graylog
API SECURITY

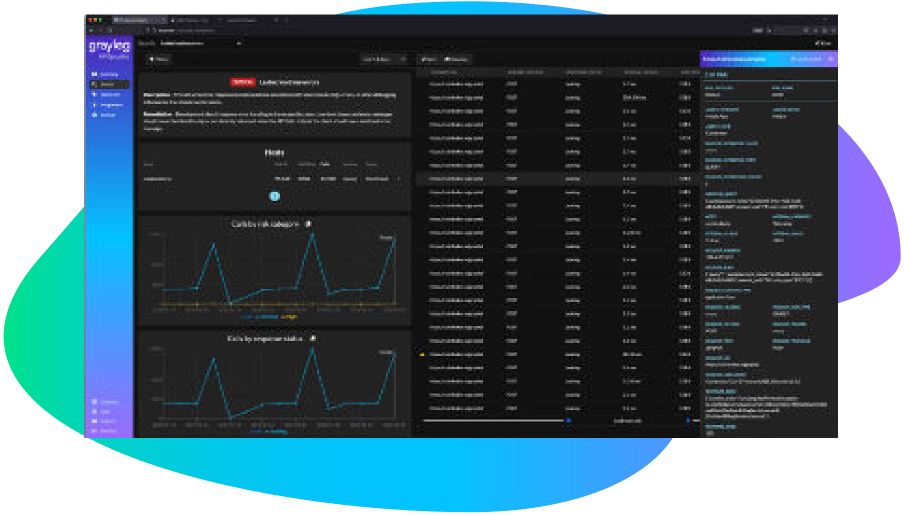
Gain Visibility & Control Over Your API Attack Surface

with complete API discovery, threat detection & incident response

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. As attackers are finding innovative ways to pose as valid users to gain unfettered access to critical production APIs, you can no longer rely on perimeter defense alone. Your security teams can now use Graylog API Security to strengthen your post-perimeter API security posture and manage your growing API attack surface. Graylog API Security provides API discovery, threat detection, and incident response capabilities that provide complete visibility into your environment, real- time monitoring for attacks, and thorough analysis of end-to-end API request and response data.

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 Discovery** — Automatically discover and categorize 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 graylog

API SECURITY

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 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

Automatically assess the security posture of your APIs and receive actionable intelligence into your current API security risk.

SEARCH

Find needed information quickly with standard SQL and regex queries.

SELF-CONTAINED DATA LAKE

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

SIEM/SOAR INTEGRATION

Automatically send critical security alerts to Graylog SIEM or your SOAR solution for incident response.

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.