imperva
a Thales company

REPORT

The State of API Security in 2024

- **About the Report** **03**
- **Executive Summary** **03**
  - The State of API Security in 2024 03
- **Findings At A Glance** **04**
- **Top API Attack Vectors in 2023** **05**
- **API Traffic Outgrowing Normal Web Traffic** **06**
- **The Role of Bots in API Security** **07**
  - Business Logic Abuse 09
  - API Account Takeover Attacks 10
  - DDoS Attacks on API Sites 11
- **API Attacks by Industry** **12**
- **API Attacks by Country** **13**
- **The Risk of Unknown APIs** **14**
  - Shadow APIs 14
  - Deprecated API Endpoints 14
  - Unauthenticated Endpoints 14
- **The OWASP API Security Top 10** **15**
  - Broken Object Level Authorization (BOLA) Risk 15
- **Top API Security Challenges** **16**
  - API Visibility 16
  - Data Leakage 16
  - Data Governance 16
  - Skills Shortage 16
- **Why Traditional Security Measures Aren't Enough** **17**
- **APIs are Easy Targets** **18**
  - API Incidents by Client Type 18
  - Top Attack Vectors 20
- **The Risk of Complacency** **21**
  - The Different Categories of API Attack Mitigation 21
- **The Importance of API Discovery** **23**
  - Discovering Sensitive APIs 23
- **API Security Options** **24**
  - Specialized API Security Solutions 24
  - API Gateways 24
  - Comprehensive API Security Protection 24
- **In Summary** **25**
- **API Security Recommendations** **25**
- **About Imperva** **26**

About the Report

The Imperva State of API security Report examines the current API security threat landscape and offers insights into potential trends for the year ahead. This report, which is aimed at security professionals and API developers, is based on intelligence gathered by the Imperva Threat Research team, drawing from data obtained from our product usage, which includes information on attacks targeting APIs. Looking at the top security challenges and attack analytics, the report offers a comprehensive view of the API threat landscape and presents practical API security recommendations for the year ahead.

Executive Summary

The State of API security in 2024

At a time when APIs, or Application Programme Interfaces, play a crucial role in enabling communication between applications and driving rapid innovation and development, it has never been more important to understand the risks and complexities of API security.

APIs play a central role in application modernization and seamless connectivity, constituting over 71% of web traffic last year. However, their widespread usage is expanding the attack surface, posing significant security challenges for organizations. The main API challenges faced by organizations today include Shadow APIs, third-party API implementations, API Governance, Business Logic Abuse, Data Leakage, and a notable API security skill shortage.

The report emphasizes the need for visibility into API ecosystems and the importance of locating every API. API Discovery is a crucial first step in establishing an effective API security posture. Advanced techniques and machine learning have enabled Imperva to uncover an average of 613 APIs per organization. This highlights potential risks like deprecated endpoints and Broken Object Level Authorization (BOLA)—recognized as one of the OWASP Top 10 API security Risks in 2023.

Automated attacks accounted for 27% of all API attacks, specifically targeting business logic. This form of abuse poses a significant challenge for traditional security tools to detect and mitigate.

API abuse often masquerades as normal traffic to a Web Application Firewall (WAF), making it impossible to detect using traditional security tools. The Imperva Threat Research team uncovered an increasing correlation between API abuse and malicious bots, emphasizing the need for improved visibility into API infrastructures to enable a comprehensive assessment and implementation of requisite security solutions such as Advanced Bot Protection and API risk assessment tools.

The State of API security in 2024 Report provides details on the ways sophisticated bad bots are exploiting business logic within APIs. The report examines the challenges and vulnerabilities organizations face in securing their API infrastructure. It stresses the importance of a comprehensive API security strategy, integrating Web Application Firewall (WAF) and API Discovery with Advanced Bot Protection and Advanced API security measures, including risk assessment, anomaly detection, and mitigation. The report concludes that traditional security measures are not enough and that an integrated approach is crucial for ensuring the protection of APIs.

[1] Based on API Discovery across Imperva customer accounts using Imperva API Security.

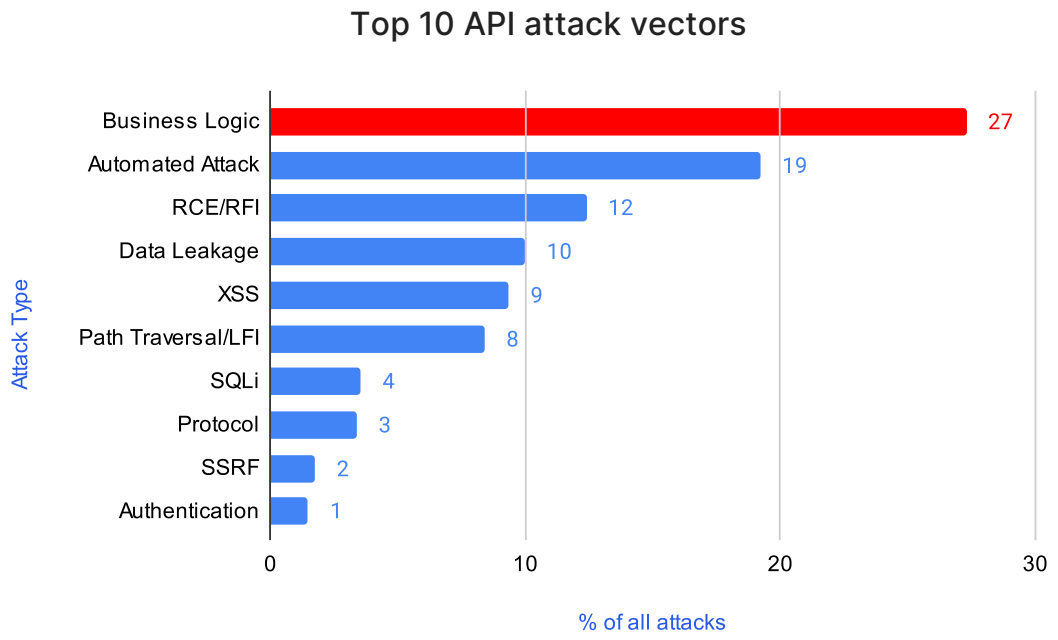
Findings At A Glance

Key findings include an average of 1.5 billion API calls per year to enterprise sites, with business logic abuse topping the list as the primary attack vector. The report delves into the impact of API traffic surpassing normal web traffic, with data revealing that APIs comprised over 71% of all web traffic in 2023. High volumes of non-human web traffic, especially automated bot activity, underline the need for robust API security measures.

613	the average number of API endpoints discovered per account
1.5B	the average number of API calls per year to enterprise sites
71%	of all web traffic is API-related
29	the average number of Shadow APIs per account
16	the average number of deprecated API endpoints per account
21	the average number of unauthenticated API endpoints per account
1.6	the average number of BOLA API endpoints per account
27%	of attacks mitigated targeted API Business Logic
46%	of all Account Takeover attacks targeted API endpoints
28%	of all DDoS attacks on APIs targeted Financial Services sites

Top API Attack Vectors in 2023

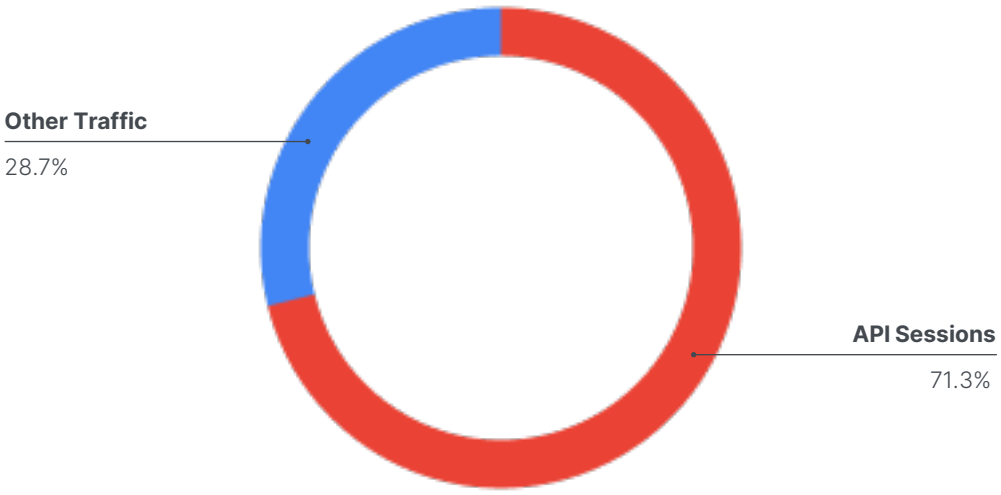
Business logic abuse was the top attack vector in 2023, with 27% of all attacks on APIs targeting their business logic, an increase of 10% vs the previous year (17% of all attacks targeting APIs in 2022 abused business logic). Not to be overlooked, 19% of attacks came from automated agents, otherwise known as bad bots.



The majority (71%) of all web traffic is API-related, surpassing normal web traffic, which poses a growing security risk across various industries. With APIs becoming a dominant channel for communication between applications, databases, and other systems, the risk of unauthorized access, data breaches, and sophisticated cyber attacks intensifies. Organizations across industries face a pressing need to strengthen their security measures to help mitigate the escalating threats associated with the surge in API traffic.

API Traffic Outgrowing Normal Web Traffic

While different reports may present varying statistics, a consistent trend is evident: API calls make up the majority of all web requests. This pattern is expected to continue, and even grow, as organizations modernize their application infrastructure.



The implications of API traffic surpassing normal web traffic is significant for high-value industries, notably impacting sectors like Finacial Services and travel. In the Finacial Services industry, where data security is paramount, the surge in API traffic introduces heightened risks of unauthorized access, data breaches, and sophisticated cyber attacks. As APIs become a dominant channel for communication between financial systems, the increased attack surface poses a considerable threat to sensitive financial data, potentially leading to substantial financial losses and reputational damage.

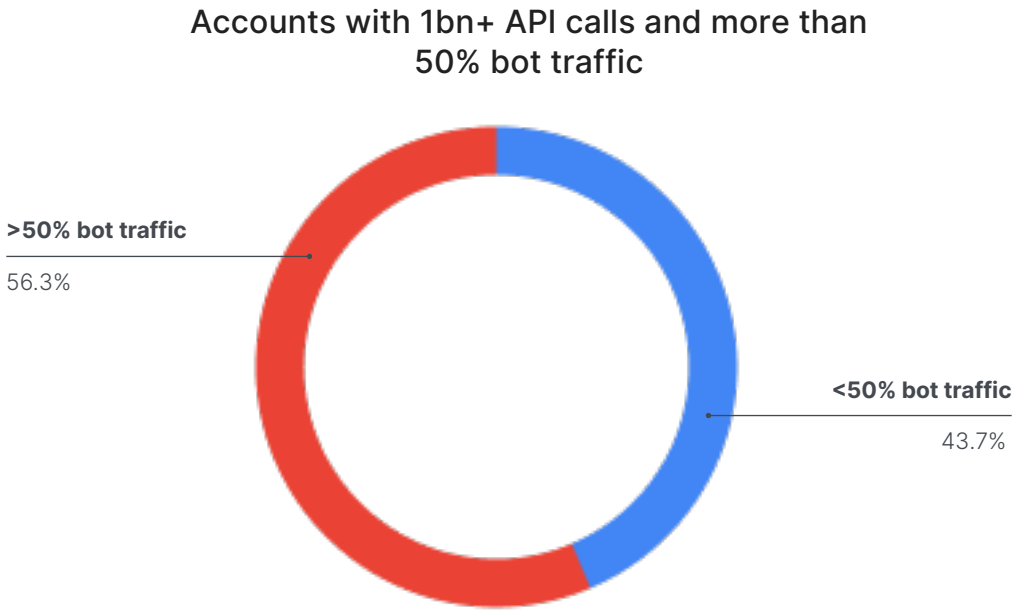
While a high volume of non-human web traffic is not necessarily an indication of abuse, it does indicate increased opportunities for an automated attack to occur, particularly for organizations lacking a robust API security strategy. The increased presence of bots in the overall traffic composition underscores the urgency for organizations to develop and implement effective API security measures to mitigate the elevated risk of automated abuse impacting systems and data.

Based on our data, we estimate that the average number of API calls per year for an enterprise site is 1.5 billion.

Source: Based on 2023 web traffic data to Imperva customer sites

The Role of Bots in API Security

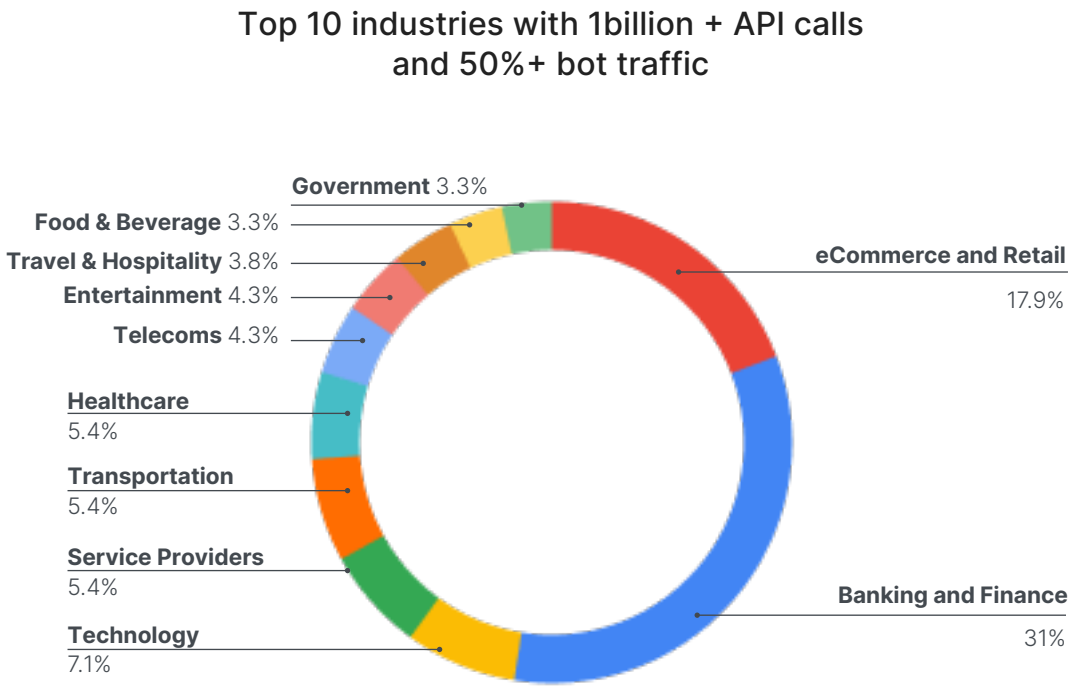
This section highlights the connection between the increase in non-human web traffic and the growing utilization of automated attack agents, creating an environment conducive to API violations.



The paramount risk to APIs comes from automated abuse by bots, making robust bot protection an indispensable element in an overarching API security strategy. As API usage expands, it becomes an attractive target for threat actors leveraging bad bots to carry out harmful actions, and an automated attack on an API can have devastating consequences.

For instance, consider a bank with an API that allows users to access their accounts, check balances, and perform transactions. Malicious actors can use automated bots to launch a large-scale attack on the API, using credential stuffing to systematically input stolen credentials. These bots mimic legitimate user behavior to avoid detection. Once inside the API, they may initiate unauthorized banking transactions, access sensitive information, or even manipulate account details. The attackers can also exfiltrate data, including personal information or financial details. As a result, the bank may suffer reputational harm, financial losses, and regulatory penalties.

Top Industries with High Volumes of API Calls and High Volumes of Bot Traffic



It's crucial to recognize the difference between good and bad bots. Not all bots are malicious, and APIs are designed to seamlessly interact with automated software applications for their intended purposes. However, the combination of extensive API calls and bot traffic presents a notable trend of concern. In customer sites with substantial API activity (1 billion+ calls), our findings reveal that over 56% of web traffic is attributed to bot activity. This emphasizes the pressing need to address this threat while acknowledging the legitimate role of automated processes in API interactions and distinguishing between malicious and good bot traffic.

[2] Estimate based on 90 days traffic
[3] Where 50% or more of web traffic is bots

Business Logic Abuse

API Business Logic abuse occurs when bad actors use automated attack agents to exploit the intended functionality of an API for malicious purposes, such as the exfiltration of sensitive data or disrupting a mission-critical application.

Automated attacks targeting APIs—credential stuffing, fake account creation, and data scraping—abuse APIs by manipulating the expected inputs and outputs to exfiltrate data. Attacks targeting APIs' business logic pose a significant threat to data security, and the repercussions extend to other areas of the business as well. Fraud costs escalate as malicious actors exploit vulnerabilities in APIs to gain unauthorized access. This leads to financial losses and compromises the integrity of transactions.

Moreover, automated attacks can substantially increase support costs as organizations grapple with the aftermath of security breaches, dedicating resources to incident response, investigations, and customer support to address the fallout. The impact extends to brand reputation, as customers and partners may lose trust in a company that fails to safeguard their sensitive information. Additionally, businesses can face non-compliance issues if they don't uphold industry and regulatory standards for data protection, potentially resulting in legal consequences and financial penalties.

The ramifications of API business logic abuse permeate through various facets of an organization, emphasizing the critical need for robust security measures to safeguard against these evolving threats.

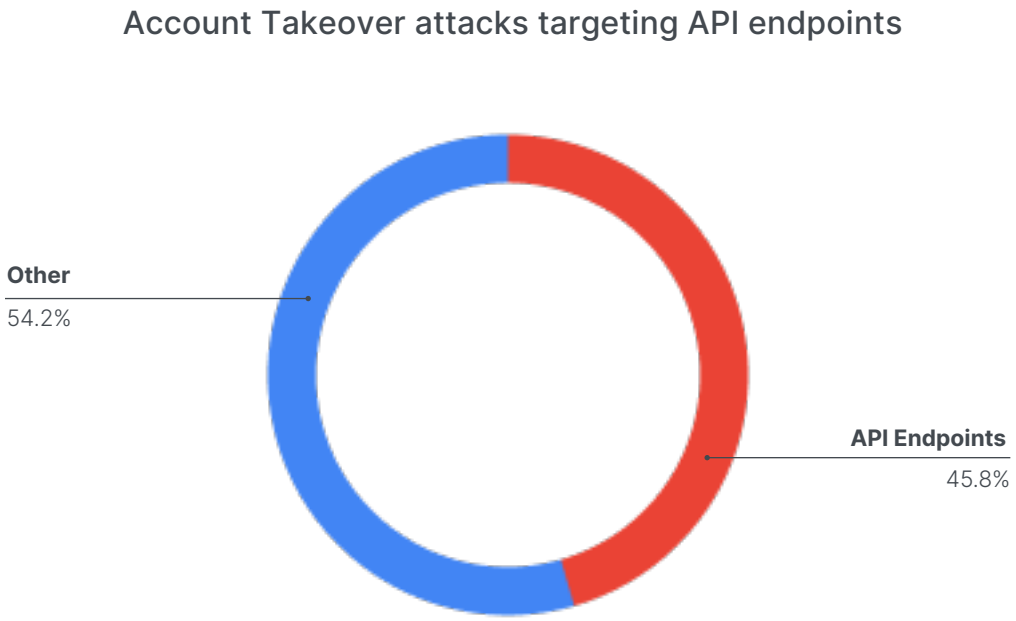
Detecting API business logic abuse is challenging because these attacks often mimic legitimate API usage, making them difficult to differentiate from normal traffic.

In 2023, 27% of attacks targeting APIs were business logic attacks

API Account Takeover Attacks

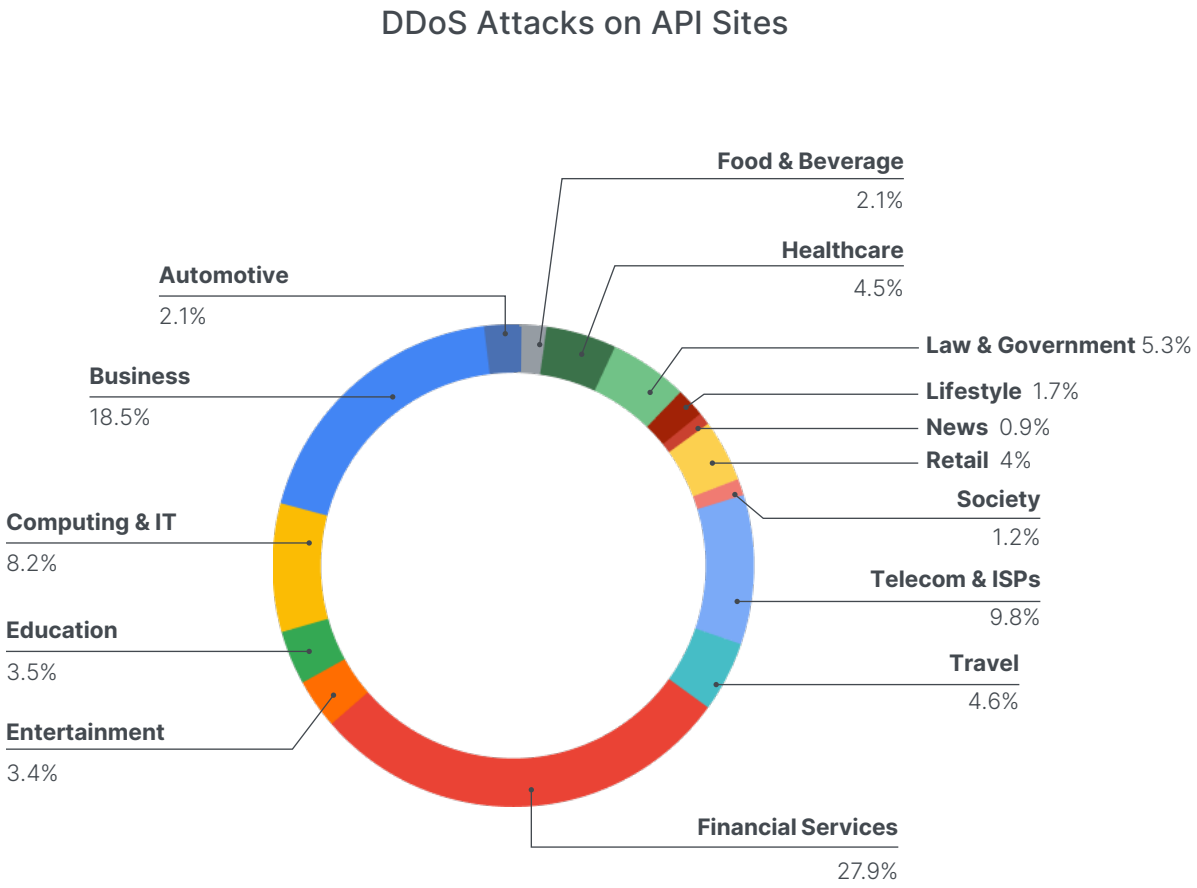
An API Account Takeover (ATO) attack occurs when malicious actors exploit vulnerabilities in an API's authentication processes to gain unauthorized access to user accounts. ATO attacks can be mitigated by Advanced Bot Protection solutions which can discern legitimate automated traffic from malicious traffic.

In 2023, 45.8% of all ATO attacks recorded by Imperva targeted API endpoints, an 11% increase over the prior year (35% of API attacks targeted APIs in 2022).



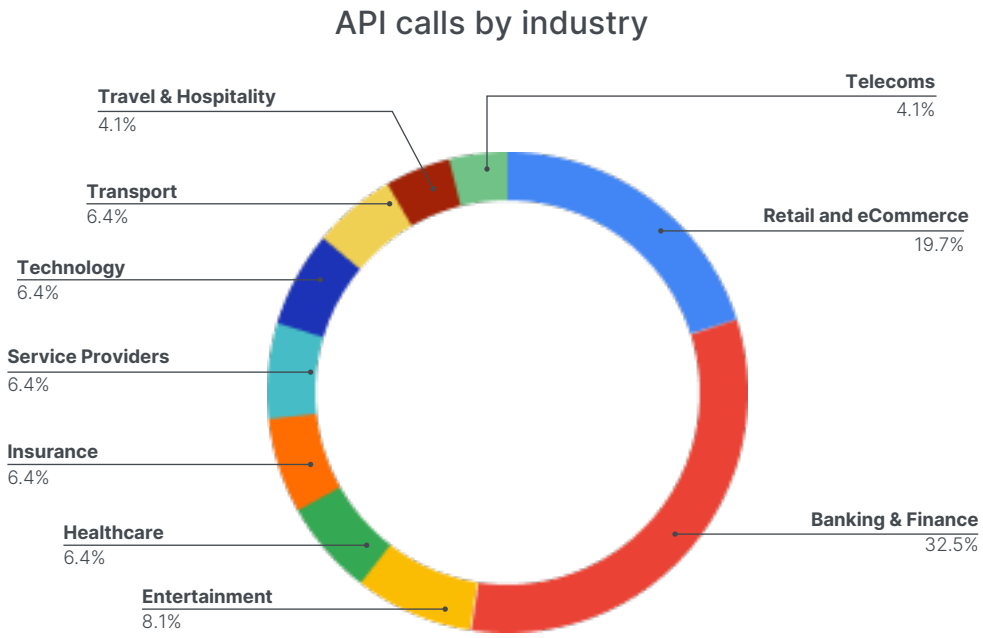
DDoS Attacks on API Sites

The Financial Services industry accounted for 27.9% of all DDOS attacks on API sites, followed by the Business sector (18.5%) and Telecoms and Internet Service Providers (9.8%). Almost 40% of all DDoS attacks on APIs targeted sites in the United States, followed by Brazil (9%), Australia (8%), and Mexico (5%).

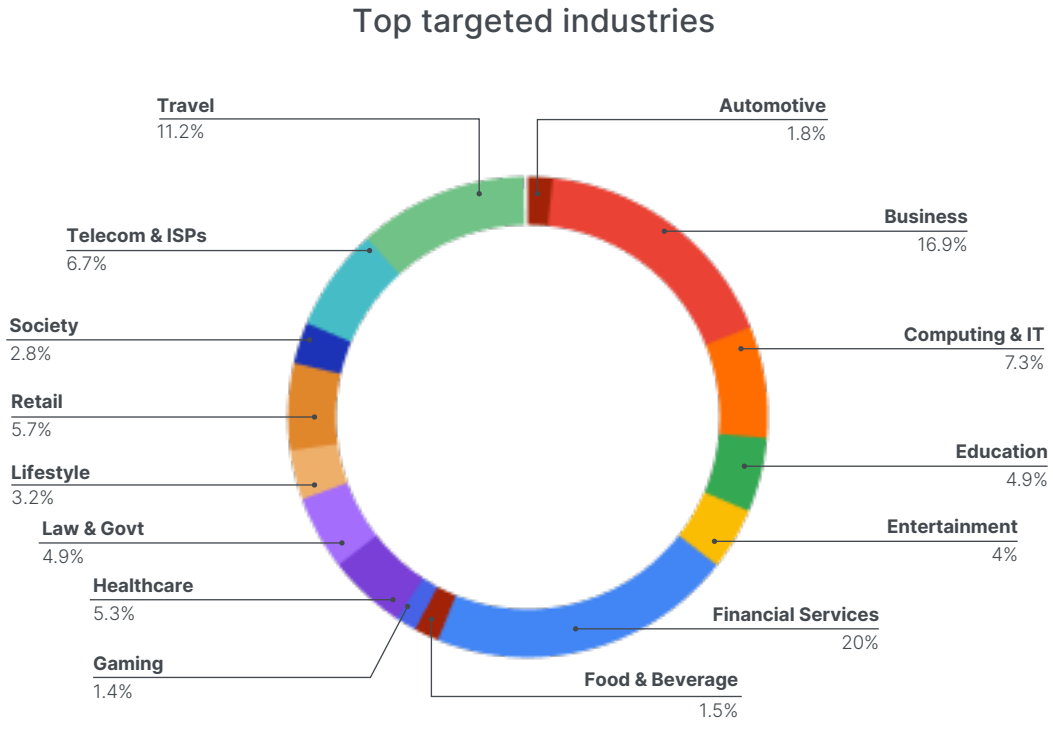


API Attacks by Industry

According to our data, the industries with the highest volumes of API traffic are Banking & Financial and eCommerce. In third place is the Entertainment industry, encompassing businesses such as streaming services and online news sites.



The industries most targeted by API attacks in 2023 were Financial Services (20%), followed by Business (16.9%), while the Travel industry accounted for 11.2% of all attacks.



[4] Estimate based on 90 days traffic.

API Attacks by Country

The top targeted country for API violations is the United States accounting for 39% of all attacks. In second place is Australia accounting for 18.9%, followed by India in third place, with 7.5% of all API violations targeting customer accounts in India.

Having extensive and **advanced digital infrastructure** makes countries attractive targets as threat actors seek to exploit vulnerabilities in sophisticated systems. In addition, the United States and Australia have a concentration of high-value industries such as Financial Services or Technology, and threat actors focus their efforts on API attacks in sectors known for handling valuable data.

The Risk of Unknown APIs

Shadow APIs

A Shadow API, also referred to as an undocumented API or undiscovered API, is an API that operates outside the official and monitored channels within an organization. These APIs may be created by well-meaning developers seeking to expedite their work, or they could be a remnant from previous software versions. While Shadow APIs can have practical uses, such as testing new features or facilitating internal operations, their existence poses a notable security risk to organizations. If manipulated and exploited, they can compromise sensitive data, potentially leading to breaches and non-compliance.

Imperva API Discovery uncovers all APIs, shedding light on previously overlooked interfaces that may have implications for security and overall risk management. The findings underscore the importance of thorough API Discovery as a crucial first step in a comprehensive API security strategy.

Imperva data shows an average of 29 Shadow APIs per account.

Deprecated API Endpoints

The presence of deprecated API endpoints poses a significant concern as they may lack updates and patches, making them susceptible to known vulnerabilities that have been addressed in newer versions. This can expose a system to potential exploitation by malicious actors. Failing to retire deprecated API endpoints increases the risk of security breaches and compromises, as these outdated interfaces often lack security updates and improvements present in more recent alternatives.

To mitigate the risk associated with a deprecated API endpoint, security teams should conduct regular audits to identify deprecated API endpoints within their systems. Continuous monitoring can help detect any attempts to exploit vulnerabilities associated with these endpoints. In addition, developers are encouraged to regularly update and upgrade APIs to ensure that deprecated endpoints are replaced with more secure alternatives.

Imperva API Discovery analysis found an average of 16 deprecated endpoints per account.

Unauthenticated Endpoints

Unauthenticated APIs are prevalent for various reasons, often created by developers to expedite the development process. During the development stages, functionality is often prioritized over security to save time. These APIs may also be employed to assess specific features without complex authentication or may stem from older software versions lacking robust security. Over time, these APIs persist without proper security measures as systems evolve.

The existence of unauthenticated APIs poses a significant risk to organizations as it could expose sensitive data or functionality to unauthorized users and lead to data breaches or system manipulation. Addressing vulnerabilities associated with these APIs is critical. To mitigate the risk, security teams should conduct regular audits and continuously monitor their APIs.

Imperva discovered an average of 21 unauthenticated API endpoints per account.

The OWASP API Security Top 10

The OWASP API Security Top 10, updated in 2023, is a compilation of critical vulnerabilities in APIs. Developed by the Open Worldwide Application Security Project (OWASP), the list acts as a guide for organizations to comprehend and tackle significant API security issues.

- Broken Object Level Authorization (BOLA)
- Broken Authentication
- Broken Object Property Level Authorization (combining Excessive Data Exposure and Mass Assignment risks)
- Unrestricted Resource Consumption
- Broken Function Level Authorization
- Unrestricted Access to Sensitive Business Flows
- Server-Side Request Forgery
- Security Misconfiguration
- Improper Inventory Management
- Unsafe Consumption of APIs

Broken Object Level Authorization (BOLA) Risk

Top priority on the list is BOLA (Broken Object Level Authorization), also known as IDOR (Insecure Direct Object Reference). BOLA arises from APIs exposing object identifiers through their endpoints, posing significant Object Level Access Control concerns. This vulnerability allows attackers to manipulate or access API data/resources without proper authorization, leading to severe consequences such as a breach. **Our analysis reveals an average of 1.6 API endpoints at risk of BOLA abuse**. While this number may seem insignificant, the risk is not. Failure to address BOLA vulnerabilities can result in unauthorized access, breaches, and misuse of critical functionalities.

To mitigate this risk, security teams should implement robust monitoring and logging mechanisms for tracking API usage, detecting anomalies, and identifying potential unauthorized access.

BOLA abuse leads to severe consequences

Top API Security Challenges

APIs are intended to expose application logic and data while providing users and applications with a technical contract for data exchange. However, they often have inadequate controls to protect against abuse. Many of today's web attacks are evolving and bypassing security, entering at API layers that may not even be on the radar of security teams. Some of the key challenges organizations currently face include:

API Visibility

Organizations lack complete awareness of their APIs, where they are located, and the associated risks. Assessing the number of unknown or shadow APIs within an organization's API ecosystem can prove challenging.

Data shows how attacks are becoming more complex and difficult to detect as threat actors use more complicated attack tools to target vulnerable APIs while evading detection. Such attacks often result in operational impact and data leakage, which can result in hefty fines for the organizations involved. Discovering every API in your ecosystem, including those previously unidentified, including Unauthenticated and Shadow APIs, is a critical step in the path to securing APIs.

Business Logic Abuse

In 2023, 27% of attacks targeting APIs that Imperva mitigated were business logic attacks. As covered in the Executive Summary, flaws within an API's logic can leave it susceptible to abuse. This risk is particularly challenging because attackers manipulate legitimate functionalities in ways that don't trigger conventional security alerts, allowing malicious activities to go unnoticed.

Data Leakage

Preventing attackers from successfully executing code or malware intended to steal data is critical in maintaining a secure application infrastructure. Unsecured APIs can become a pathway for attackers to access sensitive information, leading to the risk of data exfiltration. In 2023, Data Leakage risk accounted for 10% of mitigated attacks targeting APIs.

Data Governance

The rapid deployment of APIs without adequate security and governance protocols exposes sensitive data across mobile and cloud-native applications. Data Governance does not currently extend to APIs accessing sensitive data, and the continuous output of new APIs makes it difficult to maintain oversight and protect sensitive data effectively.

Skills Shortage

A significant hurdle is the need for more individuals with more in-depth expertise in API development, specifically to address security implications. According to the **Postman 2023 State of the API Report**, 38% of developers have less than two years of experience developing APIs.

Finding skilled professionals is crucial for organizations aiming to navigate API implementation complexities successfully. Leveraging an advanced, automated API security solution can go a long way in mitigating risks that may come about due to this lack of knowledgeable API resources.

Why Traditional Security Measures Aren't Enough

APIs are at risk of traditional application attacks such as SQL injection attacks, Remote Code Execution, and Distributed Denial of Service (DDoS) attacks, all of which are based on known signatures and can be blocked and mitigated by a robust web application platform incorporating a WAF and DDoS Protection. However, modern web attacks are finding ways to bypass traditional security measures. For example, a basic WAF lacks the ability to distinguish between malicious API calls and legitimate API traffic, which renders them ineffective at mitigating application logic vulnerabilities such as those included in the OWASP API Security Top 10.

The dynamic nature of API interactions and the sheer volume of legitimate requests make it hard for traditional security measures to discern malicious activities, necessitating more advanced API Security solutions to safeguard against such abuse. Business logic attacks, for example, often involve authorization or authentication rules.

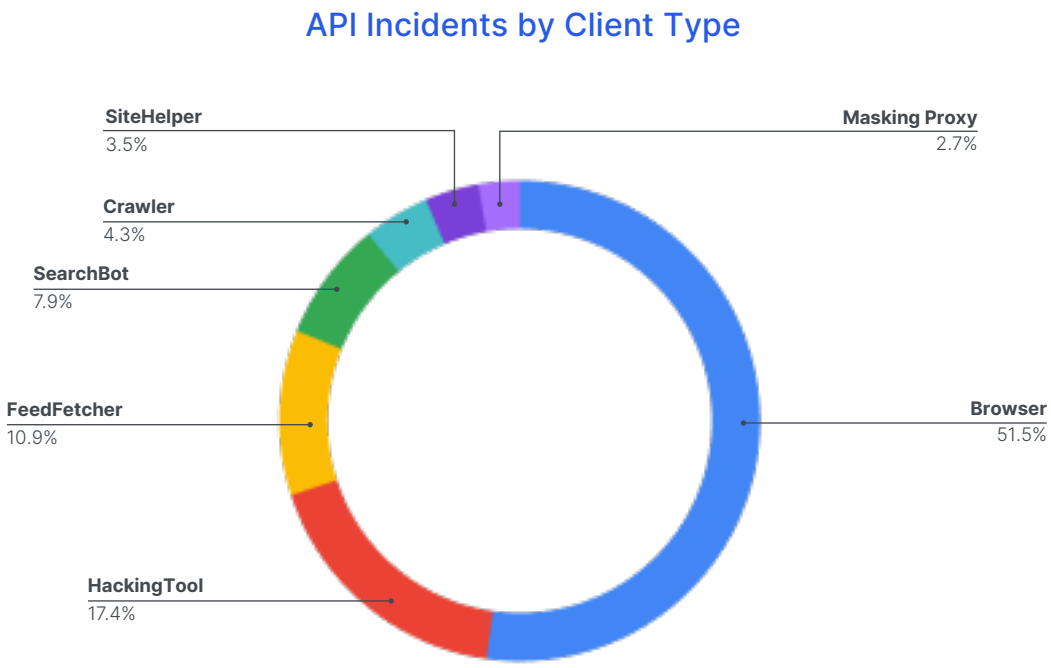
By the same coin, API gateways on their own are not enough to offer APIs the comprehensive coverage they require. API gateways primarily focus on traffic management, authentication, and authorization, but they often lack the depth required to handle the diverse array of security threats that APIs may encounter.

APIs can be targeted in a number of different ways and require a range of protection measures for full coverage. For full comprehensive API protection, a combination of WAF, Advanced Bot Protection, and API Security is the optimal strategy.

APIs are Easy Targets

API Incidents by Client Type

The data below displays the top 50 incidents by client type in mitigated API attacks against Imperva customer sites over the last 12 months.



Overwhelmingly, the browser stands out as the top client type leveraged in more than half of all attacks targeting APIs. Browsers are universally accessible, making them a common tool for both legitimate users and attackers and expanding the attack surface. There are several contributory factors as to why browsers feature so significantly in API attacks:

Browser Vulnerabilities: The widespread accessibility of browsers, combined with their ease of manipulation using scripts and automated tools, poses a heightened risk for API security. Cybercriminals can exploit API vulnerabilities by manipulating requests or injecting malicious code through the user interface of web applications, emphasizing the need for robust protective measures. To mitigate this risk, security teams should implement robust monitoring and logging mechanisms for tracking API usage, detecting anomalies, and identifying potential unauthorized access.

Sensitive Information: Browsers store sensitive information like cookies and tokens, which can be hijacked or misused by attackers.

Web-Based Applications: Many APIs are designed to be consumed by web-based applications, which are accessed through browsers.

Application complexity: The complexity of modern web applications can inadvertently introduce security vulnerabilities that are exploitable through browsers.

Front-End Interactions: Browsers handle the front-end interactions of web applications, making them a crucial client type for accessing and utilizing APIs. JavaScript, a widely used scripting language for web development, is executed within browsers and frequently interacts with APIs to fetch or send data without requiring page reloads.

User-Facing Applications: Browsers are the primary client type for end-users who access web applications. Cyber attackers will often target APIs through browsers to compromise user accounts, steal sensitive information, or execute malicious activities, as it provides a direct route to the end-users.

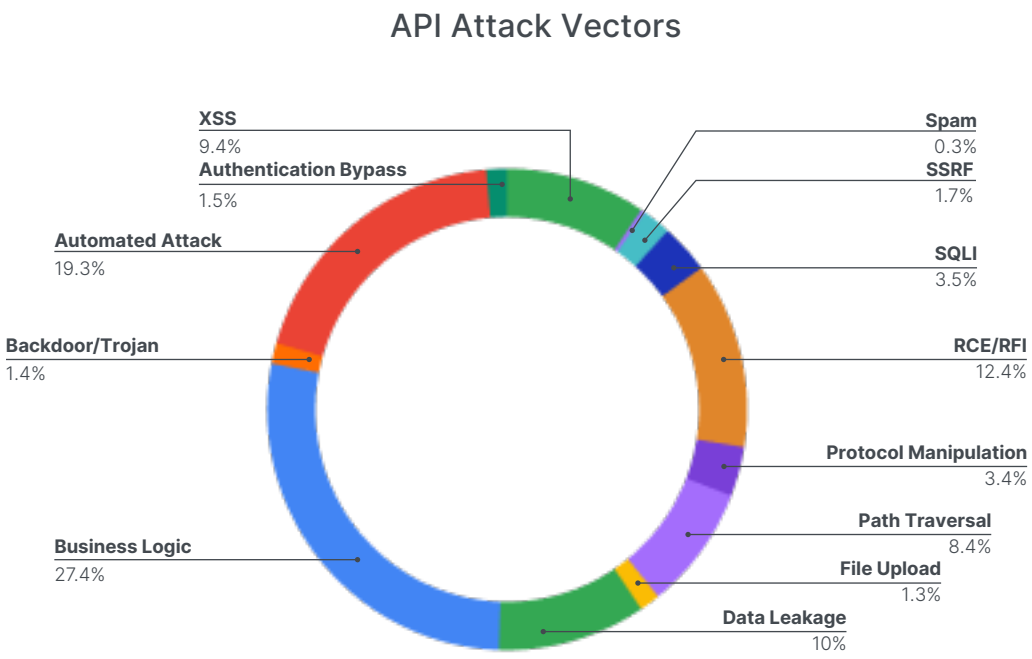
Client-Side Security Challenges: Browsers face inherent security challenges, such as the Same Origin Policy limitations and Cross-Site Scripting (XSS) vulnerabilities, which attackers may exploit to manipulate API requests or gain unauthorized access.

Session Management: Web sessions, which are often managed by browsers through cookies or tokens, play a crucial role in API interactions. Cyber attackers may focus on manipulating these sessions to gain unauthorized access to APIs and associated resources.

Due to these factors, cyber incidents targeting APIs often involve browsers as a prominent client type. As a result, organizations need to implement robust security measures, such as proper authentication, authorization mechanisms, and input validation to secure APIs against potential browser-based attacks.

Top Attack Vectors

The chart below illustrates attack vectors used by attackers.



The primary attack category is Business Logic Abuse accounting for over 27% of all API violations mitigated. The next largest category is Automated Attacks (19.3%), followed closely by RCE/RFI (12.4%) and Data Leakage (10%).

We've discussed the challenges associated with Business Logic Abuse and why it's inherently difficult to detect. Automated attack agents empower cybercriminals to execute attacks rapidly and efficiently, enabling them to systematically scan APIs for common vulnerabilities and misconfigurations that can be exploited for malicious purposes.

Remote Code Execution (RCE) and Remote File Inclusion (RFI)

RCE and RFI are popular attack vectors due to the severe consequences they can inflict, including the execution of arbitrary code and the exploitation of server-side vulnerabilities. Successful RCE or RFI attacks may also enable attackers to bypass authentication and authorization mechanisms, granting them unauthorized access to sensitive information or administrative functionalities within the API.

Data Exfiltration or Data Leakage

This is a top attack vector for cybercriminals targeting APIs because of the immense value associated with unauthorized access to sensitive information. APIs often handle and transmit valuable data, including personally identifiable information (PII), financial records, or business-critical data. Cybercriminals are drawn to data leakage attacks as successful exploitation allows them to access, exfiltrate, and potentially monetize this confidential information.

The Risk of Complacency

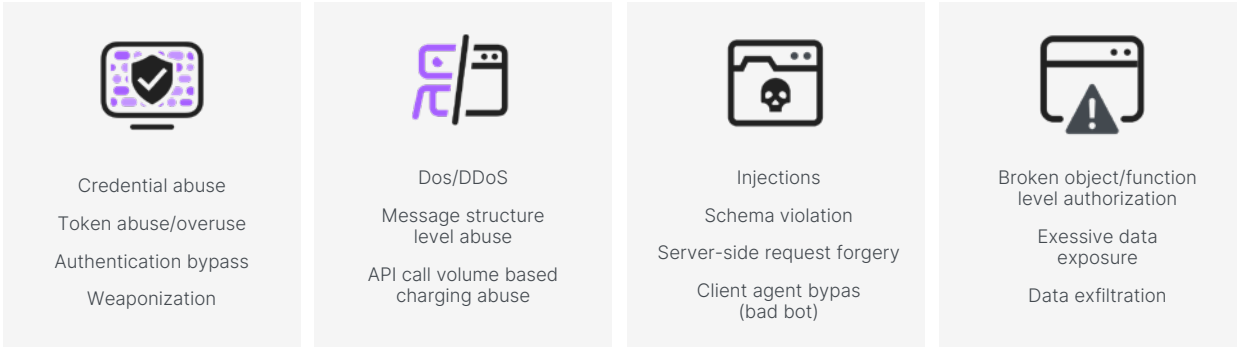
While a Web Application Firewall (WAF) is a vital component of a robust security strategy, it's not enough to protect against all forms of API abuse. Certain API violations can exploit WAF and Bot Protection limitations, necessitating a more API-centric approach to security.

Take Business Logic Abuse, a prominent API attack vector in the past year. Malicious actors employ legitimate automated tools to exploit API design flaws, allowing them to mimic expected behavior and conduct undetected malicious activities such as site scraping, credential stuffing, and data theft. Several threats identified in the OWASP Top 10 for API Security, including BOLA, Mass Assignment, and Excessive Data Exposure, fall into the Business Logic Abuse category.

API risks related to access and authorization controls, even if they appear to conform to rules and resemble valid API calls, cannot be effectively addressed by anti-bot and WAF solutions alone. Mitigating sophisticated API attacks demands additional safeguards, such as Advanced Bot Protection and API Security.

The Different Categories of API Attack Mitigation

Attackers use different attack mechanisms to target different components within the makeup of an API to achieve their malicious objectives. Depending on the attack type, different levels of mitigation are required.



Authentication Abuse

API authentication abuse targets vulnerabilities at the authentication layer, leaving APIs open to credential abuse, authentication bypass, token abuse, or overuse. This type of attack can usually be mitigated by a WAF.

Service Abuse

Another common example of API abuse is Service Abuse which can occur when an API exists in a service provider environment in a call-based charging structure. A Denial of Service (DoS) attack on an API in this environment could result in multiple repeated calls resulting in elevated charges for the services. This type of API abuse can be mitigated with a WAF.

Malicious Requests

Malicious API request attacks target APIs by mimicking normal API requests to infiltrate or manipulate the data or the functionality of an API. Some examples are SQL injection attacks, schema violations, and server-side forgery. These types of API attacks require a combination of WAF and Bot Protection to mitigate.

Business Logic Abuse and Data Theft

Finally, Business Logic Abuse and Data Theft result from a number of API weaknesses, including BOLA, Excessive Data Exposure, or Data Exfiltration, and require advanced API Security capabilities to mitigate.

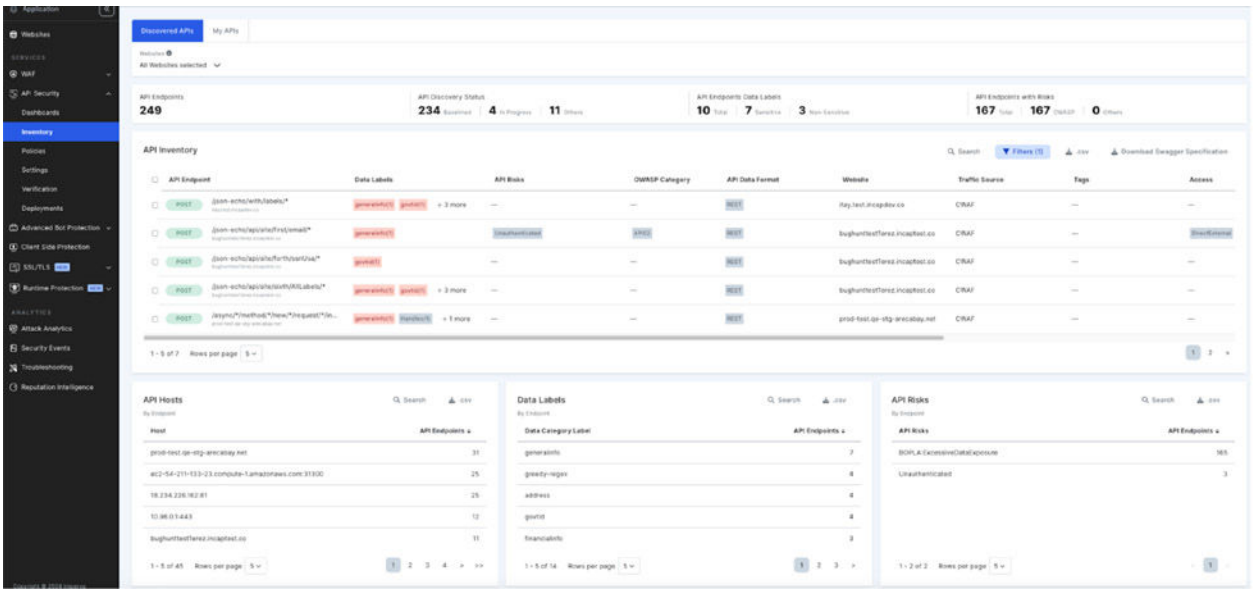
In summary, to adequately protect against API security risks, organizations should adopt an integrated approach that goes beyond relying solely on WAF. Advanced API Security measures, including Advanced Bot Protection, are essential components for addressing the evolving and sophisticated nature of API attacks.

The Importance of API Discovery

A lack of visibility is one of the top API security challenges. Understanding how attackers might exploit APIs to carry out data breaches is essential for implementing robust security measures. Knowing where all your APIs are is the first step. Classifying their risk category and conducting a risk assessment for known API abuse vectors such as Broken Objective Level Authorization (BOLA) is the next step in preventing sensitive data from falling into the wrong hands.

Discovering Sensitive APIs

API Discovery scans your entire application infrastructure to identify every API in your ecosystem.



It also leverages ongoing API endpoint discovery to detect APIs handling sensitive data. It employs personalized data labels for API attributes that are sensitive or crucial to a particular organization by autonomously categorizing Personally Identifiable Information (PII) and Protected Health Information (PHI) using machine learning and heuristics. Additionally, customers have the flexibility to incorporate their own custom data types through regular expressions or parameter names.

API Security Options

Specialized API Security Solutions

Specialized API Security vendors offer effective solutions focused on identifying and implementing targeted security measures against API attacks. However, relying solely on API-specific defenses may leave vulnerabilities unaddressed. A more robust API Security approach integrates with a comprehensive set of application security solutions, including a Web Application Firewall (WAF), Advanced Bot Protection, and API Security. This integrated approach enhances the capability to identify and thwart reconnaissance attacks, such as injection attacks. By doing so, it can potentially disrupt attackers' progress in exploiting APIs and compromising sensitive data. In summary, adopting a holistic application security strategy that combines API-specific measures with broader defenses is crucial for more effective protection against evolving threats.

API Gateways

API Gateways enable businesses to rapidly deploy APIs and act as a single point of control to route API calls efficiently. They also provide means for implementing business logic use cases, such as metering API consumption rates to help organizations monetize or manage how much API is consumed.

However, API Gateways do not provide the ability to actively inspect payloads to detect security anomalies that may constitute an attack that exploits vulnerabilities in OWASP API Top 10. Therefore, organizations must ensure that in addition to having an API Gateway, there is adequate protection through a WAAP (Web Applications & APIs) to ascertain the full security of the API endpoints.

Comprehensive API Security Protection

API threats are sophisticated and often transcend traditional application vulnerabilities. Consequently, relying solely on conventional application firewalls proves insufficient for addressing API vulnerabilities. A more effective and comprehensive solution involves integrating security tech stacks that include API Security, WAF, Bot Protection, and DDoS Protection. This approach ensures a holistic strategy for detecting and remediating threats to exposed APIs, considering the multifaceted nature of the risks involved.

In Summary

In conclusion, proactively securing APIs is crucial for organizations, with the biggest challenge being the threat posed by malicious bots. The recommendations provide a strategic guide to strengthen API security effectively. Begin with a thorough discovery process, continually updating the API inventory to address risks. Prioritize protection for sensitive APIs through targeted risk assessments and establish a robust monitoring system for active threat detection. Adopt a holistic API security approach, integrating WAF, API Protection, DDoS prevention, and Bot Protection. Embracing these measures is vital for organizations to navigate challenges, safeguard data, and enhance resilience, particularly against the prevalent threat of bad bots in the API security landscape.

API Security Recommendations

Here are some tips to improve your API Security posture for the year ahead.

- Discover, classify, and inventory all APIs, endpoints, parameters, and payloads. Use continuous discovery to maintain an always up-to-date API inventory and disclose exposure of sensitive data.
- Identify and protect sensitive and high-risk APIs. Perform risk assessments specifically targeting API endpoints vulnerable to Broken Authorization and Authentication as well as Excessive Data Exposure.
- Establish a robust monitoring system for API endpoints to detect and analyze suspicious behaviors and access patterns actively.
- Adopt an API Security approach that integrates Web Application Firewall (WAF), API Protection, Distributed Denial of Service (DDoS) prevention, and Bot Protection. A comprehensive range of mitigation options offers flexibility and advanced protection against increasingly sophisticated API attacks.

About Imperva

Imperva is the cybersecurity leader whose mission is to help organizations protect their data and all paths to it. Customers around the world trust Imperva to protect their applications, data, and websites from cyber attacks. With an integrated approach combining edge, application security, and data security, Imperva protects companies through all stages of their digital journey. The Imperva Threat Research team and our global intelligence community enable Imperva to stay ahead of the threat landscape and seamlessly integrate the latest security, privacy, and compliance expertise into our solutions.