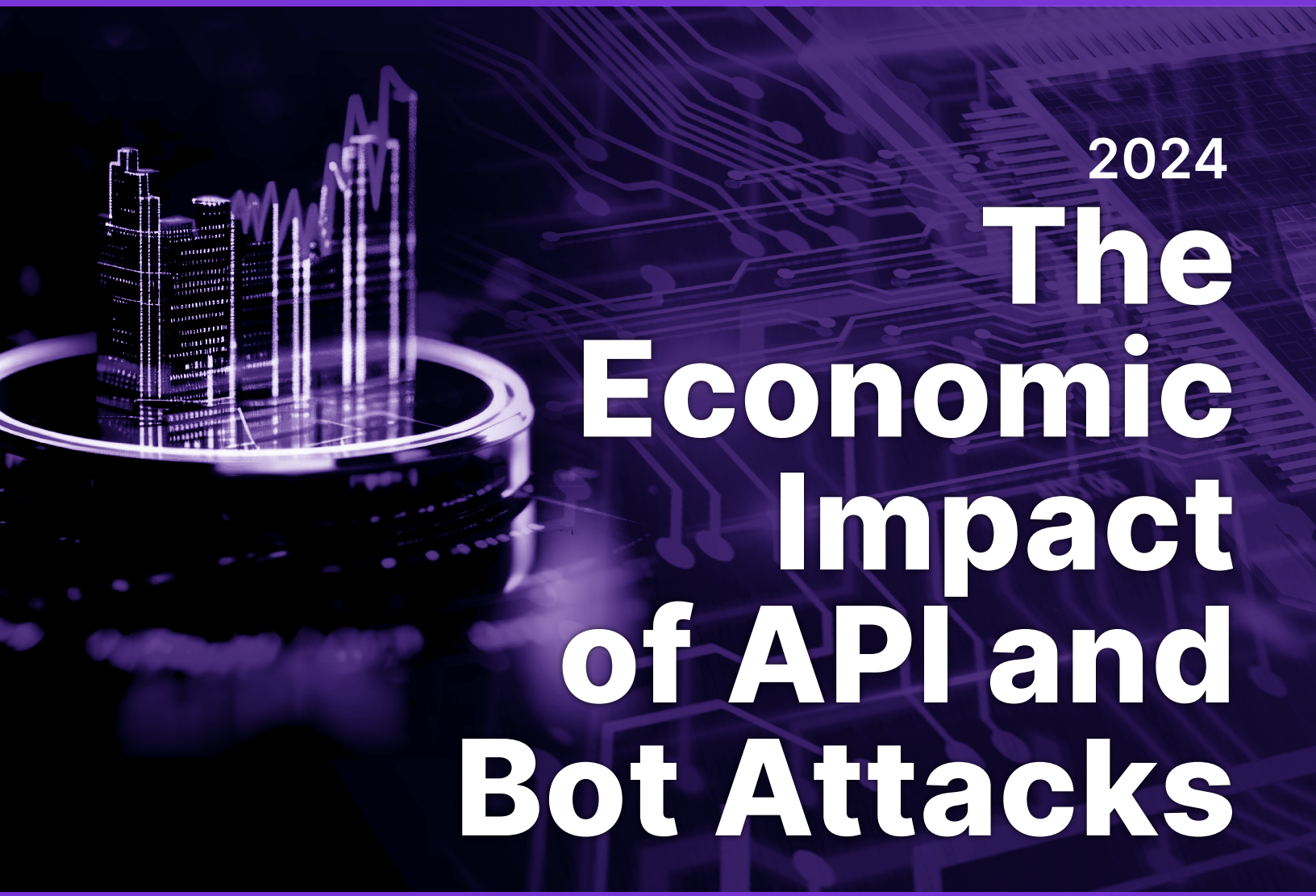
imperva
a Thales company



2024

The Economic Impact of API and Bot Attacks

imperva
a Thales company

2024

The Economic Impact of API and Bot Attacks

Table of Contents

Executive Summary

02

Application Programming Interfaces (APIs) have become crucial in today's digital environment. Their rise in popularity is primarily driven by their ability to enable rapid development, seamless integration, and enhanced user experiences across web and mobile applications. Due to this widespread adoption, APIs have become attractive targets for attackers, particularly those using highly sophisticated bots. These bots enable attackers to exploit business logic vulnerabilities, which can result in significant financial and reputational damage.

Imperva engaged the Marsh McLennan Cyber Risk Intelligence Center to analyze API-related and bot-related incident data to quantify the cost of API insecurity and bot attacks. The analysis, comprised of over 161,000 unique cybersecurity incidents, estimates that insecure APIs and lack of bot management could amount to the following financial impact:

USD 35-87 BILLION
Average annual API-related total global cyber loss

USD 68-116 BILLION
Average annual bot-related total global cyber loss

USD 94-186 BILLION
Average annual combined bot & API total global cyber loss

USD 8.9-17.9 BILLION
Average annual total global cyber loss to API abuse by bots

Imperva believes that these alarming estimates underscore entirely preventable losses. By investing in comprehensive API security and bot management solutions from the beginning, companies could substantially reduce API-related and bot-related losses, especially as API adoption grows.

The analysis indicates that large firms may face a heightened risk of API-related incidents, perhaps because their extensive deployment and utilization of APIs increase their exposure to potential breaches. When comparing API-related security incidents to non-API-related incidents in the database, the Marsh McLennan Cyber Risk Intelligence Center identified a positive correlation between company revenue and the frequency of API-related incidents. For companies with over USD 100 billion in revenue, it is estimated that up to **18%** of their cyber incidents were likely API-related.

Up to **14%** of cyber incidents for this same category of companies were estimated to be bot-related.. API-related and bot-related incidents accounted for up to **25%** of total cyber incidents for these organizations, emphasizing the need to protect APIs from sophisticated, automated threats.

This report combines data from Imperva's latest threat research with insights from the Marsh McLennan Cyber Risk Intelligence Center to provide insights on the expanding threat landscape and potential losses.

Imperva Threat Research: The API Sprawl Broadens the Attack Surface

03

MARSH MCLENNAN CYBER RISK INTELLIGENCE CENTER STUDY

Globally, up to 6% of all cyber security losses annually are API-related.

Average annual API-related insured cyber loss:
USD 174–437 million

Average annual API-related total US cyber loss:
USD 9.3–23 billion

Average annual API-related total global cyber loss:
USD 35–87 billion

Percentage of API-related events by revenue:

1-10B:	12%
10-50B:	11%
50-100B:	11%
>100B:	18%

APIs are omnipresent, and for good reason.
As per Mulesoft[1] , **99%** of organizations have already embraced APIs, with **39%** seeing increased revenues and **35%** reporting reduced operational costs. And these are just a few of the many positive outcomes of API adoption.

However, with increased adoption and usage comes an inherent risk. APIs expand the attack surface, making them prime targets for cyberattacks. Imperva's recent threat research on the matter, The State of API Security in 2024 Report, reveals alarming trends, underscoring the vulnerabilities inherent in API usage.

On average, organizations have 613 API endpoints, providing numerous potential entry points for attackers. With enterprise sites handling an astounding 1.5 billion API calls annually, the sheer volume increases the likelihood of encountering vulnerabilities. It's no wonder that **71%** of all web traffic is API-related, highlighting their critical role and the immense data they handle.

A significant concern is the prevalence of shadow APIs, with an average of 29 per account. These undocumented or hidden APIs often escape the rigorous security measures applied to known endpoints, creating blind spots that attackers can exploit. Additionally, each account typically has 16 deprecated API endpoints, which, despite being outdated, may still be accessible and vulnerable to attacks.

Unauthenticated API endpoints pose another significant risk, averaging 21 per account. These endpoints can be accessed without proper verification, making it easier for malicious actors to infiltrate systems. BOLA (Broken Object Level Authorization) endpoints, averaging 1.6 per account, further exacerbate the risk by allowing attackers to manipulate object references to gain unauthorized access to data.

[1] *https://www.mulesoft.com/lp/reports/connectivity-benchmark*

Marsh McLennan Cyber Risk Intelligence Center Study

04

The prevalence of API attacks by company revenue

In its analysis, Marsh McLennan's Cyber Risk Intelligence Center found a correlation between company size by revenue and the percentage of API-related cyber events.

Highest Risk for Largest Enterprises

Companies with revenue over $100 billion face the highest risk of suffering a cyber incident, with API-related incidents accounting for up to an estimated **18%** of all cyber incidents. Imperva's data reveals that larger enterprises are prime targets for API attacks due to their extensive API usage and valuable data.

Significant Threat for Mid-Range Enterprises

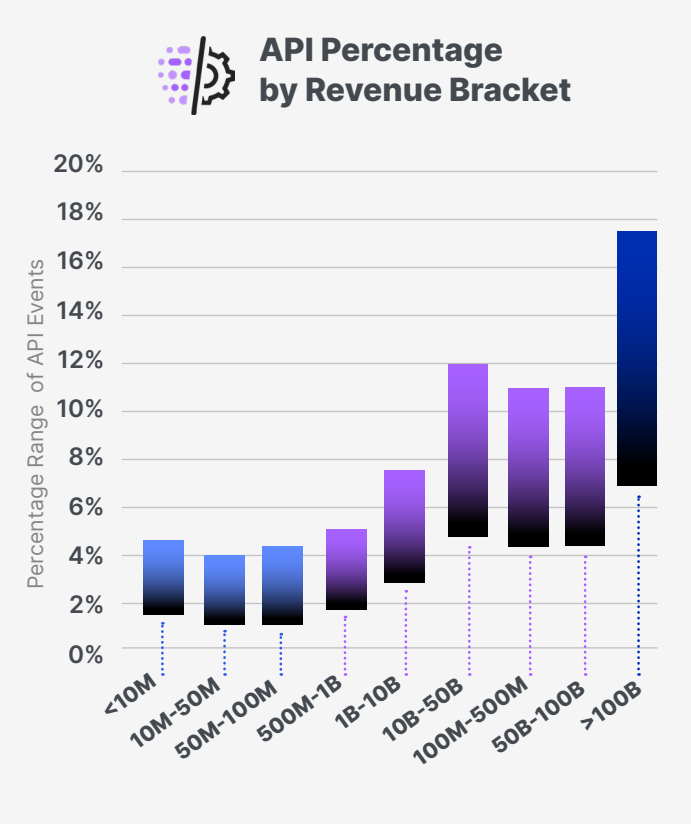
Organizations in the $500 million to $100 billion revenue bracket have had API-related incidents accounting for an estimated **8%** to **12%** of all cyber incidents. Imperva's data suggests that organizations' API ecosystems become more complex and attractive to attackers as they grow.

Lower Risk for Smaller Enterprises

Companies with revenues below $500 million reported relatively lower API-related incidents, ranging from **4%** to **5%** of all cyber incidents. Imperva's data suggests that smaller businesses might be less targeted for API attacks due to fewer APIs or less valuable data.

Imperva believes this data highlights a clear trend:

As companies grow and their revenues increase, they tend to rely more heavily on APIs, raising their risk of API-related security incidents. Large firms, with their extensive deployment and utilization of APIs, face greater exposure to potential attacks. The elevated percentage of API-related events in the largest companies underscores the critical need for robust API security measures across all business sizes, especially as companies scale and integrate more APIs into their operations.



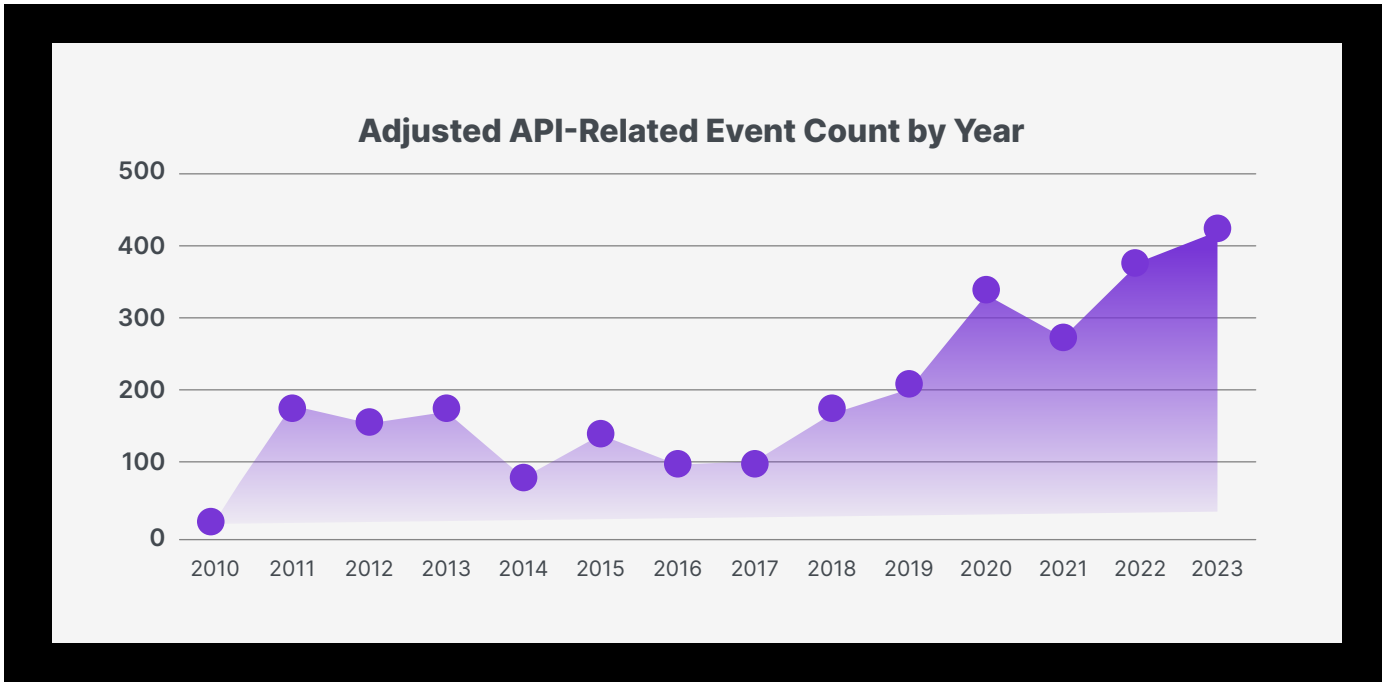
Marsh McLennan Cyber Risk Intelligence Center Study

05

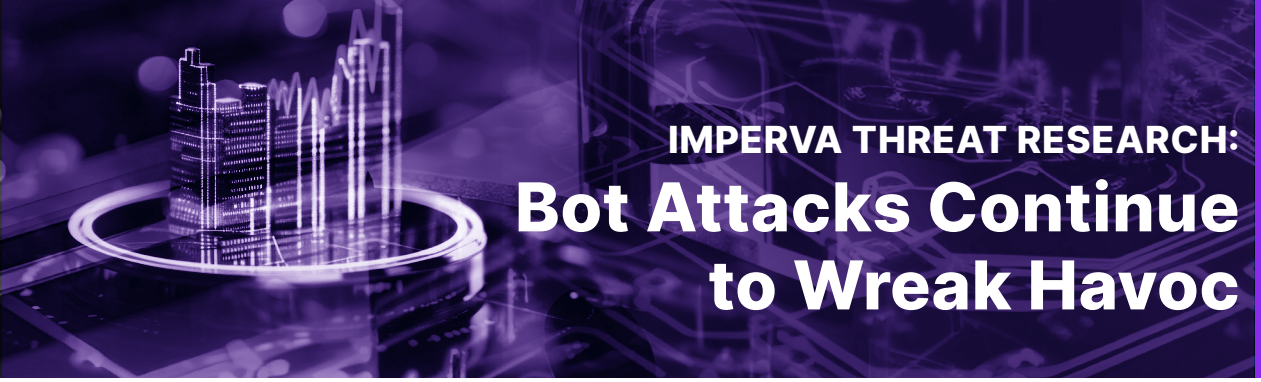
API-related incidents by year

The chart below shows the estimated adjusted[2] count of API-related events by year.

The sharp increase in incidents throughout the years shows the growing risk of API attacks. From 2010 to 2011, there was an explosive growth of **652%**, highlighting the burgeoning threat. Although the numbers fluctuated in subsequent years, the trend continued upward, with significant increases such as a **32%** rise from 2018 to 2019 and an alarming **60%** surge from 2019 to 2020. The upward trajectory persisted, with a notable **40%** increase from 2021 to 2022 and a further **9%** rise in 2023. This pattern underscores the escalating threats posed by API vulnerabilities as businesses increasingly rely on APIs for seamless integrations and data exchanges. The relentless exploitation of these gateways by attackers makes robust API security measures more critical than ever. As organizations continue to innovate and expand their digital ecosystems, the importance of fortifying APIs against evolving attack vectors cannot be overstated.



[2] Adjustments were made to the estimated count, including adjustments for incompleteness of Marsh's data set, for underreporting in Marsh's data set due to text descriptions being incomplete. Marsh scaled up the API- and Bot-related counts and total counts assuming that proportionate number of "unknown" events are actually API- or Bot-related.



IMPERVA THREAT RESEARCH:

Bot Attacks Continue to Wreak Havoc

06

MARSH MCLENNAN CYBER RISK INTELLIGENCE CENTER STUDY

Globally, up to 8% of all cyber security losses annually are bot-related.

Average annual bot-related insured cyber loss:
USD 340 - 580 million

Average annual bot-related total US cyber loss:
USD 18 - 31 billion

Average annual bot-related total global cyber loss:
USD 68 - 116 billion

Percentage of bot-related events by revenue:

1-10B	10%
10-50B	11%
50-100B	9%
>100B	14%

Bad bots interact with applications in ways that mimic legitimate users, making detection and blocking more challenging. Instead of exploiting technical vulnerabilities, they exploit business logic by leveraging an application's intended functionality and processes. This allows bad bots to facilitate high-speed abuse, misuse, and attacks on websites, mobile apps, and APIs. Bot operators and attackers can conduct malicious activities such as web scraping, competitive data mining, personal and financial data harvesting, brute-force login attempts, scalping, digital ad fraud, denial-of-service attacks, spamming, and transaction fraud. These activities consume bandwidth, slow servers, and steal sensitive data, resulting in financial losses and reputational damage.

The latest trends in automated internet traffic reveal an alarming rise in bad bot activity. The Imperva 2024 Bad Bot Report revealed that bad bots now account for almost a third of internet traffic.

Even more alarming is the rising sophistication of bad bots. Today, over **60%** of bad bots we observe at Imperva are classified as evasive—a combination of moderate and advanced bot traffic levels. These bad bots are increasingly sophisticated and employ techniques such as mimicking human behavior, using AI and machine learning to adapt and improve over time, delaying requests, and defeating CAPTCHAs to avoid detection and carry out significant attacks with fewer requests—reducing the "noise" typical of bad bot campaigns. They can even rotate IPs through random IPs, anonymous and residential proxies, and simulate human-like interactions to avoid detection by traditional security systems. These sophisticated bots can execute complex tasks like scraping data, performing account takeovers, buying in-demand concert tickets or consumer products, and more.

Marsh McLennan Cyber Risk Intelligence Center Study

07

The prevalence of bot attacks by company revenue

Bot-related events are more common across organizations of varying sizes than API-related events, which tend to become a more significant issue as company revenue size increases:

High Exposure for Largest Enterprises

Companies with over $100 billion in revenue face the highest risk, with bot-related incidents accounting for up to **14%** of all cyber incidents. Similar to API attacks, Imperva suggests large enterprises are prime targets due to their extensive digital presence and valuable assets.

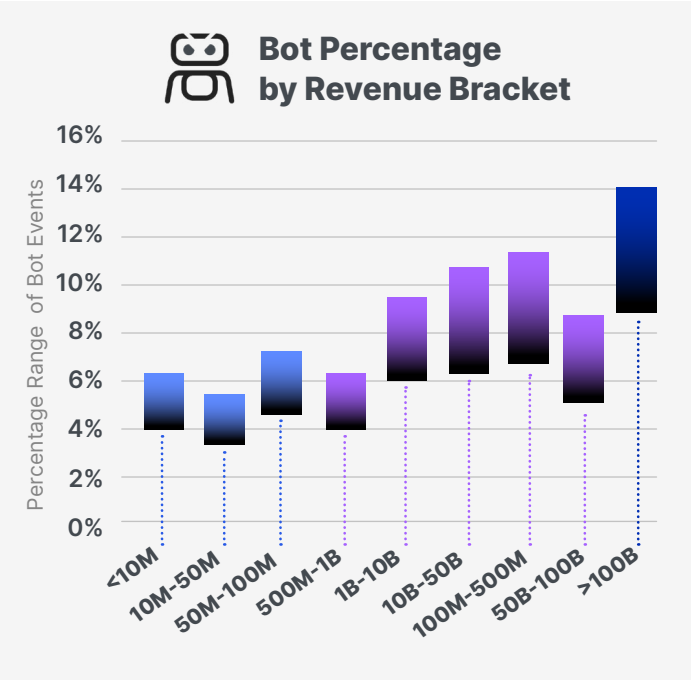
Consistent Threat for Mid-Range Enterprises

Organizations with revenues between $500 million and $100 billion show adjusted high percentages of **9%** to **11%** of all cyber incidents. Imperva suggests that this consistent threat level indicates that mid-sized to large enterprises must be vigilant against bot attacks, which can be just as pervasive as API attacks.

Widespread Threat Across All Sizes

Unlike API attacks, bot attacks show a more evenly distributed risk across revenue buckets. Even the smallest businesses (<$10 million) and mid-sized enterprises ($10 million to $500 million) face significant threats of API attacks, with adjusted high percentages ranging from **5%** to **7%** of all cyber incidents. Imperva suggests that this underscores the opportunistic nature of bot attacks, where attackers target any accessible vulnerability or business logic, regardless of the organization's size.

Imperva believes these insights highlight the critical need for comprehensive bot management strategies, a priority that it identifies as essential across all revenue sizes. The widespread availability of attack tools and knowledge has enabled even low-skilled attackers to launch sophisticated bot attacks, making small businesses as vulnerable as large enterprises. With the advent of artificial intelligence, the barrier to entry has lowered even further. Additionally, bot attacks can target multiple businesses simultaneously without significantly increasing the attacker's costs. The economic impact is particularly devastating for smaller organizations, which often lack the resources for advanced security measures and robust incident response plans. These insights highlight the critical need for comprehensive bot management strategies, a priority that Imperva identifies as essential across all revenue sizes.



Marsh McLennan Cyber Risk Intelligence Center Study

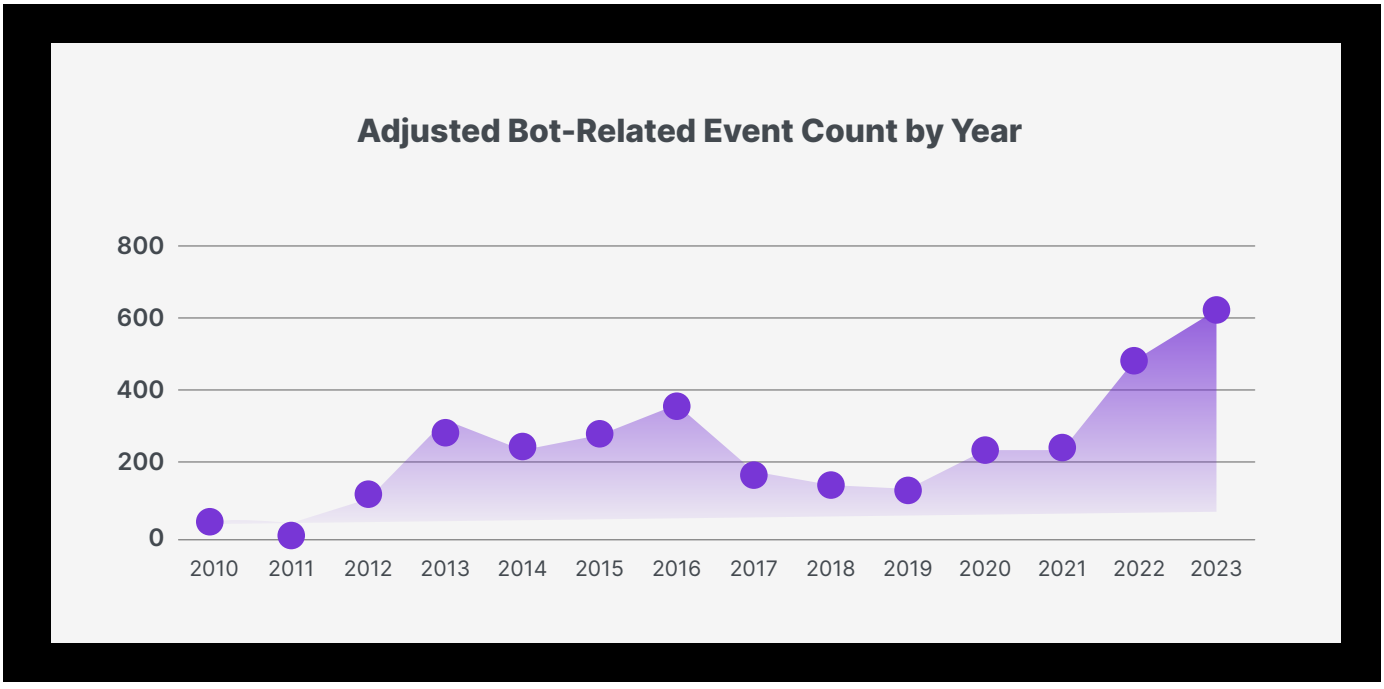
08

Bot-related incidents by year

The chart below shows the adjusted count of bot-related events by year, indicating a significant increase in recent years.

The growing threat of bot attacks is evident from the dramatic fluctuations and overall upward trend in incidents over the years. There was a **38%** decrease from 2010 to 2011, followed by a staggering **191%** increase from 2011 to 2012 and an even more alarming **102%** rise from 2012 to 2013. While there were periods of decline, such as a 48% drop from 2016 to 2017, the overall trajectory has been upward.

The pandemic has created favorable conditions for bot operators to generate profits, leading to a **61%** surge in bot-related events in 2020. With the introduction of AI and machine learning tools, bot attack and evasion techniques have evolved and become more widespread. Consequently, there has been a substantial increase in bot-related security incident count, with an **88%** increase in 2022 and a **28%** increase in 2023. This pattern underscores how bot attacks are highly opportunistic and continually evolving, targeting vulnerabilities across organizations of all sizes.



IMPERVA THREAT RESEARCH:

The Cost of Bot Attacks Targeting APIs

09

MARSH MCLENNAN CYBER RISK INTELLIGENCE CENTER STUDY

Globally, up to 12% of all cyber security losses annually are combined API and bot-related.

Average annual API and bot-related insured cyber loss:
USD 469 - 929 million

Average annual API and bot-related total US cyber loss:
USD 25 - 49.6 billion

Average annual API and bot-related total global cyber loss:
USD 94 - 186 billion

Percentage of API and bot-related events by revenue:

1-10B:	19%
10-50B:	18%
50-100B:	17%
>100B:	26%

The increasing reliance on APIs has made them a prime target for automated abuse by bots. According to the 2024 Bad Bot Report, automated threats accounted for **30%** of API attacks in the past year, underscoring the need for robust bot protection as a critical component of API security strategies. As organizations expand their API usage, they inadvertently attract malicious actors who exploit these interfaces using automated bots to carry out harmful actions. The financial and operational impacts of such attacks are considerable and multifaceted.

Financial Losses

Automated attacks on APIs, such as credential stuffing, fake account creation, and data scraping, can lead to significant financial losses. For instance, when bots successfully execute a credential stuffing attack on a bank's API, they can access and manipulate user accounts, leading to unauthorized transactions and data exfiltration. It isn't hypothetical, as **44%** of account takeover attacks in the past year have targeted APIs directly. This results in direct financial theft and incurs costs for rectifying fraudulent transactions and compensating affected customers. Additionally, the bank may face regulatory penalties for failing to protect sensitive information, further exacerbating financial repercussions..

Operational Costs

The aftermath of an automated attack on an API often necessitates extensive incident response efforts. Organizations must dedicate resources to investigate breaches, mitigate ongoing threats, and restore normal operations. This can involve deploying additional security measures, performing detailed forensic analyses, and managing customer support to address the concerns of those affected by the breach. These activities significantly increase operational costs and divert resources from other critical business functions.

Reputational Damage

The impact of bot attacks extends beyond immediate financial and operational losses. Reputational damage is a severe consequence that can erode customer trust and loyalty. When customers perceive that an organization cannot protect their data, they may take their business elsewhere, leading to a loss of revenue and market share. Furthermore, partners and stakeholders may question the organization's reliability, potentially affecting business relationships and opportunities.

Compliance and Legal Risks

Non-compliance with industry and regulatory standards for data protection can lead to severe legal consequences. Automated attacks resulting from data breaches can expose organizations to lawsuits, fines, and other legal actions. Compliance violations can be particularly damaging, as they not only entail financial penalties but also mandate corrective actions that require additional resources and time to implement.

Marsh McLennan Cyber Risk Intelligence Center Study

The prevalence of API and bot attacks by company revenue

When analyzing the combined percentage of API and bot-related incidents out of all cyber incidents by revenue size, we can see that as revenue increases, the threat level generally scales up, peaking for the largest enterprises.

High-Risk Bracket

Companies with over $100 billion in revenue face the highest risk, with API and bot-related incidents accounting for up to **26%** of all cyber incidents. This indicates that larger enterprises are prime targets for API and bot attacks due to their extensive digital footprints and valuable data

Mid-Sized Bracket

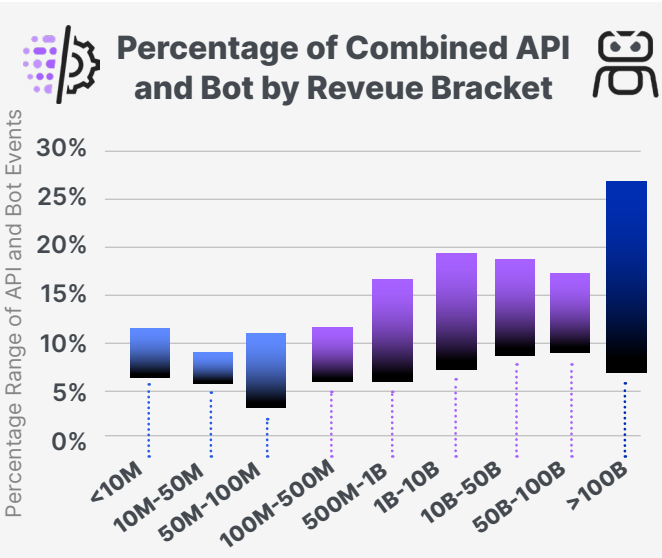
Organizations in the $500 million to $100 billion revenue brackets also experience significant threat levels, with adjusted high percentages of **16%** and **19%** of all cyber incidents, respectively. As companies grow, they become more attractive to attackers, possibly due to their API ecosystems' increasing complexity and volume.

Smaller-Sized Bracket

Companies with revenues below $500 million have a consistent adjusted high percentage of **10%** of all cyber incidents, showing that smaller enterprises are not immune to API and bot attacks. The high adjusted percentages across these revenue buckets highlight that these threats are pervasive and affect businesses regardless of size.

The smallest revenue bucket (<$10 million) has the lowest adjusted percentages (**6%** to **11%**). While still significant, these percentages are lower than larger enterprises, indicating that small businesses might be less targeted, possibly due to having fewer APIs and digital assets to exploit.

Imperva believes these observations emphasize the importance of tailored security strategies across different revenue sizes to effectively combat API and bot threats. The pattern underscores the need for enhanced API and bot protection measures as companies grow to safeguard against increasingly sophisticated and frequent attacks.



Marsh McLennan Cyber Risk Intelligence Center Study

A breakdown of API and bot attacks

Analyzing the distribution of bot attacks, API attacks, and their overlap reveals several key patterns and insights:

Largest Enterprises > $100B

High API Attack and Overlap Occurrence
The largest enterprises experience a higher estimated frequency of API attacks (**41%**) and a significant overlap between API and bot (**22%**), underscoring the critical need for comprehensive security measures that address both attack vectors.

Lower Bot Attack Frequency
The estimated bot attack frequency drops to **37%**, suggesting that while bot attacks are still a concern, the focus shifts towards securing APIs and mitigating complex, overlapping threats.

Large Enterprises $1B to $100B

Higher API Attack Occurrence
For larger enterprises, the frequency of API attacks increases, particularly in the $50B to $100B range, where it reaches **45%**.

Significant Overlap
The overlap is notably high in this range, with percentages between **18%** and **23%**. This indicates that larger enterprises with more sophisticated and numerous APIs are prime targets for combined attacks leveraging bots and API vulnerabilities.

Decreasing Bot Attack Frequency
The percentage of bot attacks decreases, ranging from **38%** to **46%**, possibly due to better defenses or a higher focus on API security.

Mid-Sized Enterprises $100M to $1B

Balanced Attack Distribution
In this revenue range, bot attacks (**55%** to **56%**) and API attacks (**35%** to **39%**) are more balanced than those of smaller businesses.

Lower Overlap
The overlap is lower, ranging from **6%** to **10%**, suggesting that as organizations grow, they become more likely to experience both attacks simultaneously, possibly due to more complex and interdependent digital systems.

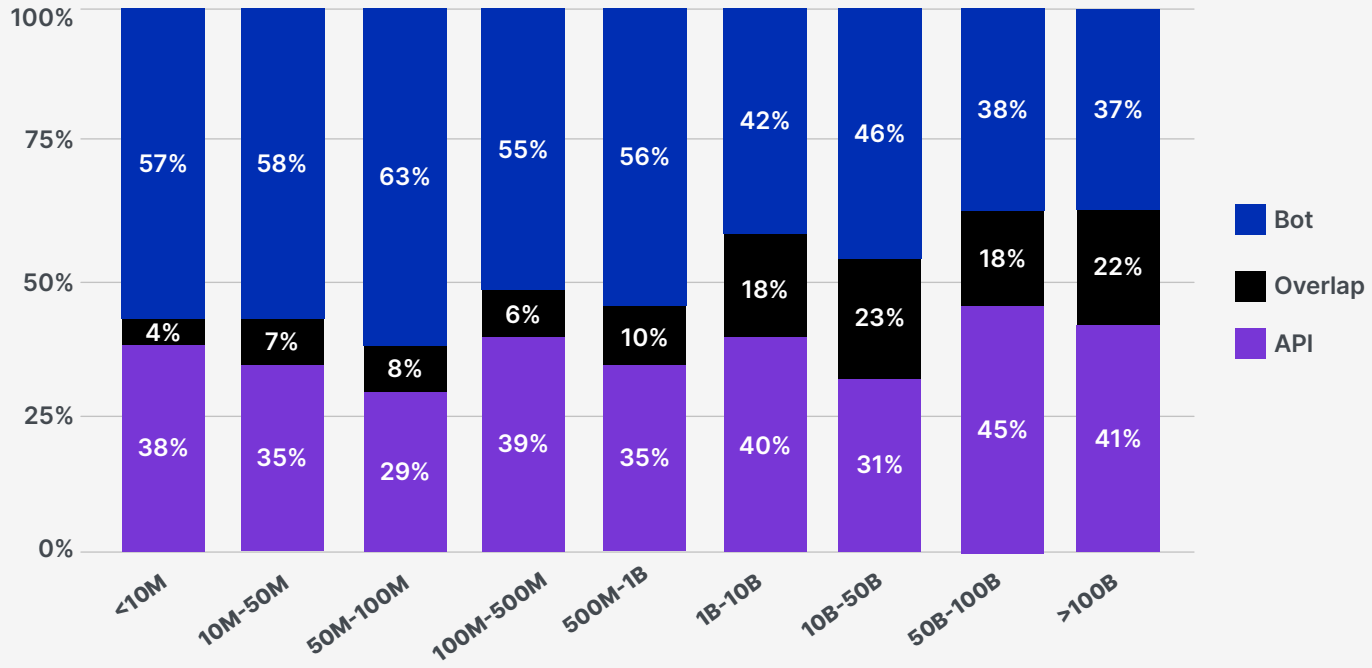
Smaller Businesses <$10M to $100M

High Bot Attack Frequency
Organizations in this range experience a high occurrence of bot attacks, with percentages ranging from **57%** to **63%**. This highlights the opportunistic nature of bot attacks, where smaller businesses are frequently targeted due to potentially weaker security measures.

Moderate API Attack Frequency
API attacks are less frequent than bot attacks but still significant, with percentages ranging from **29%** to **38%**.

Minimal Overlap
The overlap between API and bot attacks is relatively low (**4%** to **8%**), indicating that while both attacks occur, they often target different aspects of the organization's digital infrastructure.

Distribution of API and Bot Attacks



Conclusion 14

In conclusion, the financial impact of API and bot attacks is staggering, highlighting the urgency of addressing these threats.

The average annual insured cyber losses related to APIs range from an estimated USD 174 to 437 million, while bot-related insured losses are higher, between USD 340 and 580 million.

The estimated insured losses for API and bot attacks reach an alarming USD 469 to 929 million annually.

The broader financial repercussions are even more significant, with total annual API-related cyber losses in the US estimated between USD 9.3 and 23 billion and globally between USD 35 and 87 billion. Bot-related losses are higher, with estimated total US losses ranging from USD 18 to 31 billion and global losses between USD 68 and 116 billion.

When considering both types of attacks, the total annual US cyber losses amount to USD 25 to 49.6 billion, and global losses soar to USD 94 to 186 billion.

These figures underscore the substantial economic burden posed by API and bot attacks.

The analysis emphasizes the pervasive and escalating threat of API and bot attacks across organizations of all sizes. Bot attacks are particularly opportunistic and widespread, frequently affecting smaller and larger businesses. As organizations grow, the complexity and volume of their API ecosystems make them increasingly attractive targets for API attacks, with larger enterprises facing significant combined threats from both bots and APIs. The overlap between these attacks highlights the interconnected vulnerabilities in more sophisticated digital environments.

Consequently, organizations must implement comprehensive security strategies that address both API and bot attacks, with tailored measures to mitigate the specific risks associated with their size and operational complexity. As the digital landscape continues to evolve, proactive and adaptive security measures are essential to safeguard against the ever-shifting, highly sophisticated threats posed by automated attacks.

About Imperva Application Security

14

Imperva is the cybersecurity leader that helps organizations protect critical applications, APIs, and data anywhere, at scale, and with the highest ROI. The Imperva Application Security Platform stops the most advanced attacks with the highest efficacy while minimizing false positives. Its high efficiency enables organizations to quickly onboard, protecting their assets at scale. With the help of the Imperva Threat Research Team and our global intelligence community, we stay ahead of the evolving threat landscape, seamlessly integrating the latest security, privacy, and compliance expertise into our solutions

The Imperva Application Security Platform combines best-of-breed solutions that bring defense-in-depth to protect your applications wherever they live — in the cloud, on-premises, or in a hybrid configuration:

- On-Prem and Cloud Web Application Firewall (WAF) solutions for blocking the most critical web application security risks.
- API Security for continuous protection of all APIs using deep discovery and classification.
- Advanced Bot Protection for safeguarding websites, mobile applications, and APIs against today's most sophisticated automated threats.
- Account Takeover Protection to safeguard login endpoints against malicious activity, including takeover attempts and new account fraud.
- Client-Side Protection for safeguarding websites against client-side attacks and streamlining regulatory compliance with PCI DSS 4.0.
- DDoS protection for websites, networks, and DNS to ensure business continuity with guaranteed uptime.
- Runtime Application Self-Protection (RASP) for security by default against known and zero-day vulnerabilities.
- Content Delivery Network for securely delivering applications worldwide with superior speed and performance.

Start your Application Security Free Trial today
to protect your applications from Bad Bots.