPLIFIED COMPLIANCE

Ensure compliance with GDPR, CCPA, and HIPAA by tracking and securing PII across all APIs.



### SELF-CONTAINED DATA LAKE

Cost-effectively preserve API transactions for investigations and threat-hunting without needing an external database.



### GRAYLOG SECURITY INTEGRATION

Integrate API security insights into Graylog Security and augment centralized SecOps with API-specific context.



### SSO

Use OAuth or JWT for secure access to Graylog API Security.



### TARGETED ALERTING

Precise routing of alerts directly to Security and/or DevOps teams via Slack, Teams, Gchat, or Zapier.

**Get Graylog API Security – Free Edition →**

