graylog
API SECURITY

GAIN VISIBILITY & CONTROL OVER YOUR API ATTACK SURFACE
for complete 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 AT-A-GLANCE

INSIDE-THE-PERIMETER THREAT DETECTION
Because Graylog API Security is deployed behind WAFs and API gateways, it monitors your runtime environment for security issues, including attacks, threats, leaks, and performance weaknesses. Our console gives your security teams real-time visibility into API request attacks and threats that have evaded perimeter defenses and identifies leaks and performance issues in API responses.

MEANINGFUL ALERTS WITH CONTEXT FOR EFFECTIVE INCIDENT RESPONSE
Use Graylog API Security's unprecedented API context and visibility to tune alerts, reduce alert fatigue, and increase response effectiveness. Our console comes pre-configured with a base set of detections and alerts, so security teams can quickly turn search and investigation results into a customized alert unique to your API environment. All alerts link back to the Graylog API Security console, displaying the exact context that initiated the alert, and alerts can include customizable response and remediation guidance.

GRAYLOG API SECURITY BENEFITS

- **Guided Threat Detection & Response** — Get alerts with clear, actionable steps to deal with threats immediately
- **Continuous, Uninterrupted Monitoring** — Runtime scanning without impacting application performance, no matter how many threat signatures you check
- **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

API ATTACK SURFACE MANAGEMENT (ASM)

API attacks are growing in sophistication and complexity so much that high-profile breaches are occurring, despite the deployment of perimeter defenses; your attack surface extends into your API runtime environment. Graylog API Security provides API attack surface management capabilities aligned with proven ASM methodologies

MODERN ARCHITECTURE FOR EASY DEPLOYMENT

Modern software architectures leverage platforms for deploying and managing containerized workloads and services, with Kubernetes being the most widely adopted deployment platform. Graylog API Security is a containerized app (with a self-contained data lake) that quickly deploys into any Kubernetes environment along with an API collection daemon set, enabling API security implementation times that are measured in minutes and hours versus the days and weeks standard for other API security products.

REGULATORY DATA PRIVACY

Most API security products are SaaS offerings that require your data to be filtered, redacted, anonymized, etc. before being uploaded and stored in the vendor's shared cloud environment. Graylog API Security runs locally within your environment (on-prem or cloud), and no data is ever transferred beyond your privacy boundary. This eliminates the need to filter, redact, and anonymize your data, which can severely impact the effectiveness of security operations.

EXABYTE-SCALE WITH BUDGET-FRIENDLY STORAGE

Graylog API Security is built on a proven data lake technology that powers many global-brand solutions. Designed to scale from small and lightweight to exabyte-level global implementations, Graylog API Security's data lake can meet the needs of both smaller and large organizations. Data is stored in a security-centric schema and is accessible via standard SQL queries. You can also set a data retention policy to meet your needs, balancing data accessibility with resource utilization and costs.

FULL API SECURITY CONTEXT, INCLUDING THE "RESPONSE"

As each API transaction is captured, it is analyzed to flag over 70 different characteristics related to API security. This analysis includes response leaks and performance issues that perimeter security typically misses. Key header and body data are also mapped to security-related fields to aid in follow-on security functions. This unique security analysis is stored with each API transaction to power Graylog API Security's powerful search, views, monitoring, and alerting capabilities.

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 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 Security 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.

graylog
API SECURITY

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 provides API 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.

ABOUT GRAYLOG

Graylog is a leader in log management and Security Information Event Management (SIEM), making the world and its data more efficient and secure. Built by practitioners with the practitioner in mind, Graylog unlocks answers from data for thousands of IT and security professionals who solve security, compliance, operational, and DevOps issues every day. Deployed in more than 50,000 installations worldwide, Graylog is an award-winning platform built for speed and scale in capturing, storing, and enabling real-time analysis of terabytes of machine data. Graylog eliminates the noise and delivers an exceptional user experience by making data analysis, threat hunting, detection, and incident investigation fast and efficient using a more cost-effective and flexible architecture.