wallarm

PRODUCT DATASHEET

API Leak Management

Proactive Runtime Protection of API Keys and Secrets

Wallarm API Leak Management provides a comprehensive answer to the recent surge in hacks involving leaked API keys and other API secrets. It enables continuous discovery of leaked API keys and secrets, automatic implementation of controls to block their use, and neverending protection against any follow-on attacks.

API Leak Management at a Glance

Wallarm API Leak Management enables comprehensive real-time API threat protection, delivered on a single platform that provides leak detection and response which looks beyond just GitHub.

Discovery

We actively scan many (currently 20+) different sources – not just GitHub – to discover any leaked API Keys and other secrets which pertain to your APIs.

Protection

We automatically remediate any leaked API Keys and other secrets by blocking any further use of leaked secrets to prevent misuse or abuse.

Integration

We have integrated this capability into our platform, meaning you do not have to add another tool / workflow into your process, which reduces the security team workload, effort, and budget.

Wallarm delivers an integrated proactive approach, which combines automated deep-dive discovery with instantaneous protection, to minimize the blast radius caused by leaks of API Keys and other secrets.

Types of Leaked API Secrets Detected

Wallarm API Leak Management detects a host of different credentials which allow privileged access to tools, applications and data.

- **API Keys.** This is a really long list covering things like AWS, S3, GCP, custom, et cetera.
- **API Credentials.** This includes things like certificates and user credentials (UID / PW).
- **Private API Specifications.** More than just credentials, this includes your API blueprints such as endpoint documentation or authentication tokens.

Complimentary API Leaks Assessment

Concerned that your API keys and other secrets are out in the open, and about the potential fallout? Get a thorough understanding of your risk exposure due to leaked API keys and other secrets by getting a free API leaks assessment. **Register now** and you will get your report within 72 hours after confirmation.

Guard Against Leaked API Keys and Secrets

The Wallarm API Leak Management solution is offered via the Wallarm API Security Platform, and provides proactive runtime API leak management capabilities delivering continuous automated detection, remediation, and monitoring:

Detect

Wallarm constantly scans scores of public sources for leaked API secrets, which hackers can find and abuse in less than 1 minute.

Remediate

Wallarm automatically blocks requests with compromised tokens across your entire API portfolio.

Monitor

Wallarm then continuously tracks and blocks any subsequent use of these leaked API keys and other secrets.

Why Do You Need API Leak Management?

Attacks involving leaked API keys and other API secrets have taken on new importance because of the wide-ranging impact. Some representative cases include:

CircleCi. In Jan-2023, customers were alerted to rotate all secrets because of a breach.

Slack. In Jan-2023, GitHub tokens were stolen and used to download private code repositories.

LastPass. In Dec-2022, an earlier breach led to stolen keys and credentials which put end-users' vaults at risk.

Travis Ci. In Jun-2022, researchers found over 73,000 tokens, secrets and credentials exposed in public.

Leaks of API keys and secrets are accelerating for a variety of reasons:

- Engineering teams are on ever-tightening schedules, which means shipping faster with less QA coverage.
- Tech stacks are getting more complicated – securing both legacy and modern APIs, supporting more authentication/authorization methods, enabling more tooling diversity used by different teams, and covering more environments – which leads to mistakes and accidental leakage.
- Software supply chains are getting longer and more complicated, which means these leaks can occur anywhere – by your in-house teams, by your partners, by the open-source code being used, or even by your customers.

Protect any API

- Complete protocol support: REST, GraphQL, gRPC, WebSocket
- Microservices
- Serverless

In any environment

- AWS, GCP, Azure, IBM Cloud
- Private, Hybrid and Multi-Cloud
- Kubernetes / Service Mesh
- Zero-Trust

Against any threats

- OWASP Top-10 Risks and Sophisticated API Threats
- API Abuse (bots, L7 DDoS)
- Account Takeover (ATO) / Credential Stuffing

Book a Wallarm demo
or start your free trial now

(415) 940-7077
188 King St. Unit 508, San Francisco, CA 94107
www.wallarm.com