noname

In collaboration with Opinion matters

The API Security Disconnect

Research from Noname Security on API Security Trends in 2023

In this report

Introduction

Twelve months on from Noname Security's first survey and we can see that APIs continue to pose significant risk to businesses around the world. 2023 is the year when these risks are becoming so apparent that companies can no longer ignore them. For any business looking to design and execute an API security strategy in 2023, it's essential they understand the key trends, top API attack vectors and operational risks.

In our inaugural report: *The API Disconnect – API Security Trends in 2022*, we found that 76% of respondents suffered an API security incident in 2022. This highlighted that breaches continue to occur despite a growing understanding of API security.

Fast forward to 2023 and the ongoing move to cloud-native applications continues to expose both infrastructure and APIs. As a result, we have seen an increase in the number of API security incidents.

It is therefore becoming apparent that in such a vulnerable, uncertain, and increasingly regulated environment there is now a critical requirement for proper API security that can discover, monitor, and predict vulnerabilities. It is paramount that organizations can actively test and fix issues before they spread through the entire network.

With this in mind, have we moved the needle on API security? Where are we now in terms of attack vectors, approaches, and attitudes to risk? Read this report to understand how CISOs, developers and senior cybersecurity professionals are approaching the challenge of securing their APIs in a complex and intense threat environment.

Methodology

API security pioneer, Noname Security, commissioned its second annual survey on the state of API security testing in May 2023. Undertaken by independent research organization, Opinion Matters, it surveyed a total of 631 respondents, with 327 respondents from UK businesses and 304 from the USA. Role types surveyed included CIOs, CISOs, CTOs, senior security professionals, and AppSec teams working in companies employing 250+ people across six key industry sectors: financial services, retail and eCommerce, healthcare, government and public sector, manufacturing, and energy and utilities.

Foreword

APIs are indispensable in today's modern enterprise environment

The continuing increase in reported API security incidents over the two years that we have conducted this research demonstrates that this is not a fleeting trend but a pressing reality that organizations must deal with and prioritize.

A report written by the business advisory group, McKinsey, predicts that the number of threats that organizations and business technology leaders face will continue to rise. By 2025 there will have been a 300% increase in damages to enterprises from cybercrime when compared to the levels of 2015. Everyone is worried about ransomware, phishing attacks, and data breaches and this research validates why security leaders must prioritize API security.

Today every modern enterprise is heavily reliant on APIs, to the point that they are now indispensable. APIs are the tools that allow enterprises to connect with their ecosystem of partners and customers, while inspiring innovation, improving existing services, and enabling organizations to work more efficiently. This is why we were pleased to see that 81% of businesses surveyed said that they have prioritized API security more in the last 12 months.

However, unfortunately, vulnerabilities in infrastructure have huge consequences. Over half of our respondents (51%) admitted that the impact of an API security incident has resulted in loss of customer goodwill and churned accounts, with nearly half saying that it had also led to a loss of productivity (48%) and employee goodwill (45%). Unplanned fees were also incurred to help resolve the issue, not to mention the cost and brand damage of being fined by the regulators.

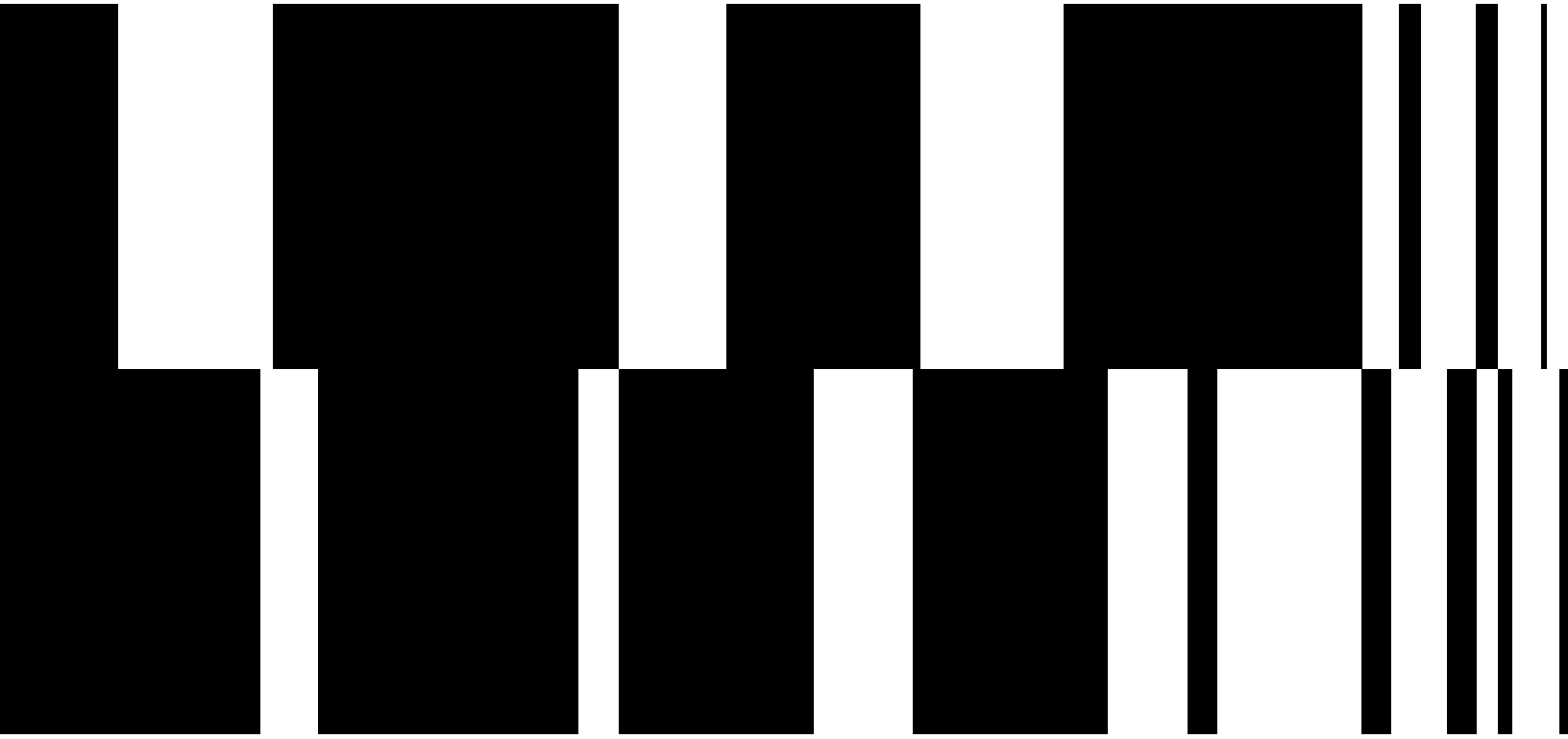
Put simply, as we continue to digitize our businesses, API traffic is growing rapidly, and API attacks are growing at the same pace. API security has become an absolute necessity for enterprises to protect their everyday services, and most importantly, customers' data. However, where real-time API security testing is concerned, while we have seen a slight improvement over the 2022 survey, it is still relatively rare with less than a fifth (18%) of respondents testing in real-time.

All the more surprising then, to see that confidence in API security has shot up to 94%. Again, as last year, we question this misplaced confidence and the disconnect between C-level technology leaders and the AppSec cybersecurity professionals at the coalface. Especially as not only is the intensity of attacks growing, but the sophistication of attacks means they are increasingly harder to find. This disconnect between C-level technology leaders and AppSec teams was identified last year and, if anything, the gap has continued to widen.

With over half of developers (53%) purporting to be spending between 26% and 50% of their time on API refactoring and remediation, and with 14% admitting to spending anywhere between 51% and 75%, how do organizations go about preventing attacks and reducing the risk of successful attacks without having to make changes to production infrastructure? How do they remediate faster while lowering their remediation costs and find and fix issues earlier? And lastly, how do they eliminate bottlenecks and improve security without sacrificing velocity?

These were the catalyst for Noname Security launching the latest iteration of its Active Testing solution in June 2023, to ensure that no API remains untested and to help empower developers to reduce the time they spend on remediation and refactoring and increase their time spent on innovating for their businesses.

We hope you find this research illuminating.



High-level findings

78%

Say they have experienced an API security incident in the last 12 months

81%

Say API security is more of a priority now than it was 12 months ago

53%

Say their developers are spending between 26% and 50% of their time on refactoring and remediation

API Security Incidents Continue to Grow

The growing severity of API security incidents should continue to sound alarm bells. After 2022 results showed that 76% of surveyed respondents experienced an API security incident in the last 12 months, this has unfortunately risen to 78% in 2023. This is further evidence of the API security 'disconnect' that was identified in our inaugural report in 2022.

Visibility of API Inventories Grows, but Gaps Remain

Nearly three-quarters (72%) of respondents have a full inventory of APIs, but of those only 40% have visibility into which return sensitive data. Yes, this represents a year-on-year increase in terms of those that have a full inventory of APIs (67% in 2022), but in this digital era, that is still unacceptable.

If you don't know what APIs you have in your inventory, it is nearly impossible to secure them. Even if you have a full inventory, if you don't know which APIs return sensitive data, it makes it hard to know which to prioritize from a security perspective.

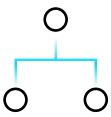
Web Application Firewalls the Primary Attack Vector

With an increase in API visibility comes greater understanding of those 'leaky' APIs that were causing unnecessary problems. As a result, the main API security attack vectors have shifted from Dormant or Zombie APIs, and Authorization Vulnerabilities in 2022, to Web Application Firewalls (WAFs), Network Firewalls, and API Gateways in 2023.

Over a quarter of overall respondents (26%) have identified WAFs as the main attack vector, up from 17% last year, with 20% and 18% of overall respondents citing Network Firewalls and API Gateways as the main threat vector, respectively.

Frequency of API Security Testing is Not Having an Impact

With the prolific number of API security incidents, testing APIs frequently to check for vulnerabilities is increasingly a requirement at many organizations. And the market seems to have noticed. The number of respondents that either test in real-time or undertake daily API security testing has increased from 39% in 2022 to 55% in 2023. However, there is still a gap between the frequency of testing and the number of attacks.

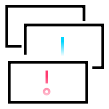


Misplaced Confidence Shows the Disconnect

Whilst the overwhelming majority of respondents (94%) said that they were very or somewhat confident that their current testing tools were capable of testing APIs for vulnerabilities, there is an ongoing lack of correlation between this confidence and the number of API security incidents reported in the last 12 months. Ultimately, surveyed

professionals can have all the confidence in the world, but if the frequency of API security incidents is increasing, something is not clicking within their organizations.

Although like-for-like analysis between 2022 and 2023 confidence is not fully comparable, as our 2022 report assessed confidence in SAST/DAST tools only, there is still a sharp increase in overall net confidence in 2023. This could simply be that confidence has grown as available tools have matured, or that organizations now have the tools to undertake the full scope of API securing testing. However, when looking at the respondents who said they are 'confident' on a more granular basis, over half of respondents (57%) are only 'somewhat' confident – suggesting that there is still work to be done to achieve complete confidence.



The Impact of API Security Incidents is Hitting Home

Overall, the high percentage of respondents saying that they have been impacted in some shape or form by an API security incident (with only 1% saying they haven't been impacted) highlights the real-world consequences that these incidents can have on businesses. This can be financially, reputationally, or when measuring efficiency. More than half (51%) of respondents cited loss of customer goodwill and churned accounts as the biggest impact and cost resulting from an API security incident.

These will undoubtedly resonate with decision-makers as they consider how much resource and budget to put behind protecting their organizations from increasingly sophisticated API security attacks.

API Security is a Priority

81% of survey respondents stated that API security is more of a priority now than it was 12 months ago. More than half of those (53%) surveyed view it as a 'necessary requirement' and 47% say that it is a 'business enabler'.

UK & USA Comparisons

API security has emerged as a key priority for protecting vital data and services. However, it is also an area where many companies lack expertise. With that in mind, we were keen to assess if there were any variations in trends between the two countries surveyed. Responses for the UK and USA were relatively similar in many aspects of the report, but there were a few significant differences.

Fluctuation in the Number of API Security Incidents

The USA has fared better than the UK in the number of API security incidents reported, both in 2023 and in terms of how this fluctuated from one year to the next. 85% of UK respondents admitted they had experienced an API security incident in the last 12 months, a 10% year-on-year increase and higher than the average of 78%. On the other hand, just over two-thirds (69%) of USA respondents in 2023 said they had suffered an API security-related incident in the previous 12 months, down from 77% in 2022.

85% **UK** respondents | 69% **USA** respondents said they had suffered an API security-related incident in the previous 12 months.

Comparing Monitoring and Visibility of APIs

USA-based respondents have greater visibility of the APIs in their inventory, but they struggle to identify which of those return sensitive information when compared with the UK. 74% of USA respondents have a full inventory of their APIs, compared to 70% in the UK. Consequently, a higher percentage of those in the UK report only have a partial inventory of APIs.

However, 28% of UK respondents have a partial inventory, but know which APIs return sensitive data, compared to 19% of those surveyed in the USA. Of those that only have a partial inventory of APIs and do not know which return sensitive data, only 2% in the UK admit this, rising to 7% in the USA. Whilst visibility of APIs within inventories is increasing from one year to the next, with only 66% of UK respondents and 68% in the USA having full inventories of APIs in 2022, the 'visibility gap' is still prevalent one year on from our inaugural report.

API Security Is a Bigger Priority in the UK

84% of UK respondents said that API security is more of a priority compared to 12 months prior, compared to 78% of USA respondents who said this, and nearly one in ten (8%) said that it was less of a priority than it was one year ago.

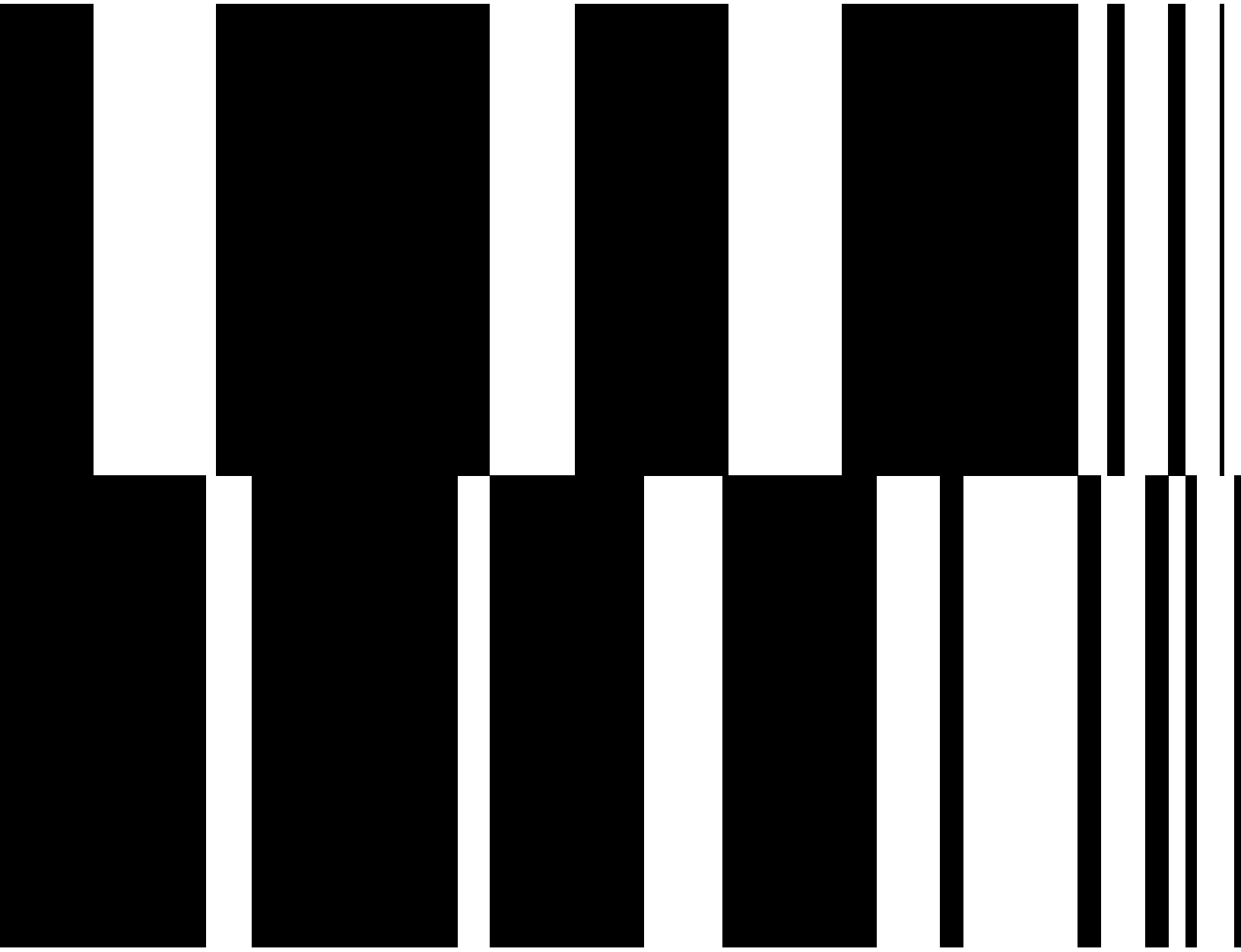
84%
UK
respondents

78%
USA
respondents

said that API security is more of a priority compared to 12 months prior.

USA Turns the Tables on Frequency of Testing

In 2022, 14% of UK respondents undertook API security testing in real-time, whereas this was true for less than one in ten (8%) of those in the USA. Fast forward to 2023, and the UK has slightly increased to 17%, whereas nearly a fifth (19%) of USA respondents now test in real-time.



Vertical Market Overview

Twelve months on from our inaugural report, and many of the familiar external political, economic, technological, and energy-related issues are still having a profound impact. With inflation high, rising redundancies, and economic uncertainty, budgets are increasingly tightening, and decision-makers in these sectors are finding it difficult to dedicate the required time and resources to ensuring resilient cyber defenses, including API security.

Therefore, it is not surprising that of the six verticals that were surveyed in this year's report: financial services, retail and eCommerce, healthcare, government and public sector, manufacturing, and energy and utilities, all but two of these saw an increase in API security incidents when compared with 2022, as per the below breakdown:

Financial services

80% ↑

Increase from 75% in 2022

Retail and eCommerce

79% ↑

Increase from 77% in 2022

Government and public sector

77% ↑

Increase from 75% in 2022

Healthcare

79% ↑

Increase from 70% in 2022

Manufacturing

73% ↓

Decrease from 79% in 2022

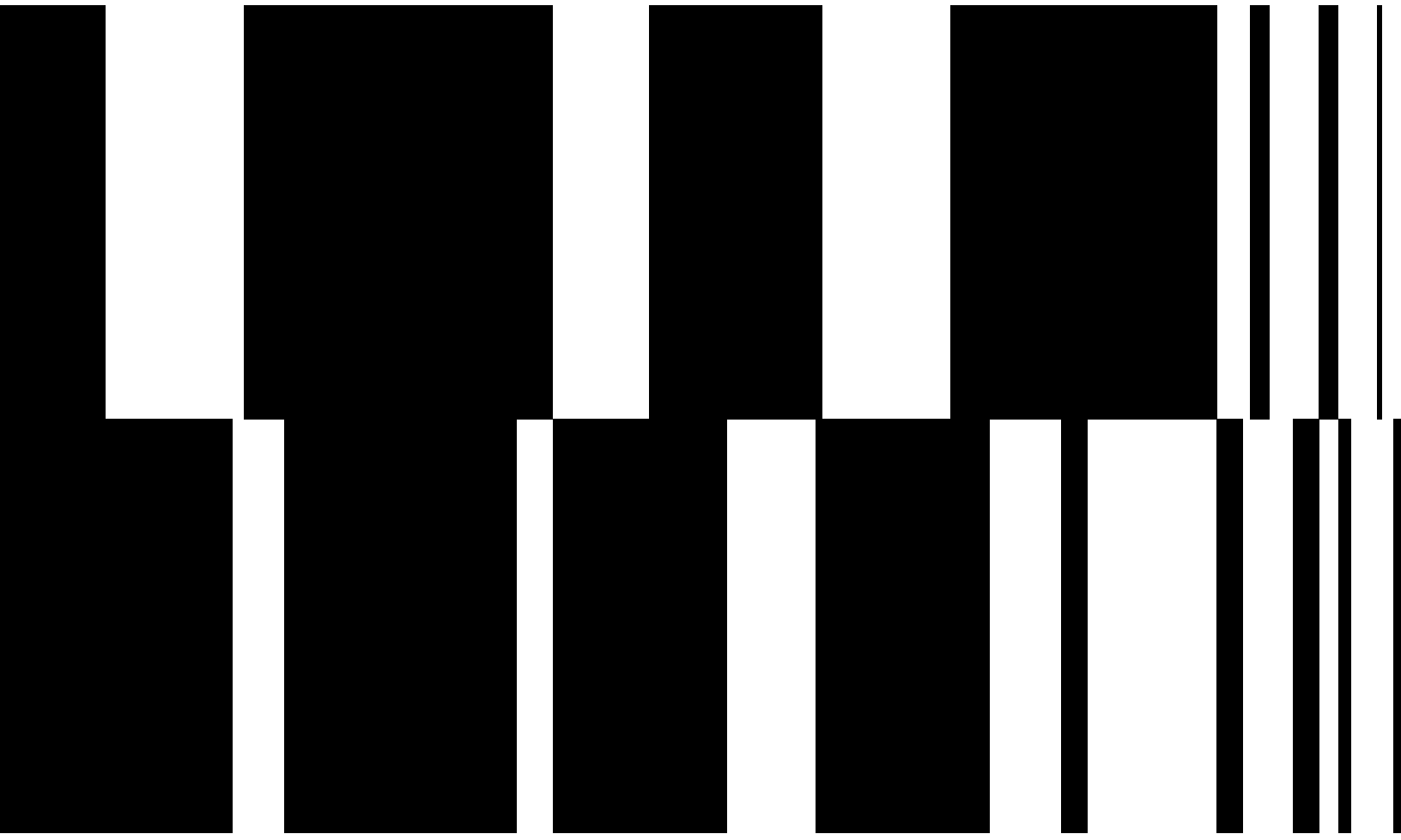
Energy and utilities

78% =

Remained at 78% in 2023

While the frequency of attacks remains relatively high in all sectors, the use of APIs as an attack vector for nation-state-sponsored and independent groups of hackers to access personally identifiable information (PII) has become ever-more appealing. With the amount of PII collected arguably lower in the manufacturing sector ecosystem, it's perhaps no surprise that other verticals have been prioritized as targets, with attempts to steal the 'crown jewels' of data available. It's no surprise then that this is having an increasingly large ripple effect across all aspects of a business and its supply chain, not to mention consumers.

The API security testing disconnect, first revealed in our 2022 research, is evidenced in the gap between real-time testing at least once per day, and the corresponding number of API security incidents. This cadence of testing APIs for vulnerabilities increased in the financial services, retail and eCommerce, healthcare, and energy and utilities sectors, with all but one of these seeing year-on-year increases in the number of security incidents reported.



Role Types and Comparisons

As in Noname Security's 2022 research, our research polled five different job functions: CIOs, CISOs, CTOs, Senior Security Professionals, and AppSec professionals. When analyzing whether organizations had suffered an API security incident, between 73% and 84% of the C-suite and senior security professionals said they had experienced an incident in the last 12 months, yet only 48% of AppSec professionals – at the very heart of the application development lifecycle – said the same.

At the same time, 84% of CTOs said they experienced an API security incident – the highest percentage of any job function and a 4% increase on the number of CTOs who said the same in 2022. This raises questions about how API security incidents have been elevated into the consciousness of the Chief Technical Officer, or whether there is a disconnect and lack of communication between CTOs and AppSec professionals in organizations, the latter of whom are at the coalface dealing with these incidents.

This perceived disconnect extends to the top security attack vectors for APIs, with AppSec teams overwhelmingly citing web application firewalls (64%) as the top security attack vector for APIs, with much more of a spread across other job functions. Furthermore, AppSec professionals have the least amount of confidence in current application testing tools being capable of testing APIs for vulnerabilities, with just 84% saying this, compared to an average of 95% across other job functions.

The disconnect between the number of API security incidents, confidence in existing tools, and what is deemed the biggest threat to API security is exacerbated by 41% of senior security professionals having no idea which APIs return sensitive data. This lack of visibility is concerning, to say the least, for the 76% of senior security professionals who claimed to have up to 500 APIs in their organizations.

Full Questions

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

When asked whether organizations had experienced an API security incident in the last 12 months, more than three quarters of overall respondents (78%) said yes, with 22% saying they hadn't experienced an API security incident. Concerningly, this is higher than the overall figure in the 2022 research with 76% saying yes.

When comparing the UK and USA, there is disparity between those that said yes. 85% of UK respondents admitted they had experienced an API security incident in the last 12 months. This represents a significant increase on those who answered 'Yes' to the same question in 2022, with 75% of UK respondents doing so. This year, 69% of USA respondents said they had experienced an API security incident, down from 77% in 2022.

The first signs of a continuing disconnect between job roles, first revealed in Noname Security's 2022 research, was evident in this question. CTOs were most likely (84%) to say that they had experienced an API security incident in 2023, with AppSec professionals least likely with 48%. In 2022, CISOs were most likely to say they have suffered an API security incident (81%), whilst AppSec professionals were lowest at 53%.

Of the six different industry sectors surveyed in 2023, financial services was the industry most likely to have experienced an API security incident, at 80%, with manufacturing the least likely at 73%. In 2022, manufacturing was the sector most likely to experience an API security incident, at 79%.

What do you believe is the top security attack approach for APIs?

The top three attack approaches cited by respondents were:

	All	UK	USA
Web application firewall	**26%**	**23%**	**30%**
Network firewall	**20%**	**24%**	**17%**
API gateways	**18%**	**17%**	**19%**

Looking at the top attack vectors used to enact API security attacks in 2023, two things are clear.

The first is the growth of web application firewalls as the leading attack vector, with 26% of overall respondents identifying this as the main approach, up from 17% last year. In the UK, 23% identify this as the main vector, whilst in the USA 30% of respondents believe this is the main threat. This is an increase of 8% and 11% in these regions, respectively.

The second is the emergence of network firewalls and API gateways as leading attack vectors, with 20% and 18% of overall respondents citing these, respectively.

In terms of job functions, AppSec professionals were much more likely than those in other roles to say web application firewalls were the leading attack vector (64%), followed by senior security professionals at 39%. This compares to the three C-suite roles surveyed, which scored between 20% and 23% when asked about this attack vector.

When looking at verticals, the top security attack vectors, by each sector, are as follows:

Financial services

26%

Web application firewall

Retail and eCommerce

33%

Web application firewall

Government and public sector

24%

API gateways

Healthcare

27%

Network firewall

Manufacturing

28%

Web application firewall

Energy and utilities

37%

Web application firewall

Do you have a full inventory of your APIs, and do you know which return sensitive data?

When asked if they have a full inventory of their APIs and if they know which return sensitive data, 40% of overall respondents said yes. Whilst this represented a promising increase over 2022 results, when only 26% of respondents said yes, there is still a concerning gap in API visibility, and identifying those that return sensitive data.

	All	UK	USA
Yes (Net)	**72%**	**70%**	**74%**
We have a partial inventory (Net)	**28%**	**30%**	**26%**

70% of UK respondents and 74% of USA respondents said they had a full inventory of APIs. Of this, 34% of UK respondents have a full inventory of APIs, but do not know which return sensitive data, compared to 29% in the USA.

When comparing year-on-year results, the total percentage of overall respondents that had a full inventory increased from 67% in 2022 to 72% in 2023. Concerningly, the percentage of overall respondents that have a partial inventory only decreased from 32% in 2022 to 28% in 2023. Those that have a partial inventory of APIs and know which return sensitive data decreased from 25% in 2022 to 24% in 2023.

In terms of verticals, retail and eCommerce was the most likely to report having a full inventory of APIs, at 76%. However, this sector also scored the highest of the six, when asked whether they have a full inventory, but don't know which APIs return sensitive data (37%). Manufacturing scored highest (33%) in terms of having a partial inventory of APIs.

When analyzing job roles, CISOs scored highest on having a full inventory of APIs at 83%, whilst senior security professionals scored lowest at 59%. 11% of the latter also admitted that they do not have a full inventory of APIs and do not know which return sensitive data.

Based on your API inventory, approximately how many APIs does your organization have in total?

Nearly two-thirds of overall respondents (61%) have between 101-500 APIs in their inventory, with 28% of respondents having between 501-1000 APIs.

Looking at the six sectors surveyed, 70% of healthcare organizations had between 101-500 APIs in their inventory, followed by retail and eCommerce (66%). In the 501-1000 bracket, government and public sector led the way with 37%, followed by financial services at 35%, whilst 4% of energy and utilities organizations had more than 1000 APIs in their inventory.

When looking at job roles, 15% of CIOs claim they have 1-100 APIs, with only 2% of senior security professionals saying this. Conversely, nearly three-quarters (74%) of senior security professionals say they have between 101-500 APIs in their inventory, whilst between 49-62% of the C-suite believe they have this number of APIs.

How often, if at all, do you undertake API security testing for signs of abuse?

	All	UK	USA
In real-time	**18%**	**17%**	**19%**
At least once a day	**37%**	**36%**	**38%**
Less than once a day, up to once a week	**34%**	**36%**	**31%**
Less than once a week, up to once a month	**9%**	**9%**	**9%**
Less regularly than once per month	**2%**	**2%**	**2%**

Overall, just over a third of respondents undertake API security testing at least once per day (37%), with 34% testing less than once a day, but up to once a week. Nearly a fifth (18%) of overall respondents undertake real-time testing, whilst nearly 1-in-10 (9%) test less than once a week, but up to once a month.

When comparing the UK and USA, there is near parity on API security testing, yet the USA undertakes more real-time (19% vs. 17% in the UK) and daily testing (38% vs. 36% in the UK). Consequently, more UK respondents (36%) say they test less than once a day, but up to once a week, compared to 31% in the USA.

Financial services scored highest for testing in real-time with 23%, whilst only 12% of manufacturing respondents do this. Retail and eCommerce and manufacturing respondents led the way (38%) in testing at least once per day, with manufacturing scoring highest in testing less than once per day, but up to once a week (40%). 18% of government and public sector respondents test less than once a week, but up to once a month, whilst energy and utilities were highest in testing less regularly than once per month. This is despite energy and utilities scoring highest when asked if they have more than 1000 APIs in their inventory.

In terms of job roles, AppSec teams scored highest in real-time testing with 28%, whilst CISOs were highest in testing at least once a day with 43%. Forty percent of senior security professionals preferred to test at least once per day.

When compared with 2022 results, more organizations are testing in real-time, and undertaking testing at least once per day. In 2022, 11% of respondents tested in real-time, compared with 18% in 2023, whilst 28% of respondents tested at least once per day in 2022, compared to 37% in 2023.

As a result, the number testing less than once a day, but up to once a week has fallen from 39% in 2022 to 34% in 2023. The number of organizations undertaking API security testing less than once a week, but up to once a month has also fallen from 16% in 2022 to 9% in 2023.

When comparing year-on-year results, the number of overall respondents saying that they test in real-time or at least once per day has, from 2022 to 2023, increased in the financial services, retail and eCommerce, healthcare, and energy and utilities sectors, indicating a greater appetite or heightened level of resources to undertake more frequent API security testing.

How confident are you, if at all, that your current application testing tools are capable of testing APIs for vulnerabilities?

	All	UK	USA
Confident (Net)	**94%**	**94%**	**95%**
Not confident (Net)	**6%**	**6%**	**5%**

The overwhelming majority of overall respondents (94%) said that they were somewhat or very confident that their current testing tools were capable of testing APIs for vulnerabilities. Only 6% of overall respondents were not confident to any degree.

When analyzing job roles, we see the biggest disparity in confidence. Between 93% and 99% of C-suite and senior security professionals were confident in current application testing tools to test APIs for vulnerabilities.

However, only 84% of AppSec teams were confident, with 16% saying they are not confident. This difference could be reflective of the ongoing disconnect between 'frontline teams' and C-level executives, in their perceptions of the state of API security testing.

When analyzing verticals, whilst all sectors were between 91% and 99% net confident in current tools, nearly one in ten (9%) of healthcare respondents were not confident, the highest such percentage of any vertical surveyed.

What costs and/or impacts, if any, have API security incidents had on the business? (Tick all that apply)

	All	UK	USA
Loss of customer goodwill and churned accounts	**51%**	**50%**	**51%**
Fees incurred to help fix the issue	**48%**	**51%**	**45%**
Loss of productivity	**48%**	**49%**	**46%**
Loss of employee goodwill	**45%**	**47%**	**43%**
Fines from regulators	**44%**	**43%**	**45%**

More than half (51%) of respondents cited loss of customer goodwill and churned accounts as the biggest impact and cost resulting from an API security incident. A similar number (48%) incurred additional fees to help fix the issue, whilst loss of productivity (48%), loss of employee goodwill (45%) and regulatory fines (44%) also took their toll on UK and USA organizations.

When comparing the UK and USA, fewer respondents from the USA (45% vs. 51% in the UK) cited the impact of additional fees incurred to fix the issue, and fewer respondents cited loss of productivity (46% vs. 49% in the UK), and loss of employee goodwill and churned accounts (43% vs. 47% in the UK) than the UK.

Looking at each sector, government and public sector scored highest (59%) on loss of customer goodwill and churned accounts, the biggest impact resulting from an API security incident across any industry. The energy and utilities sector scored highest (55%) on fees incurred to help fix the issue, with loss of productivity being the largest concern in healthcare, at 55%. The retail and eCommerce, and energy and utilities sectors were joint highest on loss of employee goodwill at 57%, whilst fines from regulators had the biggest impact in the energy and utilities sector (47%).

When analyzing job roles, senior security professionals scored highest on fees incurred to help fix the issue (55%), perhaps unsurprisingly. The loss of customer goodwill and churned accounts (64%) and loss of employee goodwill (52%) were felt the hardest by AppSec teams, with CIOs citing loss of productivity (51%) as their main impact.

How much more or less of a priority is API security now compared to 12 months ago?

	All	UK	USA
More of a priority than it was 12 months ago	**81%**	**84%**	**78%**
Less of a priority than it was 12 months ago	**5%**	**3%**	**8%**

More than eight in ten overall respondents (81%) said that API security is more of a priority than it was 12 months ago, with 5% saying it is less of a priority than it was 12 months ago. 14% of overall respondents said that their focus on API security remains unchanged from 12 months ago.

Looking more closely at the 81% who respondents who said that API security is more of a priority, 28% said it was **much** more of a priority, whilst 53% said it was **slightly more of** a priority than 12 months prior.

There is a disparity in approach between the UK and USA. Whilst 84% of UK respondents said that API security is more of a priority compared to 12 months prior, only 78% of USA respondents said this, with nearly one in ten (8%) saying that it was less of a priority than it was one year before.

In terms of verticals, three quarters (75%) of manufacturing respondents said that API security was more of a priority than it was 12 months prior, albeit the lowest of any sector to say this. Nearly one in ten (9%) of respondents in the manufacturing sector said that API security was less of a priority than it was 12 months prior.

Overall, between 81% and 88% of CIOs, CISOs, CTOs, and AppSec teams said that API security was more of a priority than it was 12 months prior. However, just 67% of senior security professionals said this, indicating that the complexity of the overall cybersecurity landscape and the multi-faceted approach needed to ensure cyber resilience in a business means that API security isn't their only priority.

How do you view API security in the context of your business?

	All	UK	USA
As a necessary requirement	**53%**	**52%**	**53%**
As an insurance policy for the business against attacks	**51%**	**51%**	**50%**
As an expense for the business	**48%**	**47%**	**49%**
As a business enabler	**47%**	**47%**	**46%**

Nearly half (47%) of overall respondents said that they viewed API security as a business enabler, yet this may increase in line with the growing adoption of API security testing tools. At the same time, 53% of respondents viewed API security as a necessity, which may be linked to the proliferation of attacks targeting APIs. 48% said that they viewed API security as an expense for the business, whilst 51% viewed it as an insurance policy for the business against attacks.

When analyzing verticals, government and public sector were highest (59%) in viewing API security as a necessary requirement. Energy and utilities ranked highest in viewing API security as an insurance policy for the business against attacks (65%), as an expense for the business (53%) and as a business enabler (52%). This is not surprising given that this sector ranked highest in terms of organizations having more than 1000 APIs in their inventory.

For what forms of regulation, if any, does your API security platform partner help you maintain regulatory compliance?

	All	UK	USA
PCI DSS	**73%**	**72%**	**74%**
GDPR	**68%**	**68%**	**67%**
PII	**52%**	**53%**	**51%**

Three-quarters of overall respondents (73%) cited the Payment Card Industry Data Security Standard (PCI DSS) as the regulation that their API security platform provider helps them to comply with. This was followed by the General Data Protection Regulation (GDPR) (68%), and PII (52%). There was little disparity between UK and USA organizations in how API security platform partners help with compliance.

Less than 1% of overall respondents claim that their API security platform partner does not help them maintain regulatory compliance of any kind.

When analyzing verticals, maintaining PCI DSS compliance was highest in manufacturing (81%), whilst GDPR compliance was highest in energy and utilities (80%) and PII (61%).

Senior security professionals were the most likely to say that their API security platform partner helped them to achieve PCI DSS compliance (80%), and GDPR compliance (73%).

When compared with 2022 findings, there was a marked increase in API security platform providers' ability to ensure GDPR compliance for organizations (53% in 2022 vs. 68% in 2023), whilst there was a surge in the number of respondents overall (28% in 2022 vs. 73% in 2023) that said their API security platform provider helped them to comply with PCI DSS[1].

1. Respondents asked if API security platform partner help them maintain regulatory compliance somewhat differently between 2022 and 2023.

Roughly what percentage, if any, of your developers' time is spent on refactoring and remediation?

More than half (53%) of respondents say their developers are spending between 26% and 50% of their time on refactoring and remediation, a significant proportion of their time when their primary role should be on the core development of applications. A further 14% say this can be between 51% and 75% of their time. These findings were consistent across both the UK and USA; it's clear that refactoring and remediation are overwhelmingly consuming developers.

When looking at verticals, 59% of developers in energy and utilities spend between 26% and 50% of their time on refactoring and remediation, the highest in this bracket of any sector surveyed. Over a third (39%) of developers in retail and eCommerce spend between 11% and 25% of their time on refactoring and remediation. Up to one fifth (20%) of developers in healthcare are spending anywhere between 51% and 75% of their time on refactoring and remediation; this is reflective of the valuable PII available for sophisticated threat actors to target in these sectors.

In terms of different job functions, 59% of CISOs believed that their developers were spending between over a quarter and half of their overall time in refactoring and remediation, whilst nearly a fifth (18%) of CIOs said that developers were spending between more than half and three-quarters of their time on this. This implies that they are aware of the time constraints placed on developers but are grappling with how to deal with the problem.

About Noname Security

Noname Security is the only company taking a complete, proactive approach to API Security. Noname works with 20% of the Fortune 500 and covers the entire API security scope across four pillars — Discovery, Posture Management, Runtime Security, and API Security Testing. Noname Security is privately held, remote-first with headquarters in Silicon Valley, California, and offices in London.

nonamesecurity.com info@nonamesecurity.com +1 (415) 993-7371