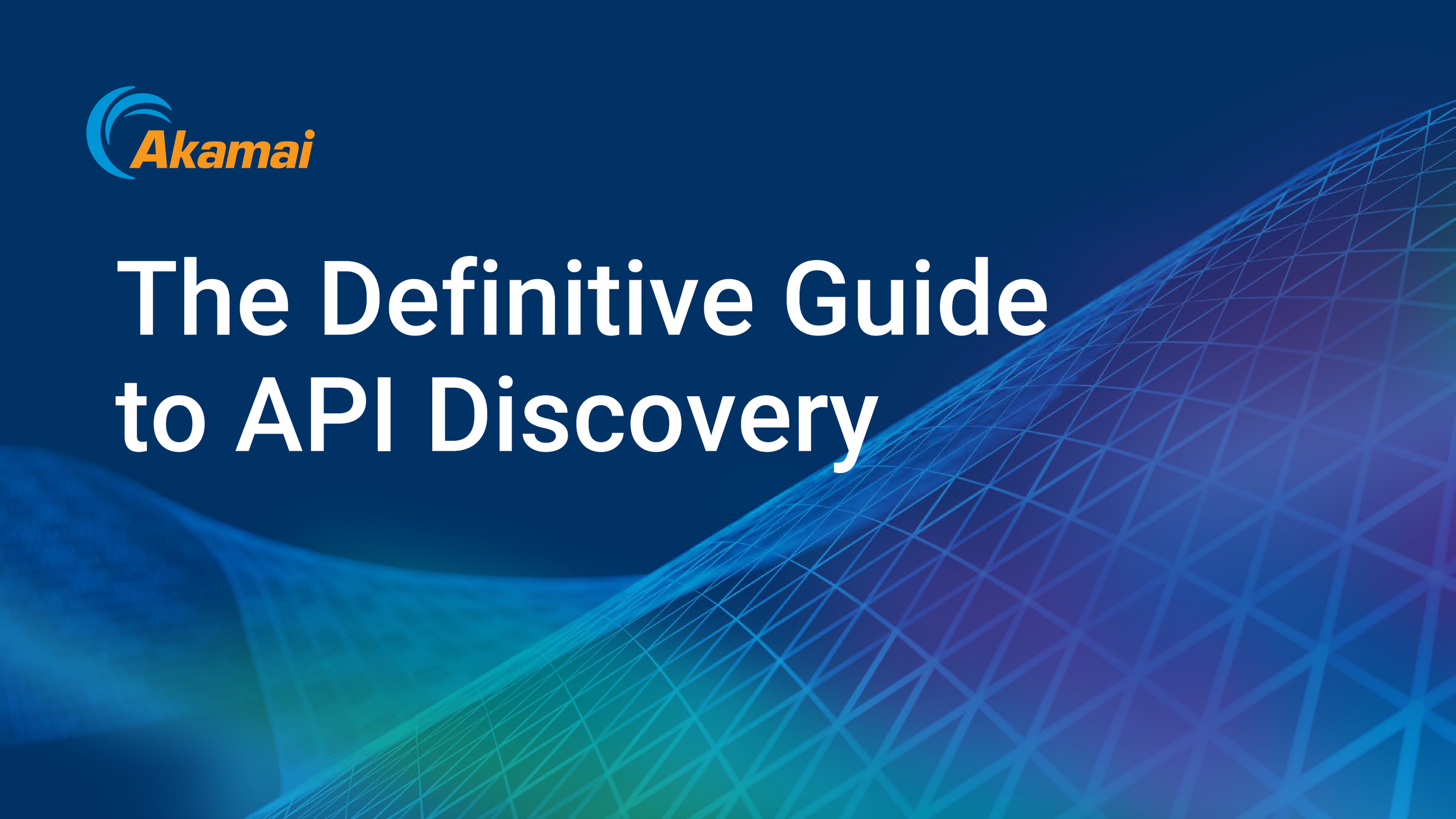


The Definitive Guide to API Discovery

Table of contents

The importance of API discovery

Whether you're getting started on API security or looking to further hone your strategy, finding and inventorying every API across your organization is a fundamental step. Why? For every application your enterprise builds, every workload it migrates to the cloud, and every tool its employees use to collaborate, there are APIs behind the scenes exchanging data – often sensitive data. The challenge is that most organizations — even those that understand the value of a complete inventory – can't actually see a major portion of their APIs.

And if you can't see it, you can't secure it.

As organizations become increasingly cloud-centric and digital, their API estate grows in scope, scale, and complexity. APIs are often spread across multiple environments, from on-prem to hybrid cloud. Adding to the complexity, your API ecosystem likely extends far beyond your own network and cloud presence. Think about the myriad connections your APIs have forged with apps, services, and systems belonging to third parties and developer ecosystems.

As your APIs increase in scope, scale, and complexity, it's difficult to gain real-time insights into:

- Where your APIs are located across various business units that in many cases have their own developer teams
- How your APIs are configured, where they're routed, and if they have proper authentication and authorization controls
- If your APIs return sensitive data when called, and who can gain access to that data

Making matters more challenging, a large portion of the APIs that organizations accumulate are unmanaged, unseen, and often unprotected. These include dormant, shadow, and zombie APIs that in many cases slip by the defenses of commonly used tools like API gateways and web application firewalls (WAFs). Granted, these tools offer benefits and baseline protection, but today's API threat landscape requires a higher degree of visibility, real-time protection, and the continuous testing that specialized API security solutions can provide.

If you can discover all your APIs, you'll have the foundation for essential next steps, such as assessing each API's risks, understanding your organization's API security posture, and using the insights you've gained to apply real-time protection that prevents attacks. In this white paper, we'll share:

- Insights on what makes certain types of APIs so elusive to security teams
- Details on API discovery capabilities that can help you gain visibility and prevent attacks

Why are APIs so difficult to find?

It's not uncommon to have unmanaged APIs in production that no one on the operations or security teams knows about, exposing the business to a range of cybersecurity risks and operational difficulties. Exposed or misconfigured APIs are prevalent, unprotected, and easy for malicious actors to compromise. And the stakes are high. Attacks on your APIs can jeopardize an enterprise's revenue, resilience, and regulatory compliance.

Here are four ways rogue APIs can arise:

1. API shortcuts and process failures

Some rogue APIs are the result of failing to inform the right people. For example, a line of business (LOB) team might create APIs to address specific needs without informing IT, or developers may be more concerned with execution than procedure. APIs that have been "inherited" as part of an acquisition are also frequently overlooked. These types of rogue APIs are often referred to as shadow APIs.

2. Old API versions

In many cases an older version of an API — possibly with weaker security or a known vulnerability — never gets removed. An old version may have to coexist with a new version for some time while software gets updated. But the person responsible for eventually deactivating the API leaves the company, gets reassigned, or simply forgets to shut down the old version. APIs can also be officially decommissioned but remain in operation due to operational oversights. Either scenario results in what is sometimes referred to as a zombie API.

3. Inherited APIs

APIs that have been "inherited" as part of mergers or acquisitions are also frequently overlooked and become shadow APIs. Inventories (if they exist) often become lost in the difficult and complicated work of integrating systems. Larger enterprises that make numerous acquisitions of smaller firms are especially at risk, as smaller firms' API estates are often sprawling and undocumented.

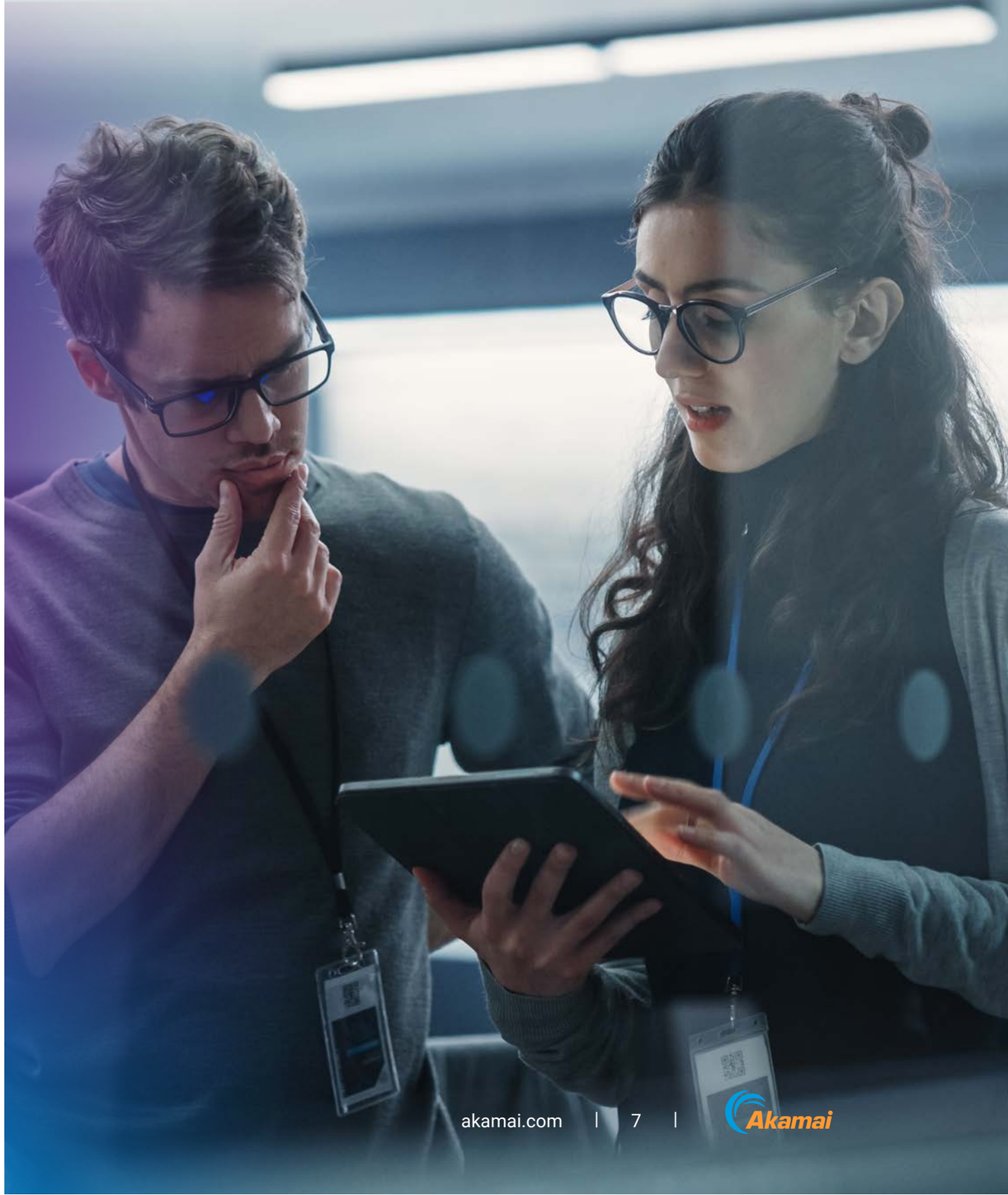
4. Commercial APIs

Some commercial software packages include APIs to connect with other applications and external data sources. These APIs sometimes get activated without anyone noticing.

What is API discovery?

API discovery is a process and set of capabilities that helps organizations identify, catalog, manage, and gauge risk among their APIs. Carried out properly, API discovery can help organizations:

- Reduce API sprawl (the fast-growing accumulation of APIs without proper documentation or oversight) and improve security posture
- Better understand their current API landscape and make informed decisions about future development
- Monitor and control access to these APIs, ensuring that only authorized users can access them



Key API discovery features to increase visibility and reduce risk

It's not uncommon to have APIs that no one knows about. However, without an accurate inventory, your enterprise is exposed to a range of risks. To effectively inventory your APIs, you need to be able to:

Locate
and inventory your APIs, regardless of configuration or type

Detect
unmanaged APIs, such as dormant and zombie APIs

Identify
forgotten, neglected, or otherwise unknown shadow domains

Eliminate
visibility gaps and uncover potential attack paths

As you evaluate new solutions for API discovery, keep in mind the following capabilities — a discovery tool should incorporate all of them.

Discovery for all API types

An API discovery tool must be able to identify APIs of every configuration or type — including RESTful, GraphQL, SOAP, XML-RPC, JSON-RPC, and gRPC.

Granular API inventory

An API discovery tool should also create an inventory that is updated automatically to prevent it from getting stale, and provide the ability to search, tag, filter, assign, and export APIs based on any attribute.

Elusive API detection

Unmanaged APIs can predate your organization's API security initiatives — your API sprawl's origins may have begun with a developer team that's no longer with your enterprise. These APIs typically lack ownership, and function without any visibility or security controls. It's critical for a discovery tool to locate these APIs.

Shadow API domain discovery

In addition to shadow APIs, you can have entire shadow domains — API domain names that you know nothing about. API discovery tools must identify forgotten, neglected, or otherwise unknown shadow domains that may pose a security risk.

Automatic API scanning

Scanning is essential to eliminate blind spots and identify critical issues, including:

- Leaked API keys and credentials
- API code and schema exposure
- Infrastructure misconfigurations
- Vulnerabilities in documentation, GitHub repositories, Postman workspaces, etc.

Identifying these and other sources of exploitable intelligence can also help teams understand potential attack paths that could be exploited by cybercriminals.

No required integrations

An API discovery tool should be able to fully discover your API estate, finding vulnerable APIs and shadow domains, without requiring any special integrations or software installation. This is critical for avoiding visibility gaps that occur simply because you've failed to install the right agent(s) or to configure the tool correctly.

Limited custom development

Finally, an API discovery tool should be designed in a way that prevents the need for custom development for traffic sources. These tools should come with pre-built integrations for major infrastructure components. Custom development is typically time-consuming, and if there are changes in the source origin, an integration would likely need to be reworked, which isn't scalable for stretched IT security teams.

How Akamai Security can help you discover all APIs

With comprehensive and continuous API discovery capabilities, organizations can realize the following benefits to their business:

- Understand the full API attack surface
- Reduce the costs of API inventories and documentation updates
- Improve compliance with regulatory requirements and internal policies

Today's threats call for a complete API security solution, encompassing four critical areas: API discovery, posture management, threat detection and remediation, and security testing. Akamai API Security provides all four of these essential modules — protecting APIs throughout their entire lifecycle, from development to production. Built for organizations that expose APIs to partners, suppliers, and users, our API Security solution discovers APIs, understands their risk posture, analyzes their behavior, and stops threats from lurking inside.

Read more about API attack methods, common API vulnerabilities, and how to secure your organization.

Learn how we can help you by scheduling a customized Akamai API Security demo.

About Akamai Security

Akamai Security protects the applications that drive your business at every point of interaction, without compromising performance or customer experience. By leveraging the scale of our global platform and its visibility to threats, we partner with you to prevent, detect, and mitigate threats, so you can build brand trust and deliver on your vision. Learn more about Akamai's cloud computing, security, and content delivery solutions at **akamai.com** and **akamai.com/blog**, or follow Akamai Technologies on **X**, formerly known as Twitter, and **LinkedIn**. Published 10/24.