



EBOOK

The CISO's Guide to API Security

Strategies for preventing data breaches, shadow APIs, abuse, and other common challenges



Content

- 3** Explosive growth in APIs is leaving security teams behind
- 4** Five challenges CISOs often face with API security and management
- 8** Compare API security approaches

Explosive growth in APIs is leaving security teams behind

APIs present exciting business opportunities to deliver products faster and improve customer experience. Now, security leaders have to balance securing their APIs, on top of their web apps, without slowing down innovation.

In recent years, data breaches and leaks through APIs have made news headlines — including [JustDial](#) in India, [LinkedIn](#) and [Twitter](#) in the social media space, and even [T-Mobile](#).

Why is this the case? Unfortunately, attackers often see APIs as a 'softer target' than an organization's core web applications. And without proper API management, this assumption often proves true.

Modern CISOs recognise the need for consolidating web application and API security. They need to secure customers' sensitive data while enabling business operations across web app and API properties.

Customer trust is at stake, after all.

58%¹
of dynamic HTTP traffic is through APIs

By 2025,
less than 50%²
of enterprise APIs will be managed, as explosive growth in APIs surpasses the capabilities of API management tools, according to Gartner®

The API security maturity curve — stages and next steps

1

LEVEL 1: Starting out with API security

Start by identifying all APIs in use within your organization.

Many ways to discover APIs: use API discovery tools, review technical documentation and agreements, speak to your developers and monitor your web traffic.

2

LEVEL 2: Using home-grown processes

Can your tools meet the visibility and compliance needs of your leadership and the usage needs of security teams?

Integrate tools better to reduce data breach, data leakage, shadow API, and availability and resilience risks.

3






LEVEL 3: Consolidating security tooling

Check out Web Application and API Protection (WAAP) if you are looking for easy to deploy, runtime-focused and cost-effective solutions for security teams.

¹ 2022 analysis from Cloudflare Radar

² Gartner® "Innovation Insight for API Protection", Analyst(s) Dionisio Zumerle, Jeremy D'Hoinne, Mark O'Neill, 10 October 2022. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

Five challenges CISOs face with API security and management

Challenge #1		Shadow APIs: Modern CISOs need visibility around all the APIs in production - be it APIs developed outside of IT or legacy APIs that are still in use. The pace of API development is only increasing in every organization.
Challenge #2		Security breaches: Modern CISOs need to ensure their organization's APIs ask for appropriate authentication and authorisation. Many API access control measures have been easily exploited by attackers till date.
Challenge #3		Data leakage: Modern CISOs need security visibility and controls over the sensitive data exchanged through APIs - be it PII/PCI/PHI data or credential or tokens.
Challenge #4		API abuse: Modern CISOs recognise that APIs being overwhelmed with abusive traffic can be just as harmful to your organization as a threat actor exploiting a security vulnerability.
Challenge #5		Compliance: Modern CISOs must ensure their customer facing APIs meet industry and organization standards - be it PCI, HIPAA, GDPR, FFIEC and FCA.

Is API security different from web application security?

Yes. APIs are a unique attack surface due to the following characteristics:

- APIs exchange data between systems. Web applications are accessed by end users through a web browser
- APIs use a different format (usually JSON) to transport data. Web apps accept user input and visualise data from the backend (using HTML, CSS and JavaScript)
- APIs access backend systems directly, often serving as the intermediary between modern web apps and their backend databases and servers
- Successful API transactions assume legitimate access
- APIs are easily overlooked as they are not visible to end users

Compared to web application security, API security requires significant business context, different discovery methods, deeper access verification controls, and intelligent abuse protection.

The detection methodology for API security differs from web app security even in overlapping vulnerability categories such as injection attacks and access risks. For example, every API operation must verify the caller's identity and permissions before performing any work on the caller's behalf.



Challenge #1: Shadow APIs

Security considerations for leaders

Shadow APIs are a growing concern in modern organizations. Most IT and security can't find and manage APIs as fast as developers build the APIs.

Many current processes for tracking APIs are broken, consisting of manual approaches with security teams pestering development teams for updates.

Some questions to ask your teams:

- How do you discover and manage public APIs today?

Security considerations for teams

Conduct regular API discovery on your environments, just as you would for IT devices and apps.

Useful metrics to report on to leadership:

- Identify the groups with the most shadow APIs, thus posing greater risks to prioritize process improvements.



Challenge #2: Security breaches

Security considerations for leaders

Security teams are more pressure than ever to prevent their organizations from becoming news headlines with security breaches. Attackers have started to exploit weak authentication and authorization measures in many APIs.

Some questions to ask your teams:

- How are you validating authentication and authorization in your APIs?
- Do your APIs follow consistent specifications and formats?

Security considerations for teams

Ensure your APIs are validating authentication and authorization tokens on every API operation

Useful metrics to report on to leadership:

- API asset inventory - highlight those carrying sensitive data, are out of compliance or use weak authentication or authorization methods

“We were facing DDoS attacks, data scrapers, and cumbersome certificate management across all our web properties as they grew in number. We wanted a security layer that could protect our web properties and APIs without adding significant overhead.”

Marut Singh
CTO, CARS24





Challenge #3: Data leakage

Security considerations for leaders

APIs will often carry sensitive data by their nature. As a CISO, you want to ensure that your APIs are not exposing the wrong sensitive data and APIs are transmitting the data under strong encryption.

Some questions to ask your teams:

- Does your data loss prevention (DLP) program include data loss through APIs?
- Are you up to date on the legal and industry-specific data security mandates?
- Is your data at rest and in transit secure? Do you use the appropriate encryption standards for your industry and jurisdictions?

Security considerations for teams

- Check for exposed/leaked credentials used in API requests
- Scan for personally identifiable information (PII), credit card data and personal health care information in API requests and responses



Challenge #4: API abuse

Security considerations for leaders

Quite often, APIs do not impose any restrictions on the size or number of resources that can be requested by the client/user.

Not only can this impact the API server's performance, leading to Denial of Service (DoS), but it also leaves the door open to authentication flaws such as brute force.

Just like with web applications, monitoring your API traffic is critical to ensure the availability of your business products and services to your customers.

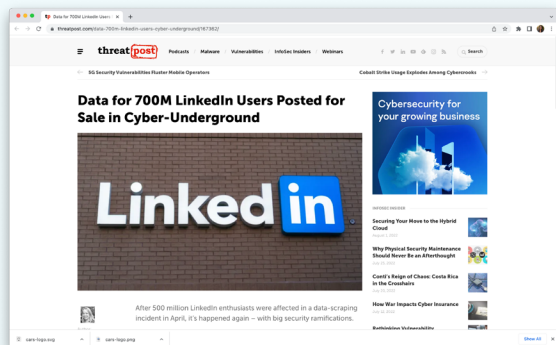
Some questions to ask your teams:

- Can your tools throttle abusive API traffic?
- How do you know what are the appropriate traffic limits for each API and the number of resources in any response?

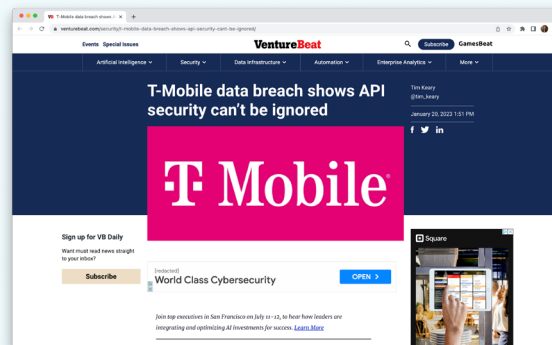
Security considerations for teams

Deploy intelligent rate limits on your APIs based on observed traffic patterns for each endpoint.

API security breaches



[Article: LinkedIn - 700 million users' data scraped](#)



[Article: T-Mobile API vulnerabilities exploited over the years](#)



Challenge #5: Compliance

Security considerations for leaders

Changing data privacy and locality regulations in many industries and global regions are nearly impossible to comply with without consistent processes and tools.

Security tools can help you by identifying sensitive data, push the relevant information into your governance solutions and integrate with your SIEM / SOAR to orchestrate appropriate responses.

Some questions to ask your teams:

- Do your security tools help you identify the relevant sensitive data seen in your APIs?
- Can you integrate your API security intelligence with other security tools?

Security considerations for teams

Scan for personally identifiable information (PII), credit card data and personal health care information in API requests and responses.

Keep audit logs on API usage, security alerts and response actions taken.

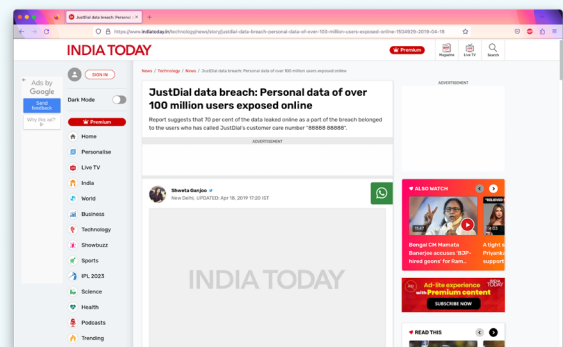
Useful metrics to report on to leadership:

- Number of instances each applicable data type was seen in your APIs

API security breaches



[Article: Twitter API exposes too much information](#)




[Article: JustDial's legacy APIs expose customer data](#)

Compare API security approaches

There are a number of approaches to manage and secure all the API growth in modern organizations - full lifecycle API management, API observability, and, holistically, Web application and protection.

For holistic security and performance around your public facing APIs without inhibiting innovation, check out the approach taken by Web Application and API Protection solutions such as Cloudflare API Gateway.

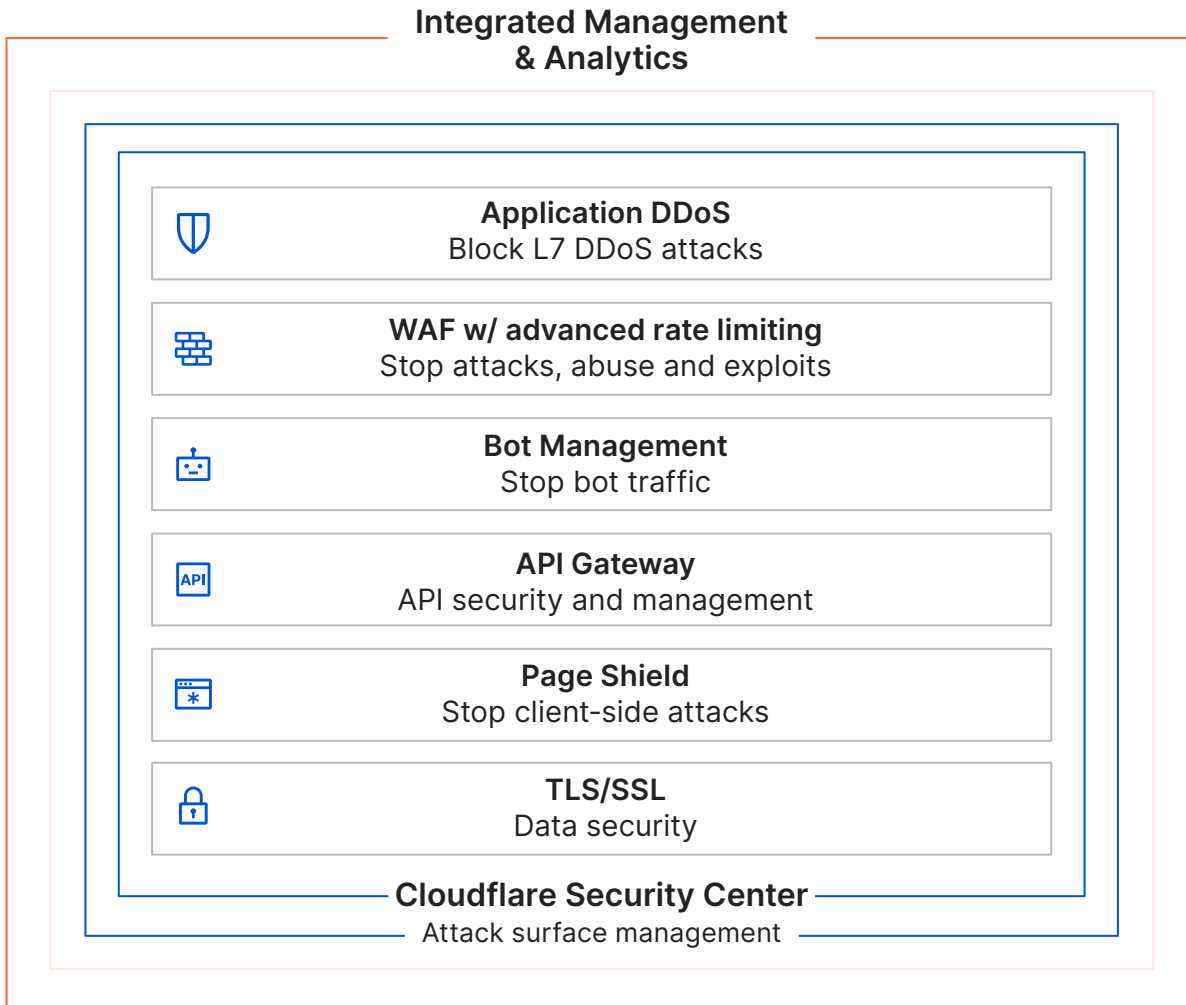
API Observability Tools	Web Application and API Protection (WAAP) 	Full Lifecycle API Management
<p>Use case: APIs in pre-production</p> <ul style="list-style-type: none"> • Will require another tool to generate API traffic • Cannot protect APIs from abuse/attacks; need to hook into a WAF to block 	<p>Use cases: APIs in production, real-time monitoring, and protection against abuse, zero days and attackers</p> <ul style="list-style-type: none"> • Provide real-time API protection compared to API security point solutions • Easier to deploy and manage than full lifecycle management solutions • Integrate with your APIs, irrespective of cloud provider, API structure and development language 	<p>Use case: APIs in highly regulated industries, legacy API standards</p> <ul style="list-style-type: none"> • These tools often focus on API management while lacking in security sophistication • These tools can be more cumbersome to integrate for developers

Key Web Application and API Protection solution capabilities

- Shadow API discovery
- Centrally manage APIs and monitor use
- Authentication validation (mTLS and JSON Web Tokens)
- Sensitive data detection for popular industry and legal requirements
- Data encryption in transit
- Positive security model for real-time blocking and traffic acceptance
- Threat intelligence from real-time traffic analysis
- Machine learning driven abuse and vulnerability exploit protection
- Optimised edge network to serve API traffic without disruptions

The Cloudflare application security portfolio

Cloudflare keeps applications and APIs secure and productive, thwarts DDoS attacks, keeps bots at bay, detects anomalies and malicious payloads, and encrypts data in motion, all while monitoring for browser supply chain attacks.



Protect your APIs without compromising innovation

Contact us



© 2023 Cloudflare Inc. All rights reserved. The Cloudflare logo is a trademark of Cloudflare. All other company and product names may be trademarks of the respective companies with which they are associated.

1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com