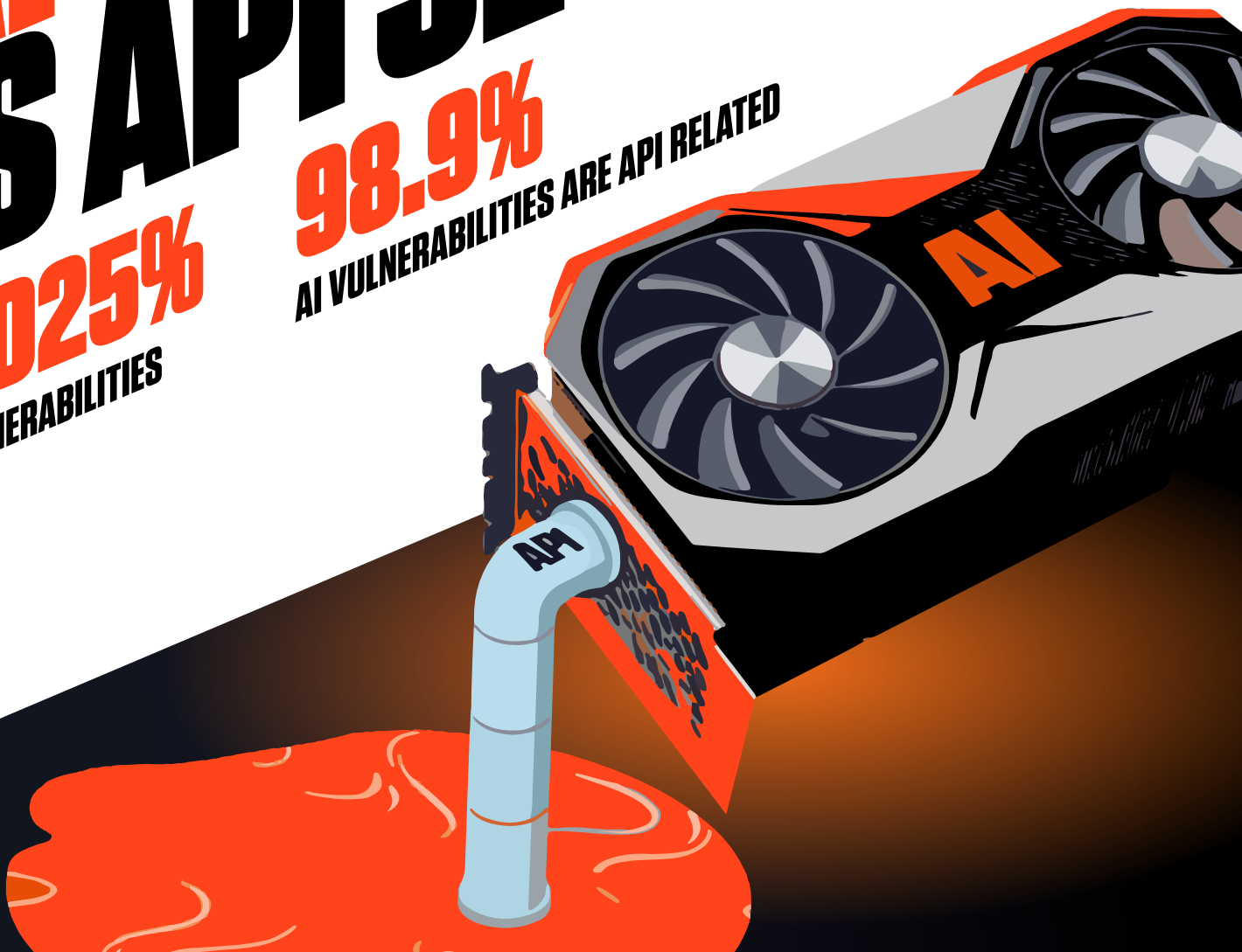


AI SECURITY IS API SECURITY

+1025%
AI VULNERABILITIES

98.9%
AI VULNERABILITIES ARE API RELATED



Introduction

This report is more than a collection of data — it's a roadmap for addressing the evolving risks that APIs present. The findings make one thing clear: **API security is not just a technical challenge; it's a business imperative.** Enterprises that fail to secure their APIs risk not only technical vulnerabilities, but also reputational and operational crises.

Wallarm remains committed to supporting organizations on this journey. From continuously monitoring the API threat landscape to empowering enterprises with tools for dynamic API discovery, security testing, and real-time protection, we are dedicated to building a safer, more resilient digital ecosystem.

AI: THE BIGGEST DRIVER OF API SECURITY RISKS IN 2024

In 2024, AI fundamentally reshaped enterprise technology, with Gartner reporting that over 50% of enterprises had adopted AI solutions in production environments by year-end. APIs enabled this growth, acting as the critical interface between AI models and the applications they power. However, this rapid expansion exposed significant vulnerabilities. Wallarm's data reveals that 57% of AI-powered APIs were externally accessible, and 89% relied on insecure authentication mechanisms, such as static keys. Only 11% implemented robust measures like bearer tokens with expiration times, leaving the vast majority of endpoints vulnerable to exploitation.

The scale of AI-driven API vulnerabilities is staggering. In 2024, Wallarm tracked 439 AI-related CVEs, a 1,025% increase over 2023, with nearly 99% directly tied to APIs. These included injection flaws, misconfigurations, and new memory corruption vulnerabilities stemming from AI's reliance on high-performance binary APIs. For example, the addition of the Memory Corruption & Overflows category in the 2025 API ThreatStats Top-10 was driven by Wallarm's analysis of how AI workloads interact with hardware, exposing APIs to issues like buffer overflows and integer overflows.

AI didn't just amplify traditional risks—it created new ones. Wallarm's threat intelligence flagged significant vulnerabilities in AI tools like PaddlePaddle and MLflow, which underpin enterprise AI deployments. These tools were exploited via API endpoints to compromise training data, siphon intellectual property, or inject malicious payloads into machine learning pipelines. This convergence of AI and API vulnerabilities underscores one of the central findings of this report: AI security is API security.

API SECURITY DOMINATES CYBERSECURITY

2024 cemented APIs as the most critical attack surface in modern cybersecurity. Their ubiquity across industries and essential role in enabling digital transformation made them a primary target for adversaries. Two key areas—**CISA Known Exploited Vulnerabilities (KEV)** and high-profile data breaches—demonstrated the extent of this trend, revealing both the scale and severity of API-related risks.

While AI has driven API vulnerabilities to new heights, APIs were the dominant cybersecurity risk across the board in 2024. Wallarm's analysis of **CISA's Known Exploited Vulnerabilities (KEV)** report revealed **that over 50% of exploits were API-related**, up from just 20% in 2023. This surge reflects the central role APIs now play in everything from modern SaaS platforms to legacy web systems. Among these, **33.5% targeted modern APIs** like RESTful and GraphQL, while **18.9% involved legacy APIs**, including AJAX backends and URL parameter-based systems.

The impact of API exploits was felt across industries. Wallarm monitored high-profile breaches like the **Dell API abuse incident**, where 49 million records were exposed due to a weak registration process, and the **Twilio Authy breach**, which compromised 33.4 million linked phone numbers. These incidents weren't just about data loss—they demonstrated how attackers exploit insecure APIs to manipulate systems and launch further attacks, from phishing campaigns to SIM-swapping operations.

AI IS API

Why We Believe This Report is Essential: The AI-API Security Imperative

2024 marked a pivotal shift, with AI becoming both a transformative enabler and a critical risk multiplier for enterprise APIs. This report dives deep into the vulnerabilities, exploits, and real-world breaches that defined API security as the most critical battleground for AI-driven systems. From surging CVEs tied to AI-enabled endpoints to the lagging security controls many enterprises deployed, it reveals how rushed adoption of generative AI has exposed APIs as a major attack surface.

With exclusive insights from survey data, bug bounty programs, and CISA's 2024 Known Exploited Vulnerabilities, this report is an essential guide for security leaders. It highlights the API-specific risks driving breaches, the vulnerabilities shaping product categories, and the security controls enterprises must adopt to safeguard their systems. For CISOs, CIOs, and security experts, this is the definitive roadmap to navigating the challenges and opportunities in securing APIs in an AI-powered world. As you explore the details in this report, you'll find insights shaped by Wallarm's direct involvement in analyzing and addressing API vulnerabilities across industries. From survey data to real-world case studies, the lessons of 2024 offer a clear path forward. Together, we can secure the APIs that power innovation and drive global business. Let's make it happen.



Ivan Novikov

CEO, Wallarm



AI IS API

2024: The AI Revolution and its impact on Enterprise APIs

2024 marked a groundbreaking year for Artificial Intelligence (AI) in enterprise environments, with generative AI becoming a central focus for digital transformation. APIs have become the indispensable conduit for AI integration, allowing enterprises to harness the power of AI for diverse workflows, from customer-facing applications to internal decision-making tools.

Gartner highlights that by 2026, over 80% of enterprises will have deployed AI applications or APIs in production environments, a monumental leap from less than 5% in 2023. Similarly, Postman's 2024 State of the API report shows a 73% year-over-year increase in AI-related API traffic, signaling the growing reliance on APIs for deploying and operationalizing AI solutions. Mulesoft's 2024 Connectivity Benchmark report echoes this sentiment, emphasizing that the evolving nature of digital transformation hinges on effective API management and integration.

Wallarm recently conducted a survey of 200 US-based enterprise leaders on the topic of AI and API security. The survey results confirm the above trend: **54% of enterprises report engaging in multiple AI deployments**, while **35% are just beginning their journey**. These deployments are largely enabled by API technology, cementing APIs as the foundation of enterprise AI adoption.

THE OVERNIGHT SHIFT: SECURITY STRUGGLES IN THE AI-DRIVEN ENTERPRISE



The rapid adoption of generative AI has placed extraordinary demands on enterprise systems, often outpacing existing security frameworks. Wallarm's survey reveals that **63% of enterprise leaders believe AI increases API security risk**, with only **12% of enterprises waiting for security controls to be ready before deployment**. This reflects a troubling trend where enterprises, under pressure to deploy AI solutions quickly, have broken or bypassed established security protocols to meet urgent business requirements.

This rush to deploy has left critical API endpoints exposed. Wallarm's customer data shows that **57% of AI-powered APIs are accessible to external users**, often without adequate protections like VPNs. Furthermore, **89% of these APIs rely on weak authentication mechanisms** such as static keys or basic HTTP authentication. Only **11% use robust methods like bearer tokens or JWTs with expiration times**, leaving the majority vulnerable to abuse.

API ABUSE AND LEAKS: KEY RISKS FOR ENTERPRISE AI APIS



As enterprises embrace AI, API abuse and data leaks have emerged as significant threats. APIs now serve as both the gateway to AI functionality and a potential vulnerability. API abuse—where attackers exploit misconfigured or poorly secured endpoints—has risen sharply, often targeting AI-integrated systems due to their complexity and high value.

TechCrunch highlights that AI integration complicates the regulatory landscape, as APIs handling sensitive AI data must comply with standards like GDPR and ISO27001 while navigating new challenges around data protection and access control. These issues are compounded by the sheer volume of data processed by AI systems, creating fertile ground for API leaks.

CrowdStrike's reports also underscore the increasing sophistication of adversaries who exploit API endpoints to exfiltrate sensitive data or manipulate AI models. AI's reliance on APIs for continuous learning and real-time processing amplifies the stakes. Adversaries target APIs to gain unauthorized access to model training data, business intelligence, and proprietary algorithms, potentially leading to intellectual property theft or compromised AI integrity.

API SECURITY CONTROLS LAG BEHIND AI DEPLOYMENTS



Wallarm's recent survey reveals an alarming gap between the pace of AI deployment and the implementation of adequate security measures. While **48% of enterprises report implementing specific security controls for AI deployments**, **34% admit their security controls are lagging behind AI's rapid deployment**. This misalignment has created significant vulnerabilities, with APIs often deployed without adequate testing or monitoring.

The lack of robust security controls has been further exacerbated by shadow APIs—endpoints that are unknown or unmanaged by IT teams. Cloudflare's analysis found that machine learning-based discovery tools often identify **31% more API endpoints** than those reported by enterprises, highlighting the visibility challenges that make shadow APIs a persistent risk.

BUILDING ENTERPRISE RESILIENCE: A PATH FORWARD



To thrive in the AI-driven future, enterprises must prioritize API security as a fundamental component of their AI strategy. This requires a multifaceted approach that includes:

- 1 Comprehensive Endpoint Visibility:**
Enterprises must inventory all API endpoints, including shadow APIs, to ensure proper monitoring and security.
- 2 Enhanced Authentication Mechanisms:**
Moving beyond static keys to implement OAuth 2.0, bearer tokens, and JWTs with expiration times.
- 3 Adaptive Rate Limiting:**
Protecting against abuse by dynamically adjusting limits based on real-time usage patterns.
- 4 Proactive Threat Detection:**
Leveraging AI-driven tools to identify and respond to threats targeting API endpoints.

2024 serves as a pivotal year, reminding enterprises that **AI security is API security**. As the integration of AI and APIs accelerates, organizations must balance innovation with robust security to safeguard their systems, data, and users. Failure to do so risks not only technical vulnerabilities but also reputational and regulatory consequences that could jeopardize long-term success.

AI security is API security

2024: The Year of AI vulnerabilities

The year 2024 marked an unprecedented surge in AI-related vulnerabilities, with a staggering **439 AI CVEs**, compared to just **39 in 2023**. This **1,025% increase highlights** the rapid adoption of AI technologies across industries and the corresponding expansion of their attack surfaces. Most significantly, **98.9% of these vulnerabilities were linked to APIs**, reinforcing the critical role of API security in safeguarding AI systems.

1,025% INCREASE IN AI CVEs FROM 2023 TO 2024

API-Related Vulnerabilities in AI: A Breakdown

The CVEs reported in 2024 reveal two primary categories of API-related vulnerabilities in AI products:

1. Directly API-Related (77.4%):

77.4%

- These vulnerabilities are, in essence, API-specific issues within AI platforms. Examples include weak API authentication mechanisms, inadequate rate limiting, and broken access controls. These vulnerabilities allow attackers to directly exploit exposed API endpoints to access or manipulate sensitive AI functionalities.
- **Example:** A high-profile vulnerability in an AI analytics platform allowed attackers to exfiltrate sensitive customer insights by exploiting poorly secured API endpoints, leading to reputational and financial damage.

2. Indirectly API-Related (21.5%):

21.5%

- One fifth of AI vulnerabilities are indirectly tied to APIs. These include flaws in third-party integrations, such as Single Sign-On (SSO) or data retrieval systems, where APIs act as intermediaries. Vulnerabilities in these dependencies can cascade into the AI system, compromising its integrity.
- **Example:** A vulnerability in a third-party SSO provider's API allowed attackers to bypass authentication, gaining unauthorized access to AI-driven business dashboards.

Only **1.1% of the vulnerabilities** in AI products were entirely unrelated to APIs, underscoring the fact that APIs are the foundational technology enabling AI capabilities. All of such issues are not related to APIs since they are directly triggered by local files, configurations, or specific hardware modules.

1.1%

⚡ 98.9% AI VULNERABILITIES ARE API RELATED

Top AI Products Vulnerable in 2024 - The API Security Connection

The intersection of AI and API vulnerabilities became a defining challenge for enterprise security in 2024. AI tools, integral to business transformation, also introduced significant risks to enterprises as they were adopted. This chapter unpacks the most vulnerable AI products of the year, explaining their usage and enterprise impact while emphasizing how API weaknesses drive these risks.

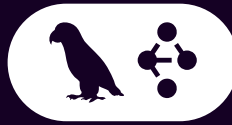
Even if these AI tools are unfamiliar by name, the likelihood of their presence within your enterprise infrastructure is remarkably high. These products often operate as integral components of larger platforms, embedded by third-party vendors or deployed by internal teams for their efficiency and adaptability. Tools like MindsDB and LangChain Experimental are frequently used to power predictive analytics and conversational AI features in customer-facing applications, while PaddlePaddle and MLflow underpin machine learning workflows and decision-making systems. Shadow IT further amplifies this risk, with employees or departments independently adopting tools like anything-llm or Flowise to address immediate needs, bypassing IT oversight. This means enterprises may unknowingly host these tools, leaving critical business processes—from customer interactions to supply chain logistics—exposed to exploitation. The silent integration of these products into enterprise systems underscores the urgency of proactive API security measures to identify and protect these hidden vulnerabilities.



PaddlePaddle



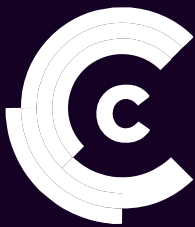
Anything-llm

LangChain
Experimental

Lunary AI



parisneo/ollms



ClearML



Flowise



MLflow

gaizhenbiao/
chuanhuchatgpt

MindsDB

AI Products with High CVEs in 2024

CWE	CVEs	What it is:	Enterprise Impact:
 1 PaddlePaddle	35	An open-source deep learning framework popular in research and enterprise AI deployments. Its flexibility and performance make it a favorite for machine learning pipelines.	Vulnerabilities in PaddlePaddle's APIs have allowed unauthorized data access, compromising models trained on sensitive customer data. In one breach, attackers extracted intellectual property (IP) by exploiting weak API authentication, threatening competitive advantages.
 2 anything-llm	25	A lightweight language model framework used for task-specific fine-tuning and rapid deployment in customer-facing applications.	Misconfigured APIs in anything-llm allowed attackers to execute model poisoning attacks. For example, a financial institution's chat assistant was hijacked, disseminating false financial advice and damaging the firm's reputation.
 3 LangChain Experimental	19	A library designed for building AI applications that integrate with external systems like databases, document stores, and APIs.	Vulnerable API integrations within LangChain enabled lateral movement attacks. In one case, an attacker used insecure API keys to access proprietary algorithms and customer databases in a manufacturing enterprise.
 4 Lunary AI	19	A platform offering predictive analytics and AI-driven decision-making for logistics and supply chain operations.	Exploited APIs exposed sensitive supply chain data, enabling attackers to disrupt operations by manipulating delivery schedules and inventory records.
 5 MLflow	15	A tool for managing machine learning workflows, including experiment tracking, deployment, and model storage.	Weak API controls allowed attackers to manipulate ML models, resulting in corrupted predictive outputs. In one attack, a healthcare organization's diagnostics models were compromised, undermining patient trust and leading to regulatory scrutiny.
 6 parisneo/loLLMs	13	A lightweight library for low-resource machine learning deployments, popular in IoT and edge computing.	Vulnerabilities exposed edge devices to data leaks, allowing attackers to exfiltrate customer metrics from industrial IoT setups, impacting downstream analytics accuracy.
 7 Flowise	11	A platform for building AI-driven workflows, integrating seamlessly with enterprise automation systems.	Unpatched vulnerabilities enabled privilege escalation, allowing attackers to disrupt business-critical processes, including automated financial reporting.
 8 gaizhenbiao/ chuanhuchatgpt	11	An open-source implementation of conversational AI optimized for multilingual contexts.	Exploited APIs were used to bypass rate limiting, allowing attackers to overwhelm systems during peak customer interactions, resulting in service outages and lost revenue.
 9 MindsDB	10	A tool for deploying AI models directly into databases to provide predictive insights during data queries.	Weak API security enabled SQL injection attacks, compromising entire databases. This resulted in customer data breaches and significant compliance penalties.
 10 ClearML	9	A platform for automating ML workflows, including training, monitoring, and deployment.	Attackers exploited ClearML's APIs to gain access to training datasets. In a high-profile case, sensitive government datasets were stolen, threatening national security projects.

TOP 10

The Path to the Top: How API Risks Dominated 2024

In 2024, the dominance of API vulnerabilities became undeniable, cementing APIs as the most dangerous attack vector in modern cybersecurity. Earlier, we demonstrated how **98.9% of AI-related CVEs were tied to API security issues**, reflecting the inseparability of API security from AI's broader adoption. Now, additional data points—ranging from real-world data breaches to the **2024 CISA Known Exploited Vulnerabilities (KEV) report**—further solidify the criticality of securing APIs. APIs are no longer just a technical component; they are a primary target for attackers, with exploit rates that eclipse those of traditional vulnerabilities like kernel and browser flaws.



2023

20%

2024

>50%

The numbers speak volumes. **Over 50%** of the vulnerabilities in the CISA KEV catalog were API-related, a significant leap from 20% in 2023. Among these, **33.5% involved modern APIs**, such as RESTful and XML-based endpoints, while **18.9% targeted legacy APIs**, often embedded in older web applications and devices. This highlights not only the pervasive use of APIs, but also their vulnerabilities across both cutting-edge and legacy systems. For example, **Ivanti** and **Palo Alto Networks** were top targets for modern API exploits, while **Adobe** and **Oracle** faced repeated attacks on their legacy API implementations.

The scope of API-related breaches was equally alarming in 2024. High-profile incidents included the **Dell breach**, where API abuse enabled data scraping of **49 million records**, and the **Digi Yatra API leak**, which exposed **1.74 million Aadhaar-linked personal details**. Meanwhile, **Twilio's Authy vulnerability** exposed **33.4 million phone numbers**, facilitating phishing and SIM-swap attacks. In healthcare, **Ascension Health** faced a devastating API breach affecting **5.6 million patients**, underscoring the far-reaching implications of insecure APIs in critical sectors.

APIs are the backbone of modern software, powering everything from AI systems to SaaS platforms and IoT devices. However, their widespread adoption has created an unprecedented attack surface. The convergence of real-world breaches, CISA KEV findings, and AI vulnerability data leaves no doubt: API security is the defining cybersecurity challenge of our time. Addressing this challenge requires prioritizing API protections across all industries, as the cost of failure is no longer theoretical—it's already playing out on a global scale.

API Related Data Breaches Tripled in 2024 – A Crisis in the Making

In last year's Wallarm Annual Report, based on 2023 data, API-related breaches were significant, but relatively sparse, with only a few incidents reported each quarter. In 2024, however, this picture changed dramatically. This year, API-related breaches have escalated in both frequency and severity, with an average of **three incidents per month**—and at times, as many as **five to seven breaches per month**. The rise of API-driven systems in sectors like healthcare, transportation, technology, and financial services has led to a surge in vulnerabilities, placing APIs squarely at the center of the cybersecurity landscape.

This alarming trend highlights the growing exploitation of APIs as the backbone of modern systems. APIs are no longer just technical enablers; they have become the **most targeted attack vector** in cybersecurity. To better understand the impact, we've identified five of the most significant API breaches of 2024, revealing not only the devastating outcomes, but also the patterns that attackers have leveraged across industries.

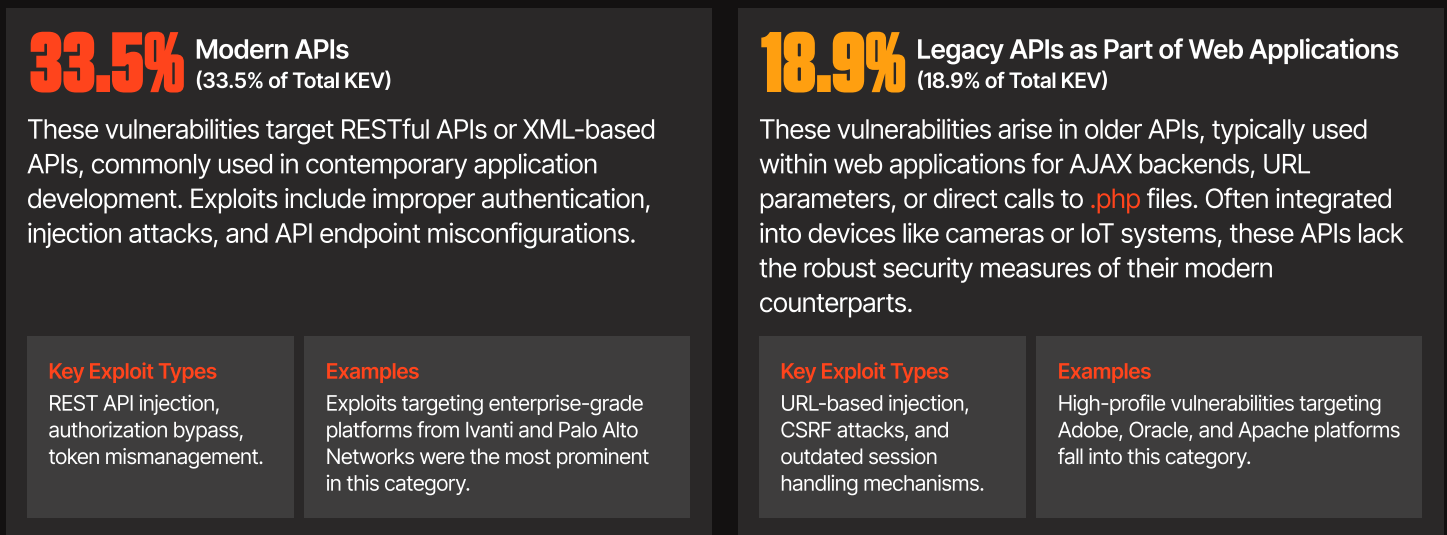
The breaches this year not only illustrate the widespread use of APIs, but also their critical role in exposing sensitive data. Organizations across industries faced damaging incidents tied to insecure APIs, from **massive data leaks** to **direct API abuse**. The calendar of breaches below illustrates how frequently APIs were exploited month by month.

APIs Dominate the CISA Known Exploited Vulnerabilities (KEV)

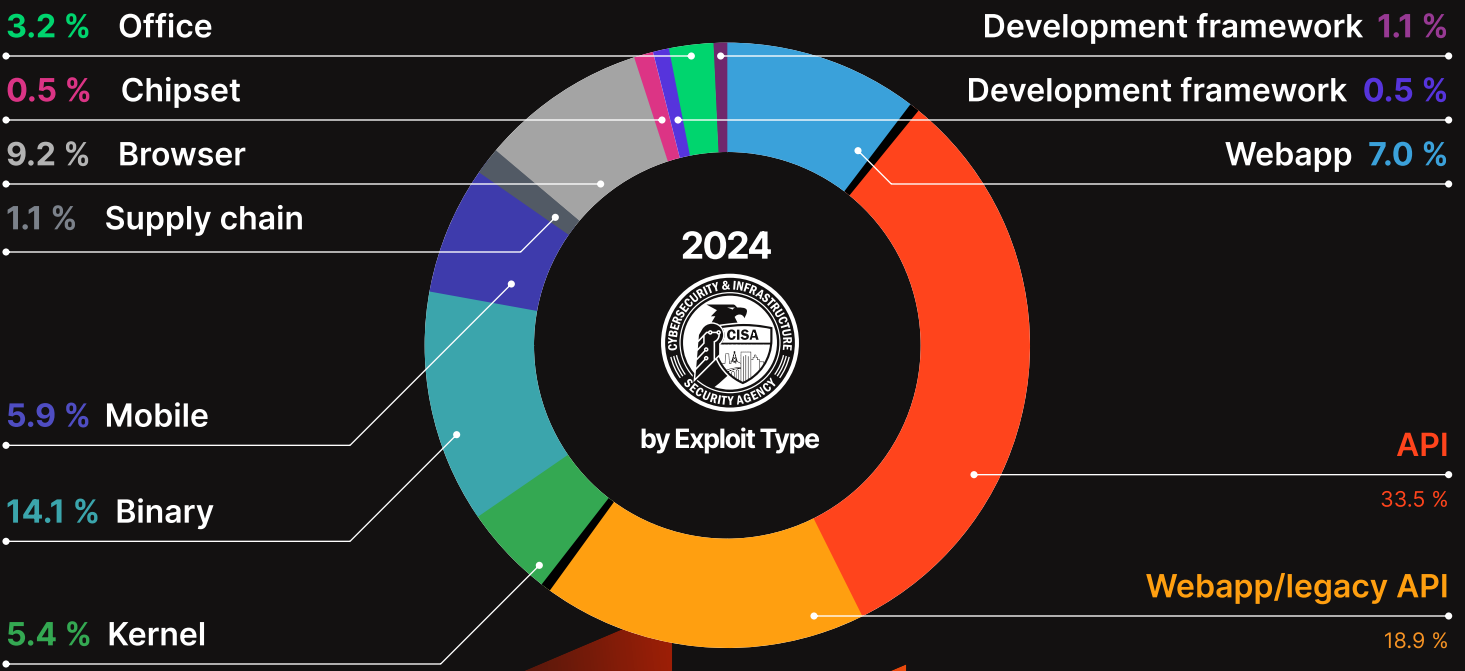
The 2024 **CISA Known Exploited Vulnerabilities (KEV)** catalog reveals a dramatic shift in the vulnerability landscape: for the first time, **more than 50% of all recorded exploits are API-related**. This marks a significant increase from just 20% in 2023, highlighting the growing prevalence and criticality of API security in modern threat environments. API vulnerabilities now surpass traditional exploit categories like kernel, browser, and supply chain vulnerabilities, underscoring their central role in cyberattacks.

Breaking Down API-Related Exploits






API-related vulnerabilities are divided into two primary categories, accounting for over half of the total KEV exploits in 2024:



The dominance of API-related exploits, split between modern and legacy implementations, reflects their ubiquity across industries and their critical role in facilitating digital interactions.

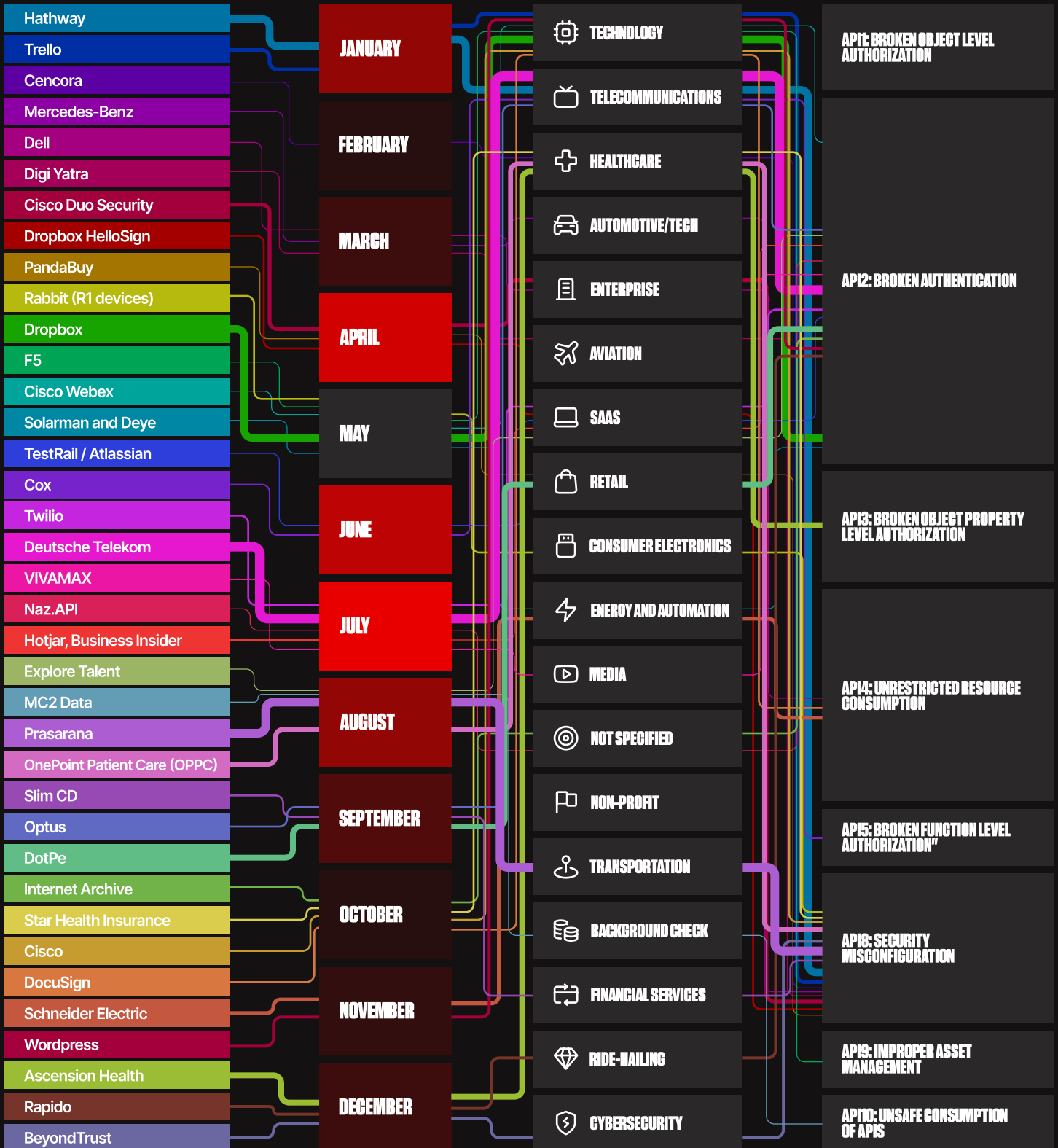


Top 5 API Breaches of 2024

<div style="background-color: #ff7f0e; color: white; padding: 5px; font-weight: bold; font-size: 24px; display: inline-block;">1</div> 	<p>Dell</p> <p>Impact</p> <p>49 m users affected</p>	<p>What Happened:</p> <p>A massive data scraping operation exploited weak API registration processes, exposing sensitive customer records.</p>	<p>Why It Matters:</p> <p>The details and scale of this breach demonstrate how the combination of poor process and poorly security APIs can result in significant compromise.</p>	<p>API ThreatStats™ Category:</p> <p>Broken Access Control (API2-25)</p>
<div style="background-color: #ff7f0e; color: white; padding: 5px; font-weight: bold; font-size: 24px; display: inline-block;">2</div> 	<p>Twilio (June 2024)</p> <p>Impact</p> <p>33.4 m linked phone numbers exposed</p>	<p>What Happened:</p> <p>An API vulnerability allowed attackers to enumerate phone numbers, facilitating phishing and SIM-swapping attacks</p>	<p>Why It Matters:</p> <p>This breach highlights the dangers of insufficient input validation and authentication in APIs handling sensitive user metadata.</p>	<p>API ThreatStats™ Category:</p> <p>Broken Access Control (API2-25)</p>
<div style="background-color: #ff7f0e; color: white; padding: 5px; font-weight: bold; font-size: 24px; display: inline-block;">3</div> 	<p>Internet Archive</p> <p>Impact</p> <p>31 m users</p>	<p>What Happened:</p> <p>Hackers exploited unrotated API tokens to access the organization's Zendesk support platform, potentially compromising user data from support tickets dating back to 2018</p>	<p>Why It Matters:</p> <p>This most recent breach was only one in a series that impacted the Internet Archive, demonstrating that failure to secure your APIs becomes a repeating problem and cost.</p>	<p>API ThreatStats™ Category:</p> <p>Authentication Flaws (API3-25)</p>
<div style="background-color: #ff7f0e; color: white; padding: 5px; font-weight: bold; font-size: 24px; display: inline-block;">4</div> 	<p>Trello</p> <p>Impact</p> <p>15 m users</p>	<p>What Happened:</p> <p>An unsecured API endpoint allowed unauthorized access to user data without authentication.</p>	<p>Why It Matters:</p> <p>Shadow APIs that lack authentication and expose sensitive data continue to be a major issue for organizations.</p>	<p>API ThreatStats™ Category:</p> <p>Broken Access Control (API2-25)</p>
<div style="background-color: #ff7f0e; color: white; padding: 5px; font-weight: bold; font-size: 24px; display: inline-block;">5</div> 	<p>Optus</p> <p>Impact</p> <p>9.5 m users</p>	<p>What Happened:</p> <p>A vulnerability in a web application was addressed, but the corresponding API was left exposed.</p>	<p>Why It Matters:</p> <p>The incident highlights the growth of APIs as a primary attack vector. Fixing your front-end is no longer sufficient.</p>	<p>API ThreatStats™ Category:</p> <p>Broken Access Control (API2-25)</p>

Infographic: The 2024 API Data Breach Calendar

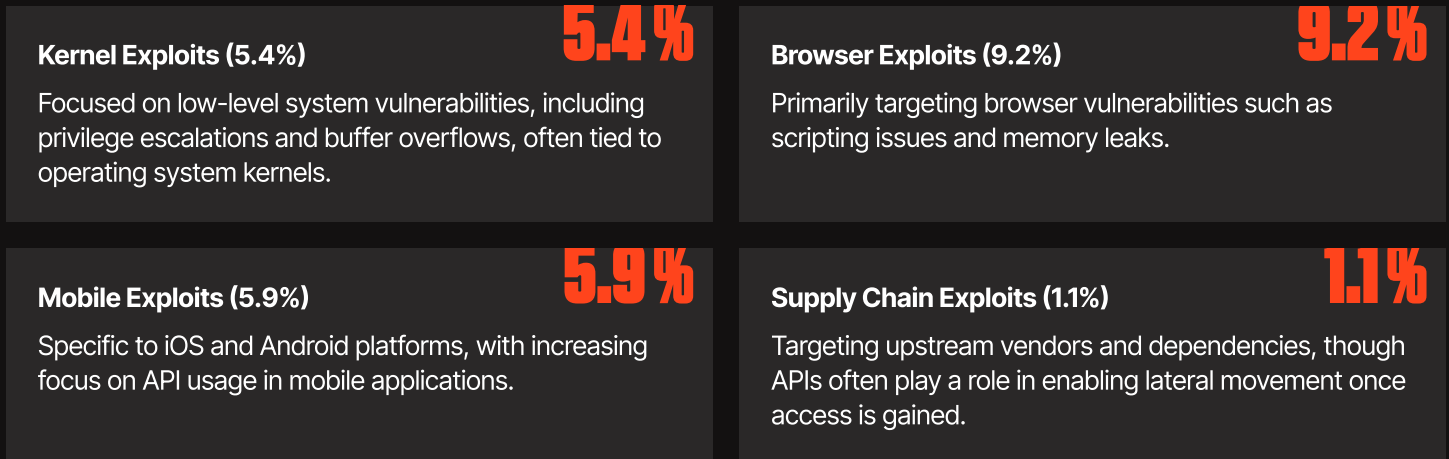
2024 marked an alarming escalation in API-related data breaches, with incidents occurring almost every week across industries. From healthcare to technology, transportation to finance, APIs have become the most exploited attack surface, leading to catastrophic data exposures and operational disruptions. To illustrate the scale and frequency of these incidents, we've compiled a month-by-month calendar infographic that highlights the most significant breaches, the number of compromised users or records, and the corresponding OWASP API Top 10 categories involved. This visual timeline not only underscores the urgency of securing APIs but also provides a powerful overview of how API vulnerabilities have reshaped the cybersecurity landscape this year.



Comparing API Exploits to Other Categories

APIs now represent the largest category of exploited vulnerabilities in CISA KEV, overshadowing other notable categories:

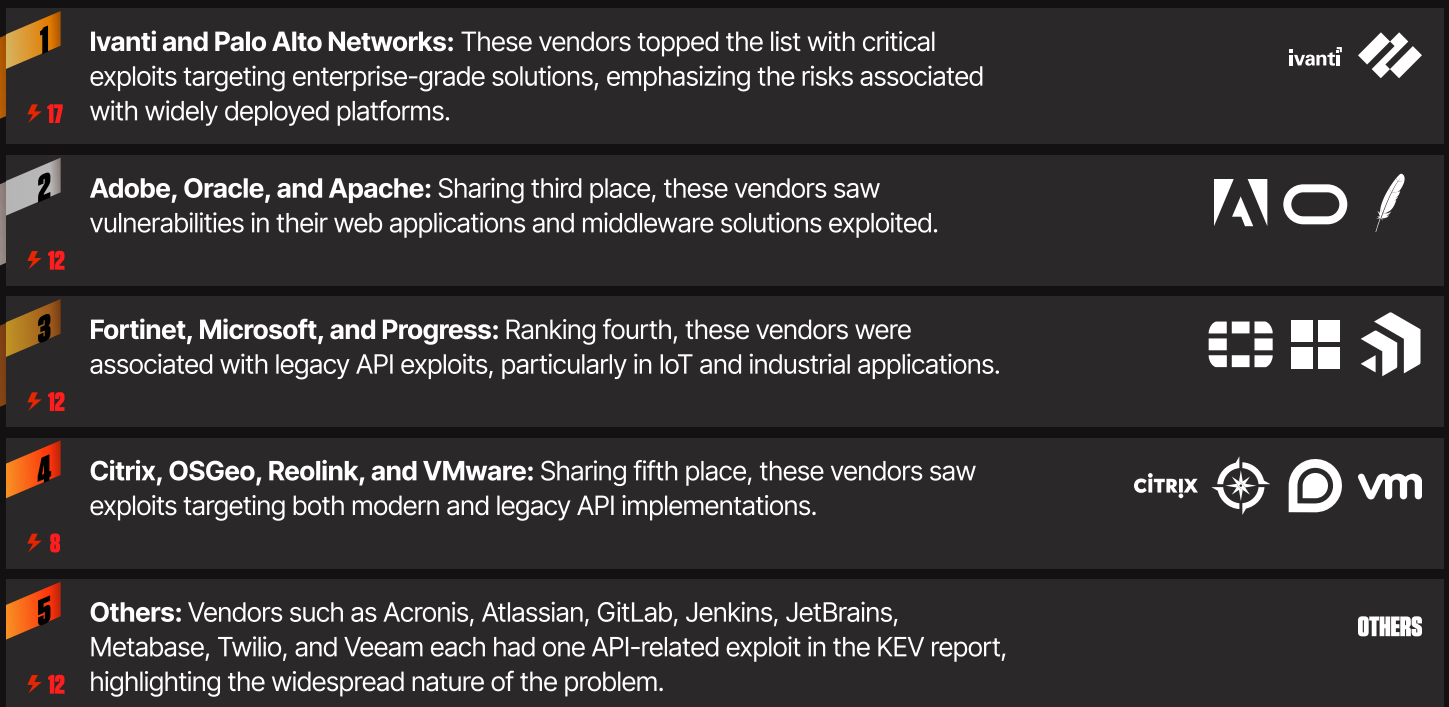
- **Kernel Exploits (5.4%):** Focused on low-level system vulnerabilities, including privilege escalations and buffer overflows, often tied to operating system kernels.
- **Browser Exploits (9.2%):** Primarily targeting browser vulnerabilities such as scripting issues and memory leaks.
- **Mobile Exploits (5.9%):** Specific to iOS and Android platforms, with increasing focus on API usage in mobile applications.
- **Supply Chain Exploits (1.1%):** Targeting upstream vendors and dependencies, though APIs often play a role in enabling lateral movement once access is gained.



The significant share of API exploits compared to these categories highlights the unique and expansive attack surface APIs present.

Top Vendors Affected by API Exploits

API vulnerabilities in 2024 spanned a diverse range of vendors, with some companies emerging as repeat offenders due to the high prevalence of their software in enterprise environments. The ranking of vendors by number of API-related CISA KEV exploits is as follows:



Why API Exploits Are Surging

Several factors contribute to the dominance of API vulnerabilities in 2024:

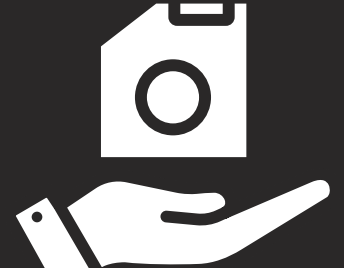
1 EXPANDING API USAGE

APIs are foundational to modern application ecosystems, from mobile apps to cloud services, making them prime targets.



2 LEGACY INFRASTRUCTURE

Many enterprises still rely on outdated API designs, particularly in IoT and industrial systems, exposing them to preventable vulnerabilities.



3 COMPLEXITY OF API SECURITY

Securing APIs involves addressing authentication, authorization, data validation, and rate limiting, leaving significant room for misconfigurations and exploits.



4 AI INTEGRATION

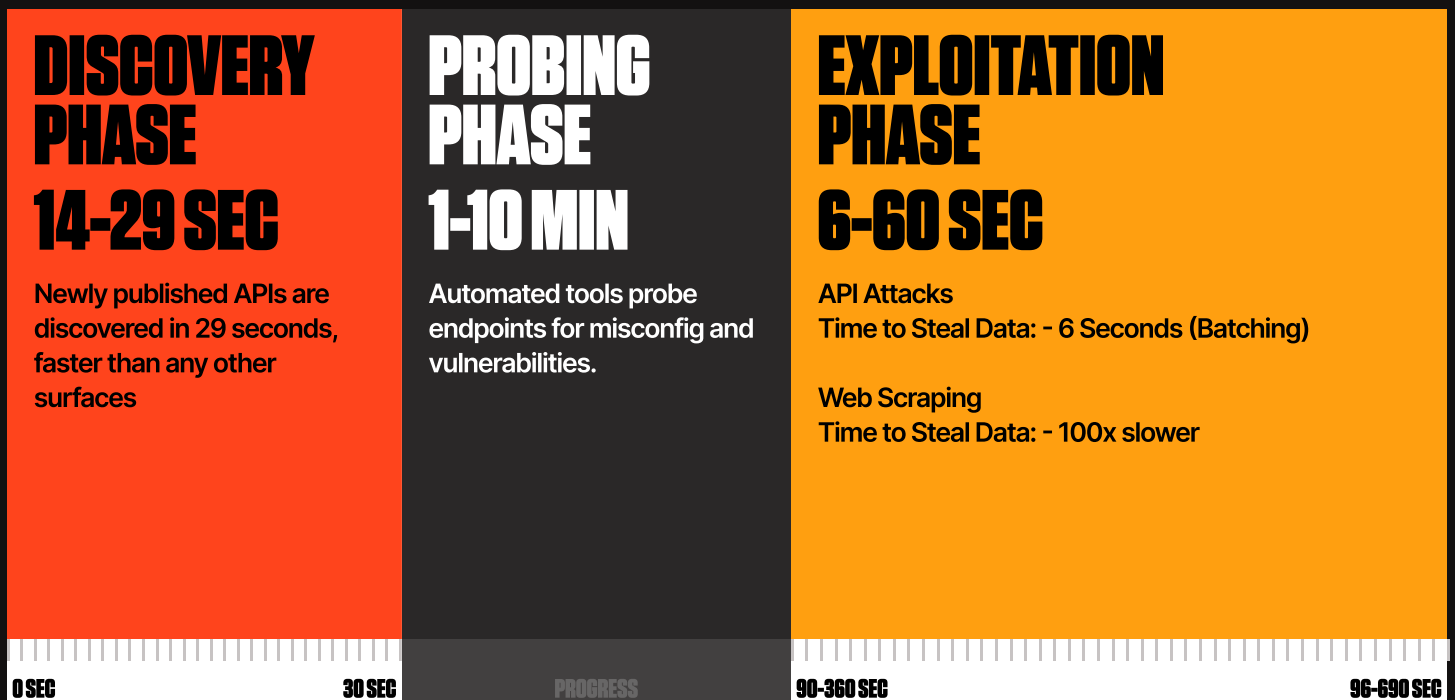
The growing integration of AI platforms, which heavily rely on APIs, has further expanded the attack surface.



API Honeypot Insights: How Fast Attackers Exploit APIs

We've already explored the exploitability and risks associated with API attacks—now let's delve into their staggering speed. Wallarm's API Honeypot Report, released in December 2024, revealed groundbreaking data on the velocity of API exploitation. Newly published API endpoints are discovered by attackers in a mere **29 seconds**, and advanced techniques allow sensitive data to be exfiltrated in as little as **6 seconds**. Compared to traditional web scraping, which operates at a fraction of this speed, APIs have become the fastest and most efficient attack vector in the modern enterprise landscape. These findings highlight why APIs are now a central security priority across industries.

Accompanying this chapter is an infographic that visually illustrates the speed and scale of API attacks, from discovery to exploitation. It highlights the alarming gap between the rapid pace of attacks and the slower remediation times of traditional security solutions, making a strong case for real-time protections.



For detailed insights, download Wallarm's API Honeypot Report at:
<https://www.wallarm.com/resources/api-honeypot-report>

Enterprises Need Real-Time API Controls

The findings from the API honeypot reveal an urgent requirement for a fundamental shift in how enterprises approach API security. Traditional API security systems, which often take **5-10 minutes** to detect and remediate threats, are no match for the speed of modern attacks. In an environment where API endpoints are discovered within seconds and exploited shortly after, only **real-time API controls** can effectively close this gap.

Real-time systems must identify, analyze, and block threats as they occur, ensuring that attackers are thwarted before they can extract data or compromise systems. Without such capabilities, enterprises risk exposing their most critical assets to attacks that move faster than traditional defenses can react. The era of delayed remediation is over; API security solutions must operate in real time to protect against the evolving threat landscape.

As APIs continue to drive innovation, particularly in AI-enabled systems, enterprises must prioritize real-time security to protect their business operations, customer trust, and long-term success.

API ThreatStats™ Top 10 2025

API ThreatStats™ Top 10 Methodology

The Wallarm API ThreatStats™ methodology represents a scientifically grounded and reproducible approach to analyzing and categorizing API-related vulnerabilities. Designed to achieve **99% coverage for API-related CVEs and bug bounty reports published in 2024**, this methodology is rooted in rigorous statistical analysis, precise CWE mapping, and a carefully validated classification system. Our methodology ensures that the insights provided are not only actionable, but also objectively derived from empirical data.

A Data-Driven Process Built on CWE Analysis

At its core, the Wallarm API ThreatStats™ framework relies on the **Common Weakness Enumeration (CWE)** system to map individual vulnerabilities to their underlying causes and mechanisms. CWEs serve as a standardized language for describing software vulnerabilities, allowing for precise categorization and analysis. Every CVE analyzed in 2024 was mapped directly to one or more CWEs based on its technical attributes, ensuring a consistent and reproducible process.

This analysis was conducted using both automated tools and manual expert review. Initial classification was assisted by the **ChatGPT-4o model**, which examined the CWE relationships and dependencies to propose groupings. These groupings were then reviewed and validated by Wallarm's expert team to ensure accuracy and practical applicability. While the grouping of CWEs into specific API ThreatStats™ Top 10 categories involves some level of interpretation, it is grounded in the **CWE relations tree**, which defines how various weaknesses interconnect and overlap.

For example:

- A CVE linked to **CWE-89 (SQL Injection)** was classified under API1: Injections due to its clear association with input handling vulnerabilities.
- A CVE tied to **CWE-352 (Cross-Site Request Forgery)** was mapped to API3: Cross-site Issues based on its impact on user session integrity.

This approach ensures that classifications are not arbitrary but are deeply rooted in the standardized relationships defined by the CWE framework.

Reproducibility and Transparency

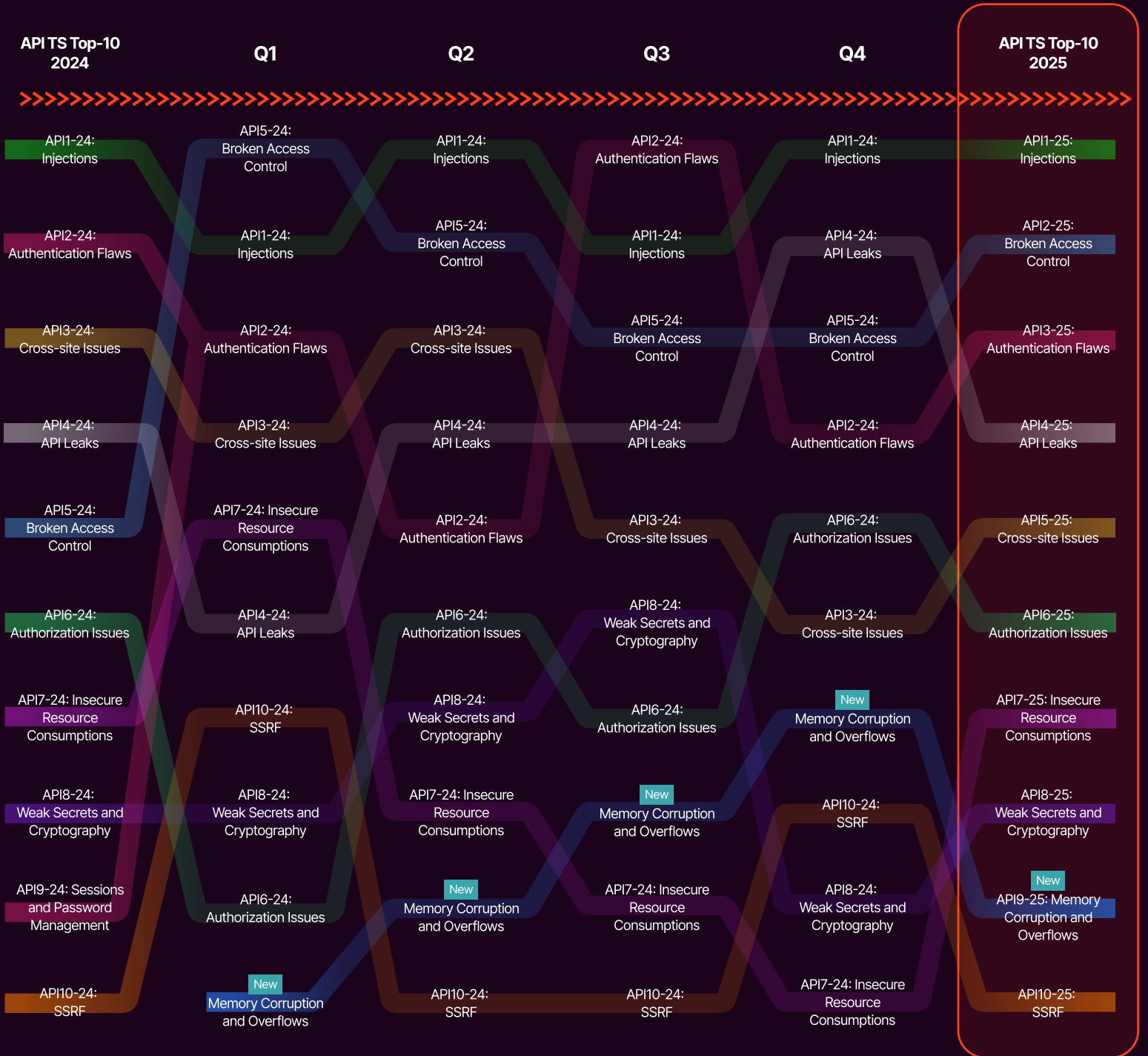
Reproducibility is a cornerstone of the Wallarm API ThreatStats™ methodology. Any researcher or organization can replicate our findings by following these steps:

- 1. Data Sources:** All data is derived from publicly available CVE databases, bug bounty disclosures, and threat intelligence feeds. No proprietary or inaccessible data is used.
- 2. CWE Mapping:** Vulnerabilities are mapped to CWEs based on their descriptions and documented technical details. This mapping process is transparent and can be replicated using CWE documentation.
- 3. Top-10 Grouping:** The classification of CWEs into the API ThreatStats™ Top 10 categories is the only subjective element in the methodology. However, this process is driven by the hierarchical relationships in the CWE tree and was refined using the ChatGPT-4o model, ensuring consistency and repeatability. Final groupings were reviewed and validated by Wallarm's cybersecurity experts.
- 4. Statistical Analysis:** The frequency and distribution of CWEs across the dataset were analyzed to identify trends and ensure comprehensive coverage of API-related vulnerabilities.

By adhering to this structured process, Wallarm ensures that the results are objective, reproducible, and free from biases.

2025 API ThreatStats™ Top 10

The **API ThreatStats™ Top 10** underwent significant shifts in 2024, driven by high-profile data breaches and the rising prevalence of AI-driven vulnerabilities. With over 50% of all major incidents directly tied to APIs, the year highlighted the criticality of securing API ecosystems in an increasingly interconnected digital landscape. This chapter explores the dynamic trends observed in 2024, using real-world data breaches to underline key vulnerabilities and the adjustments made to the **Top 10** for 2025.



Major API Vulnerabilities in 2024

API Leaks (API4-24): A Persistent Threat



Key Incidents:

- **Cisco Duo Security (April 16, 2024):** An API leak exposed 170,000 SMS logs, phone numbers, and metadata. The breach highlighted the risks associated with third-party integrations and poor API endpoint security.
- **Digi Yatra (April 22, 2024):** An API vulnerability exposed 1.74 million Aadhaar details, flight history, and personal preferences, emphasizing the dangers of transitioning to new applications and APIs without proper testing.
- **Dropbox HelloSign (April 29, 2024):** API keys and OAuth tokens for 100,000 users were leaked, demonstrating the potential fallout from poorly secured SaaS applications.

Analysis: These incidents underline how improper API security configurations and lack of oversight in endpoint management can lead to catastrophic data exposures.

Broken Access Control (API5-24):

A Leading Attack Vector



Key Incidents:

- **Tech in Asia (June 4, 2024):** A breach affecting 230,000 users revealed email addresses, roles, and other sensitive data, driven by misconfigured access controls.
- **Optus (June 21, 2024):** A prolonged API vulnerability exploited through trial-and-error techniques exposed 9.5 million customer records, illustrating the importance of rigorous API testing.
- Twilio reported a breach where enumeration of phone numbers led to the exposure of metadata for 33 million records. This attack illustrated the growing risks of improper rate limiting and endpoint security in modern APIs.

Analysis: Broken access control remains one of the most exploited vulnerabilities, particularly in industries handling sensitive user data, such as telcos and media.

Injections (API1-24): Growing Threat with AI Integration



Key Incidents:

- While not tied to specific public incidents in 2024, the rise of **AI systems relying on APIs** significantly increased the risk of injection vulnerabilities. AI-driven APIs, handling untrusted inputs in real-time, amplified the impact of SQL, command, and deserialization injections.

Analysis: The prominence of injection vulnerabilities is directly linked to the integration of AI in enterprise and consumer systems, with APIs serving as the main vector for data interaction.

API Abuse (e.g., Dell, April 28, 2024):



Key Incidents:

- Dell experienced a **massive API abuse incident**, where 49 million customer records were scraped by exploiting an overly permissive registration process. This demonstrated how attackers leverage weak API protections to execute large-scale data scraping campaigns.

Emerging Vulnerabilities: Memory Corruption & Overflows



- **Trend:** The rise of AI-driven APIs, interacting directly with GPUs and high-performance systems, introduced new attack vectors. Memory corruption issues such as buffer overflows and out-of-bounds writes were increasingly reported in 2024, emphasizing the need for robust memory management in high-performance environments.

API ThreatStats™ Top 10 Summary

Based on 2024 data, the API ThreatStats Top 10 for 2025 reflects the evolving nature of API vulnerabilities:

1 Injections (API1-25):

Remained in the top spot due to the increasing frequency of injection attacks in AI-driven APIs.

2 Broken Access Control (API2-25):

Maintained its prominence as a critical vulnerability across multiple industries.

3 Authentication Flaws (API3-25):

Consolidated with **Sessions and Password Management**, reflecting the interconnected nature of these vulnerabilities.

4 API Leaks (API4-25):

Highlighted by high-profile incidents like Cisco Duo and Digi Yatra.

5 Cross-Site Issues (API5-25):

Remained a persistent concern, particularly in web application and API interfaces.

6 Authorization Issues (API6-25):

Gained prominence due to complex role mismanagement in enterprise APIs.

7 Insecure Resource Consumptions (API7-25):

Continued relevance in denial-of-service attacks.

8 Weak Secrets and Cryptography (API8-25):

Emphasized by ongoing challenges in managing API tokens and cryptographic keys.

9 Memory Corruption and Overflows (API9-25):

A new addition reflecting vulnerabilities tied to AI and binary APIs.

10 SSRF (API10-25):

Retained its position due to its prevalence in cloud-native applications.

TOP10

Adjustments to the API ThreatStats™ Top 10 for 2025 based on 2024 Data

With the exponential rise in AI adoption and the resulting 1,025% increase in AI-related exploits, adjustments to the API ThreatStats Top 10 were made to address new vulnerabilities affecting APIs. One of the most significant changes is the introduction of a new category: Memory Corruption & Overflow. This reflects the increasing prevalence of memory-related vulnerabilities in high-performance API implementations driven by AI and binary processing.

New Category: Memory Corruption & Overflows

This category addresses vulnerabilities that arise from improper memory handling and access, which can lead to serious security breaches, including unauthorized data access, crashes, and arbitrary code execution. The vulnerabilities listed in this category occur primarily in systems where performance optimizations and low-level operations are critical—characteristics of AI-driven and binary APIs.

CWEs Included in This Category

CWE-119	Buffer Errors	CWE-131	Incorrect Calculation of Buffer Length
CWE-120	Classic Buffer Overflow	CWE-170	Improper Null Termination
CWE-125	Out-of-Bounds Read	CWE-681	Incorrect Conversion Between Numeric Types
CWE-787	Out-of-Bounds Write	CWE-243	Creation of Chained Buffers Without Checking for Overflow
CWE-190	Integer Overflow or Wraparound	-	Other memory-related issues where incorrect access, calculation, or allocation can compromise stability and security.
CWE-476	NULL Pointer Dereference		
CWE-1021	Incorrect Calculation of Buffer Size		

Memory Management and API Interaction

Memory management involves allocating, using, and freeing memory resources during an application's runtime. In high-performance systems like those implementing binary APIs for AI workloads, memory operations must be optimized for speed and resource efficiency. These systems often rely on direct memory access (DMA), hardware-accelerated processing, and low-level programming, such as C, C++, or CUDA for GPU interactions. This reliance increases the risk of vulnerabilities if memory is mishandled.

How APIs Trigger Memory Vulnerabilities

Optimized Binary APIs: APIs interacting with GPUs or optimized for binary data processing often bypass higher-level safety mechanisms for performance. While this enables faster data transfer and computation, it also introduces risks if bounds and checks are improperly implemented.


Dynamic Buffer Usage: AI systems frequently deal with high-dimensional datasets, requiring dynamic memory allocation for buffers. Errors in calculating or managing these buffers can lead to overflows or underflows.

Concurrency Issues: APIs designed for parallel processing on GPUs or multicore CPUs may mishandle shared memory spaces, leading to race conditions and undefined behavior.


Third-Party Library Integration: AI implementations heavily depend on third-party libraries for neural network operations and tensor computations. These libraries often operate close to the hardware layer, where a single unchecked operation can trigger cascading memory corruption.

Why Memory Issues Are Increasing in API Implementations


The surge in AI workloads and their tight integration with APIs has created a unique environment where performance optimizations and low-level access are prioritized:




Hardware Proximity: AI systems often rely on APIs to interface directly with GPUs, Tensor Processing Units (TPUs), or other specialized hardware, making memory vulnerabilities more likely.



Binary Data Formats: APIs exchanging raw binary data with minimal abstraction layers are prone to buffer miscalculations and overflow errors.



Real-Time Constraints: AI APIs are increasingly used in real-time applications, where performance constraints lead to aggressive optimizations that may sacrifice robustness in error handling.



High Data Throughput: Processing large datasets in parallel requires precise memory allocation and management, increasing the chances of integer overflows, out-of-bounds errors, or other memory-related issues.

SUMMARY

The adjustments to the API ThreatStats™ Top 10 reflect an evolving landscape where AI-driven APIs and memory vulnerabilities are becoming central concerns. Moving forward, organizations must prioritize robust API design, regular testing, and proactive monitoring to address these emerging threats effectively. The integration of AI into enterprise ecosystems will continue to shape the nature of API security challenges, underscoring the need for adaptive and forward-thinking strategies.



Action Items

In this report, we aim to bridge the gap between the technical and strategic aspects of API security by sharing actionable insights tailored to the distinct responsibilities of CISOs and CIOs. The included table highlights key action items for each role, drawing directly from the real-world breaches, vulnerabilities, and trends documented throughout 2024. By aligning these roles with specific, evidence-based recommendations, we hope to empower enterprise leaders to address API security challenges with clarity and focus.

The CISO's responsibilities center on creating and enforcing a robust API security framework that aligns with the evolving threat landscape. This includes proactive measures like regular audits, incident response planning, and continuous threat intelligence gathering; activities supported by real-world examples such as the Optus and Twilio Authy breaches. By focusing on technical defenses and bridging the gap between security measures and business outcomes, CISOs can build a resilient API security posture.

For CIOs, the focus shifts toward integrating API security into business strategies, fostering cross-functional collaboration, and ensuring visibility across the API lifecycle. Incidents like Digi Yatra and Ascension Health demonstrate how API vulnerabilities can disrupt operations and erode customer trust, underscoring the need for CIOs to prioritize investments in tools, education, and processes that align API security with enterprise goals.

This table is more than a checklist; it's a roadmap for aligning technical security measures with organizational priorities. By using the lessons and insights from this report, we aim to support CISOs and CIOs in their shared mission to secure APIs and drive enterprise success in 2025 and beyond.

Key Observations from 2024

1

AI as a Catalyst for New Vulnerabilities

AI integration is driving rapid API adoption across industries, but it also introduces unique risks. APIs facilitating real-time data exchanges between AI models and applications often lack adequate security measures, making them susceptible to injection, abuse, and memory-related exploits.

2

Legacy and Modern APIs Both Under Attack

While legacy APIs (e.g., used in Digi Yatra and Optus incidents) remain vulnerable due to outdated designs, modern RESTful APIs are equally at risk due to complex integration challenges and improper configurations.

3

Growing Exploitation of Authentication and Access Control

The Twilio and Tech in Asia breaches demonstrated how attackers exploit weak authentication and access control mechanisms to gain unauthorized access. These issues are exacerbated by the decentralized nature of API management in large organizations.



CISO

Establish an Enterprise-Wide API Security Framework:

Develop and enforce policies for API security, covering inventory, authentication, and access controls. Align these policies with compliance standards highlighted in the **Integrus Health** and **Ascension Health** breaches, where insufficient API protections led to massive data exposures.

Conduct Quarterly API Security Audits: Schedule and execute security audits focusing on API vulnerabilities, shadow APIs, and misconfigurations. The **Optus** breach revealed the risks of overlooked APIs, emphasizing the need for regular inventory and testing.

Drive Continuous Threat Intelligence Gathering: Monitor the evolving API threat landscape, including vulnerabilities like injection flaws and access control breaches highlighted in the **API ThreatStats™ Top-10 for 2025**. Use this intelligence to update defensive measures proactively.

Create a Proactive Incident Response Plan: Develop and maintain a specific incident response plan for API breaches, incorporating lessons from breaches like **Twilio Authy** and **Dell**, where rapid response could mitigate damage. Include simulated breach exercises to prepare for real-world scenarios.

Communicate API Risks at the Board Level: Translate technical risks into business impact to gain buy-in for enhanced security measures and resources. Use metrics like incident response times and the financial implications of breaches seen in cases like **Dell** and **Optus**.



CIO

Integrate API Security into Business Strategies:

Ensure API security considerations are built into digital transformation and AI initiatives. The **Digi Yatra** breach, caused by poorly secured APIs during a transition, underscores the importance of securing APIs from project inception.

Ensure Cross-Functional Collaboration: Foster collaboration between IT, development, and business teams to align API implementation with operational goals. Poor API configurations in Dell's breach exposed millions of records, showing the risks of siloed deployment efforts.

Oversee API Lifecycle Management: Implement processes for proper API deprecation, transition, and monitoring to prevent legacy risks and unaccounted endpoints. The **CISA KEV report** showed that 18.9% of exploits targeted legacy APIs, underscoring their persistent risk.

Champion Investments in API Discovery and Monitoring Tools: Ensure the enterprise has the infrastructure for real-time API monitoring and anomaly detection. The **Ascension Health** and **Digi Yatra** breaches illustrate the criticality of early detection for minimizing damage.

Enhance Employee Awareness of API Security Risks: Launch education programs across departments, focusing on how API vulnerabilities impact business continuity and customer trust. The **Twilio Authy** breach highlights how unsecured APIs can disrupt both operations and customer confidence.

Final Words

As we close the chapter on 2024, one thing is abundantly clear: **API security is no longer just a technical challenge—it is a business imperative.** The rapid adoption of APIs across industries, driven by innovations in AI, cloud computing, and digital transformation, has brought unparalleled opportunities for growth and efficiency. However, it has also exposed organizations to unprecedented levels of risk. The breaches, vulnerabilities, and exploits detailed in this report reveal the true cost of neglecting API security—disrupted operations, regulatory penalties, loss of customer trust, and irreparable damage to reputations.

For CIOs, CISOs, and business leaders, the stakes have never been higher. APIs are the connective tissue of modern enterprises, enabling everything from customer-facing applications to critical backend integrations. As their role has expanded, so has the responsibility to secure them. The days of relegating API security solely to technical teams are over. API risks now directly affect business continuity, revenue streams, and shareholder confidence, demanding a holistic approach that involves executives, security professionals, and development teams alike.

2024 marked a turning point where CIOs and business leaders were increasingly drawn into the conversation around API security. This shift reflects a growing understanding that API vulnerabilities are not just IT issues—they are enterprise-wide risks. Decisions about product roadmaps, digital transformation initiatives, and AI deployments must now account for the security of the APIs that underpin these efforts. Without this alignment, organizations risk falling into a reactive cycle of addressing breaches after the damage is done, rather than proactively building resilience into their systems.

Looking ahead to 2025, business leaders must champion a **culture of API security** that spans the entire organization. This involves more than just implementing tools and policies—it requires fostering collaboration between teams, investing in continuous training, and ensuring that API security is a key consideration in every strategic decision. For CIOs, this means taking ownership of the API security lifecycle, from discovery and testing to monitoring and threat mitigation. By doing so, they not only protect their enterprises but also enable innovation, agility, and growth in an increasingly competitive market.

The insights in this report provide a roadmap for navigating the complexities of API security. From the evolution of the API ThreatStats™ Top-10 to the analysis of real-world breaches, it's clear that the challenges of securing APIs will only intensify as their adoption continues to grow. However, with the right strategies and a commitment to proactive security, organizations can not only safeguard their systems but also unlock the full potential of APIs as drivers of business transformation.

As we move into 2025, the call to action is clear: **API security must be at the forefront of enterprise priorities.** This is not just about preventing the next breach—it's about building the trust, resilience, and innovation needed to thrive in a digital-first world. Together, CIOs, business leaders, and security professionals can lead the way in securing the APIs that power the future of business.