In collaboration with Opinion matters

noname

The API Security Disconnect

Research from Noname Security on

API Security Trends in 2022

noname

In this Report

Introduction

Cognizant of the growing cyber threat landscape and the risks to APIs, this research was conducted to better understand the state of the API security environment and to identify the challenges facing organizations. The research cohort involved 600 senior security executives across the UK and USA. The study examines the prevalence of API security incidents, the top API security vulnerabilities, and the frequency in which organizations are conducting API security tests. It also explores the typical challenges respondents faced when scaling API security solutions to meet expanding API requirements.

Additionally, the report delves into the sensitive topic of API inventories and investigates which organizations have visibility into APIs that return sensitive data. It includes insights into the level of confidence organizations have in leveraging Dynamic Application Security Testing (DAST) and Static Application Security Testing (SAST) tools for API testing, as well as whether the API security provided by Cloud Service Providers and Specialist Security Providers is sufficient in meeting SLAs.

Read this report to understand how CISOs and senior cybersecurity professionals are approaching the challenge of securing their APIs in an intense and complex threat and operational environment. Understand how API security platforms are helping respondents maintain regulatory compliance and operational resilience, as well as gain visibility into Dormant, Zombie, and Active APIs.

Methodology

Leading API security company, Noname Security, commissioned a survey, undertaken by an independent research organization, Opinion Matters, in July 2022.

600

Senior cybersecurity professionals in the UK and USA were surveyed from across a variety of enterprise organizations in six key vertical market sectors: financial services, retail & eCommerce, healthcare, government & public sector, manufacturing, and energy & utilities.

Foreword

APIs are Fundamental to the Modern Business Environment

The world has transitioned to an era of application interconnectivity.

APIs are the lifeblood of digital transformation and lie at the heart of corporate strategies for growth and innovation. Nearly all businesses rely on APIs to connect services, transfer data, and control key systems. In fact, APIs now drive mission-critical processes across organizations. The exploding adoption of APIs has also greatly expanded organizations' attack surfaces, increasing the need for enterprises to focus on API security. But as organizations transition into a multitude of cloud, hybrid, and on-premises digital environments, this complexity makes it difficult for security teams to find and fix problems quickly.

To this end, the industry has witnessed no shortage of API-related security incidents – resulting from shadow APIs, misconfigurations, and authorization flaws. Gartner has even predicted that in 2022, API attacks will become the most frequent attack vector, causing data breaches affecting nearly all enterprise applications.

This is reflected in the results we found earlier in the year when Noname Security commissioned 451 Research to conduct The 2022 API Security Trends Report. This report showed that the number of APIs in use had grown at 201% over the past 12 months and 41% of respondents had an API security incident, with 63% of these saying that these incidents involved a data breach and or data loss.

Noname Security undertook this new research to better understand the state of the API security environment in 2022 and to examine the challenges facing organizations. Even though many enterprises are now focusing on API security, there are still significant API security gaps. Dark Reading's 2021 Secure Applications Survey highlights that 41% of respondents treat APIs the same as web applications, and only 23% have a dedicated process for evaluating API security.

Similar to Dark Reading, our research uncovered a level of complacency and potential denial around the risks that APIs present. While three quarters of respondents surveyed said that they had experienced an API security incident, there were also high levels of confidence in their existing solutions, especially in their DAST and SAST tools with 67% saying they were happy with the protection provided and the API security provided by either CSPs or Specialist Security Providers. 71% stated that they were confident and satisfied that they were receiving sufficient API protection.

There is clearly a disconnect between what is happening in the real world, and organizational attitudes towards API security. The level of misplaced confidence around API security is disproportionately high in comparison to the number and severity of API-related breaches. This points to the need for further education by Security, AppSec, and development teams around the realities of API security.

Overall, the research exposed a disconnect between the high level of incidents, the low levels of visibility, effective monitoring and testing of the API environment, and a level of over-confidence that their tools and providers were preventing attacks.

With digital transformation initiatives accelerating, dependency on APIs will only grow, and organizations need to take action now. Key steps include more robust API security practices, such as maintaining accurate API inventories, and better insights into which APIs control and exchange sensitive information and processes. More frequent and accurate API security testing is also required, particularly in pre-production environments.

We hope you find this research illuminating.

High-Level Findings

76%

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

74%

Don't have a full API inventory or know which return sensitive data

71%

Say they are confident in the API security provided by their CSP

API Security Incidents are Growing

The growing severity of API security incidents should be sounding alarm bells. Results showed 76% of senior security professionals experienced an API security incident in the last 12 months that they were aware of. The top API security gaps identified were Dormant or Zombie APIs (19%), Authorization Vulnerabilities (18%), and Web Application Firewalls (17%).

Lack of API Inventories Combined with Poor Visibility

Nearly three quarters (74%) of respondents don't have a full API inventory or don't know which APIs return sensitive data, which means they are open to substantial risk. Put simply, you can't manage or secure what you can't see and this lack of knowledge around API inventories, or an understanding of which return sensitive data, is concerning.

Additionally, existing network infrastructure providers don't give respondents adequate visibility into APIs either, with less than half of respondents using such providers (47%) saying they have visibility into Active APIs, only 26% with visibility into Zombie APIs and just over half (59%) saying their provider gave them visibility into Dormant APIs. With Zombie and Dormant APIs cited by respondents as the number one API attack vector, this lack of visibility needs to improve.

Frequency of API Security Testing

With the prolific number of API security incidents, testing APIs frequently to check for vulnerabilities is increasingly a requirement at many organizations. A successful vulnerability exploit takes seconds to execute, therefore removing vulnerabilities swiftly and in real-time is critical. However, nearly a quarter (22%) of respondents say they are only testing APIs a minimum of once a week. In fact, only 11% said they were testing APIs in real-time and 28% said they were testing at least once a day. 39% responded as testing less than once a day but up to once per week.

Misplaced Confidence

The ability to stop vulnerabilities before they reach production is another key factor. The cost of remediating vulnerabilities is dramatically reduced when they are detected and fixed earlier in the software development lifecycle. Therefore, the high levels of confidence in traditional DAST and SAST tools (67%) for testing APIs was surprising. These tools generally do not test for API security vulnerabilities specifically, focusing instead on basic functionality or rudimentary security tests via fuzzing. **We encourage organizations to shift left and move API security testing to earlier in the DevOps process.**

Likewise, high confidence levels in CSPs/Specialist Security Providers shows a level of misplaced trust. With the high level of API security attacks and incidents that cause data breaches or compromise performance, should respondents be so complacent that their providers have this covered?

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, and 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 couple of significant differences.

Comparing Monitoring and Visibility of APIs

UK respondents were ahead of the USA, with 28% saying they have full inventories and full knowledge of which return sensitive data. In the USA this figure was lower at 24%. However, in the UK, 38% said that they had a full inventory of their APIs but were not aware which returned sensitive data. When asked the same question, 44% of USA respondents said they had this visibility.

28% **UK** respondents

24% **USA** respondents

Saying they have full inventories and full knowledge of which return sensitive data

Reporting in Real-Time

When it comes to the frequency of API security testing for signs of abuse, **14% of UK respondents reported testing in real-time, compared with only 8% of USA respondents.**

Confidence in API Security Generally Higher in the USA

Confidence in DAST and SAST tools was higher in the USA, with **74% saying they were confident compared to 61% in the UK**. However, 38% of USA respondents said that the degree of accuracy can be a concern around API security testing versus 23% of UK respondents.

Overall, USA respondents demonstrated a much higher level of confidence in their CSP and Specialist Security Providers with 80% saying they are confident, versus 62% in the UK.

All too often security assessments center too heavily on gut feeling and loose definitions of API security and this needs to tighten up.

62% **UK** respondents

80% **USA** respondents

demonstrated confidence in their CSP and Specialist Security Providers

Vertical Market Overview

Out of the six verticals that were surveyed: financial services, retail & eCommerce, healthcare, government & public sector, manufacturing, and energy & utilities: critical infrastructure sectors such as energy & utilities and manufacturing seemed to be more susceptible to attacks and security incidents.

Today's critical infrastructure sectors are being shaped by large scale economic forces, technological change, the energy crisis, disrupted supply chains, and the after-effects of the COVID-19 pandemic. While digital, connected and smart systems are on the rise, manufacturers and energy & utilities providers face ongoing challenges with legacy systems. Large plants need to be always on; halting production or downtime costs money, and they're often afraid to tamper with legacy systems. Instead, they work around these systems implementing API Gateways on the front-end, which are often targeted by hackers.

Therefore, it is not surprising that out of the six different vertical sectors surveyed, manufacturing was the industry reporting the highest percentage of API security incidents in the last 12 months (79%), closely followed by energy & utilities (78%).

Top 2 industries reporting API security incidents:

79%

Manufacturing

78%

Energy & Utilities

Dormant or Zombie APIs was the top API vulnerability for the retail & eCommerce sector (22%), closely followed by manufacturing (21%). Authorization Vulnerabilities were identified as the top approach in healthcare (23%) followed by financial services (21%). Interestingly, for the energy & utilities sector the top API security attack type cited was DDoS attacks.

When asked if they have a full inventory of their APIs and know which return sensitive data, the retail & eCommerce sector scored highest with 33%, and energy & utilities scored lowest with just 19%.

More than half (56%) of financial services organizations said they found it easy to scale their API security solution, which was higher than the other five industry sectors surveyed, whereas manufacturing respondents (30%) found it the most difficult.

All sectors unanimously agreed that their API security platform provider was helping them to maintain regulatory compliance. Out of the different industry sectors, healthcare respondents scored highest (96%), while manufacturing reported the lowest out of the six sectors at 93%. The retail & eCommerce sector scored highest in saying their provider helped them to meet GDPR compliance (59%).

In terms of visibility into APIs, the financial services sector scored highest in saying their API security platform provider gave visibility into Dormant APIs (76%). The retail & eCommerce sector scored highest with visibility into Active APIs (51%).

Testing APIs in real time for signs of abuse was highest for the government & public sector (17%) and lowest for energy & utilities (7%). Interestingly, again both the manufacturing and energy & utilities sectors reported the highest in terms of testing less than once a week but up to once a month, with just 20% and 21% respectively. By not testing in real-time or even more frequently these sectors are leaving themselves open to vulnerabilities and exploits, which correlates with the high level of API security incidents.

Manufacturing (37%) was also the least confident in its DAST and SAST tools for testing APIs.

Role Type And Comparisons

Five different job functions were surveyed including CIO, CISO, CTO, Senior Security Professional, and AppSec professional. Delving into the responses from the different job functions surveyed, CISOs were most likely to say they have experienced an API incident (81%) and AppSecs were least likely, with 53%. This raises questions as to whether there is a disconnect between senior personnel and operational teams. For USA respondents, CTOs scored highest in experiencing an API security incident with 83% demonstrating how this leadership disconnect is even further exacerbated between job roles.

When looking at the different job functions there were disparities in what respondents considered to be the top API attack approaches, indicating that attacks are coming from all sides with no one particular approach dominating. CIOs (19%) and Senior Security Professionals (21%) cited Network Firewall, CISOs said Dormant/Zombie APIs (23%), CTOs felt that DDoS was the top attack type (21%), while AppSec teams said Authorization Vulnerabilities (24%). However in the UK, Senior Security Professionals cited Dormant/Zombie APIs highest with 25% whereas USA respondents scored this considerably lower at 13%.

In terms of visibility, CIOs appeared to have the best visibility into their inventories and which APIs returned sensitive data, with 32% stating this. Surprisingly, AppSec teams had the lowest insights, with 44% saying they only had a partial understanding of their inventory or those which returned sensitive data. This could be attributed to education, with AppSecs more aware and likely to admit than other roles that there are gaps in API security. There was some disparity between USA and UK AppSec teams with 31% in the UK citing that they had a full inventory of their APIs and knew which ones returned sensitive data versus 21% in the USA.

What job title was most likely to say they have experienced an API incident in the past?

81%

CISO

53%

AppSec

Interestingly, 58% of CIOs said it was easy to scale solutions, while well over a quarter (29%) of AppSecs admitted this was difficult. Again, AppSecs are more exposed to the daily realities than senior personnel and more aware of how challenging it is to scale solutions. Delving into the country statistics and the data suggests that UK Senior Security Professionals find it easier to scale with 64% citing this versus 46% of USA respondents who said it was easy.

When asked about how their API security platform provider helped to maintain regulatory compliance, CTOs rated their provider highest (96%) and likewise in helping them to achieve compliance with GDPR (58%). Overall, AppSec teams reported the lowest levels of support in maintaining compliance out of all five roles, with 93%, but when looking across the two geographies, UK AppSecs, in particular, feel the most unsupported with only 86% saying their provider is helping them maintain compliance.

Surprisingly, CIOs were undertaking more testing in real-time (14%) compared to other roles and AppSec teams were testing the least (7%). However, there was some disparity between UK and USA CIOs with 18% of UK CIOs undertaking real-time testing compared to 10% in the USA. CISOs also scored highest in testing once per day (33%) while 45% of CTOs admitted to testing less frequently than once per day but up to once per week.

As well as their lack of real-time testing, AppSec teams also scored highest in testing less than once a week and up to once a month, with a quarter (25%) stating this.

Confidence in DAST and SAST tools was highest among USA CIOs (80%) versus UK CIOs (53%), however overall combined USA and UK CISOs were most like to say the had confidence in their tools with (70%) while AppSecs were least likely (62%). Senior Security Professionals were least confident in the API security provided by their partner, with 40% saying they were not confident, and likewise they lacked the most confidence that their partners were meeting their SLAs (33%).

In general, AppSec teams in the USA were more confident about the support from their CSP/Specialist Security Provider than the UK with 79% versus 57%. This correlated to them being more confident about their providers meeting their SLAs (82% versus 63%).

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, an overwhelming three quarters of respondents (76%) admitted that they had, with less than a quarter (24%) saying that they hadn't.

When comparing the UK with the USA, responses were relatively similar, with 75% of UK respondents stating that they had experienced an incident compared to 77% in the USA.

Delving into the different job functions surveyed, CISOs were most likely to say they have experienced an API incident (81%).

Of the six different industry sectors that we surveyed; manufacturing was the most likely industry to experience an API incident, with 79% of respondents saying this was the case.

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

The top three attack approaches cited by respondents were:

	All	UK	USA
Dormant or Zombie APIs	**19%**	**19%**	**19%**
Authorization Vulnerabilities	**18%**	**19%**	**18%**
Web Application Firewall	**17%**	**15%**	**19%**

When looking at the different job functions there were disparities in what respondents considered to be the top attack approaches. CIOs cited Network Firewall (19%), CISOs said Dormant/Zombie APIs (23%), CTOs felt that DDoS was the top security attack approach (21%), AppSec teams said Authorization Vulnerabilities (24%) and senior security professionals cited Network Firewall (21%). This highlights that attacks are coming from all sides, with no one particular attack approach dominating.

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

When respondents were asked if they have a full inventory of their APIs and if they know which return sensitive data, only just over one quarter (26%) were able to say yes. Put simply, if you don't know what APIs you have in your inventory, it is near impossible to secure it. Likewise, if you don't know which APIs return sensitive data, it makes it hard to know which to prioritize from a security perspective.

Looking at the individual countries, results were slightly higher for UK respondents having a full inventory and knowing which return sensitive data (28%), versus USA respondents (24%).

Additionally, there were some respondents who had a full inventory of their APIs (41%) but who were not aware which returned sensitive data. In the UK this dropped to 38%; in the USA it was 44%

One third of respondents (32%) only had a partial view of APIs and were not always aware of which returned sensitive data and a small minority (1%) admitted to not having an inventory at all.

When looking across the different job functions, CIOs appeared to have the best visibility of their inventories and which APIs returned sensitive data, with 32% stating this. Surprisingly, AppSec teams had the lowest insights, with 44% stating that they only had a partial understanding of their inventory, or which returned sensitive data.

Likewise, from an industry sector perspective, retail & eCommerce scored highest with 33% saying they had a full inventory and knew which APIs returned sensitive data.

How easy or difficult is it for your API security solution to scale up to meet your needs?

More than half of all respondents (52%) said that it was either very or fairly easy to get API security solutions to scale to meet their needs. This increased to 55% for USA respondents but decreased to 49% for UK respondents.

That said, just over one fifth (22%) admitted that it was either fairly or very difficult to scale solutions. This increased to almost a quarter (24%) for UK respondents and decreased to 19% for USA organizations.

Interestingly, 58% of CIOs said it was either very or fairly easy to scale solutions, while well over a quarter (29%) of AppSecs found this to be fairly or very difficult.

Financial services organizations (56%) found it the easiest to scale their API security solution out of the six industry sectors surveyed, whereas manufacturing respondents (30%) found it the most difficult.

Does your API security platform partner help you maintain regulatory compliance?

We live in a world of constantly evolving compliance and regulation. The good news is that a staggering 94% of respondents said that their API security platform provider does help them maintain regulatory compliance; this rose to 96% when assessing USA respondents.

GDPR was the most common regulation cited, with 53% of respondents stating that their API security partner enabled them to maintain compliance with GDPR. Again, this was higher for USA respondents (54%).

In terms of different job functions, CTOs rated their API security platform provider highest (96%) and likewise in helping them to achieve compliance with GDPR (58%).

Out of the different industry sectors, healthcare scored highest with 96% overall, while the retail & eCommerce sector scored highest for GDPR compliance with 59%.

Only two out of the 600 respondents surveyed said that they didn't have an API security platform provider.

Which of the following APIs does your API security platform partner provide visibility into?

Of the 598 who work with an API security platform provider, over half (59%) said that their provider gave them visibility into Dormant APIs and 47% said they had visibility into Active APIs. Just over a quarter (26%) also have visibility into Zombie APIs.

Below are the responses broken down across the two surveyed countries:

	UK	USA
Dormant	**53%**	**64%**
Active	**44%**	**51%**
Zombie	**31%**	**21%**

Respondents in the financial services sector had the highest visibility into Dormant APIs (76%) and CIOs also had the highest visibility (68%) into Dormant APIs.

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

With three quarters of all respondents admitting to having experienced an API security incident, it was interesting to understand how often respondents undertake API security testing for signs of abuse.

It is alarming, with the prolific number of incidents occurring, that only 11% of respondents admit to doing testing in real-time. This increased to 14% for UK respondents but decreased to 8% for USA respondents.

28% of respondents said they were testing at least once a day and a further 39% were testing less than once a day, but up to once a week.

Unfortunately, 8% of UK respondents were testing less regularly than once per month, compared with only 3% of USA respondents.

CIOs were undertaking more testing in real-time (14%) compared to other roles and AppSec teams were testing the least (7%).

CISOs scored highest in testing once per day (33%) while 45% of CTOs admitted to testing less frequently than once per day but up to once per week.

As well as their lack of real-time testing, AppSec teams also scored highest in testing less than once a week and up to once a month, with a quarter (25%) stating this.

Out of the industry sectors surveyed, the government & public sector scored highest for testing in real time (17%).

How confident are you, if at all, that your current DAST and SAST tools are capable of testing APIs?

Out of the 600 respondents surveyed only five did not have a DAST or a SAST tool.

More than two thirds (67%) of the 595 respondents that said they did were either very confident or somewhat confident in their DAST and SAST tools' capabilities for testing APIs. This increased to 74% for USA respondents but dropped to 61% for those in the UK.

However, just under a third were not confident (32%). This rose to 38% for UK respondents but dropped to 26% for USA.

Interestingly, more than a third (38%) of AppSecs were not very confident about their tools' capabilities versus 70% of CISOs who were either very or fairly confident about their tools. Retail & eCommerce were the most confident (72%) out of the six sectors, whereas manufacturing was the least confident (37%). This disconnect between AppSecs and the C-suite is definitely worth exploring further; is it the case that those that have hands on the challenge are much more cautious about performance success than those higher up the seniority chain?

Respondents were asked to tick various statements they agreed with and:

31% said the degree of accuracy can be a concern around API testing in pre-production, this decreased to 23% for the UK but rose to 38% for the USA.

39% said the time it takes to implement, test and deploy runtime protections and remediation integrations can be a benefit around API testing in pre-production. This decreased to 34% for the UK and increased to 44% for the USA. Conversely 27% said the time it takes to implement, test and deploy runtime protections and remediation integrations can be a concern around API testing in pre-production. This was the same for the UK but rose to 28% for the USA.

25% said API testing in pre-production can enhance innovation. This was the same for the UK and USA. While 22% said API testing in pre-production can stifle innovation; this was 22% for the UK and 21% for USA.

18% said API testing in pre-production can speed up development. This was 19% for the UK and 17% for the USA. However, 15% said API testing in pre-production can slow down development. This was 14% for the UK and 16% for the USA.

How confident are you in the following aspects of your CSP or Specialist Security Provider?

When asked to rate how confident they were in two key aspects of their CSP or Specialist Security Provider, 71% of respondents said they were either very or somewhat confident in the API security provided by their service provider. This decreased to 62% in the UK but rose to 80% in the USA.

75% were either very or somewhat confident in their provider meeting their SLAs. Only 29% were not confident with the API security provided. However, this rose to 37% for UK respondents and dropped to 20% for USA respondents.

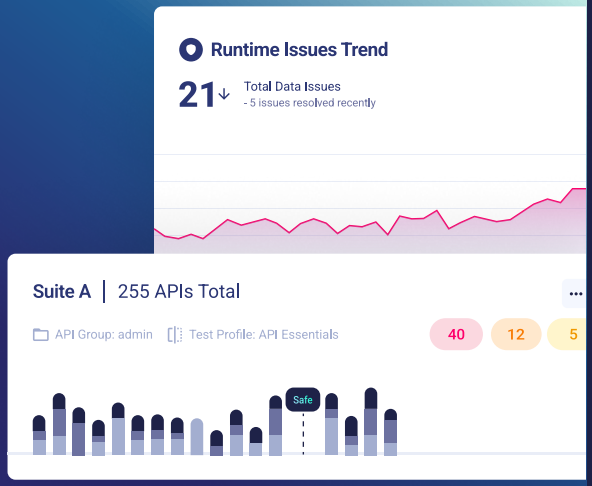
Overall, 24% said they were either not that confident or not confident at all in meeting their security SLAs. Again, this rose to 27% for UK respondents and dropped to 21% for USA respondents.

	The API security provided is sufficient	All	UK	USA
✓	**Confident (Net)**	**71%**	**62%**	**80%**
✗	**Not confident (Net)**	**29%**	**37%**	**20%**

	They are meeting their security SLAs	All	UK	USA
✓	**Confident (Net)**	**75%**	**72%**	**78%**
✗	**Not confident (Net)**	**24%**	**27%**	**21%**

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 three pillars — Posture Management, Runtime Security, and API Security Testing. Noname Security is privately held, remote-first with headquarters in Palo Alto, California, and offices in Tel Aviv and Amsterdam.



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