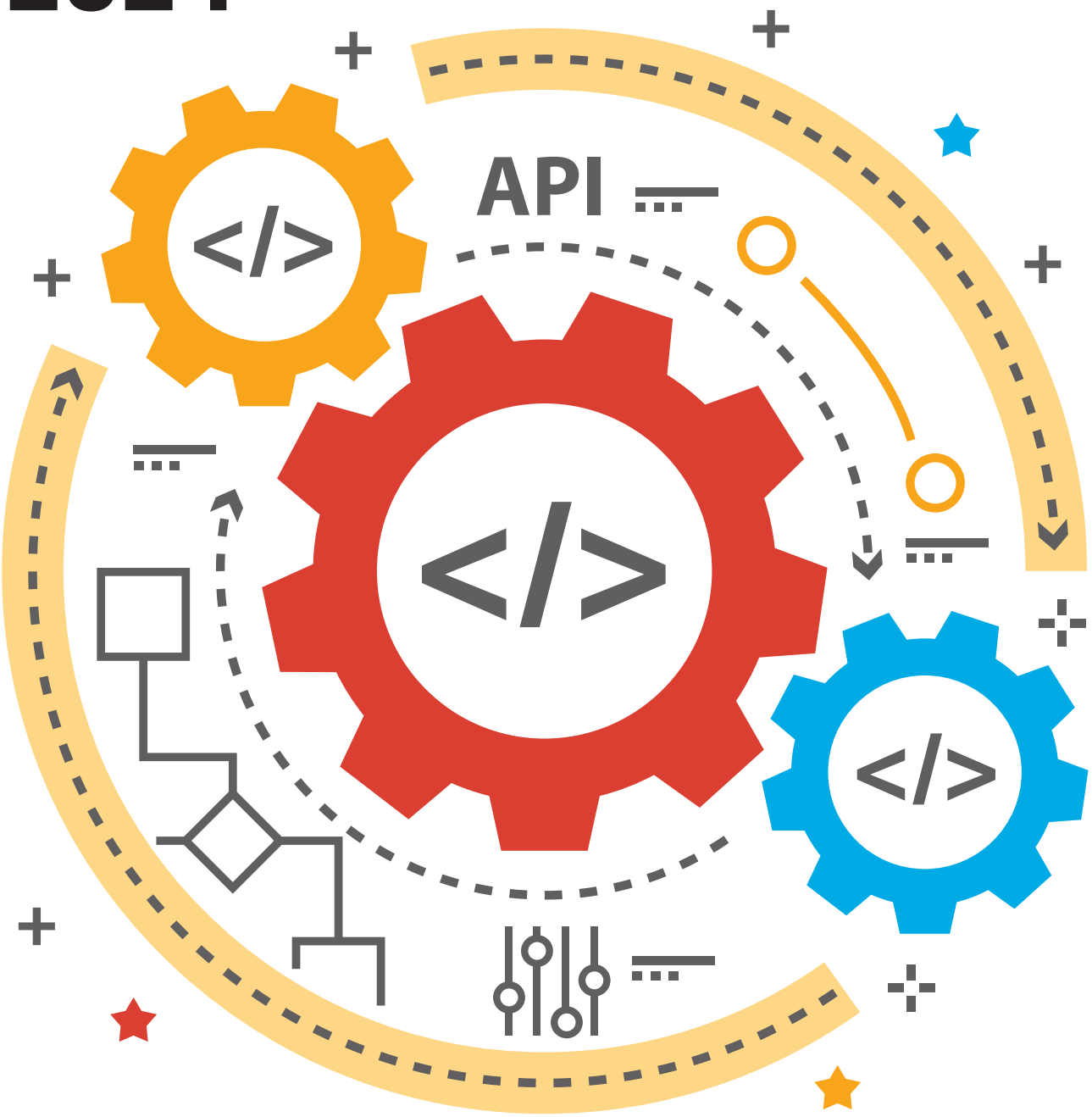
CIO CSO COMPUTERWOCHE VOICE OF DIGITAL

STUDY

API SECURITY 2024



fastly®

Simon Hülsbömer,
Senior Project Manager
Research Services

The secure link

Amidst all the focus on keeping applications and services secure in this interconnected world, one crucial aspect is often overlooked: the interface. (Cloud) applications and services communicate both alongside and with each other through these APIs, which can quickly become major security risks if there is no end-to-end protection in place. And the more complex the IT processes, the more sensitive the interfaces.

Due to the growing adoption of cloud computing, microservices architectures and mobile applications, APIs are becoming increasingly important as a link between different systems, services and platforms. However, while performing this function, they also open up potential attack vectors for threat actors. An API security breach can have devastating consequences, ranging from data leaks and financial loss to reputational damage and legal repercussions.

The edge cloud platform provider Fastly, together with the CSO, CIO and COMPUTERWOCHE Custom Research Team, surveyed 235 companies across Europe on the state of their API security. The study participants included C-level decision-makers (CISOs, CIOs, VP Security, IT Security Managers), IT personnel from platform or DevSecOps teams, as well as other security experts, analysts, architects and influencers.

The relevance of the topic is underscored by the figures from the study: 95 percent of respondents reported having issues with their API security in the past twelve months. 39 percent cited API vulnerabilities, while 33 percent mentioned authentication problems within the APIs. However, 84 percent have yet to implement specific measures to improve interface security; this is primarily due to financial constraints and a lack of expertise.

Another interesting finding: API security and web security are converging – nearly 90 percent of companies are already using or planning to use combined security solutions from a provider. This makes sense, considering that API security and web security address similar, sometimes identical attack vectors, such as injection attacks or cross-site request forgery. Moreover, APIs are often used in web applications to retrieve data from different sources or perform actions. An insecure API can therefore compromise the security of the entire web application. Conversely, security vulnerabilities in a web application can jeopardise the security of the APIs it utilises.

Overall, API security and web security work hand in hand to keep applications and services secure. By developing holistic security strategies that cover both APIs and web apps, companies can minimise potential security risks and create a secure digital environment.

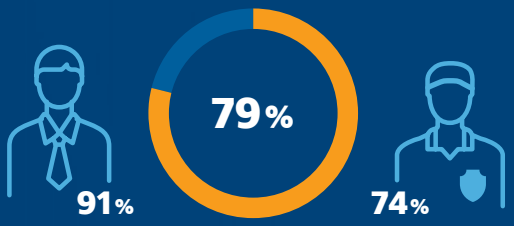
We wish you an insightful read.

Contents

API Security 2024

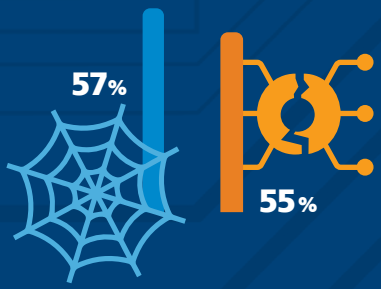
Management Summary

The key findings of our study



Secure APIs are more important at the C-level than among security specialists

79% of the companies surveyed place a high or very high level of importance on API security. **91%** of C-level and compliance experts said this, while only **74%** of security experts made the same comment.



When it comes to API risks: Age is more of a concern than manipulation

57% of respondents are more concerned with the consequences of outdated APIs. In second place with **55%** is the potential loss of integrity through APIs. C-level and compliance experts consider outdated APIs to be the top risk, whereas security experts are more concerned with API manipulation.

API and web security are becoming one and the same

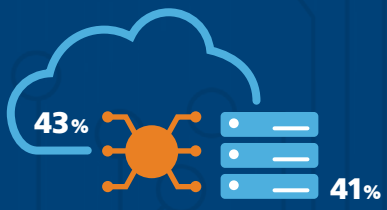
19% of the companies surveyed are already using a consolidated web application and API security solution from a single provider. **43%** are planning to adopt within the next two years and a further **26%** plan to do so, but do not have a timeframe. Only **2%** of the companies said they were not interested in such an approach.

Real-time logging and API monitoring are still the priority

55% of the companies surveyed consider API monitoring and logging as the top priority in API security. **43%** stated API analytics & evaluation as their priority. The use of AI technologies was only considered a priority by **14%** of companies.

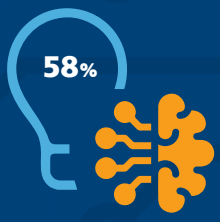
API security problems are very much on the agenda, but admittedly most companies are fairly mediocre when it comes to API security

95 % of the companies surveyed said they had experienced API security problems in the last twelve months. Of that, **39 %** report vulnerabilities in their APIs and **33 %** report authentication issues. **84 %** of the companies do not yet have any advanced API security measures in place. An insufficient budget and a lack of expertise are the most commonly stated reasons for not having implemented a comprehensive API strategy.



API security built for edge-native and cloud-native applications is becoming a growing trend

When it comes down to one of the most essential criteria in selecting an API security solution, **43 %** of the businesses surveyed revealed that they preferred an API security solution built for edge-native applications, followed by **41 %** responding that they would choose a cloud-native suitable solution to protect their APIs.

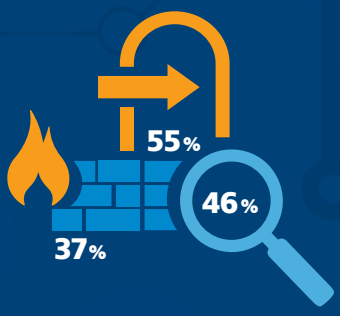


Expectations for AI are high, but awareness is low as we are currently seeing only minimal use in API security

58 % of respondents believe that the use of AI will bring about significant changes in API security over the next two to three years. This figure rises to **75 %** for financial institutions and insurers. **16 %** of the companies surveyed are unaware if they are already using AI in their API security. Just **18 %** said they are using AI while **66 %** said they are not.

API gateways, log data and WAF are among the most reliable methods to detect API attacks

55 % of respondents rely on warnings from an API gateway to detect API attacks. **46 %** search through log data looking for indications of possible API attacks. **37 %** use warning notifications from a WAF (Web Application Firewall).



API security is of high importance and affects application rollout

79 % of the companies surveyed place a high or very high level of importance on API security. Just two % of respondents consider this to be of low or very low importance. Equally, 79 % of respondents slowed the rollout or the integration of a new application into production because of API security concerns.

The high degree of importance placed on API security is shared by C-level and compliance managers as well as IT and network managers and security experts among the companies surveyed. However, while the proportion of C-level and compliance respondents with this belief was 91 %, the figure was just 74 % among security experts.

The importance of API security is not just an idea in the heads of those at the C-level and in compliance. While there have been any uncertainties regarding API security, the majority of respondents have already experienced delays in new applications going live.

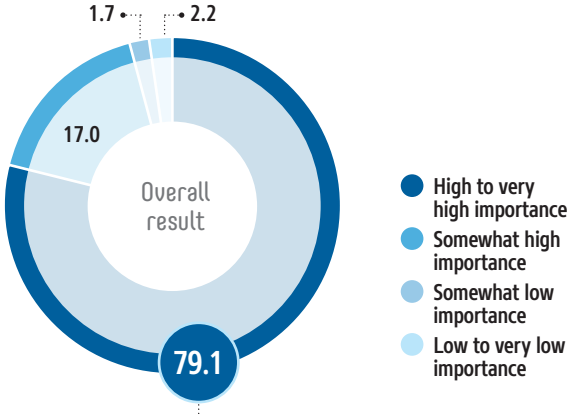
Comparing the various regions that were surveyed, we can see that API security is of particular importance to respondents in the United Kingdom with 86 % responding as such. For Nordics, 73 % of respondents gave the same level of importance to secure APIs.

We also see differences between sectors: 89 % of wholesale, retail and e-commerce companies surveyed place a high or very high level of importance on API security. In comparison, 80 % of survey participants from the finance and insurance sectors gave the same response. This result is surprising, as financial services and insurers are strictly regulated and would therefore be expected to have a higher-than-average focus on API security.

Conclusion: Even if API security is considered to be of high importance, a closer look needs to be taken at its actual implementation within individual companies as we can get a somewhat different picture from those managing the implementation.

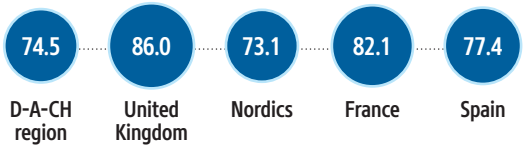
What is the current importance of API Security in your company?

All data expressed as percentages. Basis: n = 235

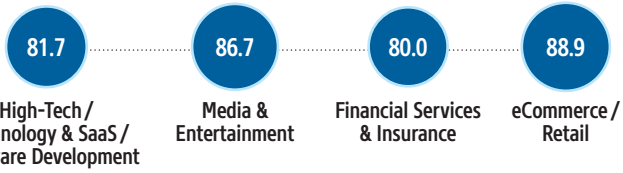


Results split by functional role in company

Results split by region



Results split by sector



D-A-CH region = Germany, Austria, Switzerland
Nordics = Denmark, Finland, Norway, Sweden

Security problems in production APIs are widespread

92 % of the companies surveyed have discovered security issues with the APIs in their production systems in the last twelve months, five % have not, and three % do not know precisely. Most API security problems are attributed to vulnerabilities, cited by 39 % of respondents.

Further security problems that companies have found in their production APIs are authentication problems, stated by one in three companies, API identity problems, which were discovered by three in ten companies, and configuration errors, reported by 30 % of respondents.

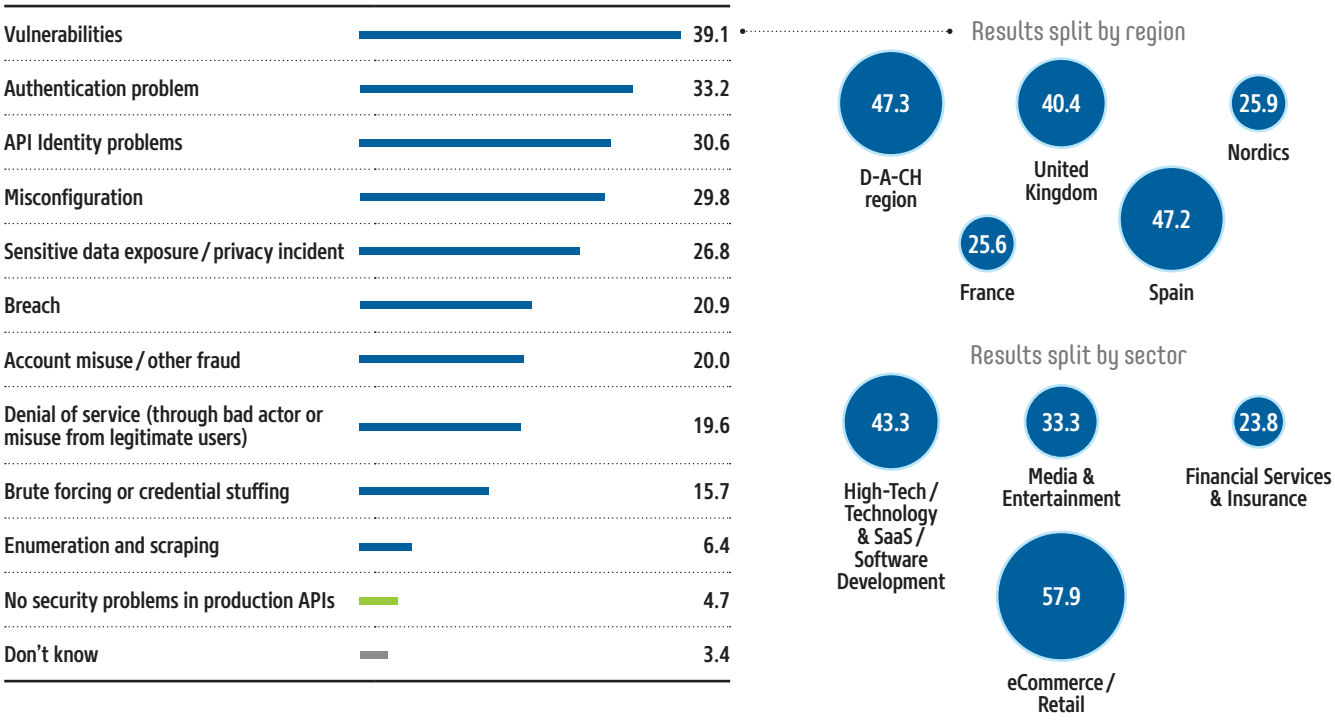
The frequency at which vulnerabilities are discovered in APIs for production systems differs between regions. Companies in the DACH region and Spain report the most at 47 %. In the United Kingdom this figure is still 40 %, and in France and Nordics it is just 26 % of respondents who reported API vulnerabilities.

Breaking these figures down into the different sectors, it is the wholesale and retail / e-commerce sector that most commonly find vulnerabilities in their production APIs with 58 % of respondents stating this. Among financial services and insurers this figure drops to 24 %. In this sector it is predominantly authentication problems with APIs that are reported, stated by 38 % of respondents.

Conclusion: API security is of key importance for production IT systems and must be part of the overall security concept or be integrated into it.

In the past 12 months, what security problems have you found in production APIs?

Multiple answers possible. All data expressed as percentages. Basis: n = 235



D-A-CH region = Germany, Austria, Switzerland
Nordics = Denmark, Finland, Norway, Sweden

3

Outdated APIs are the most commonly stated threat for web interfaces

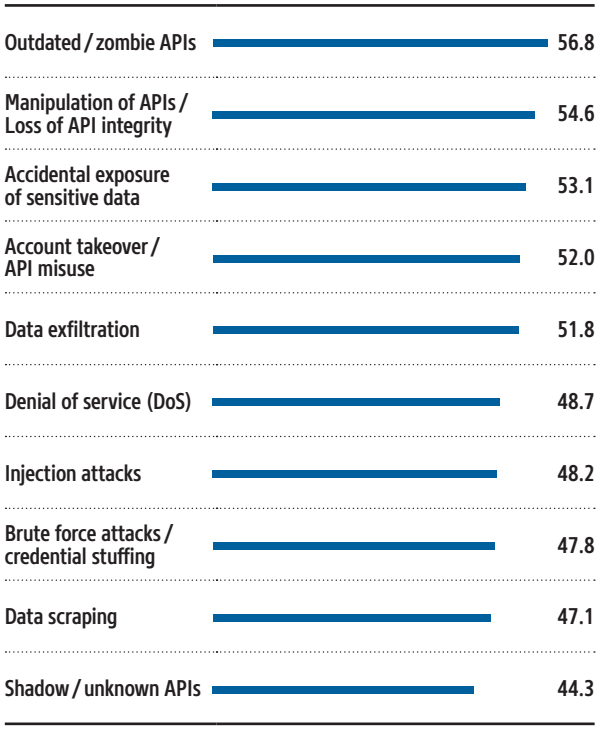
57 % of responses mentioned zombie APIs (outdated APIs), making this the most frequently stated threat among the companies surveyed. API manipulation follows in second place with 55 % with accidental disclosure of sensitive data via APIs in third place with 53 %.

The perception of the threat posed by outdated APIs is higher than average at the C-level and among compliance experts at 74 %. Just 47 % of security experts stated this API risk. Even the most commonly stated threat by security professionals, API manipulation, is stated more frequently at the C-level and in the compliance field. 55 % of security experts consider API manipulation a threat, for C-level and compliance this figure is 65 %.

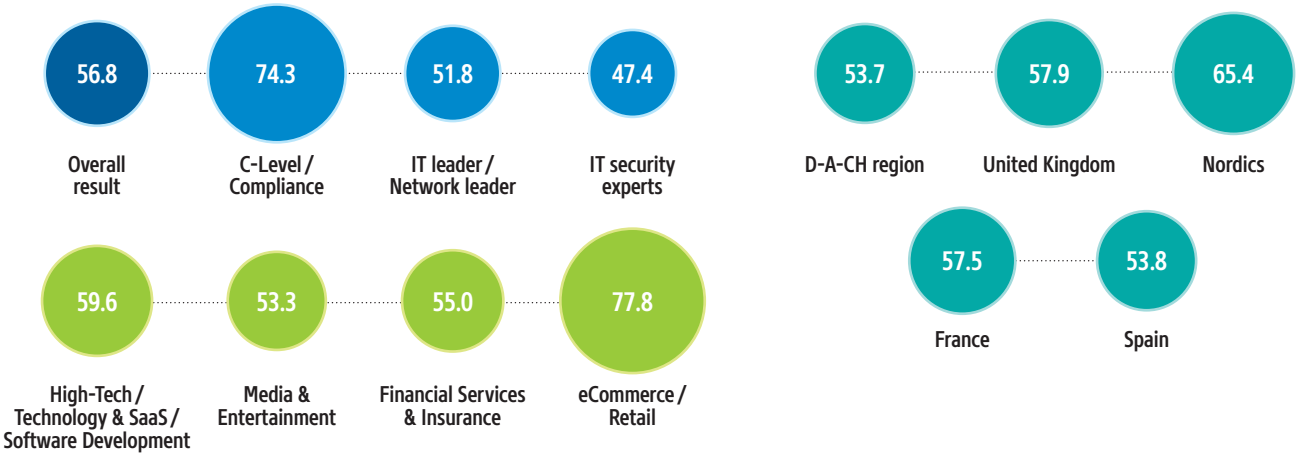
The differences in how API risks are assessed result from not just the respondent's role in the company. While survey participants in the United Kingdom and Nordics most frequently stated zombie APIs, API manipulation is a more common concern in the DACH region. In Spain, the accidental disclosure of sensitive data is the most common answer, whilst in France it is API misuse and data exfiltration.

How do you assess the threat situation in the area of API security in your company?

Multiple answers possible. All data expressed as percentages.
Rating on a scale from 1 (very high concern) to (very low concern).
Top 2 Boxes (high to very high concern). Basis: n = 235

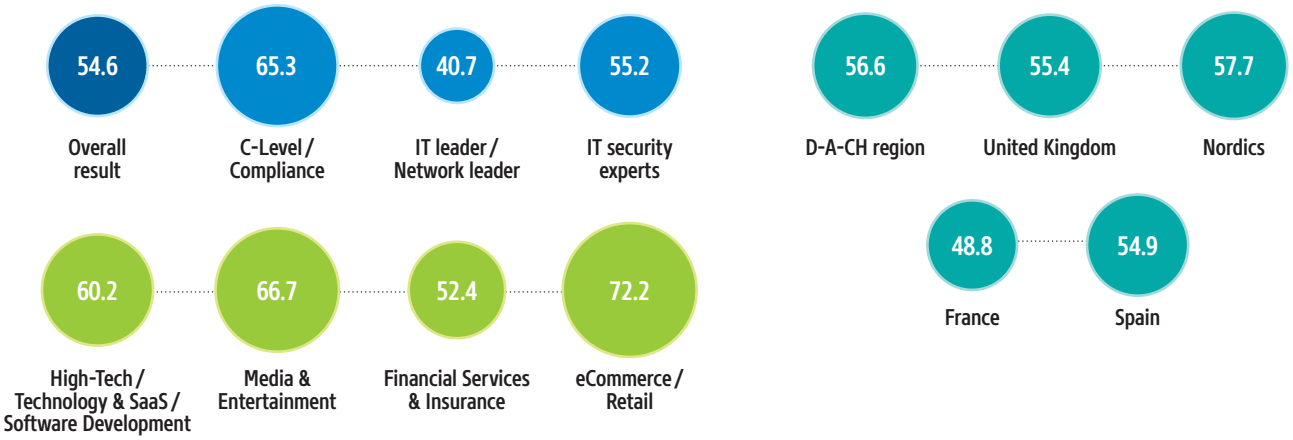


Result splits: Outdated / Zombie APIs

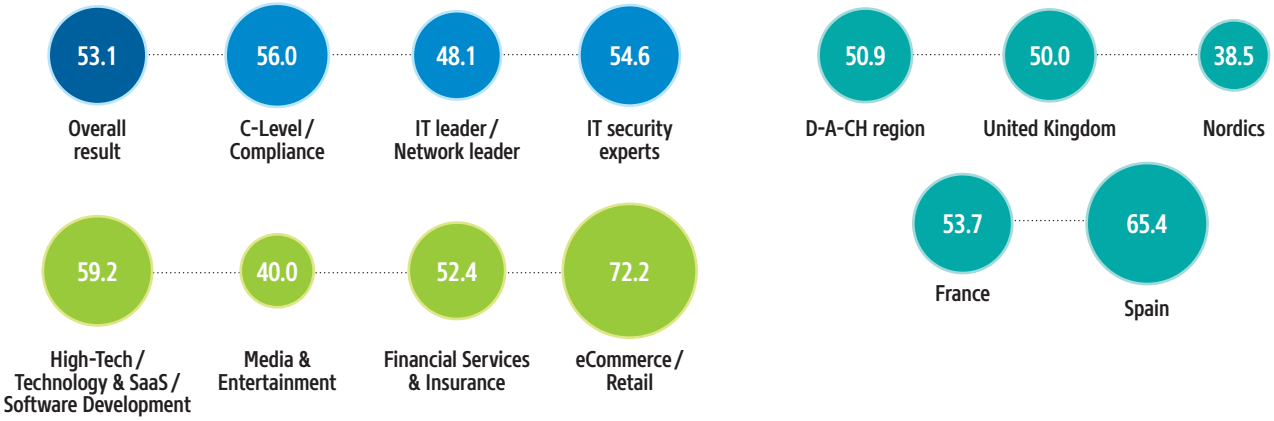


D-A-CH region = Germany, Austria, Switzerland
Nordics = Denmark, Finland, Norway, Sweden

Result splits: Manipulation of APIs / Loss of API integrity



Result splits: Accidental exposure of sensitive data



The sector in which a business operates also affects how API threats are assessed: The most commonly stated threat, zombie APIs, are of greater concern in the retail sector, whereas media, entertainment, high-tech / technology & SaaS / software development are more worried about API manipulation. For financial services and insurers, however, it is API misuse that is the most commonly stated threat.

Conclusion: Businesses should reconsider the way in which they assess API risks. In doing so, professionals from different disciplines should work together, not just security experts alone. Furthermore, it's critical to have an accurate list of APIs so that zombie APIs can be subject to more strict constraints until they are updated.

4 Advanced measures for API security are still the exception, not the rule

One in three of the companies surveyed considers the measures they have taken for ensuring API security to be fairly average. 26 % say their API security is basic only with a further 21 % still in the planning stage. Three % stated that they do not have any API security in place.

17 % of those surveys did state that their API security measures are advanced. However, if we take a look at the role of these respondents, we see that 20 % in C-level and compliance believe that their own API security measures are highly advanced. Only 14 % of security experts came to the same conclusion.

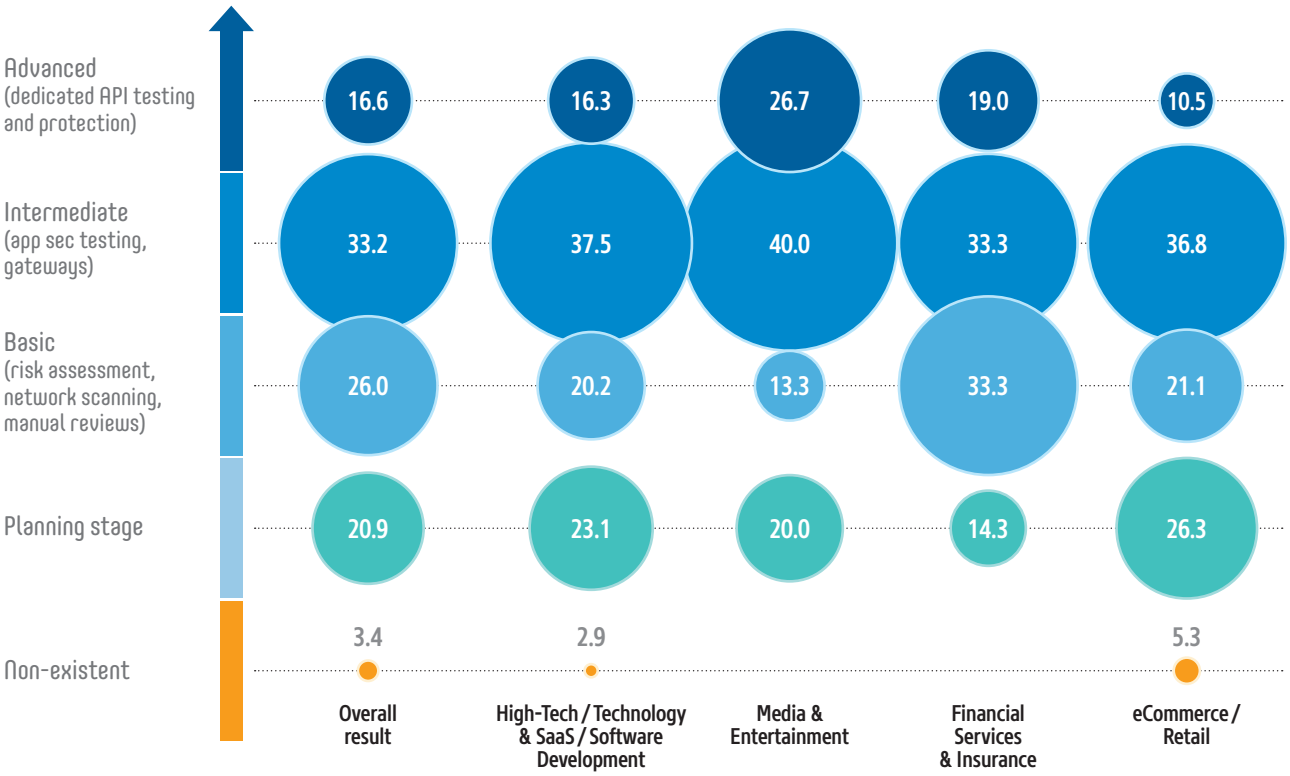
Comparing regions, more participants in the United Kingdom report that their API security is advanced at 21 %. Just 13 % of respondents in the DACH region share this view.

Comparing sectors, 27 % of representatives of the media and entertainment industry in particular see themselves as having highly advanced API security. Things look somewhat different in the retail sector. Here just eleven % report that they are using advanced API security measures.

Among these, just four % state that a lack of suitable tools and solutions are the reason why their API security strategy cannot be optimally implemented. 23 % of respondents, however, state that this is due to insufficient

Which status regarding the API security is applicable for your company?

All data expressed as percentages. Basis: n = 235



budget with a further 20 % lacking expertise. The great concern according to 31 % of responses is that not enough time is spent on fleshing out and documenting API security requirements.

When asked about the most important selection criteria when evaluating API security solutions, the top responses from companies were edge-native platform (where data is processed locally on edge devices and only sent to the cloud or a central database when required) and that the API security solution was developed specifically for cloud-native security using the latest technology. There is relative unanimity here: these are the top mentions across all company sizes, industries and (almost) all EMEA regions analyzed.

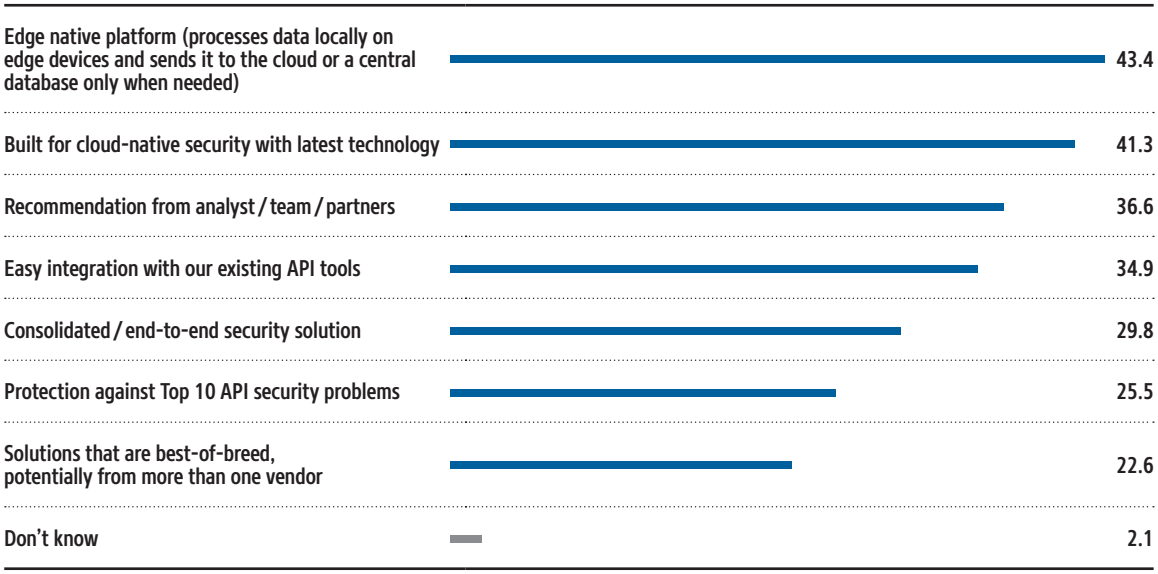
Conclusion: In the many API incidents seen by companies, and given the degree of importance placed on API security, it is necessary for many companies to take security measures even more seriously than they have been doing up to now.

What is the biggest obstacle keeping your company from implementing an optimal API security strategy?

All data expressed as percentages. Basis: n = 235

What are the most important criteria for your company evaluating API security solutions?

Multiple answers possible. All data expressed as percentages. Basis: n = 235



5

Financial service providers in particular are having difficulty detecting API attacks

Just 8 % of the companies surveyed said they are unable to detect API attacks. The picture is somewhat different for financial institutions and insurers: Almost three in ten respondents (29 %) said that they are unable to detect attacks on their APIs. Among those who discovered API attacks, 55 % use warnings issued by an API gateway.

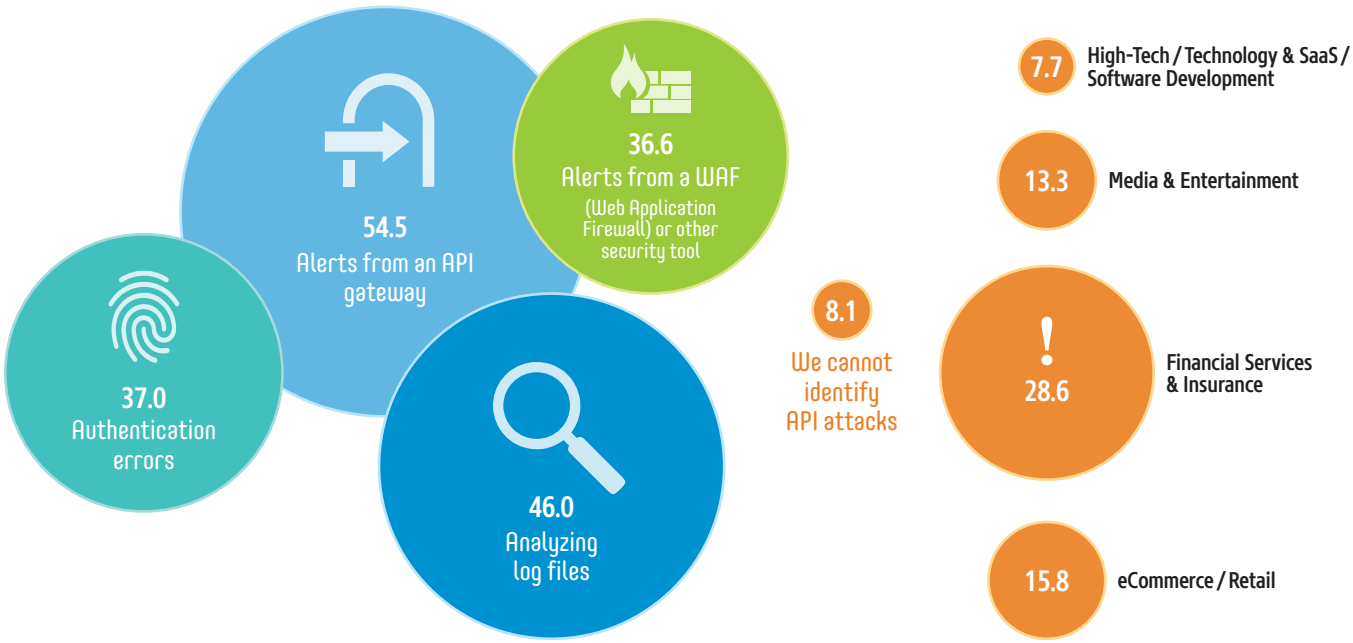
A further 46 % use log data to find evidence of API attacks, and 37 % rely on authentication error notifications or warnings from a WAF (Web Application Firewall).

API schema enforcement makes sure that incoming HTTP API calls follow a certain structure or set of rules that are outlined in a specification file. The OpenAPI Specifications language, which used to be known as Swagger files, is a vendor-neutral specification language for HTTP APIs that gives developers a standard way to describe an API. It can be extremely valuable to find and stop malicious individuals who are trying to abuse an API by blocking or logging new requests that don't follow your standards.

Warning notifications from an API gateway are the preferred means of detecting API attacks in all regions surveyed. This also applies to the surveyed sectors. Companies in France in particular, 58 %, stated that they use API gateways to warn them of API attacks. Looking at different sectors, in wholesale and retail / e-commerce the figure is 63 % who rely mostly on API gateways. In retail, 16 % of respondents say that they cannot identify any API attacks.

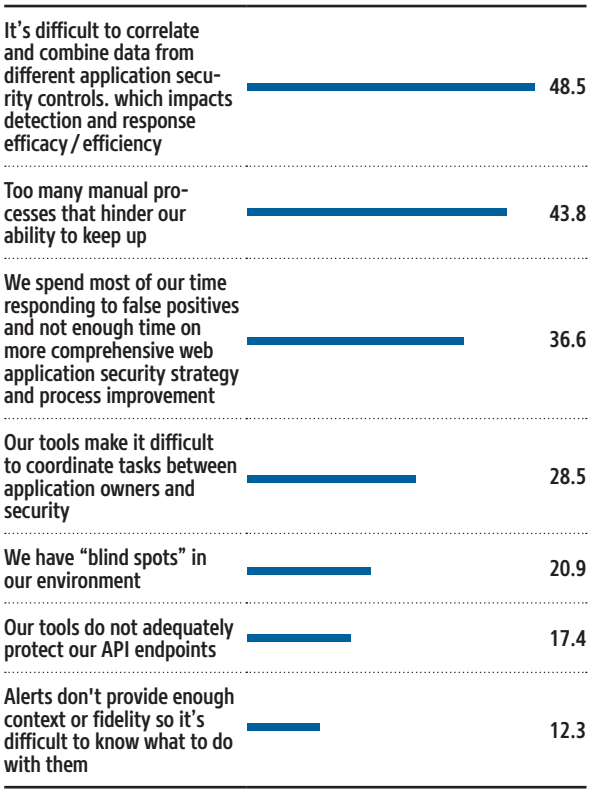
How do you identify an attack or attacker targeting your APIs?

Multiple answers possible. All data expressed as percentages. Basis: n = 235



Which of the following would you say are your organization's biggest challenges regarding web application security tools?

Multiple answers possible. All data expressed as percentages. Basis: n = 235



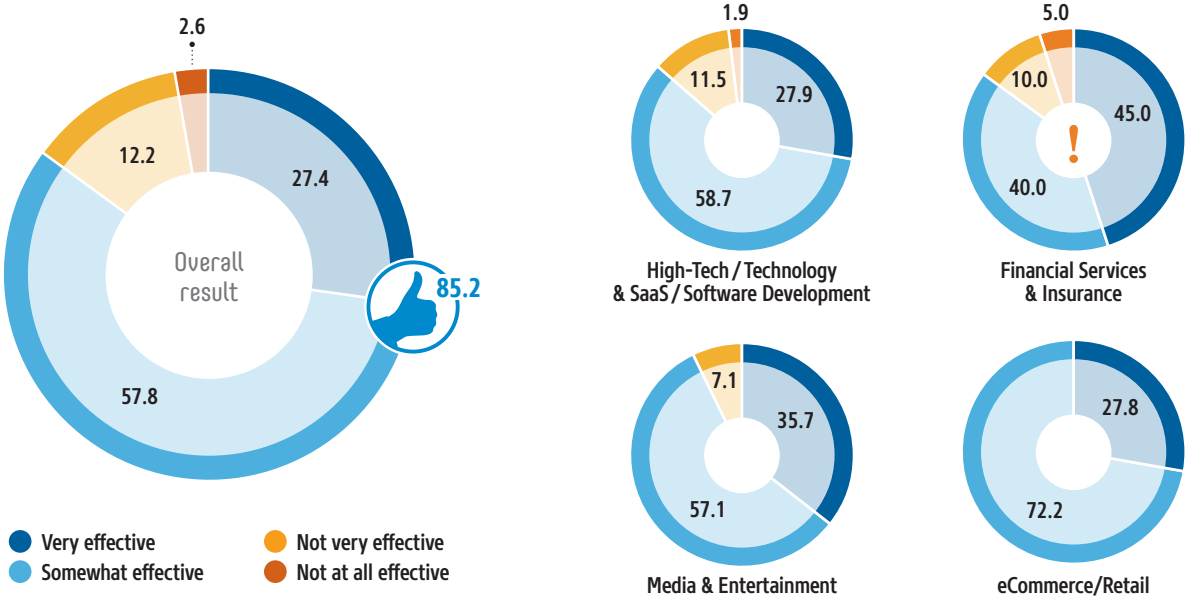
What's interesting is that 85 % of companies surveyed consider their API security tools to be effective, equally so in the finance and insurance sectors. This is somewhat surprising, as 29 % of respondents from this sector admit that they are unable to identify any API attacks.

Additionally, 49 % say that it is difficult to correlate and combine data from different application security controls, which impacts the efficacy and efficiency of detection and response.

Conclusion: The sheer volume of notifications that companies receive using their preferred solutions makes it difficult to reliably detect API attacks. This is especially true for assessing log data. It's essential that financial institutions conducting transactions via APIs conduct regular security assessments, and incident management planning to minimize risk. AI technologies that currently see only minimal use could be of great help here.

How effective are your existing security tools in preventing API attacks?

All data expressed as percentages. Basis: n = 235



6

Consolidated web and API security is becoming the standard

98 % of companies have an interest in a consolidated web application and API security solution from a single provider. 19 % of respondents are already using such a solution, 69 % are planning to introduce one, and a further 6 % are looking to find out more.

The use of a consolidated web application and API security solution from a single provider is widespread in Spain where 30 % of surveyed companies responded as such. In contrast, just seven % of companies in Nordics have moved to using a consolidated web and API security solution.

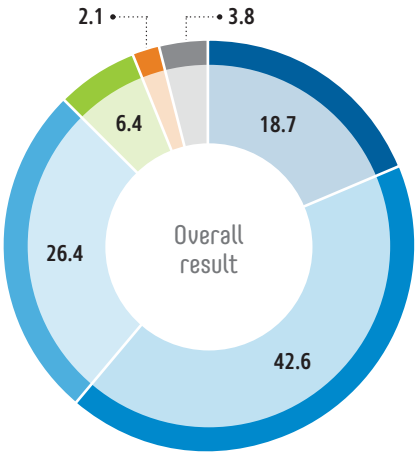
A key pillar of API security best practice dictates that keeping track of API activity by monitoring and logging suspicious, unusual or malicious requests and responses, is a must. A consolidated web application and API security solution would make instantaneous decisions in line to determine if malicious or anomalous payloads are present, and will help to improve the time to detect and prevent malicious traffic from reaching the API.

Looking at each sector we also see significant differences in shifting attitudes towards using a consolidated web application and API security solution from a single provider. 24 % of the financial institutes and insurers surveyed are currently using such a solution, but just five % of retail companies.

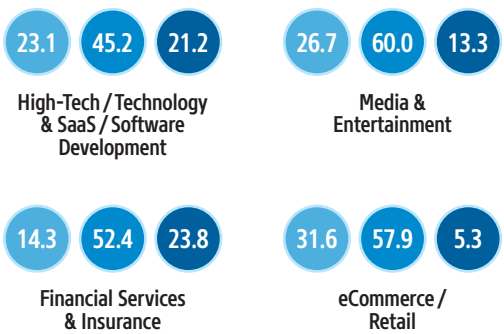
48 % of respondents said that the flexibility to protect different application architectures through different deployment models is important to them. At C-level and in compliance this figure rises to 59 %, but drops to 41 % among security experts. Regionally this flexibility is particularly popular in Spain, being stated by 51 % of respondents. Among the sectors surveyed this figure even rises to 71 % for financial services and insurers who say that it should be possible to protect various application architectures using different deployment models.

Which best describes your organization's use of, or interest in, a consolidated, web application and API security solution from a single vendor?

All data expressed as percentages. Basis: n = 235



Results split by sectors

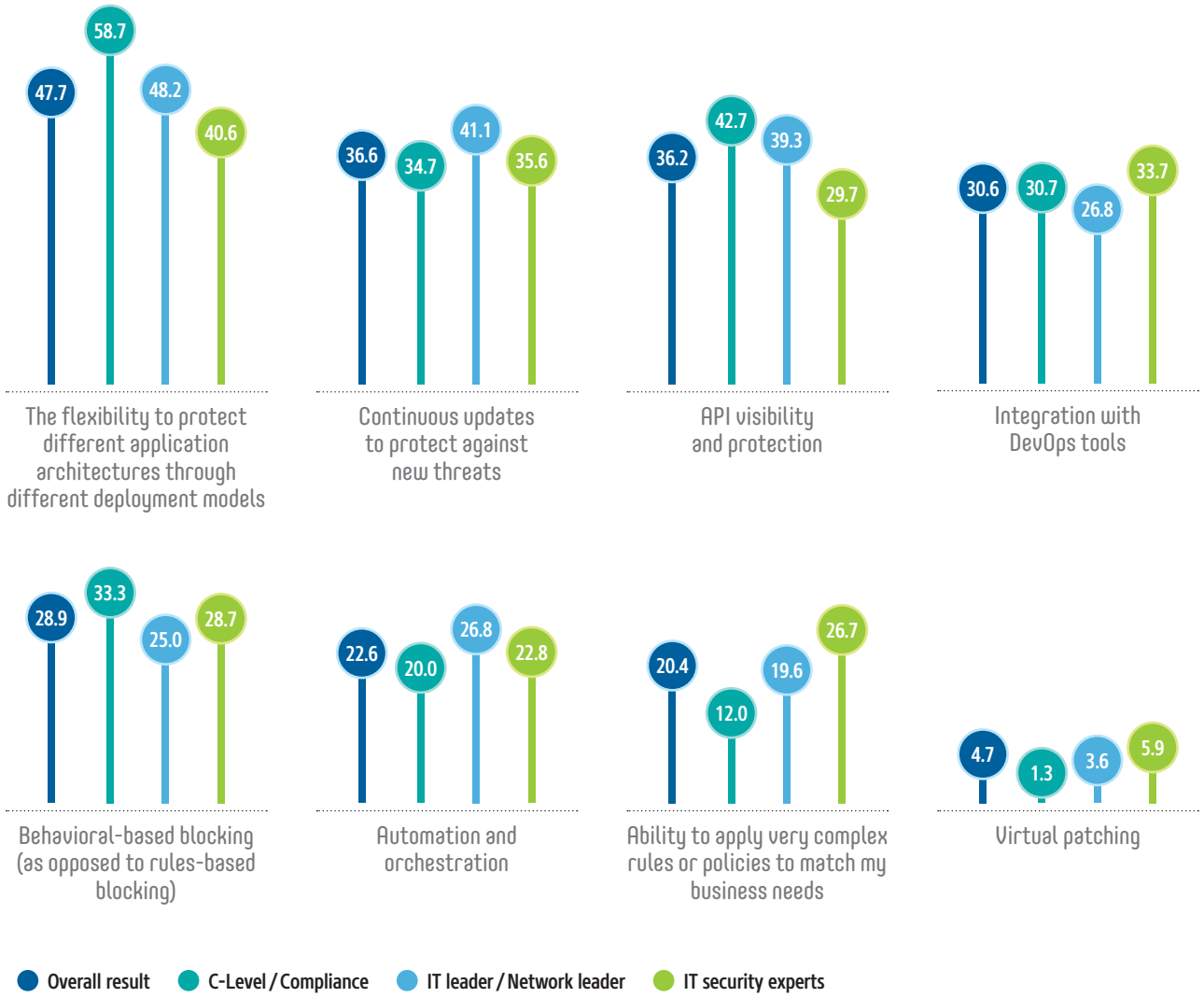


Interestingly, the C-level and compliance show below-average agreement on features for automation and orchestration, the ability to apply very complex rules or policies to match business needs, and virtual patching. For example, while the average for all respondents who consider the ability to apply complex rules and policies to match business needs to be important is 20 %, this figure for C-level and compliance is just twelve %, and for security experts 27 %.

Conclusion: There is a great desire for consolidation of web and API security and to concentrate on using a single provider. However, it appears that the C-level and compliance underestimate the complexity that must be handled by such solutions. Security experts need to be more informed about internal processes so that the desired solution is also able to deal with the complex requirements of their business.

In your opinion, which of the following attributes of a web application security solution are the most important?

All data expressed as percentages. Basis: n = 235



The great expectations for AI-based API security are not widely shared

58 % of the companies surveyed expect a high or very high degree of influence of AI on the security of APIs. Just four % have low to very low expectations. Among C-level and compliance respondents, the figure for those expecting a lot from AI in API security is 69 %.

Among the security experts surveyed, the high expectations for AI-based API security are less widely shared, at just 52 %.

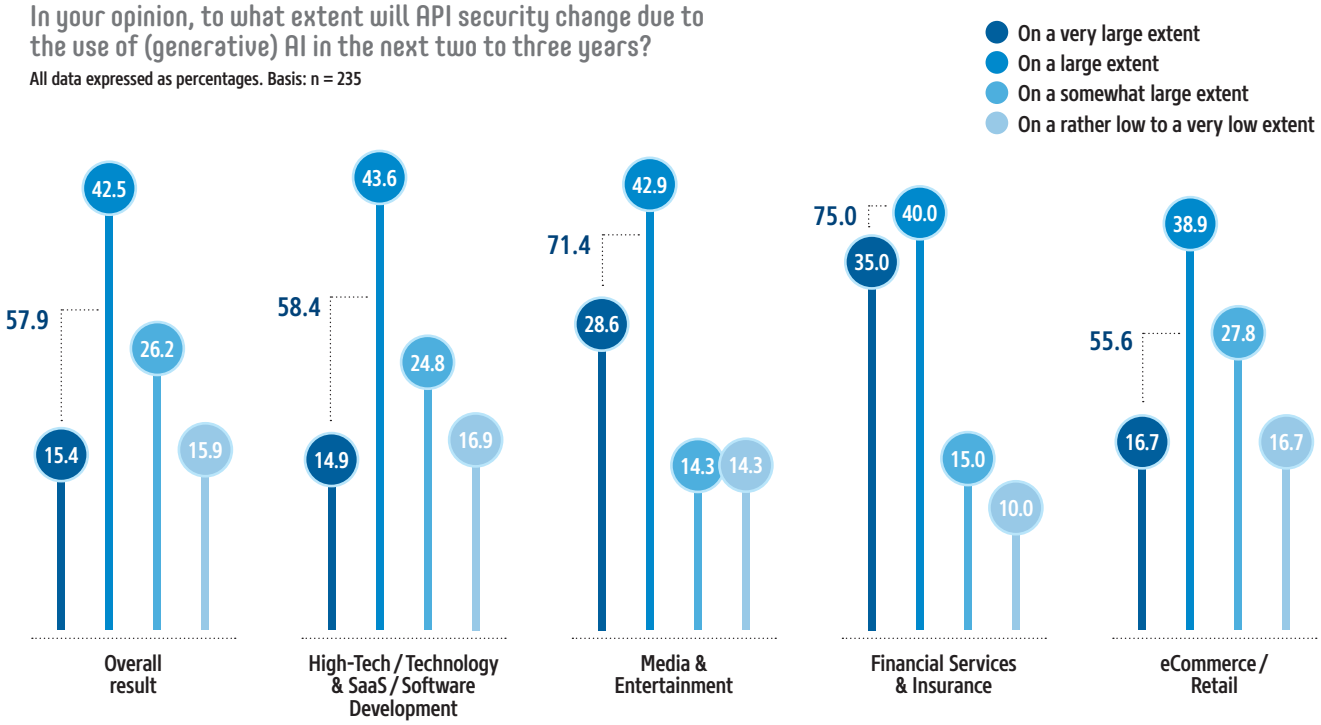
In the regional comparison, respondents from Spain and the DACH region most frequently express their belief in a high to very high degree of influence of AI on sAPI security with 65 % stating as such. Particularly low is the respective proportion of respondents in Nordics with just 48 % giving the same answer.

While 56% of companies in the retail and e-commerce sector expect the degree of influence of AI for the security of APIs to be high or very high, among financial institutions and insurers the figure rises to 75 %.

Conclusion: Across all business roles and sectors at least half of all respondents surveyed expect a high or very high degree of influence of AI on the security of APIs. This is surprising when we consider that AI-based tools – those that replace tasks that have historically required humans – for API security are not yet as widely used as expectations might otherwise indicate. There appear to be uncertainties and obstacles to implementation.

In your opinion, to what extent will API security change due to the use of (generative) AI in the next two to three years?

All data expressed as percentages. Basis: n = 235



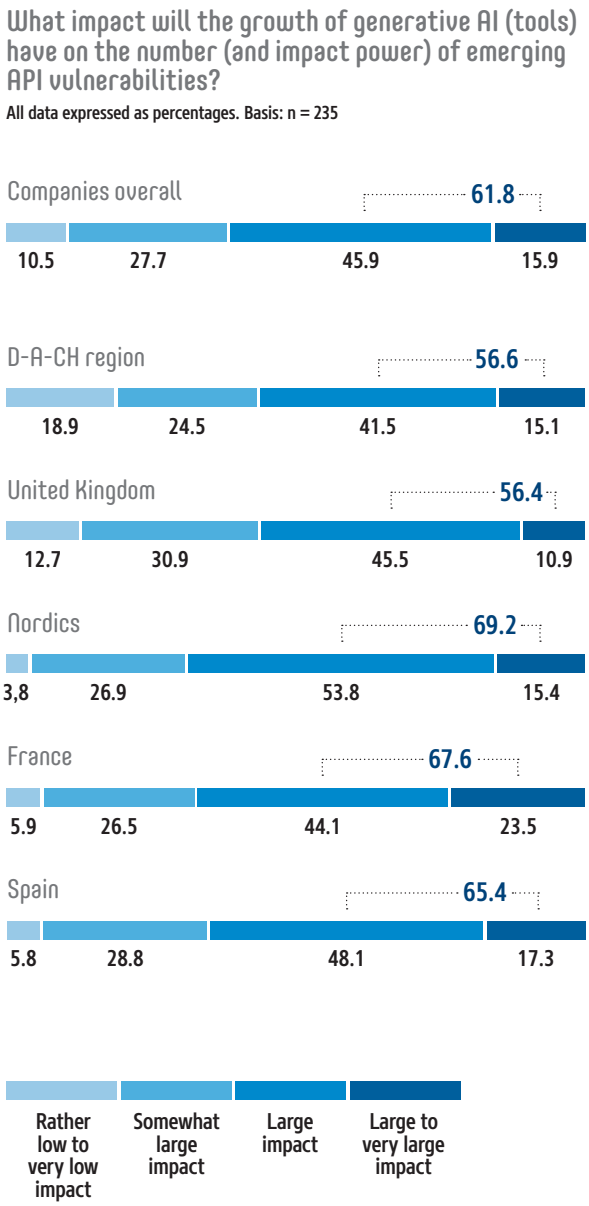
Companies also expect AI to affect the increase of API vulnerabilities

62 % of companies expect AI to have a high to very high degree of influence on the growth in newly identified API vulnerabilities, just one % say they do not expect this. The number of companies in Nordics who share this view is exceptionally high at 69 %. Just 56 % of respondents in the United Kingdom expressed this view.

The role of the respondent within the company also leads to differences. At the C-level and in compliance, 71 % say that the growth of generative AI tools will have a high to very high impact on emerging API vulnerabilities. Just 54 % of security experts said the same.

Looking at different sectors, in wholesale and retail / e-commerce there were significantly more respondents who expected a link between increasing AI use and the increasing number of API vulnerabilities with 72 % stating this. In contrast, the proportion of respondents with this view drops to 59 % among the high-tech / technology & SaaS / software development companies surveyed.

Conclusion: The majority of companies surveyed are also thinking about the possible API risks from AI use. However, taking the finance sector as an example, we see that the potential risks associated with AI should not mean shying away from its use. This is the opinion of 70 % of respondents in the finance sector where the impact of AI on increasing API vulnerabilities is expected to be high or very high. However, three-quarters of the companies surveyed in this sector also see the positive effects of AI use in API security.



D-A-CH region = Germany, Austria, Switzerland
Nordics = Denmark, Finland, Norway, Sweden

Lookin forward

API and web security are on the way to intelligent consolidation

APIs have become one of cybercriminals' favorite vectors for account takeover attacks. Credential stuffing, business logic abuse, and DDoS attacks are just some of the malicious automated bot attacks deployed to take over accounts and perpetrate identity theft and fraud. Readily available scripts and tools make orchestrating API attacks easier than ever, and legacy bot defense techniques struggle to detect these potentially devastating incursions. Given the serious threat APIs pose, the security of web applications and APIs must become more advanced, make more use of modern methods such as AI-based tools and avoid using isolated systems. Many companies have already recognised this, but need to position themselves better internally.

By Oliver Schonschek

The security of web applications and APIs is about to undergo a transformation. As this study shows, there is a lack of knowledge about the importance of secure APIs and web applications. Where there are doubts about the security of production APIs, many of the companies surveyed prefer to delay roll-outs and integrations.

New ways to look at risks and new technological priorities are needed

Certain vulnerabilities in API security are indeed seen as a significant threat, such as those in outdated APIs. In contrast, other risks such as brute force attacks on APIs take a back seat.

At the same time, companies are detecting security incidents with their APIs relating to things such as logins, permissions and identities. Given the high number of API security problems found in production IT systems, we would expect to see an increase in the security measures being taken in these areas. Experts estimate that total bot traffic is almost half of internet traffic and that bots that can perform content scraping, credential stuffing, and DDoS attacks account for over 30 %. A proactive bot defense strategy would help to understand and block bot activity before it impacts applications and APIs and can lead to significant financial losses through account compromise, data theft, fraud and increased infrastructure costs.

However, a lack of budgetary resources and expertise means this is not happening. Accordingly, most companies, 84 % of respondents, admit to not having any kind of advanced API security in place. In fact, technological priorities have not been set to look at the use of more advanced methods for better API protection. Logging and monitoring of APIs is the main focus. Whilst this is important, it is also not sufficient. The use of AI technologies was stated by just 14 % of companies as a priority.

There must be improved detection of API attacks

Even heavily regulated sectors such as finance and insurance are unable to sufficiently detect attacks on APIs. This is not surprising as companies rely more on API gateways and log data to alert them to API attacks.

However, the amount and complexity of data that indicators for API attacks can provide need to be evaluated more quickly and in a more consolidated manner so that cyber-attacks can be better detected and averted. Protracted searches through log data and isolated warnings from individual security tools cannot be the best way forward.

But improvements are coming: 88 % of companies surveyed are already using a consolidated web application and API security solution from a single provider or are at least planning to do so. This reduces the required workload and improves the visibility of API risks and attacks. Instead of using tools in silos, consolidated solutions can provide the all-around API and web application security that is required.

Consolidation and AI strengthen API security

The majority of companies also see great advantages in the use of AI-based tools to strengthen API security. This is particularly true for the companies surveyed in the financial and insurance sector who have up to now experienced great difficulty detecting API attacks.

The fact that around half of the companies cite an edge-native platform and cloud-native security as the most important (selection) criteria for the evaluation of API security solutions also gives cause for hope.

That said, there is still a need for a better understanding of the topic. 16 % said they do not know whether or not they are already using AI for their API security. Just 18 % said they are using AI for API security and 66 % said they are not.

In order to bring about the expected benefits of AI for API security, companies need to have a clearer idea about any AI-based tools they are already using or are planning to use.

The potential risks that may increase through the use of artificial intelligence (AI) must be on the security agenda. As the survey shows, the companies surveyed are highly aware of the risks that can arise, e.g. from online criminals using AI tools to more quickly and easily find vulnerabilities in APIs.

Six in ten companies expect AI to highly or very highly impact the number of API vulnerabilities. Just one % expects the effects of AI on the increasing number of API security vulnerabilities to be small or very small.

Conclusion: The majority of companies surveyed in the various sectors and regions have recognised the benefits of consolidating API and web security and have already implemented this or are planning to do so. Equally great are the interest in and expectations for using AI to support API security. However, more progress needs to be made on implementation in this regard. It is good to see that concerns relating to some extent to AI do not seem to mean that companies are ruling out AI for optimizing API security.

AI and consolidation must be prioritized or remain a priority in order to further advance the security of web applications and APIs. Attacks targeting web applications and APIs are already getting more advanced. The defense of APIs needs to catch up. This survey shows that things are looking good.

Case Study: Nine

Nine strengthens and streamlines security with Fastly's Managed Security Service

Nine, Australia's largest locally-owned media company, is home to Australia's most trusted and loved brands in news, business and finance, lifestyle, entertainment, and sport. Nine's investments include the 9Network television channel, major publications such as The Sydney Morning Herald, digital properties such as nine.com.au, subscription video platform Stan, and several radio stations.

The challenge

As Nine prepared to grow their web application security footprint, their platform engineering team realized they needed to consolidate on a single partner to help manage the security of their web applications. The partner would proactively deliver threat detection and response for Nine web applications as well as collaborative security expertise when needed. The right managed security service would also reduce the overhead of multiple service vendors and streamline tools and management with Nine's infrastructure-as-code approach. With a managed service to monitor for and proactively mitigate attacks, the Nine engineering team would have more time to focus on products and services to build the company's brands.

> "Fastly Managed Security Service is expanding our security capability – from bot protection to rate limiting to emerging threats. And we'll be able to continue to expand to our protection over time."
>
> Andre Lackmann,
> Technology Director at Nine

The solution

Nine chose the Fastly Next-Gen WAF and Managed Security Service for the security expertise, scalability, technology fit, and value.

Security expertise

Rather than Nine having to train their engineers as web application firewall (WAF) experts, they knew it would be more beneficial to use Fastly's Managed Security Service and let Fastly's experts proactively manage the Next-Gen WAF. "Nine welcomed the opportunity to allow Fastly to come in and make changes on our behalf," said Lee Webb, senior engineering manager at Nine.

"My principal engineers are impressed by the security experts that we've been given from Fastly — there's a high level of respect. It helps build trust when you've got folks who are just as talented as you are."

Nine's own SOC found great value in the threat-hunting reports that are a part of the Managed Security Service. "Fastly provided tuning recommendations as well as actionable threat intelligence and recommendations with concrete steps we could use to mitigate. It was on the strength of that we went down the path of implementing the Fastly Managed Security Service for all our public sites," said Webb.

By onboarding all of Nine's public-facing sites to Fastly's Managed Security Service, Nine removes complexity and duplication from its environment, including fewer toolsets. "There's a lot of time saved," said Webb.

Trusted partner

Nine engaged with Fastly in 2017 to re-platform legacy systems to a microservices approach. At that time, the company took on Fastly as a Content Delivery Network (CDN) provider. Over the years, Fastly proved to be easy to work with and capable. During a beta program, the Fastly Managed Security Service team proved its ability to proactively protect web apps from cyber threats and provide expert cybersecurity collaboration.

When Nine used the Managed Security Service during some of its biggest sporting events, such as the Australian Open tennis tournament, Fastly's Customer Security Operations Center (CSOC), which provides 24/7 monitoring and response for the Managed Security Service, proved to be a proactive and service-oriented partner. "We were very happy with the security service Fastly provided," said Lee.

"Our relationship with Fastly is trusted but verified," said Webb. "We trust that Fastly can get the job done because they've proven it as our relationship has grown."

Reduced toil

"Fastly enabled our teams to not focus as much on that toil aspect, on that day-to-day monitoring. It's enabled us to focus on the implementation side and how our services might be delivered from a technology perspective and focus on the user experience," said Andre Lackmann.

About Nine

Industry: Streaming Media, Digital Publishing

Location: Asia Pacific

Customer since: 2017

Favorite features: Managed Security Services, NG WAF, CDN

Nine is Australia's largest locally owned media company with investments spanning television, video on demand, print, digital, and radio. Nine's assets include the 9Network, major mastheads such as The Sydney Morning Herald, The Age and Australian Financial Review, digital properties such as nine.com.au, 9Honey, Pedestrian Group, and Drive, subscription video platform Stan, talk-back radio and majority investments in Domain and Future Women.

www.nineforbrands.com.au

A related benefit that Nine has seen is the substantial reduction of alert spam going to their security operations center (SOC). Not only does the Fastly Next-Gen WAF feature far greater accuracy and virtually no false positives, but with Fastly's CSOC monitoring the WAF, only escalated alerts come through. The team appreciates the use of Slack as the primary notification channel with guidelines for when SMS and phone calls are warranted.

Natural technology fit

Fastly's edge cloud platform, including its CDN, security products, and managed services fit well into Nine's infrastructure-as-code approach to software delivery. Fastly slots in easily, rather than Nine having to accommodate a different approach from another vendor. "The technology fit is amazing," said Webb.

Nine engineers look after their applications all the way to the edge and can do that with Fastly security tools such as Next-Gen WAF, as Fastly empowers Nine to maintain control over their technology stack while seamlessly integrating advanced security measures. "Other managed security vendors didn't allow for that," said Webb.

Focus on the next three Summer Olympics

Looking forward, as the threat landscape evolves, Nine values the peace of mind that Fastly's Managed Security Service gives them. "There's professional security assistance that stays on top of emerging threats, monitors continuously, and helps us respond. And that becomes really important as Nine takes on the rights for the Summer Olympics," said Andre Lackmann, technology director at Nine. "We're no stranger to larger events but there isn't any event larger than the Olympics. It's a massive undertaking from a technology point of view, including security. So, we're looking forward to working with Fastly as we deliver a high-quality user experience for our Australian viewers and readers."

Study profile

Publisher	CSO, CIO and COMPUTERWOCHE
Exclusive study partner	Fastly
Population	C-Level Executives – CISOs, CIOs, VP Security IT Security Leaders or IT leaders within the platform or DevSecOps teams (decision makers) Security experts, Security Analysts, Security Architects (influencers) from the following regions: DACH, Nordics, UK, France and Spain
Participant generation	Personal e-mail invitation via the exclusive decision-maker database of CIO, CSO and COMPUTERWOCHE and – to meet quota requirements – via external online access panels
Total Sample	235 completed and qualified interviews
Investigation period	15. to 23. November 2023
Method	Online-Survey (CAWI)
Questionnaire development und Durchführung	Custom Research Team of CSO, CIO and COMPUTERWOCHE in coordination with the study partner

Sample statistics

Functional role	C-Level (CSO, CISO, CIO, CTO, VP IT Security)	30.2 %
	IT leader, IT manager with dedicated IT security responsibility	17.0 %
	IT Security leader, IT security manager	20.4 %
	Director Cybersecurity	6.0 %
	DevSecOps team	5.1 %
	Security expert, Security Analyst, Security Architect	11.5 %
	Network leader	6.8 %
	Compliance / Risk Management	1.7 %
	Others	1.3 %
Annual spending on IT-system	Less than 5 percent of total IT budget	13.6 %
	5 to less than 10 percent of total IT budget	35.7 %
	10 to less than 20 percent of total IT budget	27.2 %
	20 to 30 percent of the total IT budget	13.6 %
	More than 30 percent of total IT budget	4.3 %
	Don‘t know / no answer	5.5 %

Imprint

Exclusive study partner

Fastly
179 Great Portland St
London W1W 5PL, United Kingdom
Phone: +44 1908 038958
Email: team-emea-sales@fastly.com
Website: www.fastly.com

Overall study management

Matthias Teichmann
Director Research
Foundry Global Services
Phone: +49 89 36086 131
mteichmann@idg.de

Study concept / questionnaire development:
Matthias Teichmann (Foundry),

Final Review / Managing Editor for Final Study Report:
Matthias Teichmann

Analyses / Comments:
Oliver Schonschek, Bad Ems

Hosting / Coordination of Field Work:
Armin Rozsa (Foundry)

Layout:
Patrick Birnbreier, Munich

Cover design using an illustration from ©shutterstock.com/BadBrother

Editing:
Elke Reinhold, Munich

Contact:
Matthias Teichmann
matthias.teichmann@foundryco.com

Publisher:

Foundry
(formerly IDG Communications)

IDG Tech Media GmbH
Georg-Brauchle-Ring 23
80992 Munich, Germany
Phone: +49 89 360860
Fax: +49 89 36086 118
Email: info@idg.de

Authorised representative:
Jonas Triebel, Managing Director

Court of Registration:
Munich District Court HRB 99110

VAT ID Number: DE 811 257 834

Further information available on:
www.foundryco.com

About Fastly

Fastly's programmable edge cloud platform helps the world's top brands deliver the fastest online experiences possible, while improving site performance, enhancing security, and empowering innovation at global scale. With world-class support that achieves 95%+ average annual customer satisfaction ratings, Fastly's suite of edge compute, delivery, security and observability offerings have been recognized as leading solutions by industry analysts. Compared to legacy providers, Fastly's powerful and modern network architecture is one of the fastest on the planet, empowering developers to deliver secure websites and apps at global scale with rapid time-to-market and industry leading cost savings. Thousands of the world's most prominent organizations trust Fastly to help them upgrade the internet experience, including Reddit, Pinterest, Stripe, Neiman Marcus, The New York Times, Epic Games, and GitHub.

Security is an essential part of every online business, and customers rely on Fastly to help rapidly secure their business-critical websites, apps, and APIs. Fastly modern approach to application security provides the accuracy, flexibility, and ease-of-use that our customers have come to know and expect. Fastly provides a range of security solutions for businesses that focus on protecting websites, apps, and APIs from various threats, including DDoS attacks, application layer attacks and abusive behavior from automated software. These solutions are designed to be real-time, scalable, and customizable, offering businesses the ability to tailor their security to their specific needs. With a focus on performance and flexibility, Fastly enables businesses to safeguard their digital experiences.

Fastly provides the proactive protection modern apps require while integrating into your DevOps and security toolchains for unparalleled visibility. Our flexible architecture can advance your application security strategy by providing developers, operations, and security teams insight into where and how your web applications and APIs are attacked.

fastly®

Learn more about Fastly at www.fastly.com