graylog
API SECURITY

GAIN VISIBILITY & CONTROL OVER YOUR API ATTACK SURFACE

for 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 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

Alerts are generated that include a summary and description of the underlying security issue that generated the alert, as well as a high-level histogram to provide immediate context for activity and intensity. It provides you with Automatic Remediation Tips and actionable solutions to resolve issues and help you optimize critical metrics like Mean Time to Respond (MTTR).

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

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.

CONTINUOUS API DISCOVERY

Incoming API traffic is sorted into domain buckets based on your top-level domain. Combining discovery with automated risk assessment scoring capabilities allows Graylog API Security to provide a 2-pronged approach to TDIR, bridging the communication gap between DevOps and Security teams so they can work in concert to identify potential issues and devise informed remediation strategies.

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"

Graylog API Security is the only solution that captures the unfiltered API request and response detail enhanced with runtime analysis, creating a readily accessible datastore for attack detection to identify common threats and API failures swiftly and accurately by using Integrated Threat Signatures aligned with OWASP and MITRE guidance to help you reduce operational metrics like Mean Time to Detect (MTTD), detect zero-day issues, and search all API calls retroactively to identify patterns and track actions.

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.

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 discover, 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.