May 2021

The state of application security in 2021

Bad bots, broken APIs, and supply chain attacks put business data at risk. »

Barracuda

Your journey, secured.

Contents

Introduction

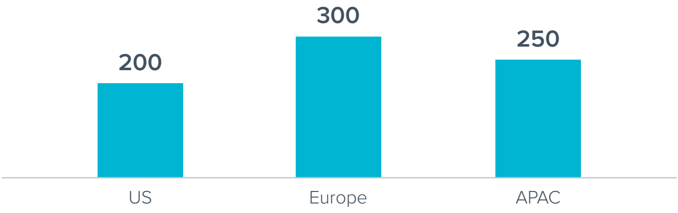
The state of application security in 2021

Businesses are facing an array of challenges when it comes to application security. Over the years, web applications have been rising steadily as the top attack vector for breaches — and the move to remote work in 2020 intensified this shift. Many organizations had to expose internal applications to the internet, and a significant number had to rapidly lift and shift applications to the cloud.

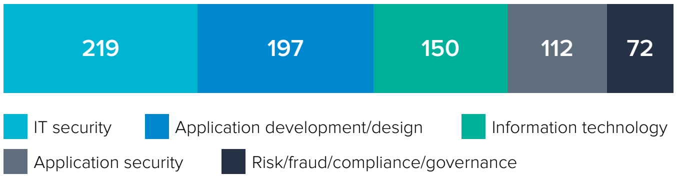
As part of this survey, we asked organizations about the number of times they were breached in the past year as a direct result of a vulnerability in one of their applications, and the worldwide average was two breaches in the past 12 months.

Respondents stated that the vast majority of these attacks were due to web application vulnerabilities. Bot attacks, struggles with API security, and software supply chain attacks are among the main contributing factors to these breaches. Survey respondents readily admit that significant improvements are required in all three areas — and while there were some interesting regional and sub-regional differences, the trends were very similar globally.

Respondents by region



Respondents by job function



Methodology

Barracuda commissioned independent market researcher Vanson Bourne to conduct a global survey of **750 application security decision makers** responsible for their organization’s application development and security. Survey participants from the **U.S., Europe and APAC** represented organizations with 500 or more employees globally. Since IT responsibilities and cybersecurity threats vary by region, respondents from a variety of job functions and industry sectors were surveyed, to get an understanding of application security risks from multiple perspectives. The survey was fielded in March and April 2021.

Top global challenges

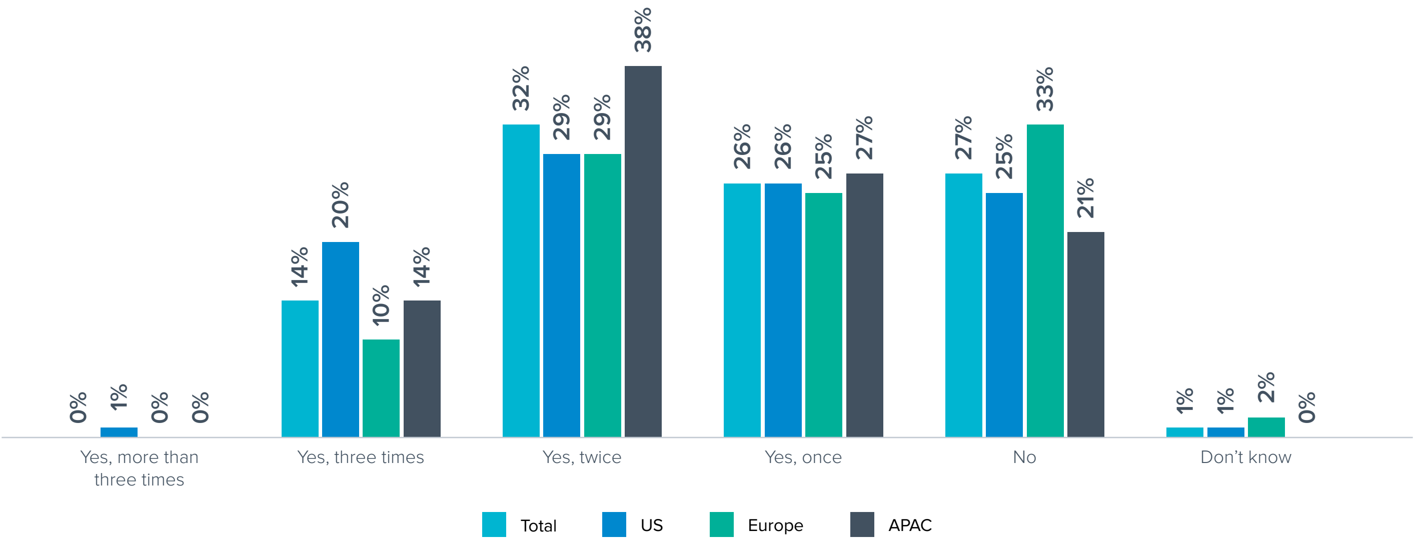
FINDING #1

On average, respondent organizations were successfully breached twice in the past 12 months as a direct result of an application vulnerability.

With 72% of respondents saying their organization suffered at least one security breach from an application vulnerability, it's plain to see how aggressive and pervasive application-based cyberattacks have become. This is likely due to the huge range of security threats trying to harm organizations and the internal difficulties many organizations are facing.

In the past 12 months has your organization suffered a successful security breach as a direct result of a vulnerability in one of its applications?

(n=750)



Top global challenges

FINDING #2

The range of application security-related challenges facing organizations extends beyond difficulties securing multiple attack vectors.

While it's clear that organizations are being troubled by specific security threats against their applications such as bot attacks, software supply chain attacks, and securing their APIs, these aren't the only challenges. Efficiency demands are also causing an issue, as evidenced by the 35% who report that adding security significantly slows application development time.

The top five challenges from a worldwide perspective are bots, supply chain attacks, vulnerability detection, API security, and security slowing down app development.

There are some interesting regional variations. In the U.S., vulnerability detection doesn't make the top five. Instead, implementing security into continuous integration and continuous development practices is a top challenge.

Europe, on the other hand, is less concerned about supply chain attacks and app security slowing down development. Threat remediation is seen as a bigger challenge.

In APAC, security slowing down app development is a much larger concern than in other regions.

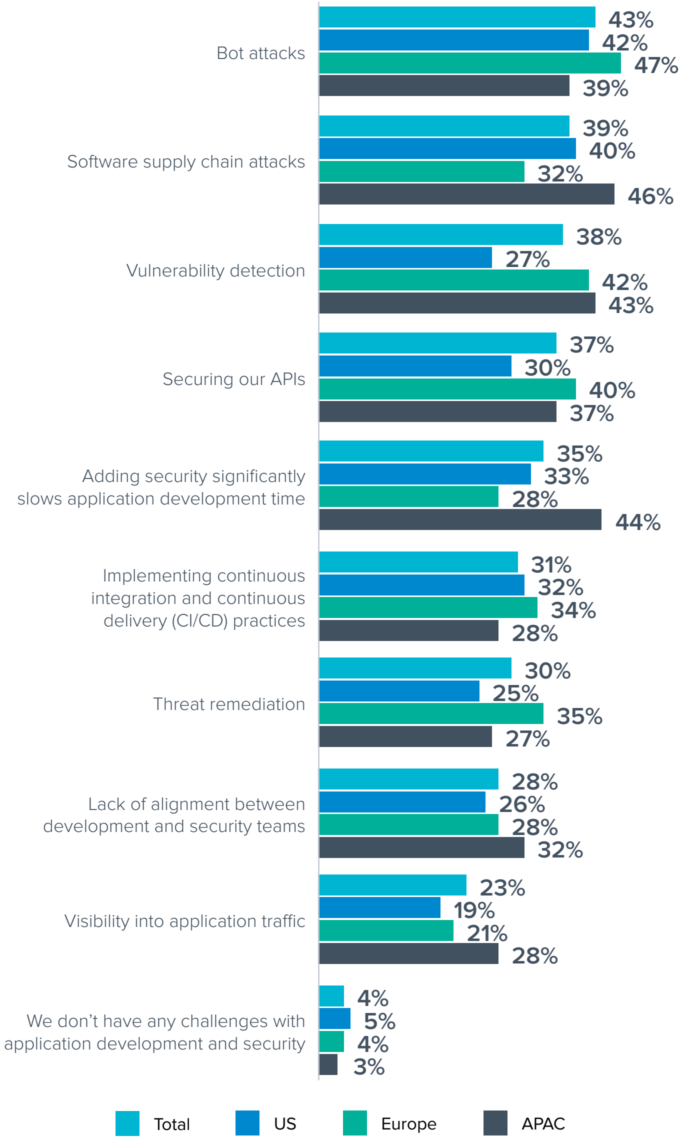
Vulnerability detection is a challenge with many relatively mature solutions available, and the challenge of implementing security in the development phase, especially in DevOps environments, is in itself a complex subject.

In this report, we focus on the newer challenges of:

- Bots
- Supply chain attacks
- API security

Which of these challenges does your organization experience with application development and security?

(n=750)



Top global challenges

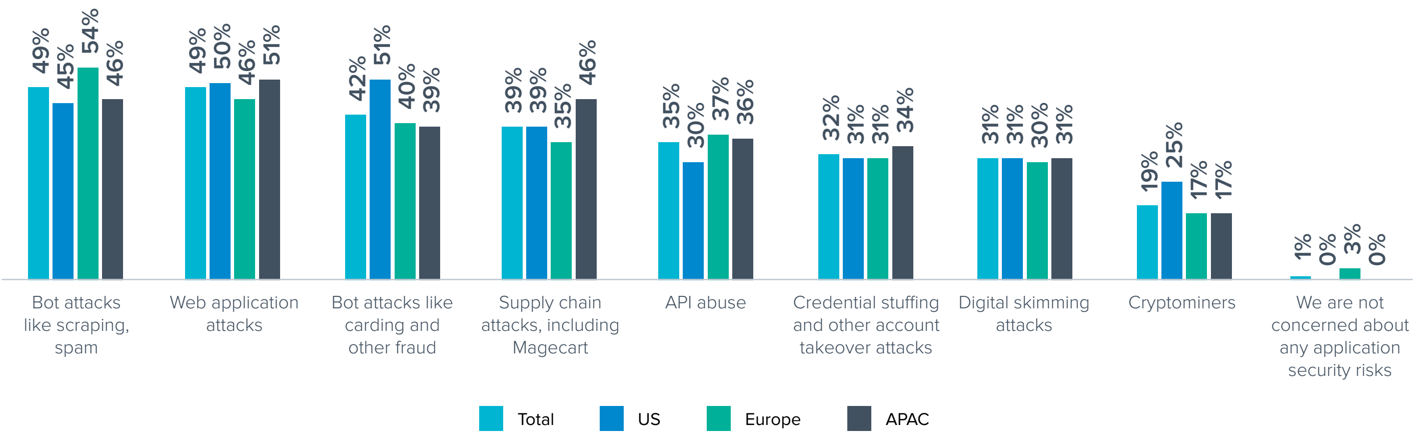
FINDING #3

A wide range of application security risks are causing concern, with the variations of bot-based attacks being a particular worry.

It's no secret that bots have become a growing problem for organizations over the past few years, and this is reinforced by the fact that bot-based attacks make up two of the top three application security risks most commonly cited by decision makers as part of their top three risks. This is closely followed by API attacks and supply chain attacks. Organizations must not lose focus on the importance of application security: One of these risks could easily exploit a vulnerability, and it could be hard to recover from the ramifications. This is illustrated by the number of respondents choosing web application vulnerabilities/zero-day attacks as one of the top risks.

Which AppSec risks are you most concerned about at your organization?

(n=750)



Bot attacks

FINDING #4

The range of bot attacks that can exploit applications is a real problem.

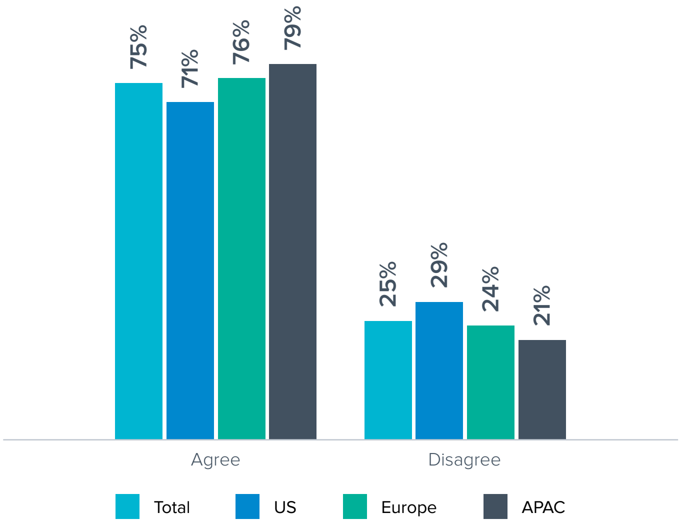
Three-quarters of decision makers confirm that the range of bot attacks are causing genuine difficulties in their organizations when it comes to protecting applications. It appears organizations simply can't keep up. With an entire bot economy existing online, complete with bot marketplaces and brokers to ensure that bot users themselves don't get scammed, this problem is only going to continue growing over the coming years. Automated attacks cover such a wide variety of vectors and intelligence on the tooling side that this has become a massive issue worldwide

Organizations will need external help from expert vendors for application and bot security to put up an effective resistance against bots targeting their applications. Without proper defenses, they will inevitability be breached, or, in some cases, breached again.

In our data, respondents from organizations that were breached more than once were most likely to agree with this statement, suggesting that bots were likely a cause of many of these breaches.

The varied range of bot attacks that could exploit our applications makes them increasingly difficult to defend against.

(n=750)



Bot attacks

FINDING #5

Bot-based attacks are the most likely contributor to successful security breaches resulting from application vulnerabilities in the past 12 months.

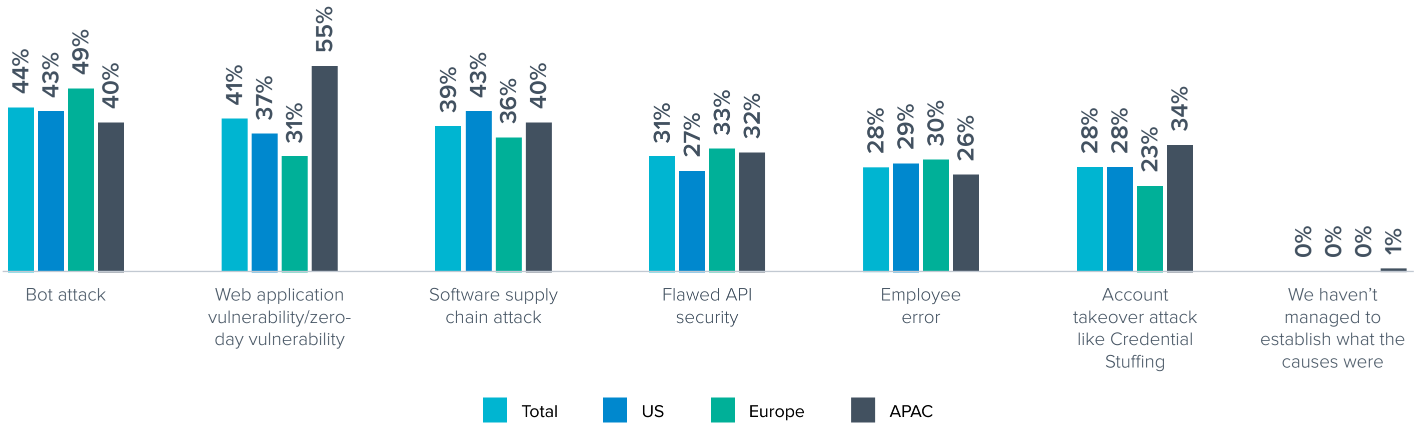
The concern levels around bots are well founded, as they have been particularly successful at breaching applications over the past year. But this certainly isn't the only vector that has contributed.

On average, respondents report that there were two contributing factors to the most recent breach suffered by their business, indicating the extent of the challenge.

The situation becomes even more concerning when considering that more than a quarter (28%) report that employee error was a factor in the most recent breach. Organizations can put as many security tools in place as they see fit, but if an employee makes a mistake that leaves the door open, then a bot-based attack, software supply chain attack, or any other attack will be quick to exploit this vulnerability.

Which of the following contributed to the successful security breach that exploited a vulnerability in one of your organization's applications in the last 12 months?

(n=541)



Bot attacks

FINDING #6

The wide array of bot attacks that target applications makes it a struggle for defenders to block them.

With so much variety in this attack vector, it's no surprise that so many organizations are struggling to defend their applications against bots. While bot spam is more of a nuisance attack, it is often used as a smokescreen to hide something more malicious, so it must be dealt with, not ignored. Depending on its frequency and authenticity, bot spam can become really tricky to defend against and can evolve from benign annoyances to operational problems quite easily.

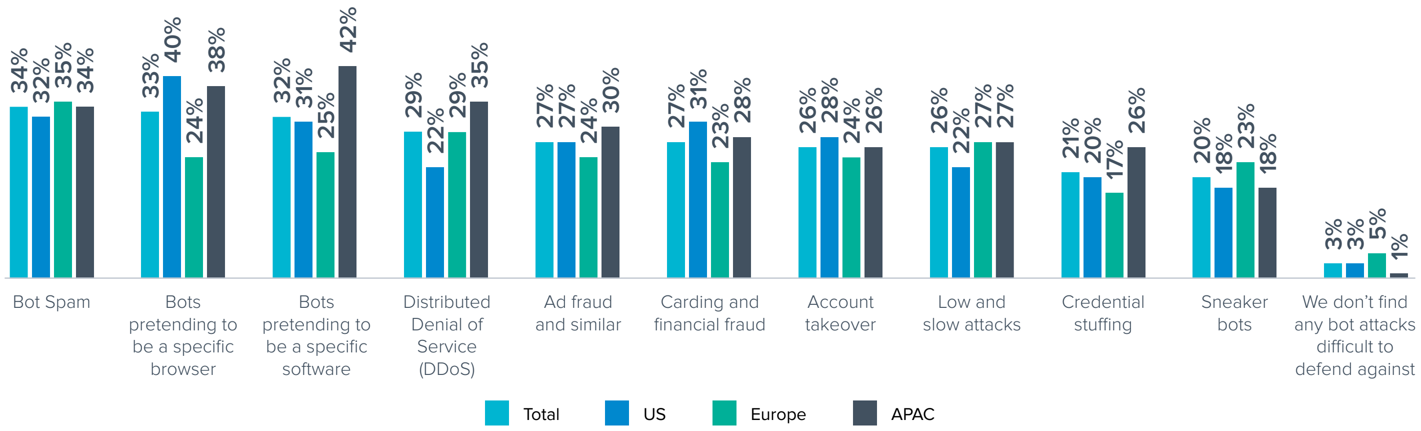
Bots spoofing browsers and apps are also major problems. These spoofs range from simple to complex, from a user trying to hide their real browser to bots running compromised versions of apps in click farms for ad-fraud or other malicious purposes.

Any of these bots used in conjunction with one another increases their chances of being successful. Multi-vector low and slow bot attacks are at the core of the problem and most likely contributed to successful breaches in the past year.

There are some interesting regional variations. APAC is the region most worried about DDoS attacks, far exceeding other regions and the worldwide average. Browser spoofing was top of mind for the U.S., and software spoofing came out highest in APAC. In Europe, sneaker bots are a concern.

Which types of bot attack targeted at applications does your organization find it difficult to defend against?

(n=750)



Bot attacks

FINDING #7

Preventing, detecting, and identifying bots will be critical functionality for vendors that help organizations defend against bot-based attacks.

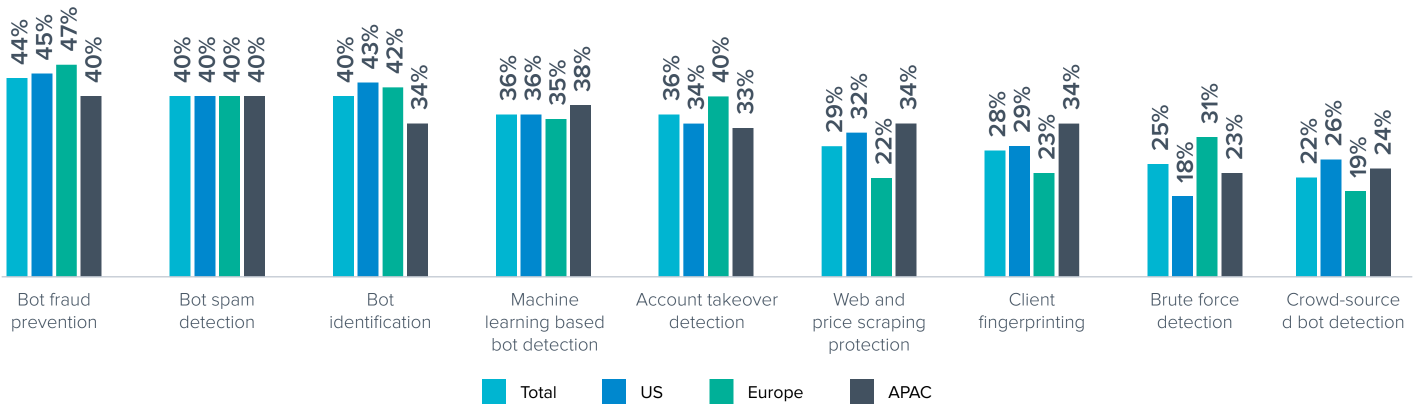
Whether organizations are struggling with spam bots, fraudulent bots, or bots that can spoof software and browsers, they urgently require improvements when it comes to defending against this attack vector. After all, bots are the most prolific contributor to successful breaches against applications in the past year. According to respondents, there are three clear areas that would be among the most desirable when choosing a security solution to fend off bots: fraud prevention, spam detection, and bot identification.

Which features would be most important to your organization when choosing a security solution to help defend applications against bot attacks?

(n=750)

These types of features would be critical for defending against most attack types, but any vendor that can provide these characteristics within a single solution will be improving the existing bot protection capabilities of most organizations beyond measure.

In these two key findings, Europe is consistently seeing account takeover detection and brute force detection as more important features than the U.S. and APAC. This is likely due to the privacy protections, and the cost of a breach in the GDPR regime. The fact that these attacks are being performed by low and slow bots also makes them difficult to defend against.



API security

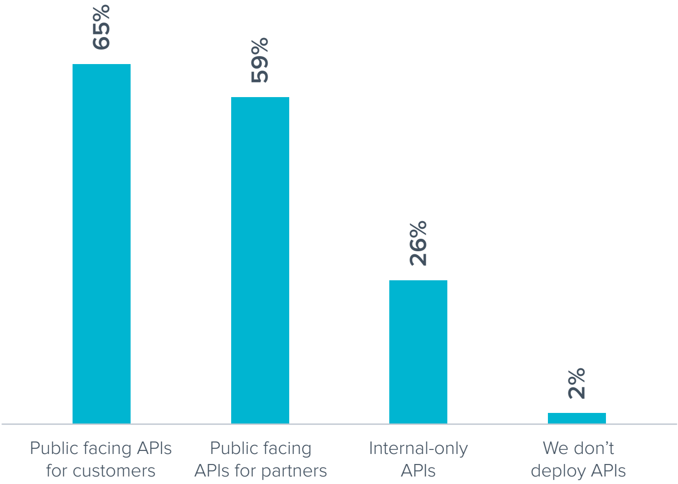
FINDING #8

Public facing APIs are commonplace, making it imperative they are properly secured.

Quite a large percentage of the surveyed organizations deploy public facing APIs for their customers (B2C) and partners (B2B), which speaks to the fact that most organizations are moving to API-first development. APIs make development of newer versions of applications much faster and extend the usability of these applications, but they also create a large new attack surface for cybercriminals. Flawed API security continues to be a big contributor to significant data breaches in the past two years, so organizations must ensure they cover all their bases when it comes to protecting APIs.

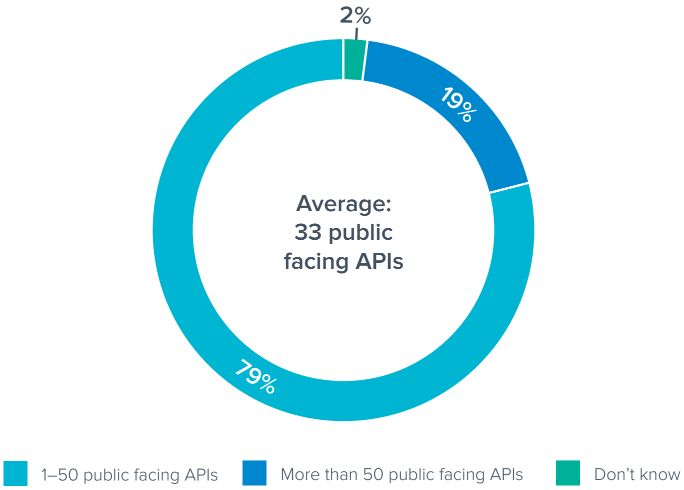
What types of APIs does your organization deploy?

(n=750)



How many public facing APIs does your organization deploy?

(n=642)



API security

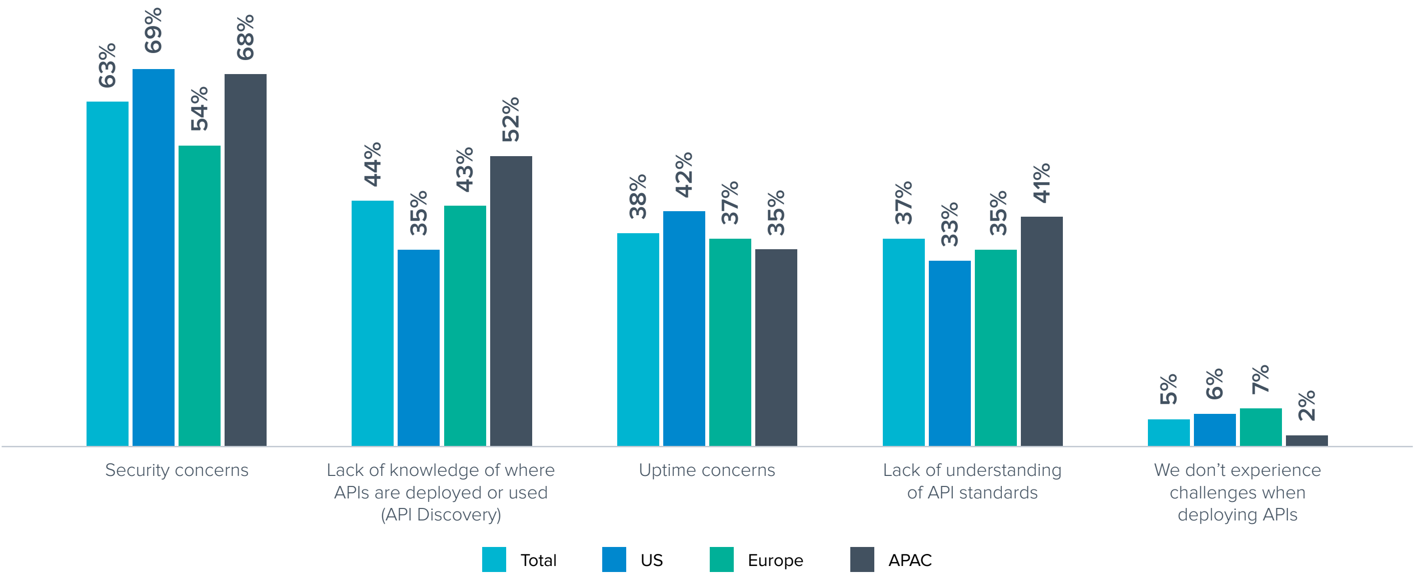
FINDING #9

Security concerns are top of mind when it comes to APIs.

It should come as little surprise that decision makers across all regions place security concerns atop the list of challenges that their organizations struggle with when deploying APIs. An API-based application is significantly more exposed than a traditional web-based application, due to the way it's deployed with direct access to all the sensitive data for the application. Undoubtedly, the gaps in knowledge cited around where APIs are deployed or used, as well as API standards, will be contributing to these concerns.

What are the main challenges your organization experiences when deploying APIs?

(n=728)

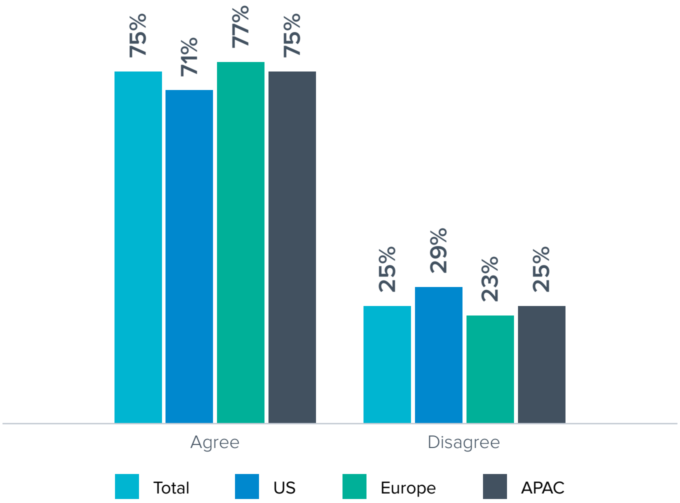


Organizations have raced toward APIs, due to the benefits they can deliver, but security hasn't fully kept up. This presents increased opportunities for attackers to exploit flaws. Some reasons for this are a lack of understanding of API security, configuration/employee errors, a misguided belief that the end user will not know that there is an API at work in the background, and in many, many cases, application teams publicly deploying test APIs with direct access to production data without any security in place.

We also asked the respondents if the use of APIs presented a security challenge for their organization, and 75% agreed. Most clearly understand the risks of APIs, and this is a good sign for the future of API security.

The use of APIs has presented security challenges for my organization

(n=728)



API security

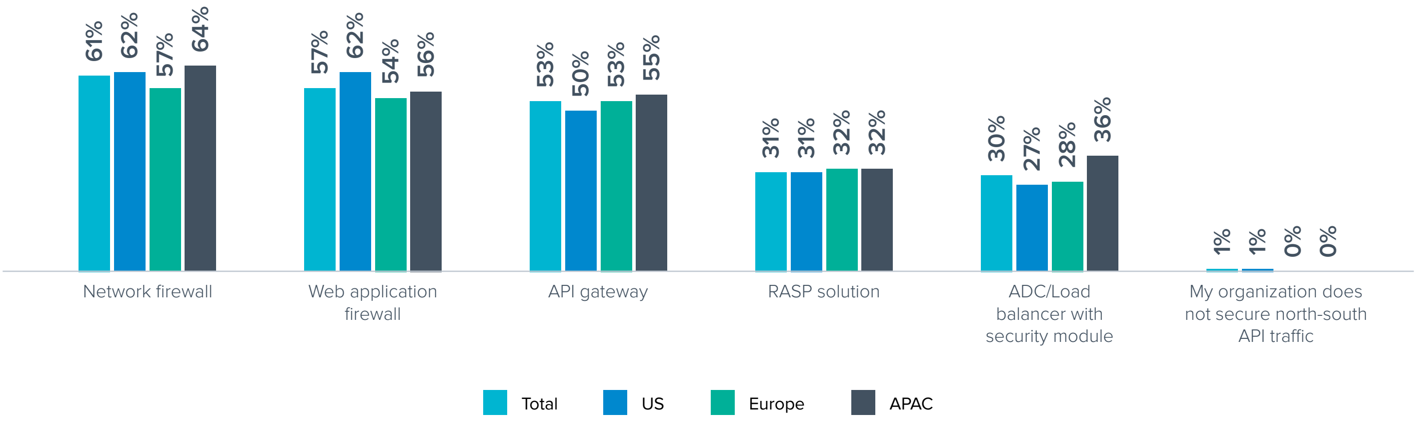
FINDING #10

Organizations have put in place a number of solutions to secure their APIs — both for inbound-outbound and inter-API traffic — but a majority feel that significant improvements are required.

On average, organizations are using more than one tool to secure their API traffic. However, clearly this hasn't done much to ease concerns around API security, and it indicates that the current solutions in place for securing all forms of traffic either aren't working to the desired level or aren't integrating well together to secure APIs from all angles. API security is still very much an area that is in its growing stages, and many of the solutions that are being used to protect APIs may not provide enough security. For instance, network firewalls cannot enforce more than signature-based security, IP-based rate limiting or IP-based access controls for the APIs. They cannot enforce positive security for the API or import an API spec to automatically configure controls. API gateways perform very well in the API management/traffic management sphere but may not offer complete API security in their toolset. It is interesting to see organizations evolving their multi-layered protections for APIs, but there is a lot of room to improve.

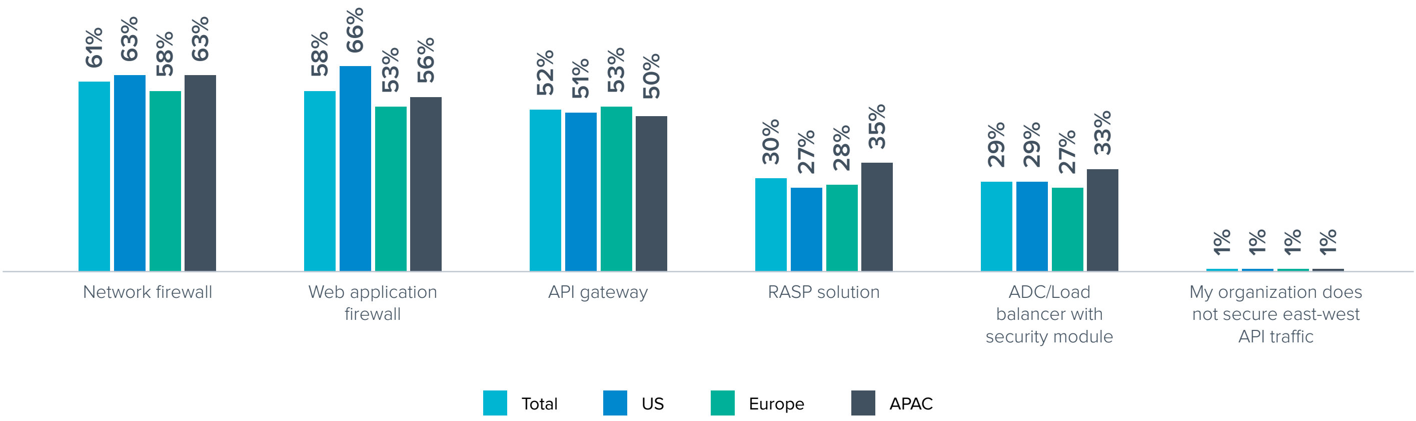
Which solutions does your organization use to secure north-south API traffic (inbound-outbound)?

(n=728)



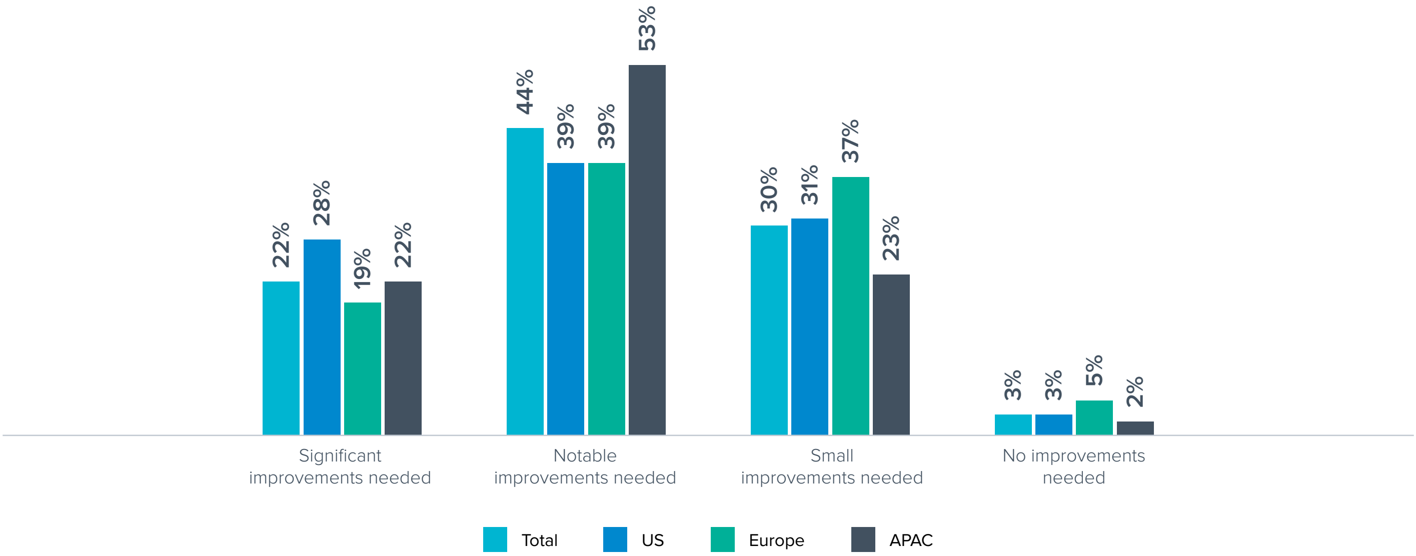
Which solutions does your organization use to secure east-west API traffic (application-application and API-API)?

(n=728)



What level of improvement do you believe is needed in your organization when it comes to API Security?

(n=728)



Software supply chain attacks

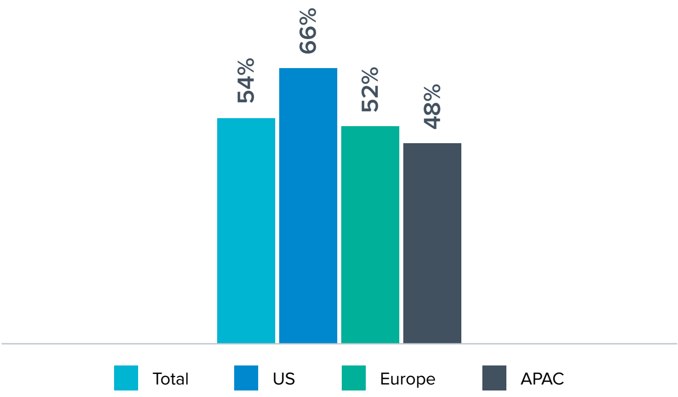
FINDING #11

The use of third-party scripts for web applications is fairly widespread, with organizations using varying methods to deliver scripts to a browser.

The drive for efficiency when it comes to application development is once again evident, with more than half of organizations, on average, using ready-made third-party scripts for web applications. Security should be a big concern when using third-party code. This is especially true when code is being delivered to a browser directly from the source platform, such as GitHub. If the code has been tampered with, a software supply chain attack, such as Magecart, could be just around the corner. Organizations should be wary of this approach to application development.

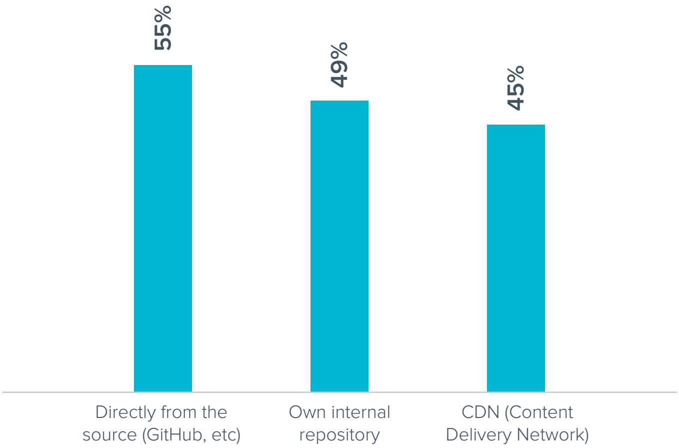
Approximately, what percentage of your organization's web applications use third-party scripts?

(n=750)



What are the ways your organization's websites deliver client-side scripts to a browser?

(n=750)



Software supply chain attacks

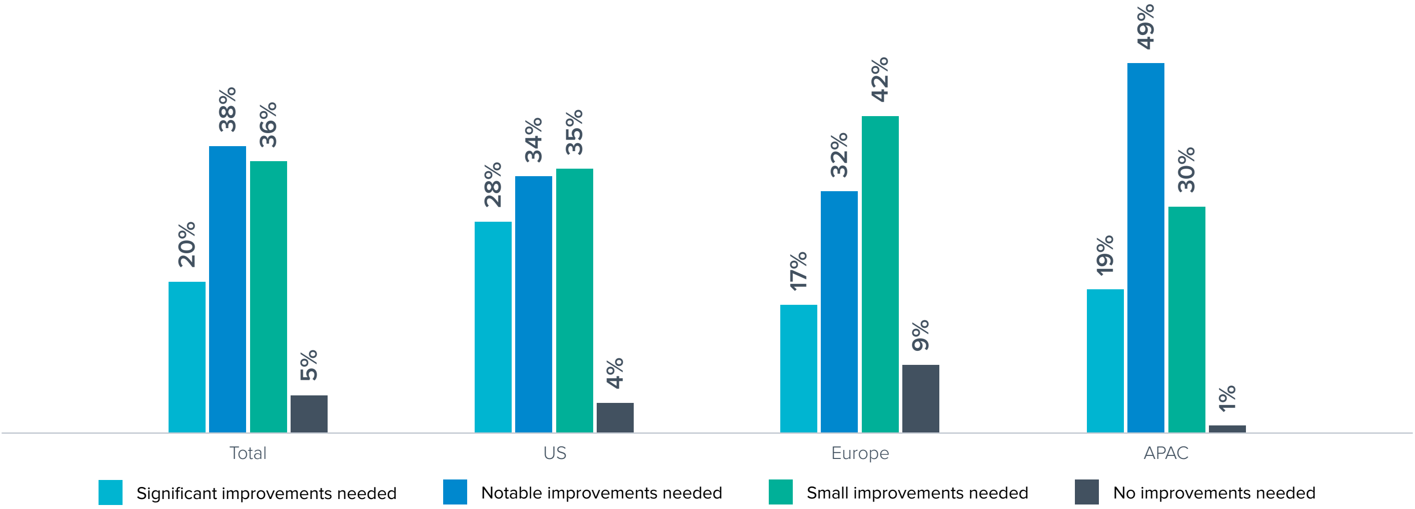
FINDING #12

Regardless of the technologies in place for protecting against software supply chain attacks, respondents are keenly aware that their organization must improve in this area.

Software supply chain attacks have become increasingly mature, with some scripts even able to avoid executing malicious code if they detect that a web vulnerability scanner is running, making them extremely difficult to defend against. This adds another layer of complexity to the ever-evolving threat landscape. Although organizations are deploying a range of technologies to protect themselves, it appears that this attack vector, much like bot attacks, is always one step ahead. And with recent high-profile breaches in mind, most regions understand that considerable improvements are needed when it comes to software supply chain attacks.

What level of improvement is needed in your organization when it comes to defending against software supply chain attacks?

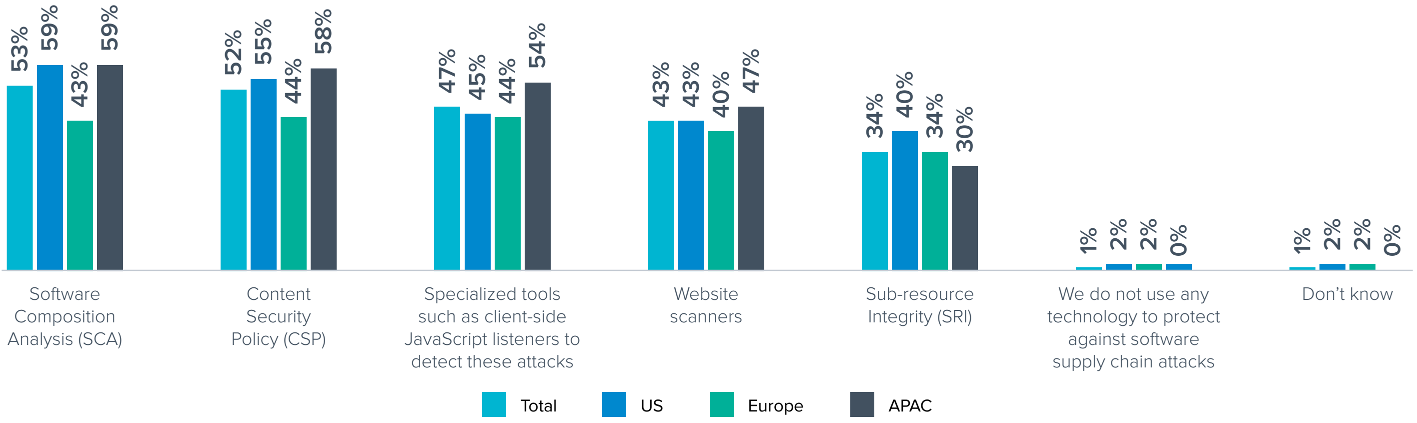
(n=750)



Relatively standard protections are in place for supply chain attack mitigations. APAC respondents use specialized tools, including client-side JS listeners, to detect attacks more than other regions. Such listeners have a better chance of detecting the more advanced attackers than website scanners. Website scanners are the fourth most popular technology on this list, but they are easily spoofed, as evidenced by the Baka skimmer detected by Visa. Sub-resource integrity (SRI) is difficult to set up and maintain, which could be a reason for its low popularity.

Which technologies does your organization use to protect against software supply chain attacks?

(n=750)



Conclusion

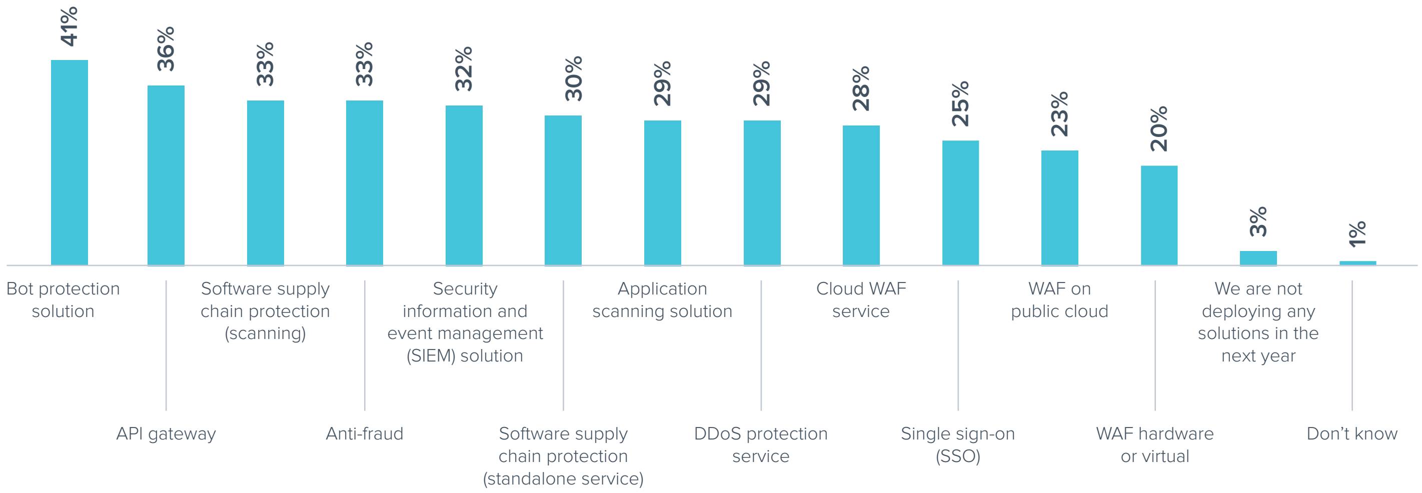
With such a high portion of organizations getting breached multiple times through their web applications in the past 12 months, it's clear more needs to be done to protect against these threats, particularly to protect against newer threats like bot attacks, API attacks, and supply chain attacks.

Organizations seem to understand this, with many looking to deploy new solutions in the coming year such as bot protection (41%), API gateway (36%), and software supply chain protection (scanning) (33%).

It is a good sign that organizations are moving to fill these gaps, but the more solutions they add, the more complex application security becomes. To provide effective protection, an application security solution needs to be a platform that is able to protect customers against all of these attack vectors. A platform approach to application security can provide powerful protection against both traditional and emerging threats while remaining easy to use and manage.

Which of the following solutions will your organization be deploying in the next year?

(n=750)



About Barracuda

At Barracuda, we strive to make the world a safer place.

We believe every business deserves access to cloud-enabled, enterprise grade security solutions that are easy to buy, deploy and use. We protect email, networks, data and applications with innovative solutions that grow and adapt with our customers' journey.

More than 200,000 organizations worldwide trust Barracuda to protect them—in ways they may not even know they are at risk—so they can focus on taking their business to the next level.

Get more information at barracuda.com.

Barracuda
Your journey, secured.

THE STATE OF APPLICATION SECURITY IN 2021 • US 1.0 • Copyright 2021 Barracuda Networks, Inc. • barracuda.com