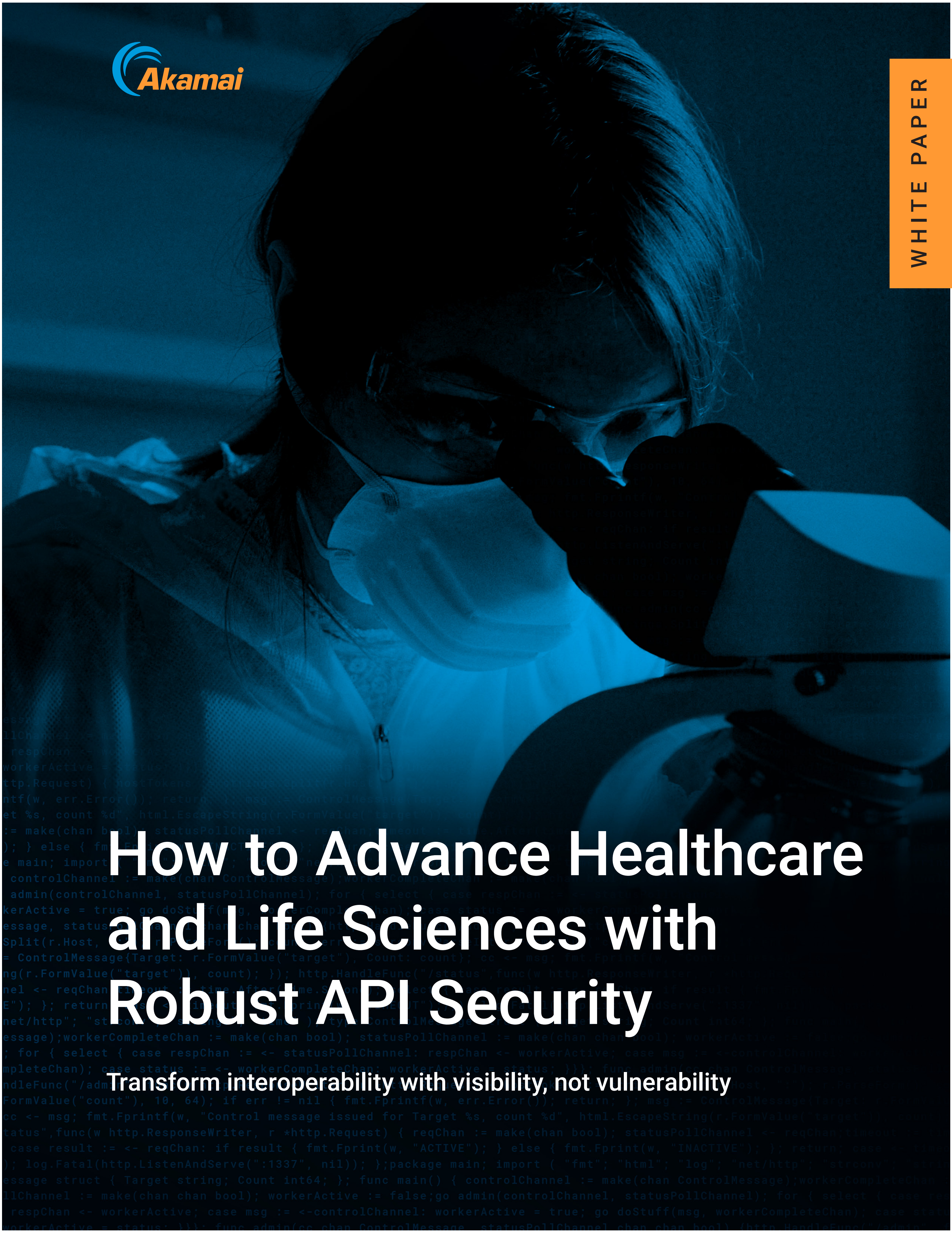
WHITE PAPER



How to Advance Healthcare and Life Sciences with Robust API Security

Transform interoperability with visibility, not vulnerability

Executive summary

From sharing population health data to remote patient monitoring, data exchange between payers and providers facilitated by electronic health record (EHR) systems, and the expansion of the Internet of Medical Things (IoMT), healthcare's digitization is increasing rapidly.

What's the linchpin that's holding together this complicated ecosystem of providers and payers, healthcare IT (HCIT), and life sciences organizations? Application programming interfaces (APIs). APIs play a crucial role behind the scenes, powering applications and facilitating data exchange and aggregation across multiple, disparate systems. According to the U.S. Office of the National Coordinator for Health Information Technology (ONC):

- 9 in 10 hospitals use APIs to enable apps to grant patient access to EHR data, and 6 in 10 hospitals use APIs to allow patients to submit data through apps
- More than two-thirds of hospitals reported using a Health Level Seven (HL7) Fast Healthcare Interoperability Resource (FHIR) API to enable patient access to data in 2022, an increase of 12% from the prior year
- 4 in 5 hospitals use APIs to enable apps to write data to EHR systems, and 4 in 5 use APIs to read EHR data; 50% use APIs to enable apps to read non-EHR data

But as the healthcare ecosystem harnesses APIs for good — to create better patient experiences and access, streamline operations, and gain a business edge in the digital age – ecosystem players may unwittingly increase their vulnerabilities. Though essential, APIs are often implemented in an unsecure manner. Misconfigurations and poor security deployments by application developers and aggregators that are handling vast volumes of patient and financial data can introduce critical blind spots.

Consider that 78% of healthcare organizations experienced an API security incident between September 2022 and September 2023. Moreover, 55% reported a productivity loss following an incident. **In 2023, healthcare data breaches more than doubled compared with 2022,** and they're predicted to increase. Such exposure is accompanied by the risks of compliance violations and system downtime, which can lead to patient care challenges.

29%

of all web attacks targeted APIs in 2023.

— Akamai State of the Internet (SOTI) Report, March 2024

SOTI

V10 ISSUE 01

Lurking in the Shadows

Attack Trends Shine Light on API Threats

Akamai

State of the Internet/Security

The evolution of APIs in healthcare

The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 established baseline standards for EHR use and data practices in healthcare. But it wasn't until more recently — in 2022, when the provisions of the 21st Century Cures Act granted patients ownership of and unrestricted access to their full health records in electronic format — that healthcare organizations entered a new era of interoperability standards driven by FHIR APIs. Although this evolution is driven in part by regulation, there are myriad clinical and financial use cases to support the technical (and, in many ways, cultural) transition (Figure 1). Data sharing can reduce duplicative medical services, reduce medication interference, and enhance the customization and capabilities of providers' EHRs (such as ingesting remote patient monitoring data, for instance).

APIs in healthcare

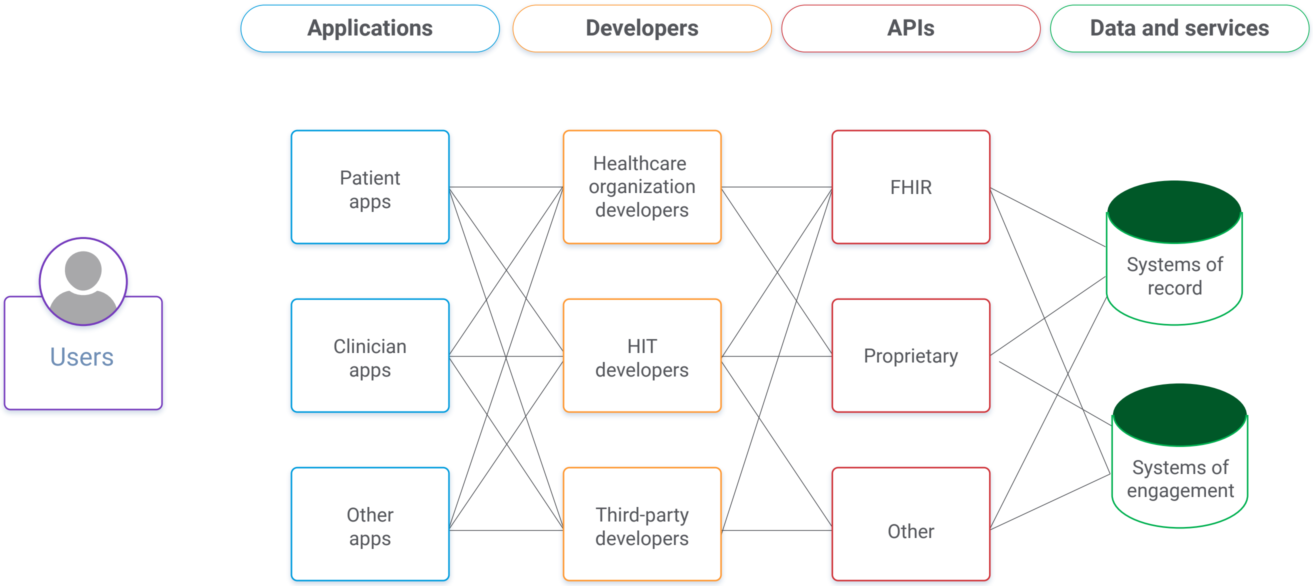


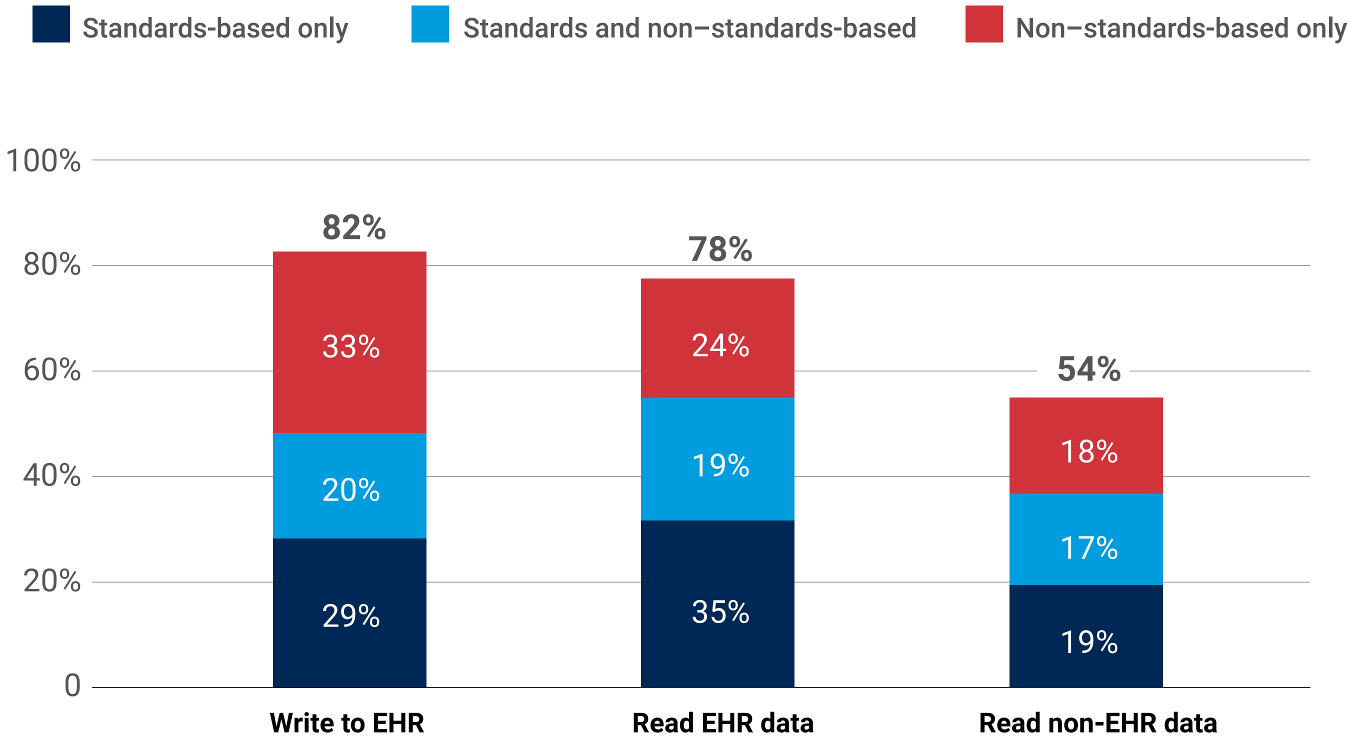
Fig. 1: API use in healthcare

The main challenge, however? Although there may be a growing acceptance of APIs as a new standard, there may also be a lack of translating additional endpoints to new potential exposure points. That becomes even more complex given the volume of proprietary APIs across the healthcare ecosystem.

The American Hospital Association and the ONC shared findings in 2023 about the percentage of all nonfederal acute care hospitals that reported using APIs to exchange data with apps (Figure 2). Overwhelmingly, these hospitals used a hybrid standards-based and non-standards–based approach to APIs — or even non-standards–based only — to write to EHRs, read EHR data, and read non-EHR data.

Given a lack of both human and fiduciary capital in healthcare, this transition to standardization will perhaps be most inspired by laws that promote digitization and by well-resourced organizations that are anticipating future compliance requirements.

The groundwork for this is the Trusted Exchange Framework and Common Agreement (TEFCA). TEFCA promises to create a centralized framework for national interoperability, to reduce dependence on legacy and regional exchanges, and to establish FHIR APIs as the standard.



Note: Percentages are calculated among non-federal acute care hospitals with inpatient or outpatient sites.

Fig. 2: Percentage of all nonfederal acute care hospitals that reported using APIs to exchange data with apps (Source: 2022 AHA Annual Survey Information Technology Supplement)

Compliance concerns

Healthcare and life sciences organizations traditionally focus on north-south traffic (command and control and exfiltration). **However, APIs expose core business functions via east-west traffic, which introduces the possibility of lateral movement in the case of a successful attack.** Even if partners are compliant with regulations like the Health Insurance Portability and Accountability Act and the System and Organizations Controls 2, connections among partners and network traffic create exposure points. That means Individual system compliance is not enough. Healthcare organizations need the ability to analyze both network (east-west) and partner (north-south) traffic for full visibility.

In the context of accepted API traffic, allowlisted traffic can bypass web application and API protection (WAAP) or API gateway controls, potentially exposing poorly configured rogue APIs to the internet without undergoing scrutiny. Internal east-west API traffic also circumvents these controls. API security addresses these challenges by collecting API activity data from any WAAP or gateway and sending it to a centralized data lake for comprehensive monitoring. It operates like a traffic camera by recording all API activity and performing behavioral analyses to enhance security measures.

From January 1, 2023, through November 30, 2023,

115,705,433

healthcare records were exposed or compromised — more than the combined total for 2021 and 2022.

—The HIPAA Journal

Healthcare's already vulnerable landscape

John Riggi, the National Cybersecurity Advisor for the American Hospital Association, noted that 2023 was a record-setting year **for cyberattacks targeting healthcare organizations**. Hacking and ransomware — primary and growing cyberthreats in healthcare — have resulted in 239% and 278% increases, respectively, in large breaches over the past four years. In 2023, hacking accounted for 77% of large breaches (defined by ONC as more than 500 patient records).

In fact, according to Akamai data, **daily web application and API attacks against the healthcare industry rose significantly in 2023** (Figure 3). The data includes the broader ecosystem of payers, providers, pharmaceutical and life sciences organizations, and HCIT companies.

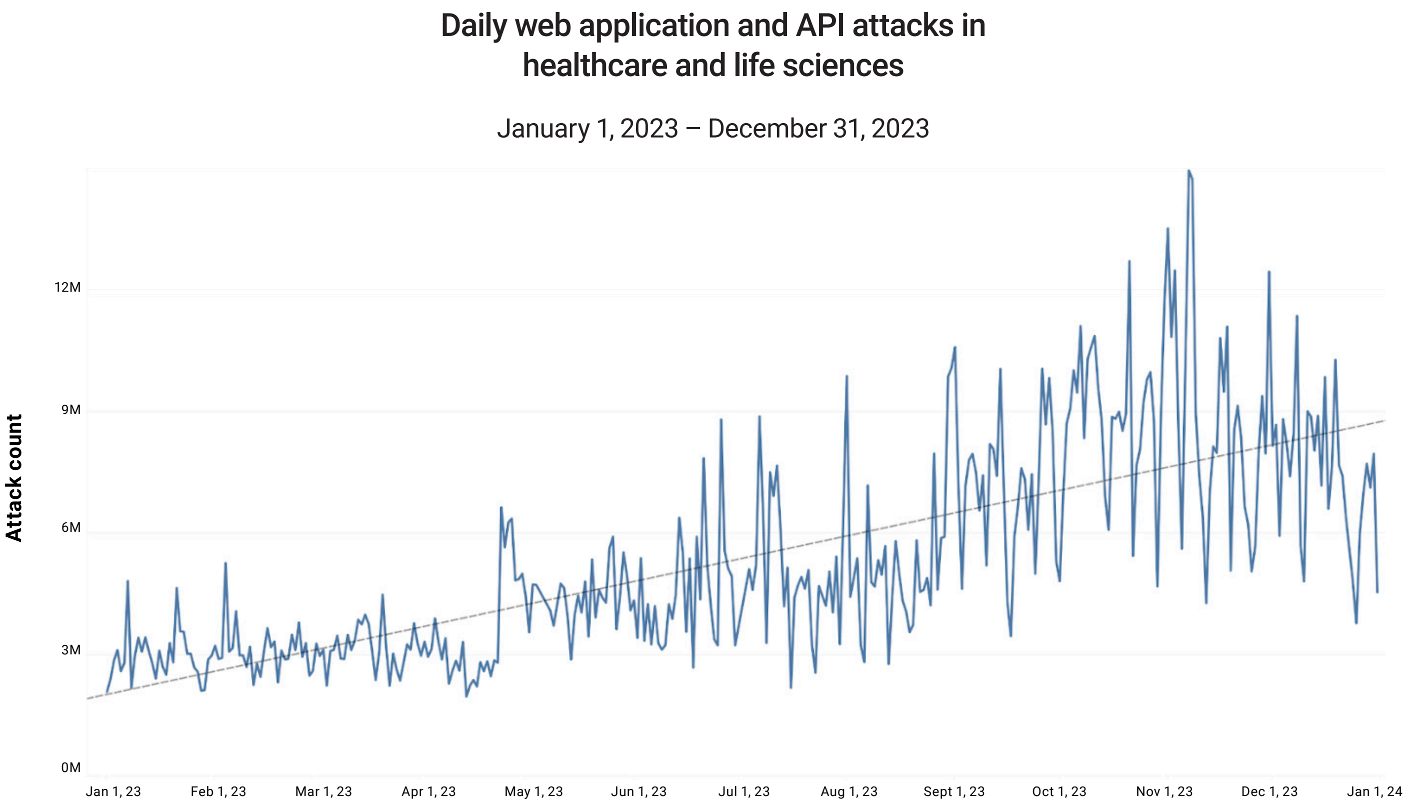


Fig. 3: Web application and API attacks on the healthcare industry show steady activity and a growing number of attacks per day (Source: Akamai)

Cybercriminals target medical data

APIs are frequently targeted for the data they provide access to, with personal health information being one of the most valuable datasets on the dark web. These records sell for up to US$1,000 each, versus an average of US$1 for Social Security numbers.

For healthcare organizations, the average cost of a data breach is the highest of any industry — and continues to climb. Healthcare experienced the highest average cost of any industry for the 13th consecutive year — US$11 million — a figure that takes into consideration detection isolation, notification, postbreach response, and lost business costs. But there's no turning back in this API-powered ecosystem, which is increasingly complex due to the expansion of IoMT.

Though highly beneficial to patients, IoMT assets such as MRI machines, insulin pumps, and wearables have elevated cybersecurity risks. Healthcare organizations are already challenged to secure their perimeter because of healthcare ecosystem complexity, vulnerable legacy technology, and IT and cybersecurity staffing issues. Additionally, timely patching in this environment can be a Herculean task. With updates coming from various vendors for multiple systems or applications, patching is extremely challenging to implement and track.

Unpatched IoMT devices are some of the most vulnerable assets across all industries, and they can introduce more nefarious threats like ransomware. As IoMT grows exponentially — and with it, the use of APIs — the vulnerabilities also grow, and they can be abused or potentially become pathways for attackers to gain a foothold in their targets. A joint report by Cynerio and Ponemon Institute revealed that **more than half of the hospitals and healthcare systems surveyed in the United States experienced cyberattacks as a result of security gaps in IoMT devices.**

Although Congress introduced the Protecting and Transforming Cyber Healthcare (PATCH) Act with an eye toward ensuring that digital health tools meet strict cybersecurity guidelines. The legislation's strongest regulations concern imposing cybersecurity requirements on manufacturers who have applied for premarket approval through the Food and Drug Administration after September 2023. But older and outdated systems are still vulnerable to breaches and it is more difficult to protect them and gain visibility into them.

Ponemon Institute's report found that 45% of health IT leaders believe attacks involving IoT/IoMT devices had an adverse impact on patient care. Resulting adverse effects on patient care include an increase in the mortality rate (53%) and an increase in complications from medical procedures (28%; Figure 4).

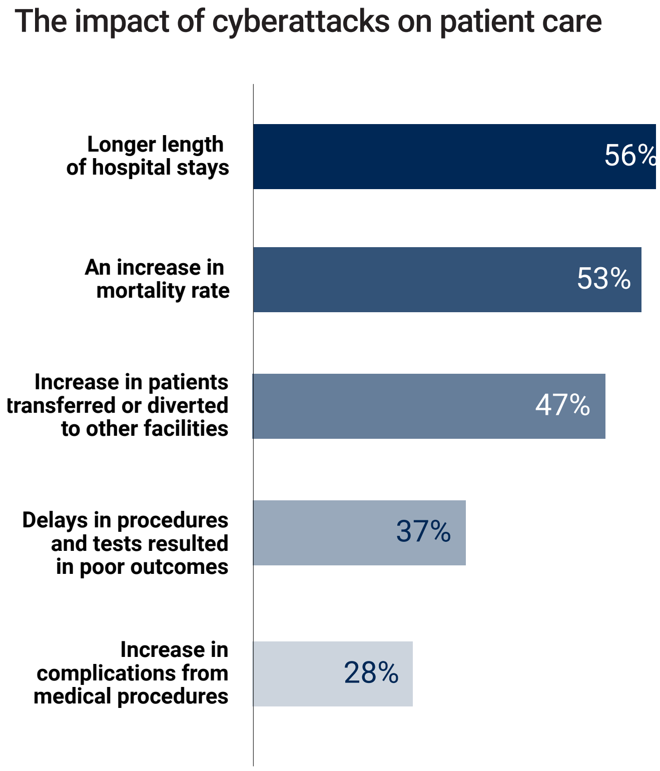
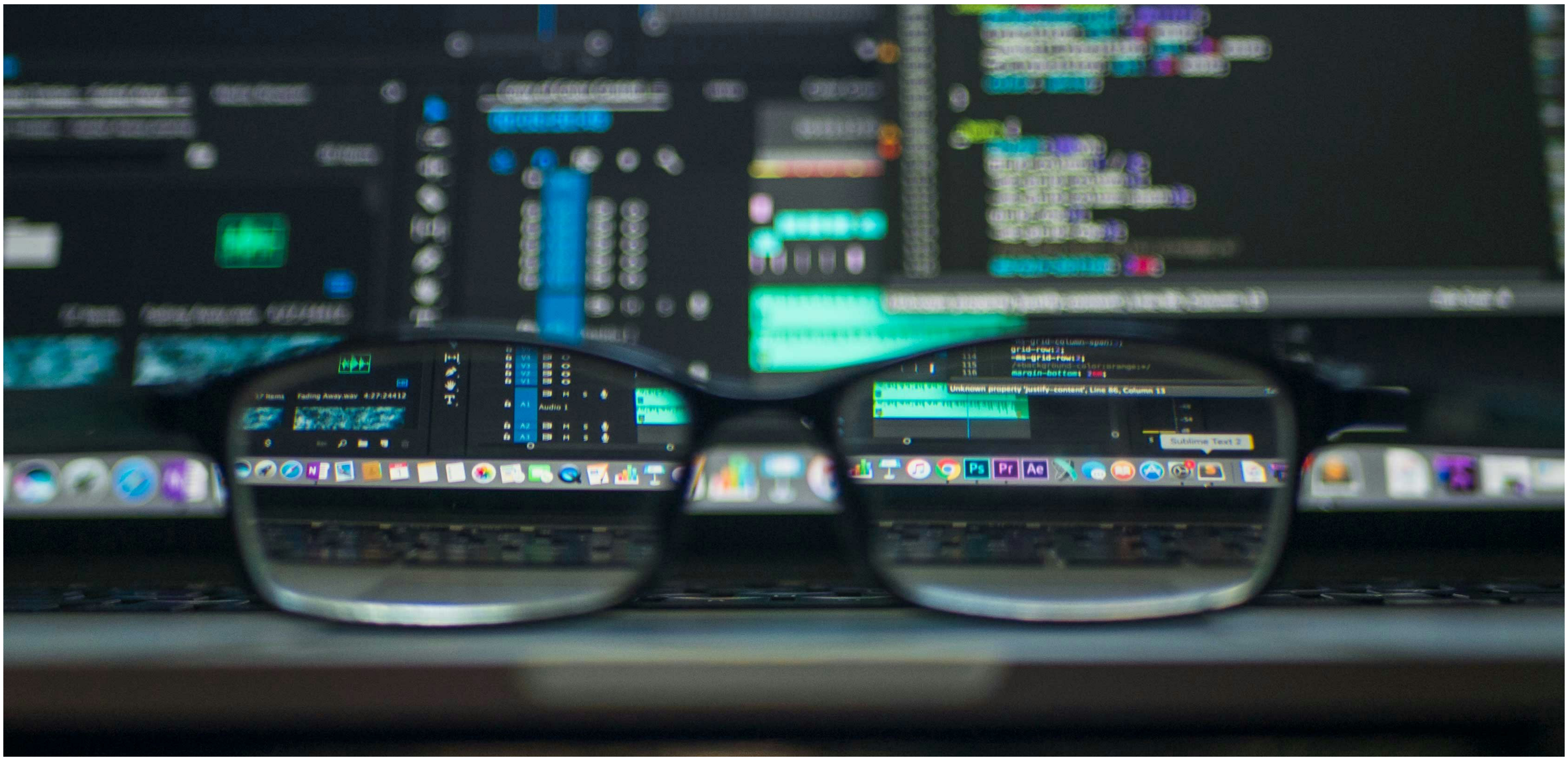


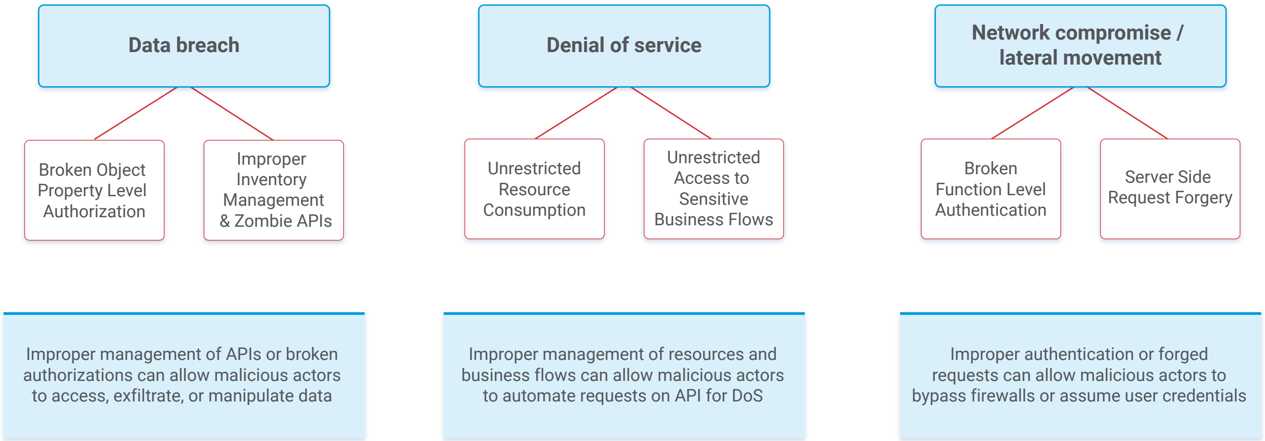
Fig. 4: Examples of adverse effects on patient care due to IoMT vulnerabilities (Source: Ponemon Institute)



API exploits are increasing and evolving

The rising volume of API exploits led to the recent introduction of the Open Web Application Security Project (OWASP) API Security Top 10 (Figure 5). In addition to their surging frequency, attacks are also growing in complexity. Attackers are evolving their techniques and looking for innovative ways to exploit this ever-growing attack surface.

Industry API risks — OWASP API security Top 10, simplified


Data breach
Broken Object Property Level Authorization
Improper Inventory Management & Zombie APIs
Denial of service
Unrestricted Resource Consumption
Unrestricted Access to Sensitive Business Flows
Network compromise / lateral movement
Broken Function Level Authentication
Server Side Request Forgery

Improper management of APIs or broken authorizations can allow malicious actors to access, exfiltrate, or manipulate data

Improper management of resources and business flows can allow malicious actors to automate requests on API for DoS

Improper authentication or forged requests can allow malicious actors to bypass firewalls or assume user credentials

Fig. 5: API risks to the healthcare and life sciences industry include data breaches, denial of service attacks, and network compromise (Source: OWASP Foundation)

Take Broken Object Level Authorization (BOLA), the top-ranked API vulnerability in the latest OWASP API Security Top 10. In this scenario, hackers exploit a flaw in API logic, such as gaps in authentication or authorization controls. Since the attacks resemble legitimate traffic, they are challenging to detect.

Attackers scan for API endpoints vulnerable to BOLA attacks, and — if successful — they can access the information of other users, such as stored personally identifiable information (Figure 6) and even launch denial-of-service (DoS) attacks.

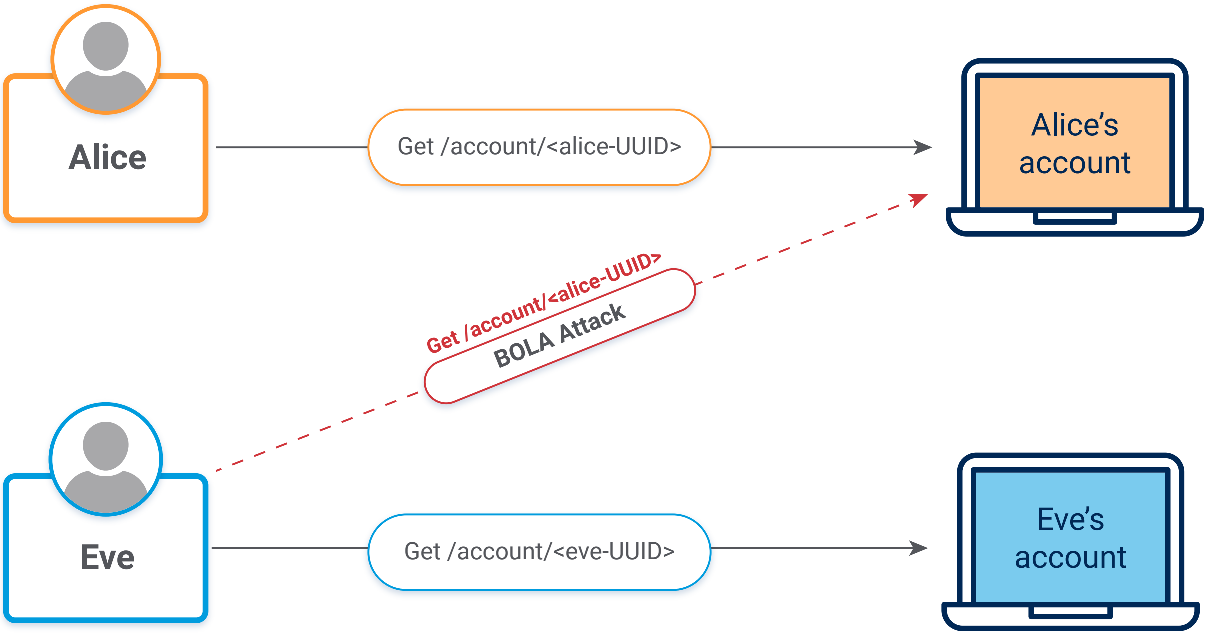


Fig. 6: A normal request versus a BOLA attack

As API-focused attacks shift from those based on transactions (such as Structured Query Language injections) to ones that exploit API business logic, traditional security tools, including web application firewalls (WAFs), fall short (Figure 7). **Although WAFs are important for blocking transaction-based attacks, different solutions are necessary to address business-logic-based attacks.**

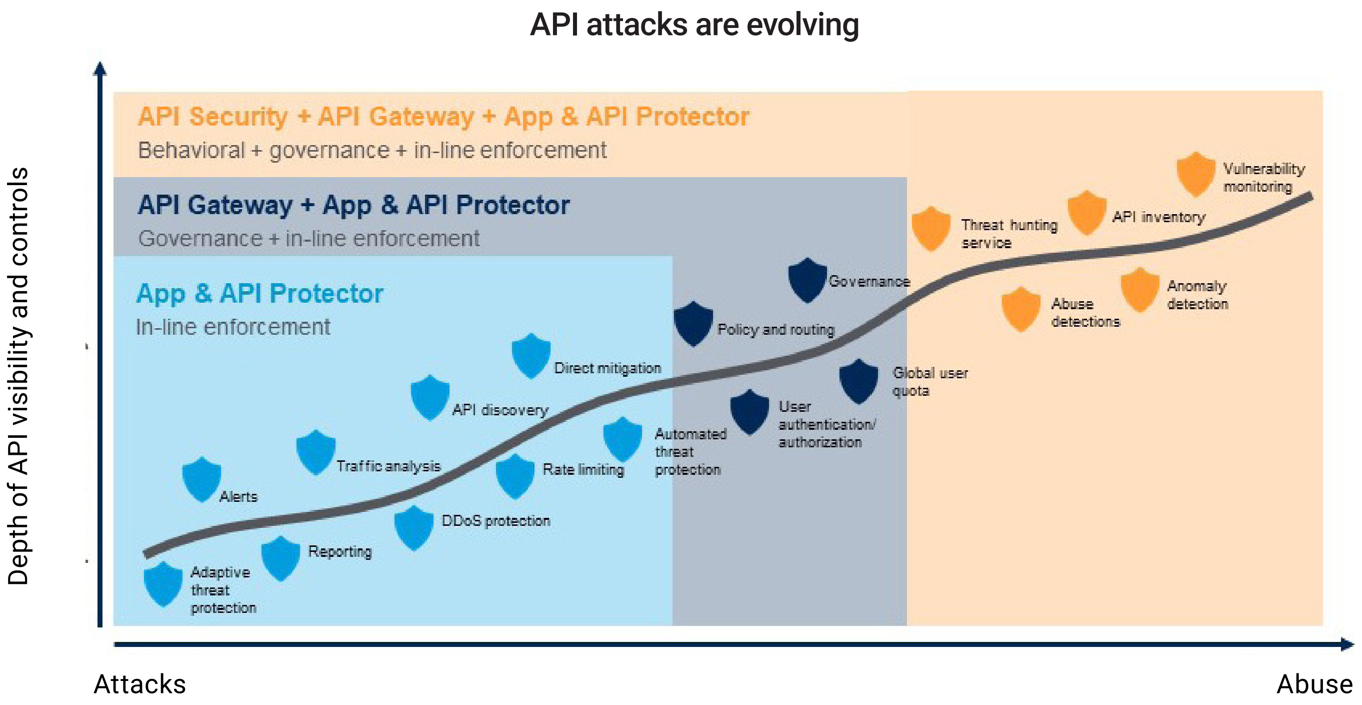


Fig. 7: The continuing evolution of API attacks

Key API security risks

APIs can be vulnerable to a wide range of security risks, which can lead to data breaches, unauthorized access, and other forms of abuse. Key API security risks include shadow and zombie APIs, vulnerable APIs, API abuse, sharing of sensitive information, and credential stuffing attacks.

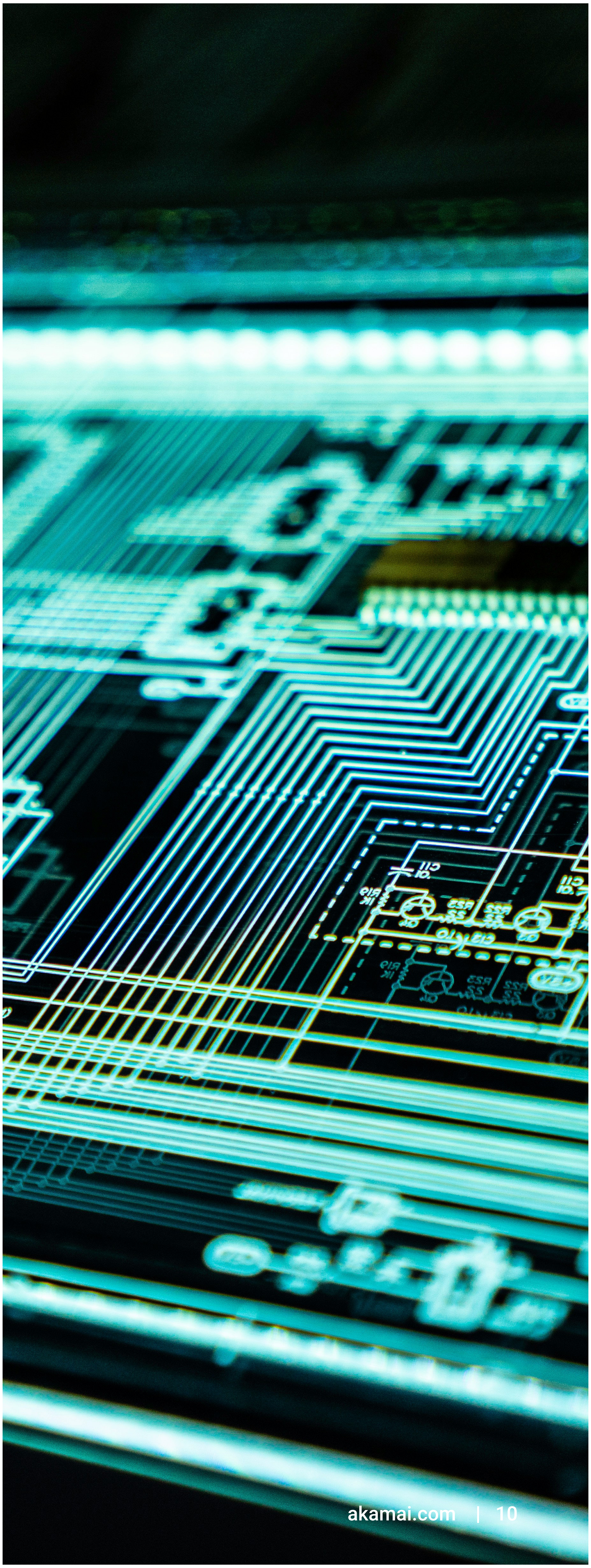
- **Shadow and zombie APIs**. In most healthcare organizations, no one person or team is responsible for managing all APIs. This lack of oversight creates a significant security gap. Discovering and cataloging APIs across the organization is crucial to governing and securing them. It is important to bridge the gap between developers and security teams and detect shadow APIs in their environment. Ongoing discovery keeps you updated about newly discovered APIs or changes to existing ones, which can eliminate shadow APIs.

- **Vulnerable APIs.** Once APIs are discovered, healthcare organizations must assess their risk posture and identify vulnerabilities, especially those carrying sensitive data. This step is vital to prioritizing security efforts effectively.

- **API abuse.** As digitization accelerates, the number of web attacks across North America continues to rise. Threat actors relentlessly target APIs, requiring robust security measures to thwart abuse and misuse.

- **Sharing sensitive information.** Modern apps share sensitive data, which presents a new attack vector. Attackers can intercept traffic and gain unauthorized access to this information.

- **Credential stuffing attacks.** Threat actors are targeting healthcare-related organizations using APIs to automate credential stuffing attacks.



Vulnerabilities across each part of the healthcare and life sciences ecosystem

API vulnerabilities pose unique challenges for the healthcare ecosystem that extend beyond WAAP. These challenges include discovering APIs across diverse landscapes, determining risk posture, understanding normal behavior, and identifying potential abuse.

Providers generally have limitations resource capacities, technical capabilities, funding, risk tolerance, and internal processes to implement APIs, according to the ONC. A lack of visibility into APIs and other robust security measures can lead to successful attacks that compromise the network and risk data breaches and patient safety.

Payers hold financial *and* health data — both highly desirable targets for cybercriminals and at risk of exposure via the Patient Access API, Provider directory API, and payer-provider and payer-payer APIs they are required to maintain. API-enabled attacks can result in service disruptions that impact open enrollment, scraping that disrupts claims operations, costly downtime, and damaged brand reputation.

Pharmaceutical companies increasingly use APIs to enable research and development collaboration, big data, and mergers and acquisitions. No wonder these are three of the biggest threat vectors for cyber theft of intellectual property in life sciences. Additional risks associated with successful attacks include delays to research or trials due to service disruption, regulatory compliance violations, and compromised business operations.

HCIT vendors are often the source of the third-party apps and APIs that enable modern healthcare — and are also viewed as cybersecurity weak points. As a result, cybersecurity thought leaders are increasingly advising that healthcare organizations audit and vet API and HCIT vendors. Data breaches that expose patient data, bad code that causes downtime, and even abuse of "get token" calls to increase rate limits can all damage the reputations and revenue streams of HCIT vendors.

API inventory blind spots

A significant concern across the healthcare ecosystem is the lack of visibility into API ecosystems and the absence of enterprise-wide API inventories. **According to the 2023 SANS survey, API inventory remains a critical issue for healthcare organizations and other leading verticals** (Figure 8). These organizations may not even be aware of all the APIs within their infrastructure, creating a governance and security blind spot.

How accurate do you think your inventory is of APIs in use on your production network at any given time?

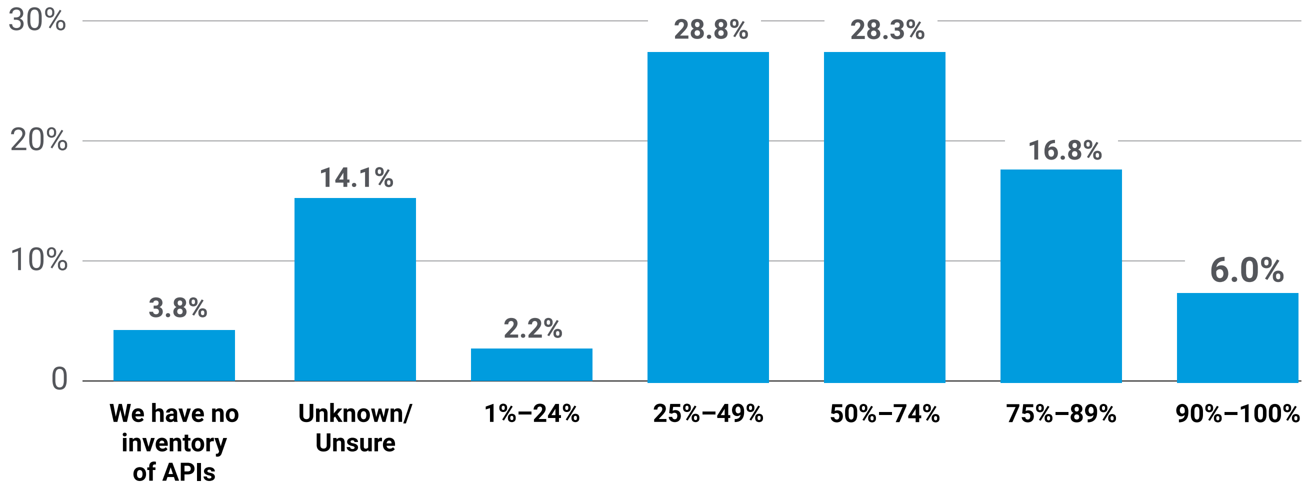


Fig. 8: Most (57.1%) leaders at healthcare, technology, finance, and education organizations reported API inventory accuracy of between 25% and 75%, with 20% reporting under 25%, and 23% reporting at least 75% (Source: 2023 SANS Survey on API Security)

This lack of visibility may be one of the key factors that contribute to the fact that API attacks often go undetected and unreported. API gateways — designed primarily for authorization, authentication, and rate limiting — lack advanced detection capabilities.

API sprawl has made it increasingly complex to identify and catalog healthcare APIs. Organizations must prioritize important APIs based on business impact, compliance violations, behavior monitoring, and serious misuse and criminal activity mitigation.

6 steps to building a robust API security strategy

The strategy of preventing API-based attacks by guarding endpoints and checking credentials is no longer enough. Today, a robust API security strategy must include the following six steps.

1. Collaborate with partners

Healthcare and life sciences organizations and their security partners must collaborate closely by aligning people, processes, and technologies to establish a robust defense against API security risks. This collaboration includes development teams, network and security operation teams, identity teams, risk managers, security architects, and legal/compliance teams.

2. Discover and catalog APIs

To bridge the gap between developers and security teams, discovering and cataloging APIs across the organization is crucial. This process allows security engineers to understand the scope of the attack surface and the potential exposure of sensitive information. Ongoing discovery keeps organizations updated about newly discovered APIs or changes to existing ones, which can eliminate shadow and zombie APIs.

3. Test vulnerability and assess risk

Once APIs are discovered, healthcare organizations and ecosystem partners must conduct vulnerability tests and risk assessments to identify and address vulnerabilities in a timely manner. This process should be integrated into API development and upgrade cycles to ensure ongoing security.

4. Implement behavioral detection

API protections are critical components of the overall application security framework. Behavioral detection is a key strategy to prevent vulnerable APIs from being exploited. This approach involves continuous monitoring and analyzing of API behavior to identify potential threats.

5. Prioritize OWASP Top 10 controls

Healthcare organizations should prioritize the 2023 OWASP Top 10 API Security Risks to ensure comprehensive protection (Figure 9). These controls cover the most critical vulnerabilities and attack vectors that affect APIs. Our data validates the OWASP API Security Top 10. The inclusion of API vulnerabilities in the OWASP list seems to indicate a shift away from the heavy focus on web application threats, and brings to the forefront the growing risk of API attacks that organizations need to heed.

OWASP API Top 10 coverage by Akamai

☑ **API1:2023 — Broken Object Level Authorization:** BOLA vulnerabilities can occur when a client's authorization is not properly validated to access specific object IDs.

☑ **API2:2023 — Broken Authentication:** BA refers to broad vulnerabilities in the authentication process, exposing the system to attackers that can exploit these weaknesses to compromise API object protection.

☑ **API3:2023 — Broken Object Property Level Authorization:** BOPLA is a security flaw where an API endpoint unnecessarily exposes more data properties than required for its function, neglecting the principle of least privilege.

☑ **API4:2023 — Unrestricted Resource Consumption:** This is a type of vulnerability, sometimes called API resource exhaustion, where APIs do not limit the number of requests or the volume of data they serve within a given time.

☑ **API5:2023 — Broken Function Level Authorization:** BFLA can occur when access control models for API endpoints are incorrectly implemented.

☑ **API6:2023 — Unrestricted Access to Sensitive Business Flows:** This risk arises when an API exposes critical operations like business logic without sufficient access control.

☑ **API7:2023 — Server Side Request Forgery:** SSRF allows an attacker to induce the server-side application to make HTTPS requests to an arbitrary domain of the attacker's choosing.

☑ **API8:2023 — Security Misconfiguration:** This refers to the improper setup of security controls, which can leave a system vulnerable to attacks.

☑ **API9:2023 — Improper Inventory Management:** This is a challenge for every organization managing APIs. API security solutions can protect known APIs, but unknown APIs — including deprecated, legacy, and/or outdated APIs — may be left unpatched and vulnerable to attack.

☑ **API10:2023 — Unsafe Consumption of APIs:** This refers to the risks associated with the use of third-party APIs without putting proper security measures in place.

Fig. 9: The 2023 OWASP Top 10 API Security Risks include more API-specific attacks and emphasize authorization issues (four of the top five attacks)

6. Learn from peers

Healthcare-related organizations can learn from their peers and share best practices. Membership in the Health information Sharing and Analysis Center (H-ISAC) provides the advantages of their intel platform, resources, and trusted peer-to-peer network of experts to help anticipate, mitigate, and respond to cyberthreats. A clear understanding of how other organizations address API security challenges can help enhance security measures for the industry as a whole.

Conclusion

In this era of rapid digital transformation and widespread API adoption — which was designed to facilitate flexible, swift, and cost-effective integration across a wide spectrum of software, devices, and data sources — safeguarding APIs is of paramount importance for healthcare organizations. Nonetheless, API security presents a complex juggling act, involving various features, functions, and demands of the business. Neglecting API security can lead to severe consequences, including cyberattacks, data breaches, regulatory infractions, damage to an organization's reputation, and even loss of life.

Enable secure, API-powered innovation

Our data indicates that API functionality ranks among the top targets for threat actors who continuously evolve and adapt their methods of attack. Therefore, it is imperative that API security shifts toward the edge, moving away from an organization's infrastructure and closer to the digital touchpoints where patients and partners engage with data and applications. This strategic adjustment is crucial to ensuring robust protection for digital assets.

Learn more about Akamai for healthcare and life sciences