Akamai

When an API Gateway Is Not Enough:
Commerce Execs Weigh In on the State of API Security

APIs are essential for retail, travel, and hospitality organizations, allowing them to not only enhance customer experience, but also connect with third parties and partners that stimulate growth.

However, APIs can be vulnerable to attacks and abuse, leaving the organization open to:

Data scraping and exfiltration

Account takeover and credential stuffing attacks

Business logic abuse that enables theft of loyalty points

OWASP Top 10 API vulnerabilities
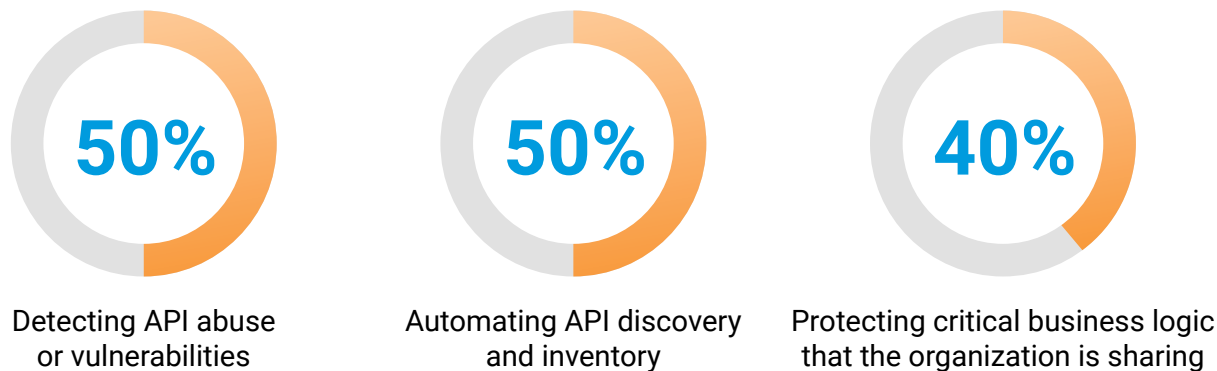
DDoS attacks ... and more

Reducing risk means gaining a line of sight into API traffic and thinking beyond the organization's API gateway or other perimeter defenses to address the unique challenges of protecting these essential interfaces.

In a recent API Security Strategies survey from Akamai and Gatepoint Research, commerce executives shared their experience about the state of API security and created a wish list for an advanced solution.
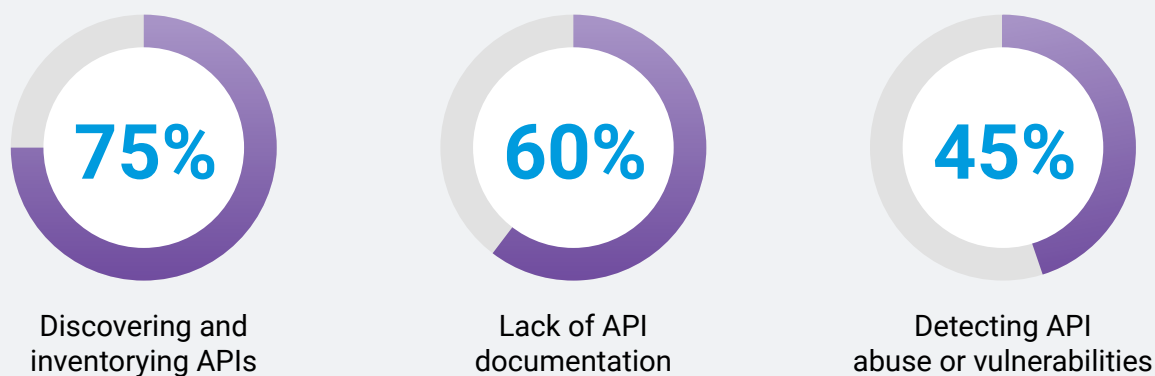
65% of those surveyed use APIs with partner/third-party integrations and loyalty/customer engagement programs.

85% rely on their web application firewall for protection against API abuse – leaving them in a reactive position.
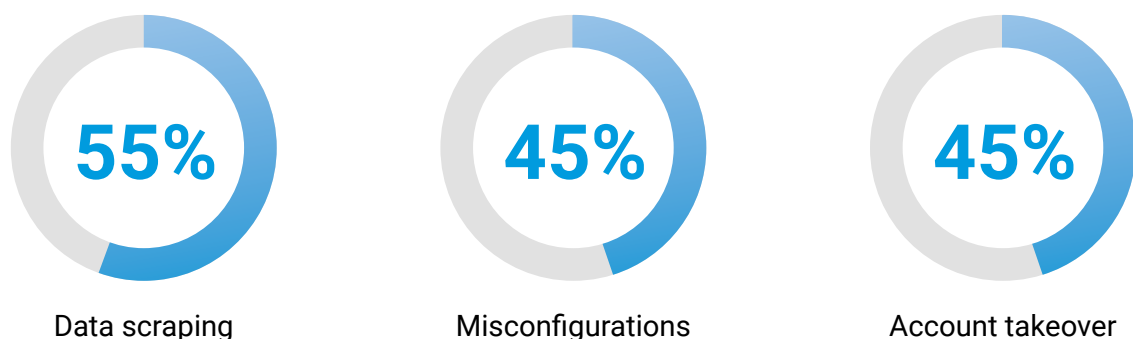
Top 3 API security objectives

50%
Detecting API abuse or vulnerabilities

50%
Automating API discovery and inventory

40%
Protecting critical business logic that the organization is sharing

Top 3 API challenges

75%
Discovering and inventorying APIs

60%
Lack of API documentation

45%
Detecting API abuse or vulnerabilities

Top 3 API security concerns

55%
Data scraping

45%
Misconfigurations

45%
Account takeover

An advanced API security wish list

To respond to these challenges and concerns, survey respondents reported that they were looking for an advanced API security solution to help improve business outcomes. Their wish list includes:

Top 3 benefits

70%
Protecting brand reputation

65%
Resolving gaps in security compliance requirements

50%
Quickly detecting and responding to API abuse and vulnerabilities

Top 3 business outcomes

75%
Reduced risk of API threat/abuse

60%
Increased revenue/ROI

60%
Enhanced brand reputation and protection

Akamai leverages behavioral-based API security protection to help close the visibility gap for commerce organizations

Web application firewalls, bot management, API gateways, and DDoS mitigation solutions are not enough to stop today's sophisticated API attacks and abuse. Complete API security requires context-rich behavioral analytics in the API layer itself through 24/7 continuous discovery and monitoring to detect threats that others miss.

An **award-winning provider of advanced API security**, Akamai helps commerce organizations deliver safe, engaging online experiences that drive business — and digital innovation — forward.

Learn more about protecting your entire API estate with Akamai API Security.