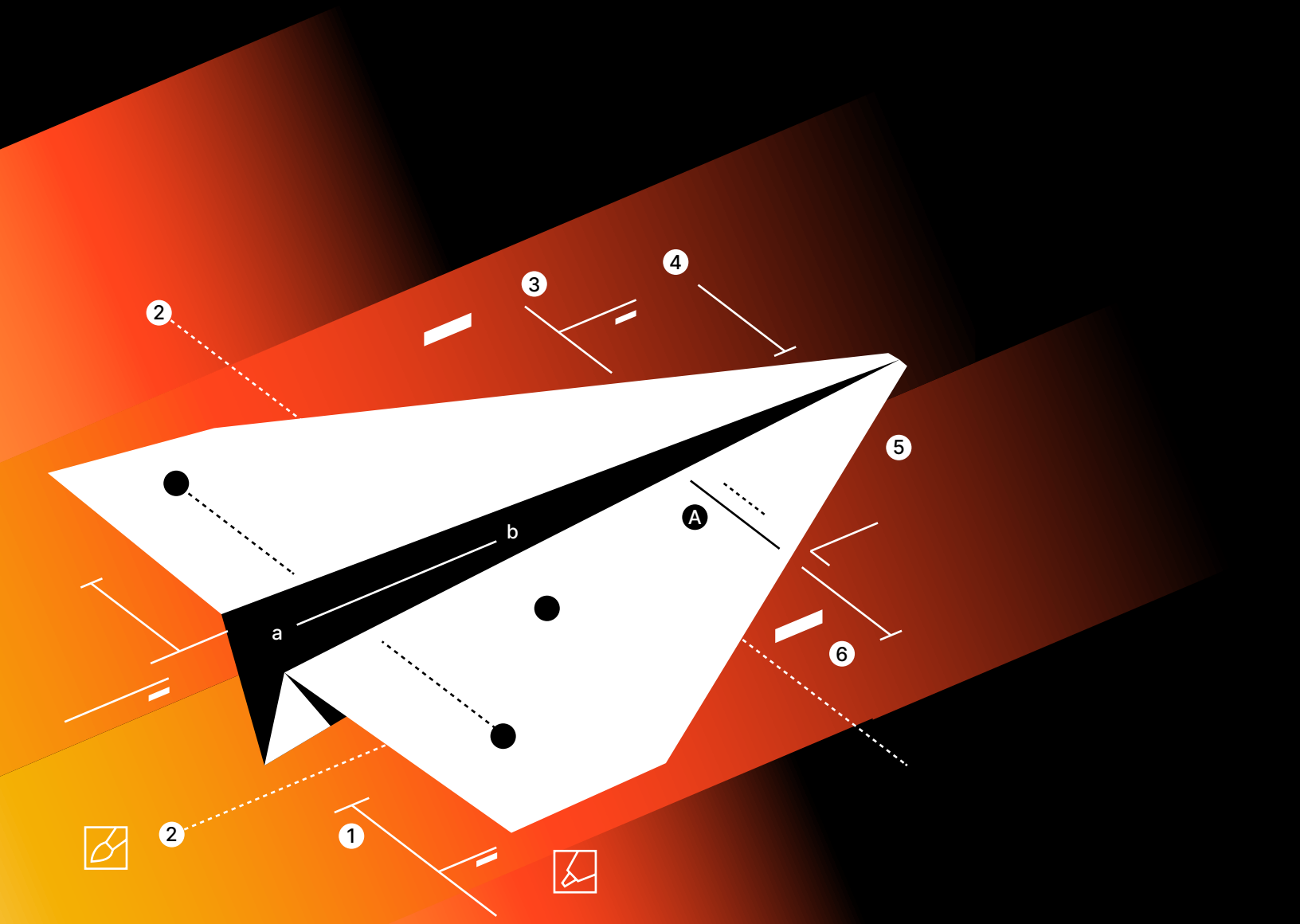
wallarm

WALLARM.COM

A CISO's Guide to API Security



Introduction

APIs are the connective tissue that allows organizations to generate revenue, service customers, and integrate with partners. Far from being just another piece of infrastructure, they are business-critical components.

The CISO's role is to manage technology risk, and connect those risk management decisions to business outcomes. As a CISO, you must understand your API estate and the threats that can impact your APIs because they directly impact business outcomes.

This whitepaper provides a framework for understanding, communicating, and addressing API Security. Designed with the CISO in mind, it provides guidance for those who are just getting started and those who are further along in their API security journey.

APIs drive your business — securing them protects your outcomes.

The API Threat Landscape

APIs now make up the vast majority of Internet traffic, and their prevalence has long garnered the attention of attackers. APIs provide programmatic access to data and applications, which attackers can leverage for their objectives, whether that's monetization or disruption. But beyond platitudes about how serious API-related incidents can be, what are the threats that matter most for CISOs? Let's break them down.

Simple, Stateless Attacks

Despite what lawyers like to put in breach disclosures, most attacks are not sophisticated. Attackers aim to be efficient, and if a simple attack is sufficient, that's what they'll use. This category of attacks includes those that can be carried out in a single request, such as SQL injection, path traversal, or remote code execution. Attacks like these don't require the attacker to develop any complex logic for interacting with the API. They can be run as 'spray-and-pray' against a large number of targets simultaneously. Their simplicity doesn't make them less dangerous, however. One good SQL injection can wreak havoc, and the Progress MOVEit incident is a good example.

> **Simple doesn't mean harmless — one request can break everything.**

These attacks appear in the OWASP API Top 10 under categories like:

- API2 Broken Authentication
- API8 Security Misconfiguration
- API10 Unsafe Consumption of APIs

Stateful Attacks

Stateful attacks are more behavior-based, and require that the attacker interact with the API multiple times, often within the context of a session, in order to successfully carry out an exploit. Examples include brute forcing through paginated endpoints, abusing session tokens, or manipulating workflow sequences. These attacks exploit assumptions about how a user is expected to interact with an API, and they can bypass controls that only focus on single-request validation. They are a risk because they mimic normal user activity, making detection more difficult, and because they often target sensitive workflows like account creation, password reset, or money transfers.

> **They look like normal users — but drain your system from within.**

These attacks are covered in the OWASP API Top 10 with categories such as:

- API2 Broken Object Level Authorization
- API5 Broken Function Level Authorization
- API6 Unrestricted Access to Sensitive Business Flows

Business Logic Abuse

Business Logic Abuse (BLA) is one of the most challenging threats facing APIs. Unlike injections or misconfigurations, BLA exploits the intended functionality of an application in ways that harm the business. In other words, the application works as designed, but not as expected. These attacks exploit gaps in developers' assumptions about user behavior, pricing models, or transaction flows. For example, attackers might repeatedly apply a coupon code, bypass a sequential workflow, or exploit orphaned states in a transaction process.

When your app works too well — attackers turn logic into leverage.

Business Logic Abuse is sophisticated, harder to detect with traditional security tools, and often goes unnoticed until significant damage is done. Detection requires contextual awareness of how an API is intended to function and how it ties to business objectives.

OWASP has released a Top 10 list for Business Logic Abuse. It's designed to be technology agnostic, so these categories of threats apply to any technology, not just APIs:

BLA1:2025	Action Limit Overrun (ALO)
BLA2:2025	Concurrent workflow order bypass (CWOB)
BLA3:2025	Object state manipulations (OSM)
BLA4:2025	Malicious Logic Loop (MLL)
BLA5:2025	Artifact Lifetime Exploitation (ALE)
BLA6:2025	Missing Transition Validation (MTV)
BLA7:2025	Resource Quota Violation (RQV)
BLA8:2025	Internal State Disclosure (ISD)
BLA9:2025	Broken Access Control (BAC)
BLA10:2025	Shadow Function Abuse (SFA)

AI Security is API Security

No discussion of technology is complete today with the inclusion of generative AI. It's important to note that whatever we include here will become out-of-date quickly.

While the details may change, it's safe to say that generative AI is driving a massive increase in the number of APIs. Not only do users access generative AI apps and agents via APIs, these tools themselves connect to other systems via APIs. The result is exponential growth.

That growth in the API landscape leads to corresponding growth in the threat landscape. While these APIs are subject to the same attacks discussed previously, they also open up the possibility of new types of attacks. Injections aren't new, but prompt injections are a variation specific to generative AI. Logic abuse isn't new, but AI logic abuse is specific to AI. Because of the role that APIs play in the deployment and usage of generative AI, they represent the ideal, and ultimately required, security control point for addressing these kinds of attacks. AI security is API security.

> **As AI expands through APIs, every prompt becomes a new attack surface.**

Enterprise API Security Requirements

Modern API security programs require more than just fixing vulnerabilities; they must address the full lifecycle of APIs. This lifecycle can be broken down into four major requirements: Discover, Protect, Respond, Test. These cover the breadth of what a CISO needs to operationalize API security and tie it directly to business outcomes.

Discover

API Discovery is the foundation of an effective API security program. You can't protect what you don't know exists. API Discovery must identify all the APIs in your environment, managed and unmanaged, internal and external, across multiple API protocols, so that you have a complete view of your API attack surface. As a function, it supports business outcomes like compliance (PCI DSS, DORA, etc.), reduced risk exposure, and improved governance.

> **You can't secure the unknown — discovery is where protection begins.**

Key API Discovery Requirements

- **Continuous, automated discovery of API endpoints**
  API Discovery can't be a one-time operation. It must be continuous in order to capture the most current state of the environment and identify changes as they happen.

- **Identification of rogue API endpoints (shadow, orphan, and zombie)**
  API governance requires matching the actual state of the environment to the desired state, and that means identifying endpoints that should and shouldn't be present.

- **Support for API protocols (REST, GraphQL, gRPC, SOAP, and WebSockets)**
  API Discovery that doesn't support the protocols in your environment leaves critical blind spots. If you can't identify it, you can't effectively protect it.

- **Automated and manual business flow identification**
  Discovery isn't just about an inventory of endpoints. It should also provide the ability to identify the associated business flow for the APIs in use.

- **Ability to identify sensitive data used within APIs**
  Understanding where sensitive data is in use across your API landscape is critical for mitigating sensitive data exposure.

Protect

Protection is the ability to stop attacks in real time. It's not enough to simply detect an attack. You must be able to block attacks before they cause damage. API Protection provides the enforcement mechanisms that prevent attackers from exploiting vulnerabilities, logic flaws, or misconfigurations. It supports outcomes such as preventing breaches, ensuring uptime, and protecting revenue.

> **Detection isn't defense — protection means stopping attacks in motion.**

Key API Protection Requirements

- **Inline blocking of malicious requests**
  Protection requires more than just detection; It requires blocking of malicious activity. Timeliness and latency are key factors in effective blocking.

- **Support for multiple API protocols (REST, SOAP, GraphQL, gRPC, WebSockets)**
  Blocking must support full request parsing for the API protocols in your environment. Tools that are limited to only request/response headers, or limited depth are insufficient.

- **Dynamic detection of both stateless and stateful attacks**
  API Protection tools must be able to identify both stateless and stateful attacks. That means monitoring behavior inside of API sessions.

- **Flexible blocking options at the level of individual requests, sessions, or IPs**
  Blocking attacks requires precision and flexibility to be effective. Simple attacks require blocking individual requests. Malicious IPs should be blocked entirely. Complex attacks require blocking individual sessions. It's critical to ensure legitimate requests are not blocked.

Detection and blocking of behavior-based API Abuse
API Abuse, such as account takeovers and data scraping, are critical threats impacting businesses today. API Protection must detect and block these types of attacks.

Detection and blocking of Business Logic Abuse
Business logic abuse is the new frontier of API attacks, but it's fast approaching mainstream. Business logic abuse detection should be built on the foundations of stateful attack detection.

Respond

There's no such thing as perfect risk reduction, so organizations must be prepared to respond to attacks. Response capabilities ensure that when an attack occurs, you can rapidly analyze, contain, and mitigate its impact. For CISOs, effective response translates into minimized dwell time, reduced financial losses, and better regulatory reporting.

You can't prevent every attack — but you can control the damage.

Key Response Requirements

Real-time visibility into attacks and affected API sessions
Security analysts need to understand the details of an attack, whether stateless or stateful. API security tools must provide those details.

Contextual analysis to identify attacker intent and progression
Attack data itself is insufficient for meaningful analysis. API security tools should provide sufficient context around attacks for analysts to understand what happened both before and after the attack itself.

Custom mitigation controls tailored to your organization's workflows
Automated mitigation is a key component of an API Security program, and there are cases where automated mitigation requires customized configurations. Ensure that your API security tool supports these needs.

Automated integration with SIEM, SOAR, and incident management systems
No security tool is a silver bullet. API Security tools must integrate with the existing security tools in your organization in order to be operationally effective.

Test

API Security Testing aims to identify vulnerabilities and remediate them before attackers can exploit them. This is not just about static code analysis. It's about testing APIs in the ways attackers actually interact with them. For CISOs, testing supports outcomes like reduced breach probability, faster development cycles, and improved DevSecOps maturity.

Find weaknesses before attackers do — test like they attack.

Key API Security Testing Requirements

- **Threat Replay testing to simulate real-world attacks**
  Security testing can be overly artificial. Connecting security testing to real-world attacks provides an important check in the process to ensure that tests are applicable.

- **Schema-Based testing**
  Generating API security tests based on a schema or specification ensures that all known parts of the API are tested. This testing should be paired with threat replay testing for comprehensiveness.

- **Integration into developer workflows**
  Security testing pre-production is the most effective way to remove risk before it's exposed. API security tools should integrate with your development environment to be effective.

- **Coverage for both stateless vulnerabilities and business logic flaws**
  Incomplete testing tools leave gaps, and gaps in testing leave exposed risk. While no tool is perfect, ensuring that your testing tools provide adequate coverage is a key requirement.

Conclusion

For CISOs, APIs represent both opportunity and risk. They power digital transformation, revenue generation, and customer engagement, but they are also prime targets for attackers. An effective API security strategy must balance business outcomes with robust protection, spanning discovery, protection, response, and testing. By adopting a lifecycle approach and leveraging the right tools, CISOs can ensure that APIs remain a driver of innovation, not a source of compromise.

wallarm

Book a Demo

About Wallarm

Wallarm is the only unified platform for API and agentic AI security successfully deployed in enterprise production environments. Wallarm was founded to protect APIs, and has built a market leading platform for API protection, including API discovery, API abuse prevention, and AI protection. With Wallarm, customers receive the fastest, easiest, and most effective way to stop API attacks.

Organizations choose Wallarm to protect their APIs and AI agents because the platform delivers a complete inventory of APIs, real-time blocking, and patented AI/ML-based abuse detection. The Wallarm platform is built for modern tech stacks, and supports the deployment options that organizations need today. Wallarm supports full SaaS, hybrid, and on-premise deployments. The platform detects and blocks API attacks across legacy and modern API protocols, including REST, gRPC, GraphQL, SOAP, Websockets, XML-RPC, and more.

Wallarm is headquartered in San Francisco, California, and is backed by Toba Capital, Y Combinator, Partech, and other investors.

Learn more..... wallarm.com
Follow us..... Blog | X | LinkedIn | YouTube
Explore product..... tour.playground.wallarm.com