Kong

Powering the API world

API Security Perspectives 2025

AI-Enhanced Threats and API Security

Executive Summary

83% of developers and business leaders said that AI investments had already created the opportunity for new products or services, according to Kong's **2024 API Impact Report**.

But what are IT leaders concerned about in the year ahead? And what have they seen so far related to API security incidents and AI-enhanced threats?

Our latest survey of 700 IT leaders reveals a critical inflection point in API security as organizations navigate the rising risk of AI-enhanced threats and the adoption of AI tools and large language models (LLMs).

Nearly 75% of respondents express serious concern about AI-enhanced attacks, but a notable disconnect emerged. While 55% of organizations experienced an API security incident in the past year, 85% say they're confident in their organization's security capabilities.

This confidence may be misplaced, given 77% acknowledge the potential for significant security risks from AI and LLM integration into their API ecosystem.

What's more, the cost of API security incidents is substantial, with 20% reporting remediation costs exceeding $500,000 in the past 12 months.

Other key findings include:

- **40% are unsure their current security investments are sufficient** to address emerging AI-related risks
- AI-enhanced cyberattacks are ranked as the top security threat
- **92% are taking measures to counter AI-enhanced threats**
- Shadow APIs can be a dangerous blind spot for the majority of organizations

While organizations recognize the changing threat landscape, many lack the comprehensive security measures needed to protect their API infrastructure in the AI era.

The gap between perception and reality requires attention, particularly as API attacks are projected to increase — and API breaches lead to more leaked data than the average security breach, Gartner **reports**.

AI-Enhanced Threats and API Security Incidents

Kong surveyed 700 IT leaders about API security and the rising risk of AI-enhanced threats.

88%

report that API security is a top priority

IT leaders say API security is a top security concern

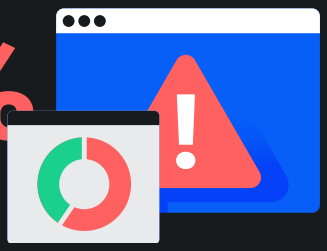
97% view API security as greater than or equal to other cybersecurity concerns, like network security and endpoint security.

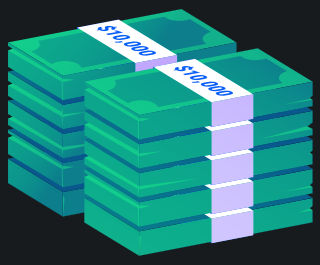
API security incidents are common — and pricey

More than half have experienced an API security incident in the last 12 months; 27% lack confidence in their API security measures.

55%

experienced an API security incident in the past year





Nearly half experiencing an incident spent over

$100,000

in remediation

47% who experienced an API security incident in the past 12 months reported remediation costs of more than $100,000; 20% reported costs exceeding $500,000.

Leaders lack confidence in their ability to stop AI-enhanced threats

AI-enhanced attacks top the list of the biggest perceived threats to API security today, followed by unauthorized access/breaches and insufficient data protection/encryption.

74%

are very concerned about AI-enhanced attacks

92%

are taking measures to counter AI-enhanced attacks

40%

aren't confident in their current security investments

Kong Inc., a leading developer of cloud API technologies, is on a mission to enable companies around the world to become "API-first" and securely accelerate AI adoption. Kong helps organizations globally — from startups to Fortune 500 enterprises — unleash developer productivity, build securely, and accelerate time to market. For more information, visit www.konghq.com.

API security and the rising risk of AI-enhanced threats

APIs (application programming interfaces) enable our digital world. There's **no AI without APIs**, but even more basic online interactions like ordering pizza or public transit route planning are powered by APIs.

However, without proper management, visibility, and processes in place, APIs can be a potential hole in your security.

Gartner **reports** the average API breach leads to at least 10 times more leaked data than the average security breach. And Kong **forecasts** API attacks are on the rise, projecting a 548% growth in the number of attacks by 2030.

The rapid adoption of AI tech and large language models (LLMs) is leading to previously unfathomable innovation — but has also resulted in a total reshaping of the cybersecurity threat landscape.

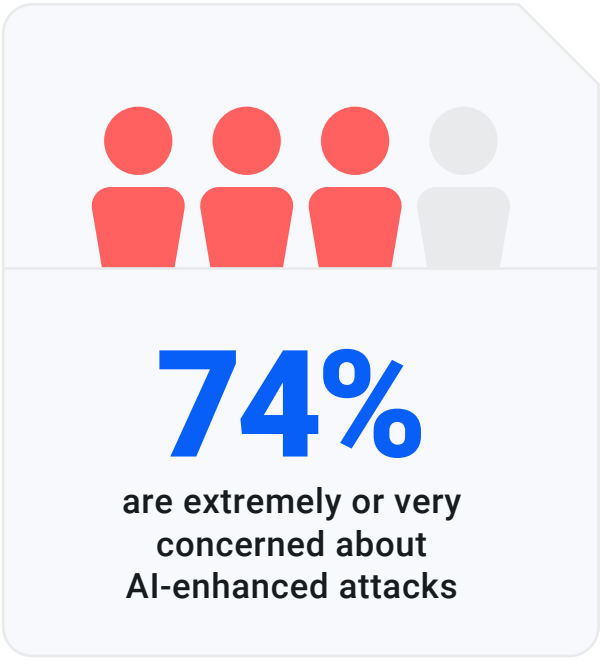
How are these new AI-enhanced tools and threats impacting **API security**? And what concerns do IT leaders have for the year ahead?

To find out, we surveyed 700 IT leaders in the US and UK about AI's role in the current API security landscape.

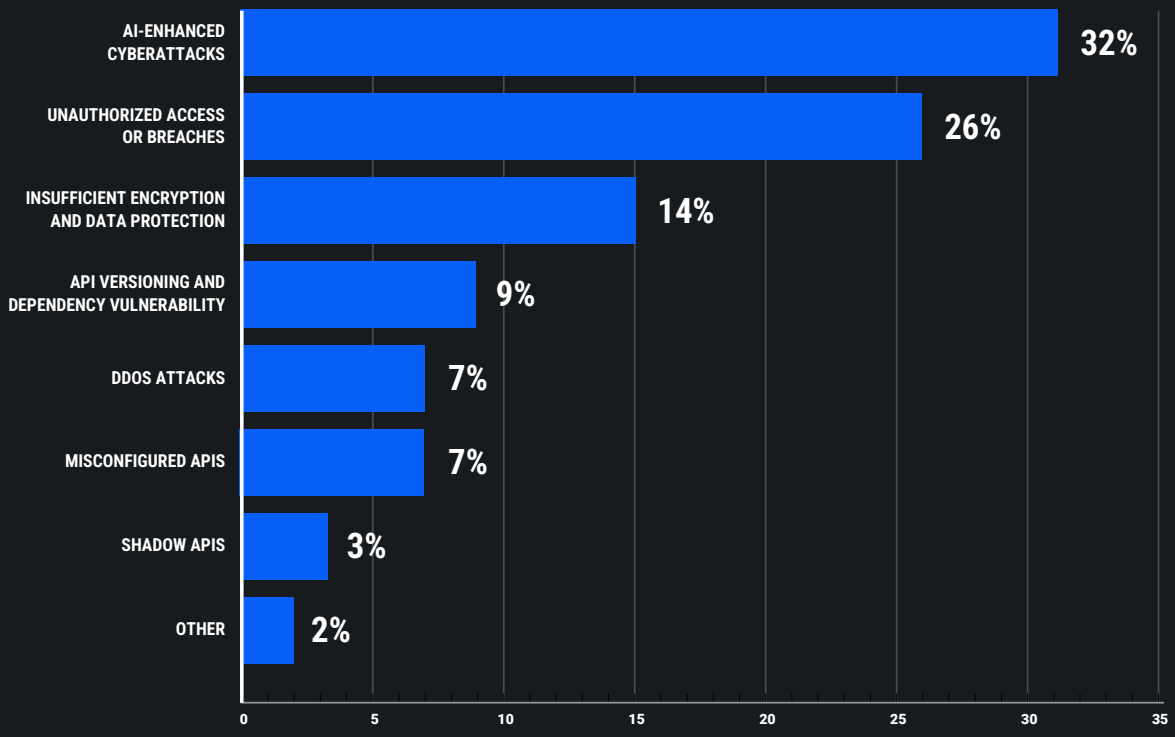
AI-enhanced threats top list of potential security threats

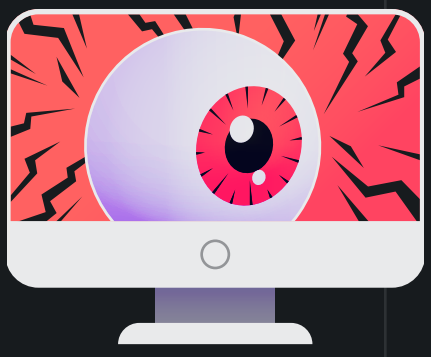
AI can lower the barrier to entry for cyberattacks and provides another attack vector to potentially breach organizational defenses around API security. And because so many technologies rely on APIs, API attacks can have a growing impact on data security.

Those working in tech clearly recognize the risk, with 74% saying they're extremely or very concerned about AI-enhanced attacks, and 32% say they're *the* single biggest security threat to organizations today. These types of attacks top the list of most significant threats to API security today, followed by unauthorized access or breaches.



What's the biggest security threat to your organization today?





Spotlighting the risk of shadow APIs

While shadow APIs may land lower on the list of perceived threats, these undiscovered and unmanaged APIs can pose massive security risks in organizations without an up-to-date system of record of services and APIs. As Gartner reports in the 2024 Market Guide for API Protection, "APIs — especially shadow and dormant ones — are causing data breaches among organizations that, on average, exceed the magnitude of other breaches."

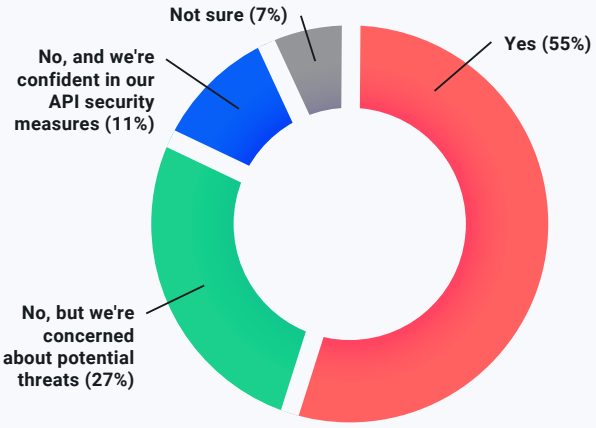
Gaining visibility into services and APIs is essential. Among the tens of thousands of API endpoints that may be running in an organization's infrastructure, each can be thought of as a unique attack vector, especially if left unprotected without authentication, authorization, and rate limiting.

Learn more about how to shine a light on shadow APIs lurking in your IT infrastructure.

Half experienced an API security incident in the past 12 months

55% reported an API security incident within the past 12 months, and one-third of those said it was “severe.” Only 11% have not experienced an incident but remain confident in their API security measures.

Have you experienced an API security incident in the past 12 months?



32%

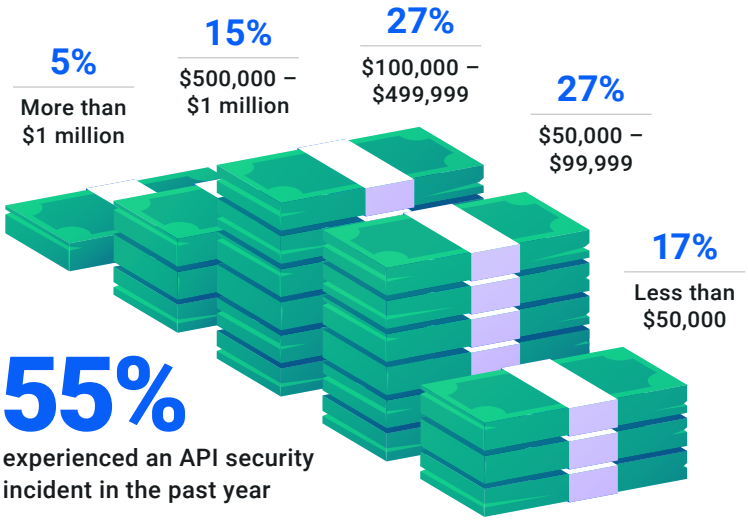
who experienced an API incident say it was “severe”

1 in 5 report an API security incident costing more than $500,000

47% of those who experienced an incident in the past 12 months reported remediation costs of more than $100,000; **20% report their organization paid more than $500,000.**

These costs takes into consideration internal resources, such as hours worked, and external resources, like consulting, security tools, and legal fees.

Cost to remediate an API security incident in past 12 months



55%

experienced an API security incident in the past year

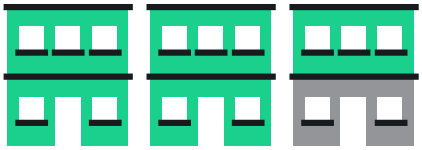
9% were not sure or preferred not to say

There's a surprising disconnect between confidence and the number of security incidents

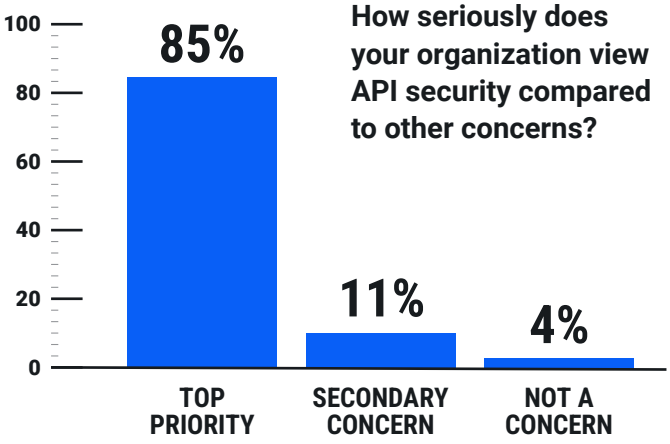
Despite the number of people who have recently experienced an attack — and dealt with the accompanying costs — most are confident in their ability to secure APIs against current and emerging threats. Is this a false sense of security, or have organizations buckled down after previous incidents? Only time will tell.

85%

are confident in their in their ability to secure APIs



4% are not confident; 11% are neutral



Most view API security as a top cybersecurity concern

97% view API security as a cybersecurity concern greater than or relative to others, such as network security and endpoint security.

40% are unsure that their organization's investment is enough

45% of people report more than 20% of their cybersecurity budget is dedicated to API security, and **40% are unsure or doubtful that their organization's investment is enough to cover API security risks,** especially in light of new AI projects and AI-enhanced threats.

40%

are unsure their org's investment is enough to cover API security risks

Organizations rely on monitoring and API gateways to maintain control

When it comes to what preventative measures organizations are taking to mitigate API security risks, API monitoring and anomaly detection tools top the list. Comparing the UK and the US, UK respondents are more likely to report implementing an API gateway — 71% in the UK vs 50% in the US. This difference may be due to greater compliance and regulatory requirements in the UK.

What steps are you taking to mitigate API security risks?

1. API MONITORING AND ANOMALY DETECTION TOOLS (63%)
2. IMPLEMENTING API GATEWAY SOLUTIONS (61%)
3. API ENCRYPTION AND TOKENIZATION (58%)
4. REGULAR PENETRATION TESTING AND AUDITS (57%)
5. ADOPTING ZERO-TRUST ARCHITECTURE (35%)
6. NOT TAKING ANY SPECIFIC STEPS (6%)

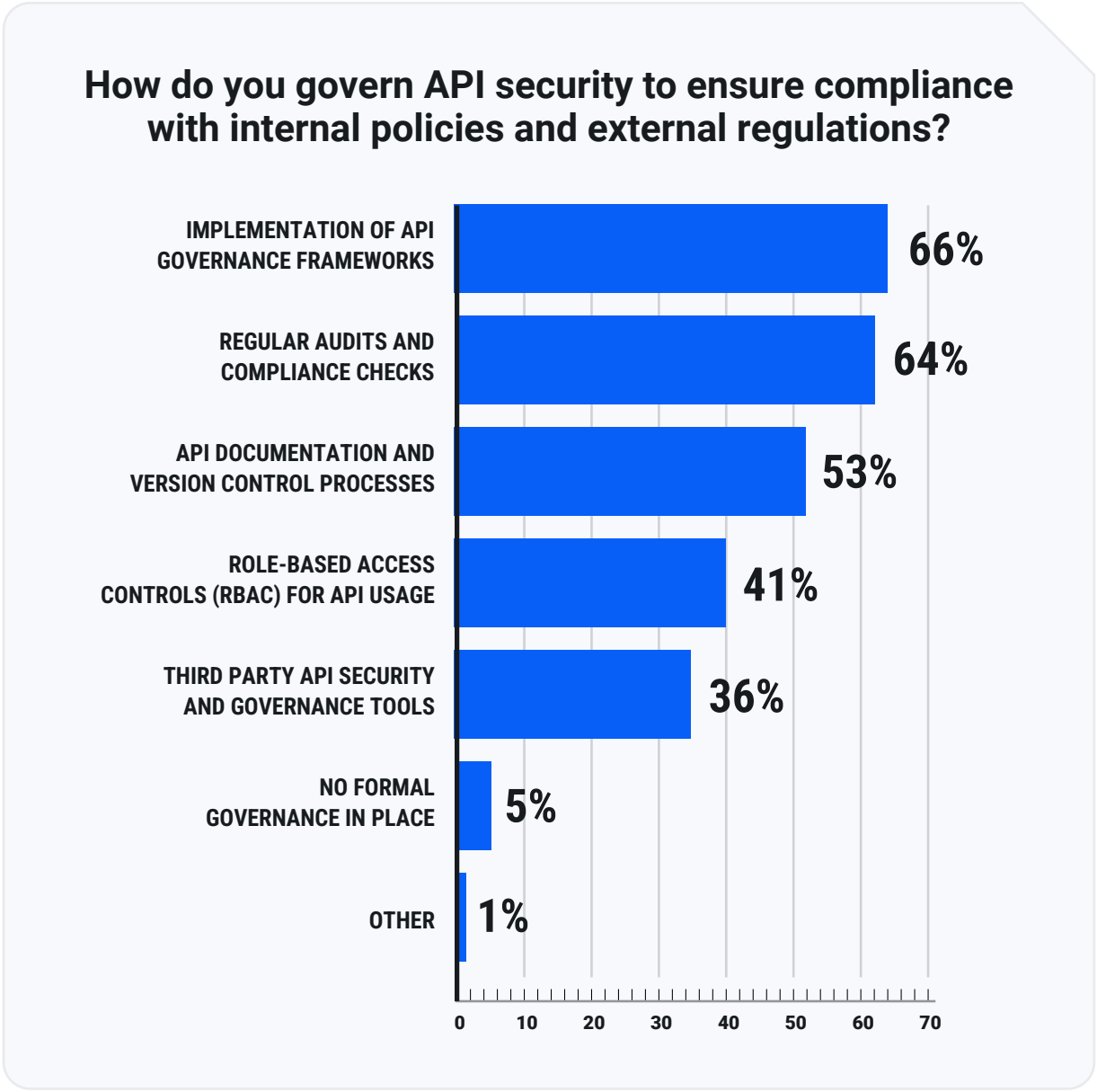
Only 35% report adopting zero-trust architecture, surprising given how established and generally accepted as best practice this comprehensive approach to API security is.

92% are taking measures to secure APIs against AI-enhanced threats

Increased monitoring and traffic analysis top the list of measures organizations are taking to secure APIs against AI-enhanced threats. There's a notable difference between how seriously organizations in the UK and the US seem to consider AI-enhanced threats: 13% in the US say they're taking no specific measures for AI threats compared to only 4% in the UK.

What measures are you taking to secure APIs against AI-enhanced threats?

1. INCREASED MONITORING AND TRAFFIC ANALYSIS (66%)
2. EDUCATING STAFF (60%)
3. AI-DRIVEN THREAT DETECTION SYSTEMS (51%)
4. LEVERAGING API SECURITY SOLUTIONS WITH AI/ML CAPABILITIES (44%)
5. PARTNERING WITH THIRD-PARTY SECURITY SERVICES FIRMS FOR THREAT DETECTION AND MITIGATION (40%)
6. NONE (8%)

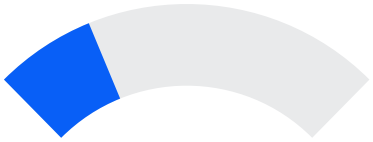


API governance frameworks, auditing top compliance-focused efforts

To govern API security to ensure compliance with internal policies and external regulations (e.g., GDPR, HIPAA), organizations rely on API governance frameworks, regular audits and checks, and API documentation and version control processes.

AI models and LLMs complicate security, introduce vulnerabilities

77% say there's a significant risk that AI models such as LLMs may introduce security vulnerabilities when integrated into their API ecosystem.



25%

have encountered AI-enhanced security threats related to APIs or LLMs

65%

are developing a strategy or preparing for AI-enhanced security threats

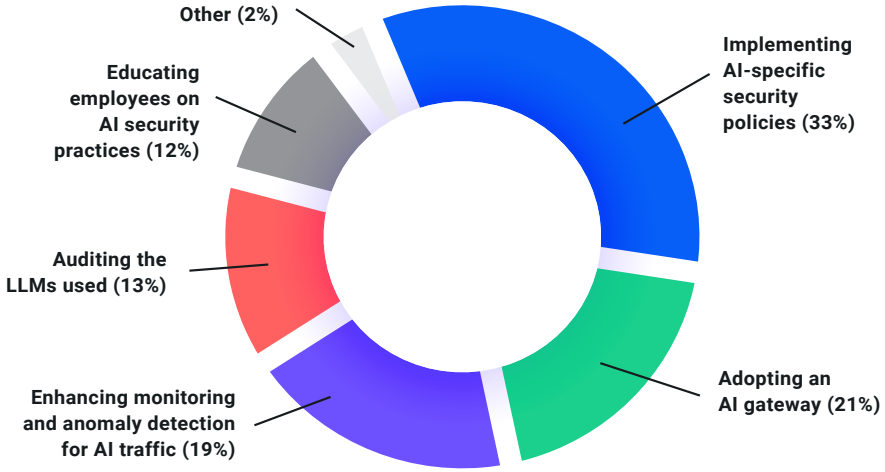
84%

say AI and LLMs will increase complexity of securing APIs over next 2–3 years

As AI usage increases within organizations, it will be crucial to block external AI-enhanced attacks and properly govern and secure AI-generated traffic resulting from new initiatives. To mitigate these risks, IT leaders report implementing AI-specific security policies, adopting an AI gateway, and enhancing monitoring and anomaly detection for AI traffic.

An AI gateway is a central place to manage AI consumption that can be used to accelerate adoption of AI without compromising on observability, security, and governance.

How does your organization plan to mitigate risks related to AI?



Securely implementing AI and the weakest link

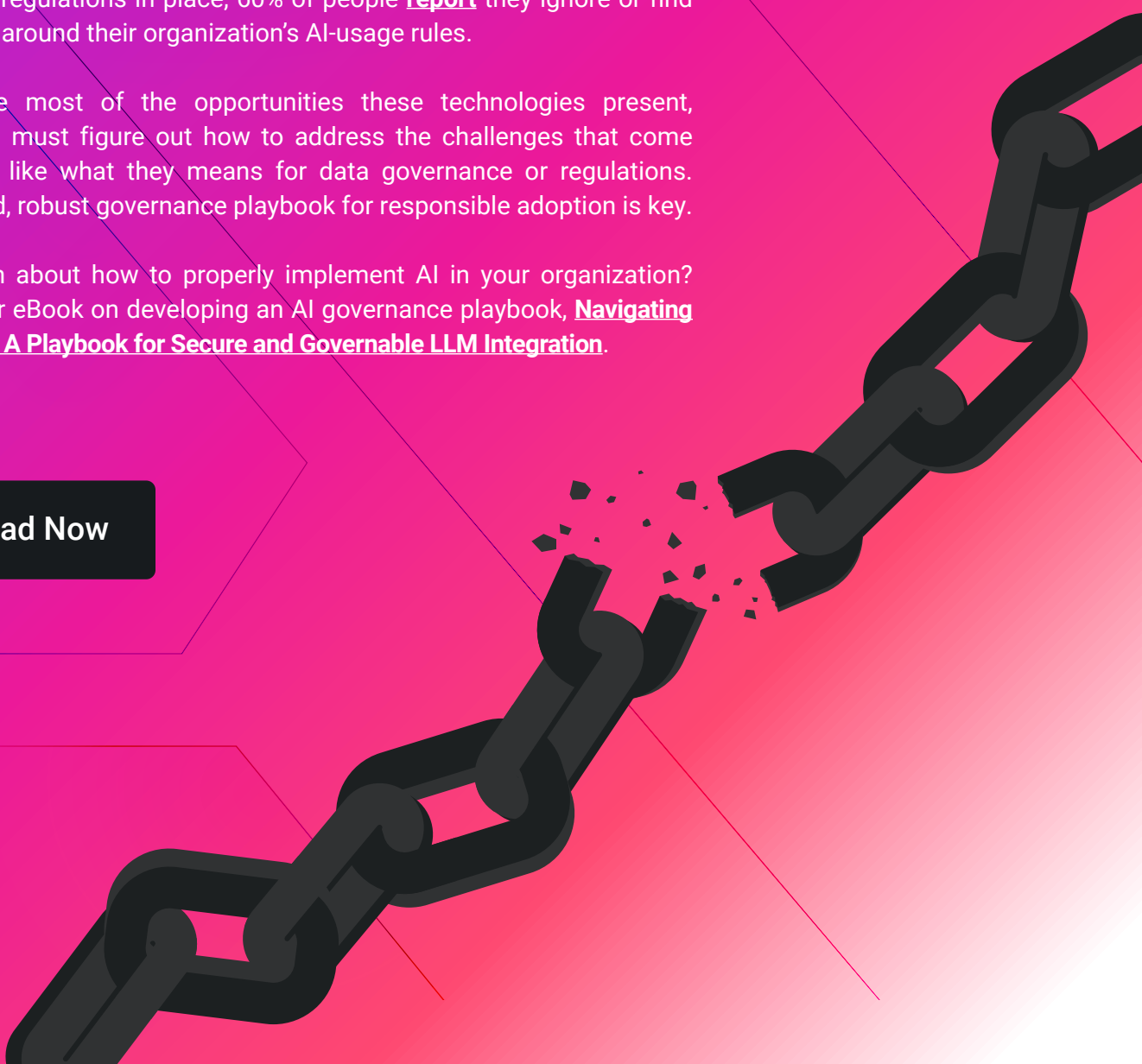
Humans remain one of the weakest points in cybersecurity, so investing energy into education about best practices around GenAI and LLMs is wise.

But education alone is not enough. While most organizations have AI guidelines or regulations in place, 60% of people **report** they ignore or find ways to work around their organization's AI-usage rules.

To make the most of the opportunities these technologies present, organizations must figure out how to address the challenges that come with them — like what they means for data governance or regulations. A well-defined, robust governance playbook for responsible adoption is key.

Want to learn about how to properly implement AI in your organization? Check out our eBook on developing an AI governance playbook, **Navigating AI Innovation: A Playbook for Secure and Governable LLM Integration**.

Download Now



CONCLUSION

API security is more critical than ever in the AI age

The convergence of AI and APIs presents both unprecedented opportunities and risks. While most organizations report being extremely concerned about AI-enhanced attacks, 40% remain unsure whether their current security investments are sufficient. Many still underestimate critical vulnerabilities like shadow APIs, and as many as 13% of organizations in the US say they're taking no specific measures against AI-enhanced threats.

With API attacks projected to grow by 548% by 2030, the time to act is now. Kong's unified API platform helps organizations navigate these challenges by providing robust security, complete visibility, and simplified management across your entire API ecosystem.

Visit **konghq.com** to learn more about how Kong can help your organization simplify API management and unlock AI innovation.

Methodology

This report examines the evolving landscape of API security by analyzing expert opinions on current trends and dynamics. To gather these insights, a comprehensive survey was commissioned with a professional polling firm in Q4 2024. The survey included 700 IT professionals and business leaders across two key markets: the United States and the United Kingdom.

About Kong

Kong Inc., a leading developer of cloud API technologies, is on a mission to enable companies around the world to become “API-first.” Kong helps organizations globally — from startups to Fortune 500 enterprises — unleash developer productivity, build securely, and accelerate time to market.

For more information about Kong, please visit www.konghq.com or follow us on X @thekonginc.

Learn More

Powering the API world

Konghq.com

Kong Inc.
contact@konghq.com

77 Geary Street, Suite 630
San Francisco, CA 94108
USA