radware

RADWARE RESEARCH: THE STATE OF WEB APPLICATION AND API PROTECTION

Protecting APIs and Securing Applications So Business Can Thrive

Table of Contents

Executive Summary

Organizations around the globe rely on web and mobile apps for connections to customers, business partners, suppliers and staff. From sophisticated ecommerce engines, to cloud-based productivity solutions and personal tools on mobile phones, applications power how things get done.

To accelerate their digital transformation journeys, organizations have increased their focus on the creation and enhancement of apps. As a result, development and production environments are more amorphic and elastic than ever before, bringing together many independent components that interoperate and facilitate secure application delivery.

As a result, the attack surface of apps is far more expansive with vulnerabilities that pop up in correlation with complexity. Developers rely on application programming interfaces (APIs) to create connections between apps to share data and drive functionality. Yet, APIs are often the most vulnerable points of entry for bad actors to target networks.

To find out more about the state of application and API security, Radware partnered with Osterman Research to study recent developments in the field of application infrastructure and data security. The companies fielded a survey of more than 200 professionals from medium and large enterprises in all sectors from around the globe.

This report examines organizations' application security level of awareness, visibility, practices and strategies. It sheds light on different use cases and business benefits, looks at how different roles view app security and explores the impact of security decisions on business outcomes. Special attention was focused on API security to better understand business objectives vs. security risks across various application development and production environments.

KEY FINDINGS:

The State Of Application Development And Delivery

- Ninety-eight percent of respondents reported attacks against their applications in 2020.
- Seventy percent of production applications are hosted in private clouds or by public cloud providers, rather than in corporate data centers. **Applications in development, however, are much less likely to be hosted in public clouds.**
- Fifty-seven percent of organizations are already using containerized applications yet **52% of respondents believe that the use of containers has provided no financial efficiency.**
- The majority of senior level respondents are confident that new technology provides equal or better levels of app security, yet **confidence amongst respondents varies depending whether they have a security-focused position or not.**
- In 92% percent of organizations, security staff have no say regarding the continuous integration/continuous deployment (CI/CD) architecture and, for all intents and purposes, are required to secure it as-is. **In 89% of organizations, the information security team does not own the budget for security solutions.**

The Threat Landscape

APIs are the next big threat

- Easy-to-build and easy-to-consume APIs speed application development while passing sensitive data between systems. More than one-half of applications of nearly two-in-five organizations are exposed to the internet or third-party services via APIs.
- Organizations see API security as an area of growing concern. Fifty-five percent call it "top priority" while 59% say they want to "invest heavily" in it during 2021.

Enterprises are not prepared to properly manage bot traffic

- Eighty-two percent report suffering a bot attack.
- Despite the availability of dedicated solutions to detect and fend-off illegitimate bot activity, only one-quarter of organizations use it. Respondents said bot attacks are more likely to be successful than other types of attacks, yet only 39% of those surveyed have confidence in dealing with sophisticated bad bots.

Denial-of-service (DoS) attacks are still very common and mostly volumetric, even against applications

- Considered a network-level attack, DDoS is the most common attack vector against applications. Eighty-nine percent of those

98% of respondents reported attacks against their applications in 2020.

70% of production applications are hosted in private clouds or by public cloud providers

57% of organizations are already using containerized applications

92% of organizations, security staff have no say regarding the continuous integration/continuous deployment (CI/CD) architecture

KEY FINDINGS: *(CONTINUED)*

surveyed have experienced such an attack that has targeted their web applications, one-third of which occur on a weekly basis. DDoS attacks at the application layer are frequently in the form of HTTP/S floods.

- Eighty percent report suffering DoS attacks against their applications.

Mobile Apps Are Far Less Secure

Mobile apps played a critical role during 2020 as most information workers shifted to at-home work and relied on them for work tasks, education, entertainment, social interaction and other functions. However, mobile app development is far less secure.

- A large proportion of organizations do not maintain the same security practices for mobile apps as they do for web apps. Only 36% of mobile apps have fully integrated security into their mobile application development lifecycle, and a large proportion have either no security (22%) or only "bolted-on" security (42%). While mobile apps are more commonly developed by third-parties, enterprises that own sensitive data should be mindful of secure development practices.

Migration To Public Clouds Provokes Trust Issues

- Only 27% percent "completely trust" the security offered by their cloud provider(s).
- Of those that have already migrated to public cloud, 47% are using more than one infrastructure provider for hosting their production apps.
- Migration to the public cloud often leads to misunderstanding and trust issues around application security. The survey found that confidence in applying robust security to the public cloud declines as organizations increase their use of it.
- Thirty-seven percent of organizations are not aware of a data breach that might have occurred.

36%

Only 36% of mobile apps have fully integrated security into their development

Application Security In The Near Term

- Top application security management concerns are cross-platform policy coherence and visibility into events.
- API abuse will be the leading threat and area for investment in the near term.
- Fifty-five percent of organizations reported that application and API security will be a high or very high priority during 2021.
- Fifty-nine percent of respondents said they are investing or heavily investing in API protection during 2021 to address their consistency and visibility concerns.

A large proportion of organizations do not maintain the same security practices for mobile apps as they do for web apps.

Changes in the Application Infrastructure

As the use and sophistication of apps increases, how apps are developed, enhanced and secured changes as organizations must evolve network infrastructures. End-users rely on organizations to make sure apps meet their needs for how they interact with the world. For example, e-commerce has grown by more than 30% in the US in 2020, spurred by the COVID-19 pandemic, reaching levels not expected until 2022.[1]

Moving to Multiple Clouds

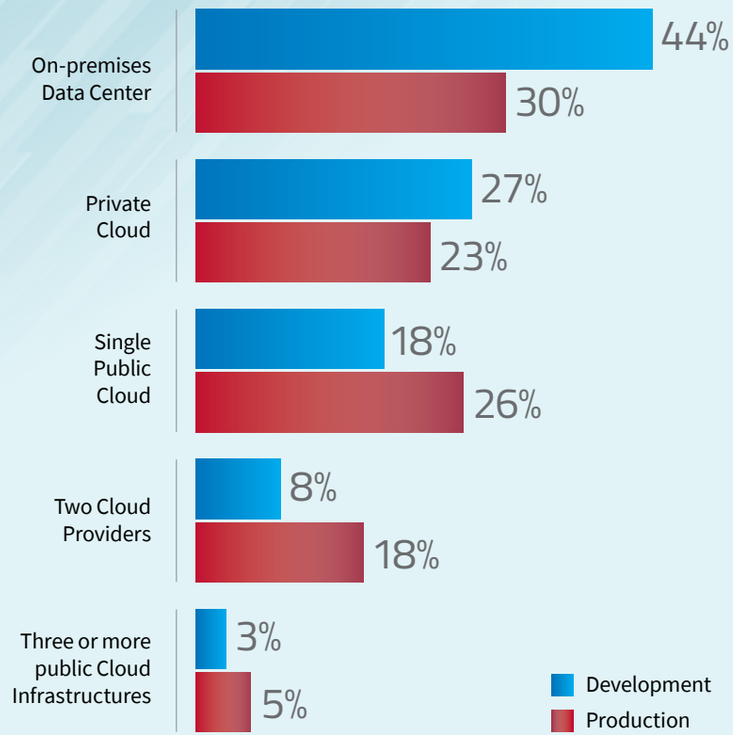
Survey respondents indicated that currently the development of applications occurs primarily within their enterprises' data centers or private clouds (see figure 1). Seventy-one percent of application development occurs either on-premise or in private clouds, while the remaining balance is mostly housed in single public cloud environments.

While organizations kept data and intellectual property (IP) close during development, applications released to production are hosted predominantly in the cloud. Forty-seven percent are hosted on one or more public clouds and 23% on private clouds. Thirty percent of application are housed on-premise in data centers.

IMPACT: Migrating production applications to the public cloud enables more economic utilization of computing resources, especially with consumption-based pricing models. It also provides the flexible and elastic infrastructure that is required to make the most of serverless architecture and containerized applications ecosystems.

Figure 1

Where applications are housed for development vs. production



98% of respondents report attacks on their applications

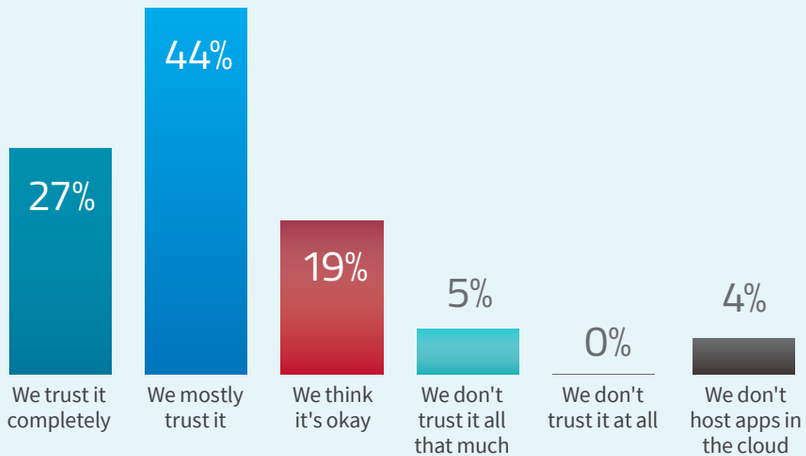
[1] https://www.emarketer.com/content/us-ecommerce-growth-jumps-more-than-30-accelerating-online-shopping-shift-by-nearly-2-years

Trust for Cloud Security Providers' Security

A majority of respondents mostly or completely trust the level of security offered by their cloud providers (see figure 2). Another 19% consider their cloud providers' security for hosted applications to be acceptable, while another 5% have little trust in the security offered by these providers.

IMPACT: Although it may seem like good news that 71% of respondents indicated that they mostly or completely trust the level of security offered by their cloud providers, the result could be considered less than encouraging. For example, a professional that "mostly" trusts the security offered by their cloud provider is, in effect, saying, "I mostly trust that we will not have our customers' data compromised by a bad actor," or "I mostly trust that our organization will not be hit with a €100 million fine from the European Union for a violation of the GDPR."

Figure 2 **Level of trust in cloud providers' security for cloud-hosted applications**



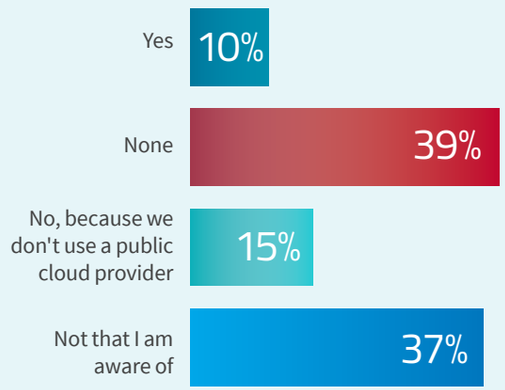
Misunderstandings Create Data Breaches

Respondents who indicated their organizations have migrated applications indicate there are uncertainties about the shared responsibility model for protecting their data and the infrastructure. Data exposures can happen when organizations have misunderstandings about what security measures are the responsibility of their public cloud provider(s). Ten percent of survey respondents indicated that confusion about which entity was responsible for specific security protocols resulted in a data exposure (see figure 3). Another 39% reported no data exposure issues, while 37% said they that there were no such data exposures "they were aware of," implying that there could have been some issues among this group, as well.

> ! **IMPACT:** A lack of proper understanding about the security responsibilities of public cloud providers versus those of their customers can lead to inadvertent data exposures. This is a serious issue that can result in the breach of large numbers of records. Businesses should take a "shared responsibility" versus "no responsibility" approach and do whatever they can to protect their cloud-hosted assets.

Figure 3

Data exposures as a result of a misunderstanding about whether the organization or the public cloud provider was responsible for network security.



Emerging Architectures

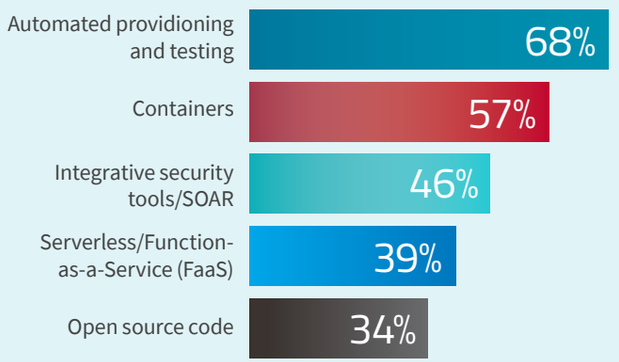
One-third of organizations do not use automated provisioning and testing as part of their application development lifecycle. This response is alarming because these tests assess for bugs, performance and security (see figure 4).

Containerization has been adopted by nearly three in five organizations so far. A variety of other technologies and concepts have also been adopted, including integrative security tools/Security Orchestration Automation and Response (SOAR) capabilities, Function-as-a-Service (FaaS) capabilities and open-source code. Surprisingly, the latter is only common among one-third of business enterprises, while others refrain from integrating third-party code into their apps.

IMPACT: The primary goal of development teams is to facilitate agile and continuous development. The emerging tools available in emerging architectures provide more efficient resource utilization, advanced automation, flexibility and elasticity that is required for a well-orchestrated development lifecycle, leading to faster time-to-market of fixes, functions and application-based services. But they do not offer actual enforcement of security protocols.

Figure 4

Adoption of application development technologies/ concepts



The Impact of Role on Responses

Whether respondents hold a security or non-security focused position within their organizations affected their responses to how emerging technologies have affected their application security posture (see figure 5). Security staff are more suspicious of the effectiveness of emerging security tools in comparison to DevOps staff who are more inclined to want to move forward quickly with new technologies. The anomaly noted in security professional responses to automated provisioning and testing and open source code is surprising.

The perception of emerging technologies increasing application security posture, by role

Figure 5

	SECURITY	NON-SECURITY
Automated provisioning and testing	66%	61%
Containers	48%	57%
Serverless/Function-as-a-Service (FaaS)	34%	27%
Integrative security tools/ SOAR	38%	47%
Open source code	20%	12%

Figure 6

Perception of containers impact of improvement of an organization's security posture, by role

45%
Senior management

60%
Non-senior management

Key Issues Affecting App Dev Security

Survey respondents identified a number of problems associated with the integration of security best practices into the application development process at their organizations.

- Only 45% of organizations agree or strongly agree that security is *well* integrated into their continuous integration/continuous delivery (CI/CD) pipeline
- Forty-three percent agree or strongly agree that security considerations should not interrupt the application release cycle
- Only 42% agree or strongly agree that their DevOps team and security staff know their responsibilities very well
- One in seven organizations agrees or strongly agrees that they have no visibility into the open-source code that they use
- One in seven organizations agrees or strongly agrees that they have no control over which third-party services are processing sensitive data, and nearly the same proportion strongly agrees that they have no visibility into which apps are processing sensitive data

IMPACT: Many organizations understand they have significant gaps in visibility, control and supervisory capabilities in the context of how applications are processing sensitive data and the overall security management process itself.

When it comes to mobile applications, research clearly shows a lack of oversight when using third-party apps for security

Mobile Apps Less Secure by Default

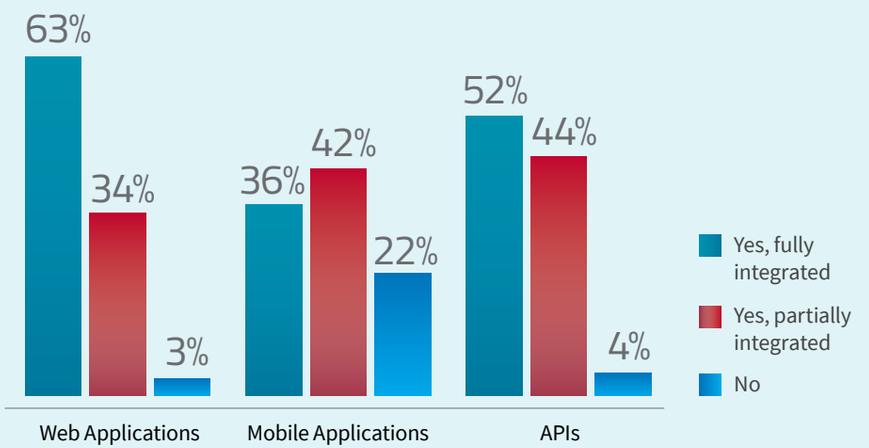
Survey respondents considered the extent to which security is integrated with the continuous delivery of web applications, APIs and mobile applications (see figure 7). The results highlight the lack of security practices and oversight of the use of third-party app builders to secure mobile apps. As a result, mobile apps are inherently less secure.

Web applications — Security is most commonly integrated with 63% fully integrated and 34% percent partially integrated

APIs — Slightly more than one-half of organizations fully integrate security within the continuous delivery of their APIs.

Mobile applications — Organizations place less emphasis on fully integrating security for mobile apps.

Figure 7 **Extent to which security is integrated within continuous delivery of various applications**



Confidence in Security Could Be Better

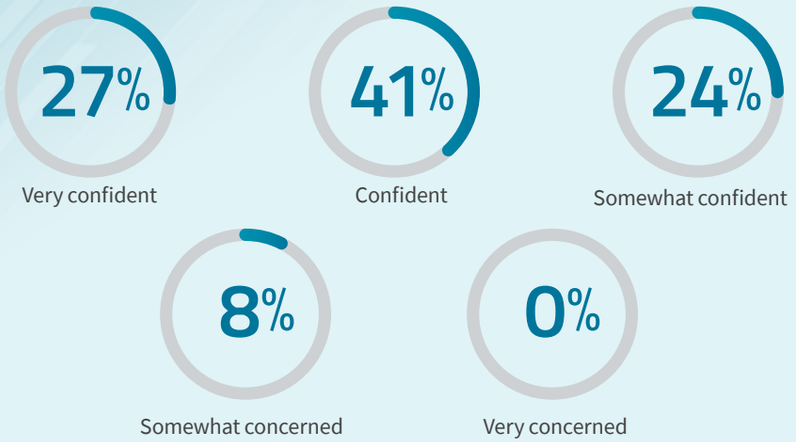
Twenty-seven percent of respondents are very confident in their ability to apply consistent and robust security across all their platforms, while 41% consider themselves to be confident (see figure 8). However, roughly one-third of respondents are only somewhat confident or are concerned about their ability to apply security properly.

IMPACT: Respondents confidence in their ability to apply consistent and robust security is inversely related to their use of the public cloud. In other words, as organizations' use of the public cloud increases for deploying production applications, their confidence in being able to secure these applications diminishes. **For example:**

- Among organizations that have more than 50% of their production applications in public clouds, only 25% are very confident
- Among organizations that have 25-50% of their production applications in public clouds, 26% percent are very confident
- However, among organizations that have less than 25% percent of their production applications in the cloud, 31% percent are very confident

One-third of respondents are concerned about their ability to apply security properly across all hybrid environments

Figure 8 **Level of confidence in applying consistent and robust security across all platforms**



Confidence Levels in Security — Impact by Role

61% Senior management	76% Non-senior management
63% Security	73% Non-security

App Security is Retrospective

Survey respondents were asked which entity in their organizations have the greatest influence on the application development environment architecture and security as well as who owns the application security budget. The Information Technology (IT) department was the dominant influence across the board. IT had greater influence over architecture and security in a plurality of organizations — 40% and 37% percent, respectively. Moreover, IT is the leading budget owner for application security in 42% of organizations, while business owners administer the budget in 36% of organizations (see figure 9).

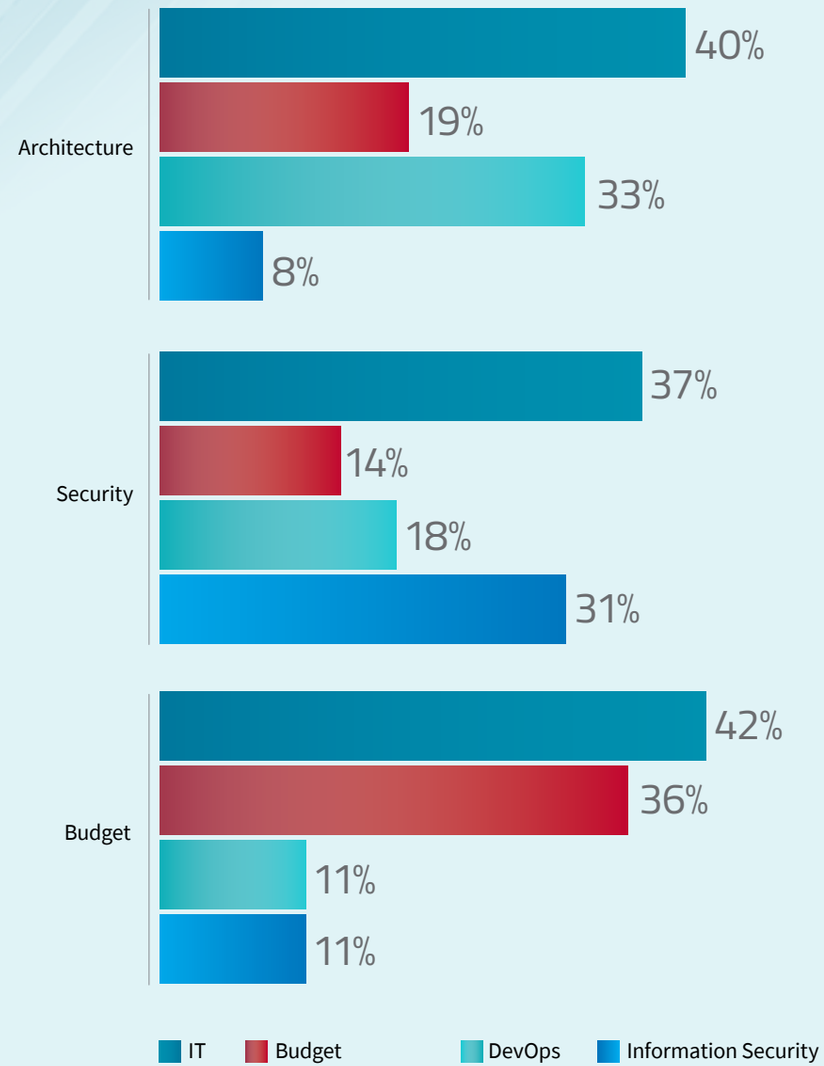
Interestingly, while DevOps has the greater influence on the application development environment architecture in one-third of organizations, only 18% have the greatest influence on security. A mere 11% own the application security budget in their organizations.

Moreover, while information security teams have the greater influence over application development environment security in 31% of organizations, they still take a back seat to IT and other groups in most organizations.

IMPACT: What this distribution of power reveals is that while respondents may be aware of and understand the importance of security in application development architecture, security and budgeting, the information security group has relatively little influence over application development in most organizations.

In 9 out of 10 organizations, security staff are not the prime influencer on application development architecture nor its security budget

Figure 9 **Influence on app dev architecture, security and budget**



Grasping the Threat Landscape

Our research found that the vast majority of respondents — 70 percent — feel they have a good understanding of how to deal with web application exploits, while about one in five admit that some attacks were successful (see figure 10). However, some respondents feel they are not aware of DoS attacks, API abuse or how to address sophisticated bot attacks.

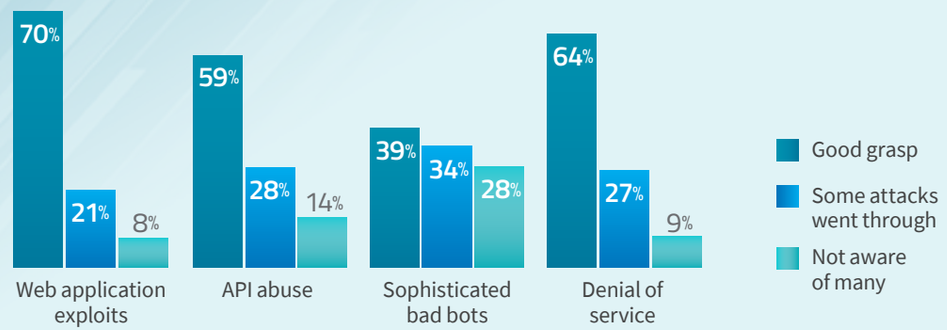
The survey revealed that organizations without a dedicated bot management tool are generally not as well-equipped to deal with various types of threats. Eighty-two percent of respondents say they have suffered a bot attack. Figure 12 shows a comparison of the proportion of respondents that report they have a "good grasp" on the threats shown in figure 8 based on whether or not their organization has a dedicated bot management tool (DBMT) in place. It is evident that DBMT improves visibility substantially.

The research also found that the higher the percentage of apps that are exposed to the internet and/or third-party services via APIs, the less that respondents feel they have a good grasp on how to address API abuse. For example, among organizations that have 50% or fewer of their apps exposed, 68% of respondents consider that they have a good grasp on how to manage API abuse. However, among those with more than 50% of their apps exposed, the percentage that feel they have a good grasp on API abuse drops to just 33% (total does not equal 100 percent because of rounding error).

IMPACT: For a variety of potential reasons — which might include a lack of trust in cloud providers, third-party services or the current set of security solutions — the more apps that are exposed to the internet and/or third-party services via APIs, the less confident that respondents are that they can properly address API abuse directed toward them.

Figure 10

Assessment of the grasp that organizations have on various threats



Impact of Roles on Responses

When asked their perceptions of how in control they are of security threats, respondents in security roles were less likely to say they had a good grasp on different threats, (see figure 11).

Figure 11 **Sense of control over threats, security vs. others**

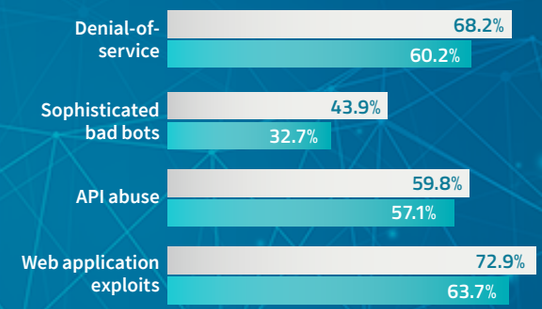


Figure 12

The impact of dedicated bot management tools (DBMT) on an organization's assessment of threats

THREAT	Have a DBMT	Do Not Have a DBMT
Web application exploits	78%	68%
API abuse	72%	54%
Sophisticated bad bots	54%	34%
Denial-of-service	64%	65%

Key Security Issues

The development of apps is inherently a tradeoff between two business needs: accelerated productivity and security. DevOps teams are charged with moving quickly to meet the needs of customers, partners and the supply chain with updated features and functionality. The security team wants to support this objective but also needs to ensure the applications are protected.

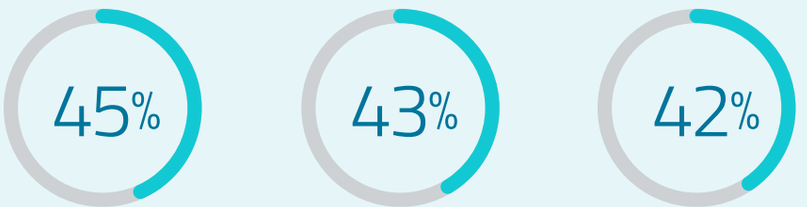
Fewer than one-half of respondents feel that security is well integrated into the CI/CD pipeline, while 43% said security should not interrupt the end-to-end automation of the release cycle (see figure 13).

Forty-two percent of respondents are confident their DevOps and security staff are adequately managing their responsibilities and are eliminating blind spots in application protection.

IMPACT: The need for speed in the application development process sets up a conflict between DevOps and security teams. Based on survey responses, organizations seem to recognize secure development practices are an area of concern that is likely exposing their applications to attack.

Figure 13

Key security issues about the application development process

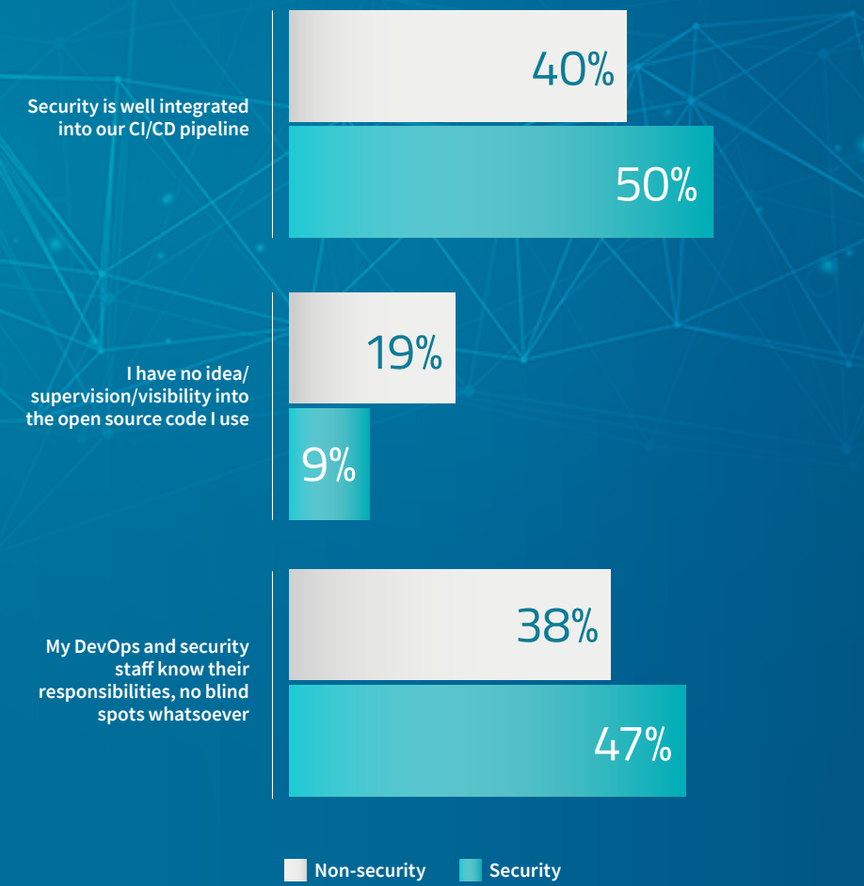


Impact of Roles on Responses

When asked their perceptions of security in the app development process, responses varied by whether the respondent was in a security or non-security role (see figure 14).

Figure 14

Perceptions of security integration into CI/CD, by role



The 2020 App Threats Landscape in Review

As more organizations place a priority on application development, production and hosting, new vulnerabilities and threats emerge. The need for a faster time to market, improved user experience and better resource utilization can influence what security protocols are implemented before an application is deployed, if at all.

In 2020, 98% of survey respondents saw a wide variety of attacks on applications and web servers and expressed concern about how to protect APIs and the transfer of sensitive data.

Widely Varying Frequency of Attacks

The survey revealed the top three most frequent application and web server attacks (see figure 15). SQL or other injections occur monthly or more frequently for 57% of organizations, whereas attacks like cross-site request forgery (CSRF), session/cookie poisoning or protocol attacks occur far less frequently. In some cases, respondents report that they have not seen these types of attacks in their organizations.

> **IMPACT:** Attacks are launched from a variety of browsers and target application servers to exploit vulnerabilities native in an application's code or logic, such as the ones listed in the OWASP Top 10. Organizations must consider all the ways attackers can infiltrate each vulnerability to fulfill their ultimate goals of data theft or service disruption.

Figure 15

Top four most frequent application and/or web server attacks

ATTACK TYPE	# OF ORGANIZATIONS REPORTED
DoS	89%
SQL or other injections	85%
API manipulations	84%
Bot attacks	82%

RPA & Automated Attacks Rising, Yet Businesses Aren't Ready to Manage Bot Traffic

While Robotic Process Automation and other good bots help accelerate productivity and business processes such as data collection and decision making, bad bots target websites, mobile apps and APIs to steal data and disrupt service.

Organizations continue to rely on conventional security solutions to assess bot traffic. Today's sophisticated bad bots can mimic human behavior and bypass CAPTCHAs and other older technologies and heuristics.

WAF is the Most Common Tool Used to Classify Bots

Despite the limitation of these technologies in detecting sophisticated, human-like bot traffic, nearly one-half of organizations use web application firewalls (WAFs) to distinguish between real users and bots, and nearly the same proportion use IP-based detection to do so (see figure 16). Other techniques in use include in-session detection and termination and CAPTCHAs. The least commonly used method for distinguishing between real users and bots is a dedicated anti-bot/anti-scraping solution.

The top three types of bot attacks reported by respondents are DDoS, web scraping and account takeover (see figure 17). A variety of other attack types occur with some frequency, including digital fraud, denial of inventory and payment data abuse.

IMPACT: Bot attacks are automated programs scripted to achieve a specific goal, depending on the attackers' objectives. Businesses need to safeguard all the functions within their organizations — no matter what industry sector(s) they serve — because attack goals can vary, including breaking into user accounts, stealing identities, payment fraud, scraping content, pricing, coupons or data, spreading spam or propaganda and impacting competitive business activities.

Figure 16 **Techniques used to distinguish between real users and bots**

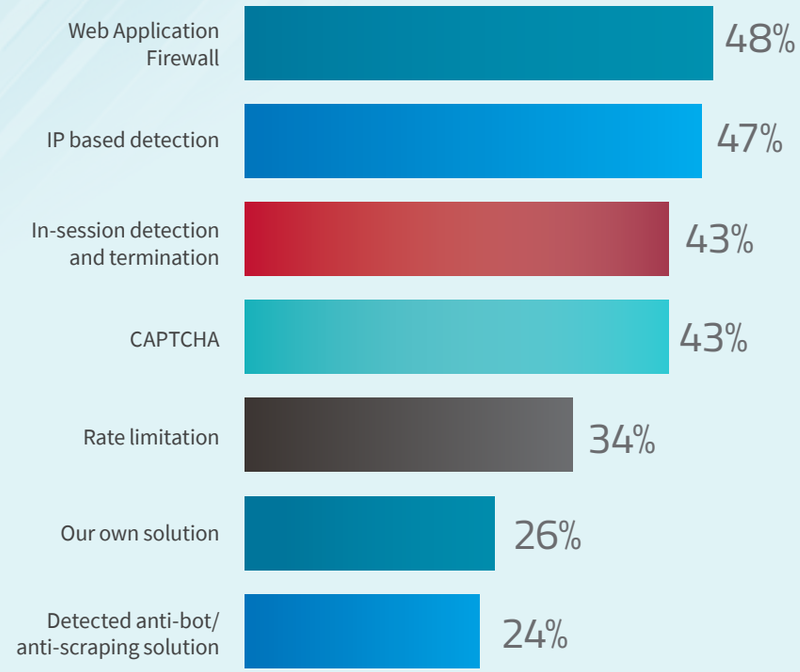


Figure 17 **Top three most frequent types of bot attacks**

BOT ATTACK TYPE	OCCURRENCE
DoS	86%
Web Scraping	84%
Account Takeover	75%

Exhausting Application Resources via DDoS

Eighty percent report having suffered DoS attacks against their applications. Just like DDoS attacks targeting network infrastructure, the most common technique to take an application down is by flooding it with incoming requests. Nearly three in five organizations experiences an HTTP Flood at least once per month, if not more frequently. Almost two in five experience HTTPS Floods at least this often. A variety of other DoS attacks occur with some frequency, including buffer overflows and resource depletion attacks (see figure 18).

IMPACT: Denial-of-service (DoS) attacks – volumetric or not – target the application servers to take them down. There are many types of DoS attacks, but the most popular is to flood application servers with requests. While network-level floods are often mitigated, application-layer floods that get through crush the server, rendering it non-functional. Other than volumetric DDoS we also see low and slow attacks and other forms that aim to exploit resource utilization (like CPU or physical memory), preventing the app from being able to respond to legitimate users. Low and slow attacks leave connections open on the target by creating a relatively low number of connections over a period of time and leaving those sessions open for as long as possible. Attacks can also send small data packets or "keep alives" to prevent the session from going to idle timeout.

HTTP Flood is the most common DoS vector against applications

Figure 18

Frequency of denial-of-service attacks during the last 12 months

DoS ATTACK TYPE	% OF ORGANIZATIONS REPORTED
HTTP Flood	80%
HTTPS Flood	79%
Resource Depletion	73%

Protecting APIs

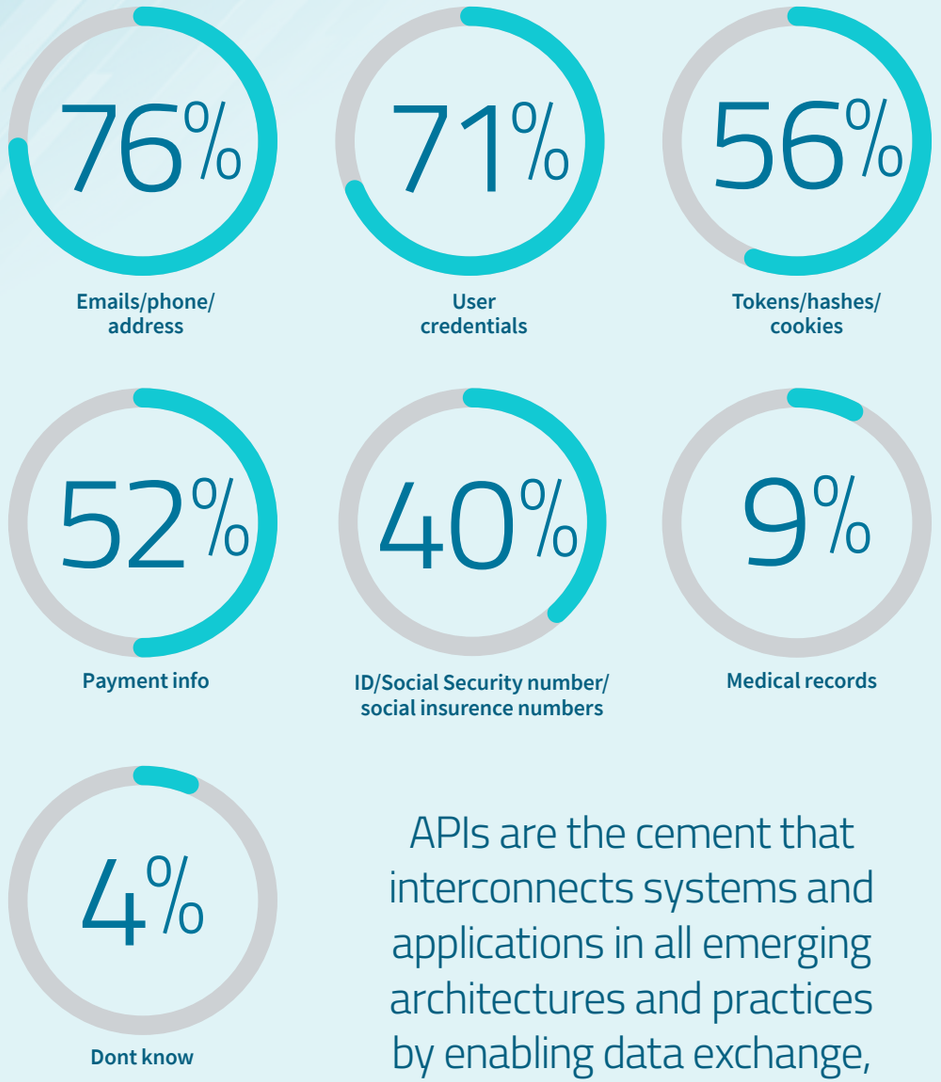
APIs are the cement that interconnects systems and applications in all emerging architectures and practices by enabling data exchange, integration and automation. APIs are used in internet of things (IoT) devices, microservices, mobile apps, event-driven processes and a variety of application integration use-cases. Protecting APIs from cyberthreats is a growing concern in application security.

APIs Process a Variety of Confidential Data Types

The survey found that a wide variety of data types are processed by APIs. In the vast majority of organizations, APIs process sensitive personal data such as email addresses, telephone numbers, addresses, user credentials, tokens, hashes, cookies and payment information (see figure 19). Many organizations also use APIs to process information that includes identification information about individuals, including medical records in some cases.

IMPACT: The combination of large volumes of sensitive and confidential information that is processed by APIs — coupled with the lack of visibility into how these APIs and third-party applications operate — creates a dangerous situation for most companies in the context of how easily their data can be breached.

Figure 19 **Types of sensitive data processed by APIs**



APIs are the cement that interconnects systems and applications in all emerging architectures and practices by enabling data exchange, integration and automation.

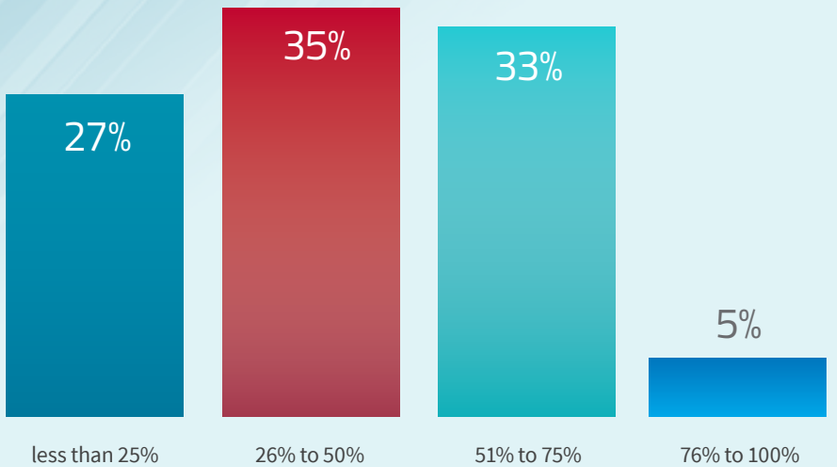
Most Apps Expose Sensitive Data Through APIs

Respondents indicated the vast majority of applications are exposed to the internet and/or third-party application services via APIs (see figure 20). While 27% of organizations have fewer than one-quarter of their apps exposed, 35% have between one-quarter and one-half of their apps exposed, and 38% have more than one-half of their apps exposed.

- The lurking danger is in the challenges faced by application development teams to secure their applications in the new cloud environment where the security of data of applications running on containers is still not well understood, and while there are some tools available, no best practice has emerged yet. Fifty-seven percent of organizations are already using containerized apps yet 52% of respondents believe that the use of containers has provided no additional financial efficiency.

IMPACT: Exposure of this magnitude does not absolutely mean that all data exposed to the internet and/or third-party apps is subject to breach, but it creates a significant opportunity for data breaches to occur. The survey finds that a large proportion of organizations are using third-party code in their applications, and the vast majority of them do not have proper insight into how these apps manage data or otherwise operate. This situation creates an enormous potential for data breaches and potentially damaging consequences on a variety of fronts: regulatory (e.g., from violations of the General Data Protection Regulation [GDPR] or the California Consumer Privacy Act), legal, financial and reputational.

Figure 20 **Percentage of apps organizations expose to the internet or to third-party services via APIs**



Substantial Concerns About the Use of APIs

The survey revealed that three in five respondents are concerned or extremely concerned about the potential for security breaches with regard to their use of APIs. A large portion of respondents are concerned about unintentional data loss, management and maintenance overhead, and overcomplexity regarding their use of APIs (see figure 21).

The research revealed a relationship between the level of concern about the use of APIs and the extent to which applications are exposed to the internet and/or third-party applications. For example, among those who are "very concerned" about these issues, 40 percent of respondents have more than one-half of their applications exposed to APIs. However, among those who are only minimally concerned, none have more than one-half exposed to APIs.

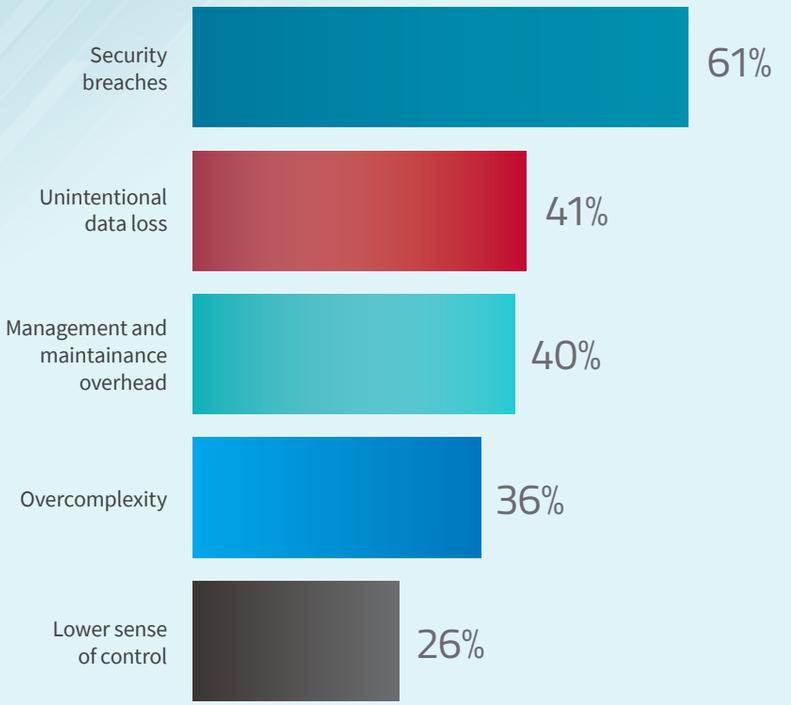
IMPACT: The security of APIs is often overlooked because the APIs run deep at the backend of an application or between services. Unfortunately, sensitive data is transferred by APIs and organizations are concerned about how to deal with the challenges of protecting the digital assets. The complexity of threats creates a confusing security environment that can be difficult to control.

Security breaches are the #1 concern of respondents regarding the use of APIs

Figure 21

Level of Concern About Issues Regarding Use of API

(% responding "concerned" or "extremely concerned")



Senior Management Far More Concerned with the Impact of Data Leakage

49% Senior management

33% Non-senior management

API Attacks are Common

API attacks of various types are fairly common. Figure 22 list the top three types of API attacks reported by respondents. The survey revealed that 55% of organizations experience a DoS attack against their APIs at least monthly, 48% experience some form of injection attack at least monthly and 42% experience an element/attribute manipulation at least monthly.

WAFs Are the Most Common Defense

Respondents were asked about the variety of technologies that they use to protect their APIs (see figure 23). At 77%, the vast majority use web application firewalls (WAFs) to protect their APIs, while 61% use API gateways and 50% use an additional cloud service. Only one in four organizations are currently using any sort of dedicated bot management tool to protect their APIs.

IMPACT: The API security challenge is triple – requires threat coverage, easy integration and complete visibility, also for undocumented APIs. The data tells us most enterprises rely on different tools that are not purpose-built and are forced to make compromises. For instance, APIs are also exposed to bot attacks. The lack of dedicated bot management tools in most organizations reveals that they are not well prepared to manage bot traffic. As such, these organizations are at a greater risk for potential bad actors launching successful attacks through APIs, such as credential stuffing, brute force and scraping attempts. Security teams likely also have lower levels of confidence to deal with attacks against their APIs. Fewer security respondents said they rely on an API gateway, which is more popular amongst non-security roles (54% vs. 67%). API gateways can monitor authentication and IP-filtering but do not look into HTTP payload and do not provide complete API protections. Security professionals are more aware of the limitation of these tools.

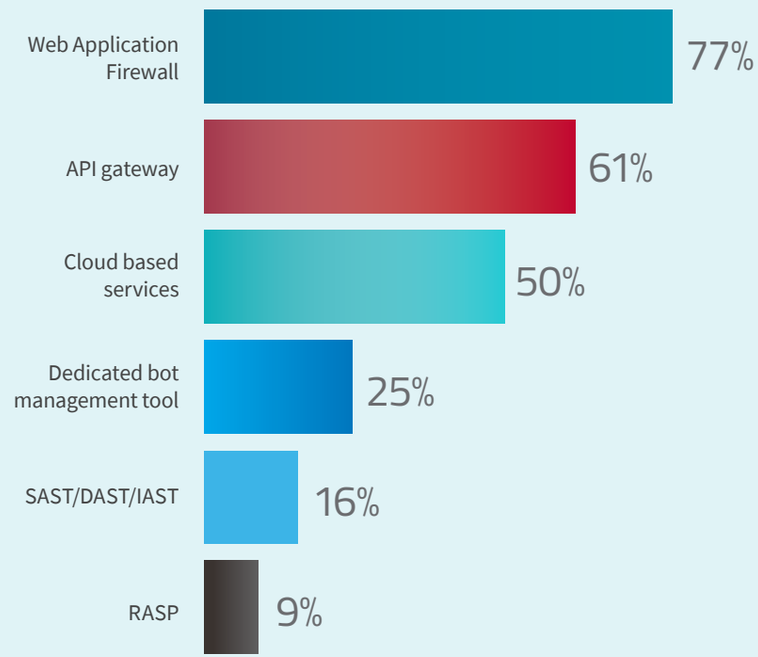
Figure 22

Top three API attack types

API ATTACK TYPE	OCCURRENCE
DoS	87%
Injections	80%
Access violations and brute force/credential stuffing (tied)	74%

Figure 23

Technologies used to protect APIs



Application Security in 2021

Even as the world went into lockdown in 2020 to deal with the COVID-19 pandemic, hackers continued to launch attacks on networks. Lockdowns and travel restrictions forced many in organized to shift their activity to cyber space. In parallel, the increased use of mobile apps for private and business matters created an even more exposure points for bad actors to target.

Looking ahead in the new year, how will organizations adapt and secure their networks?

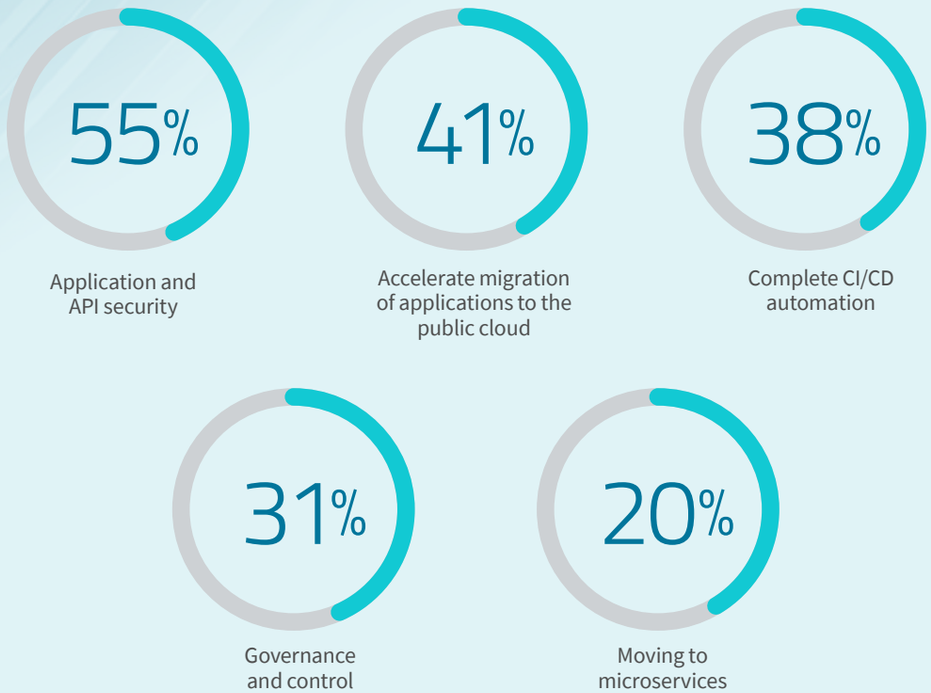
Application and API Security are High Priorities

When asked how their application infrastructure would evolve in 2021, most respondents reported that application and API security would be either a high or very high priority in the coming year (see figure 24). Two in five respondents said that they would focus on accelerating the migration of applications to the public cloud as a high priority, while 38% said completing their CI/CD automation was important.

IMPACT: Recent changes in the application infrastructure — as well as business demands of which some are related to COVID-19 — require adjustments from app development and product divisions. These teams need to balance efforts to secure their infrastructures with the benefits of migrating apps and workloads to the public cloud (with all the benefits — and risks — that come with it), operational efficiencies achieved with more automation and better governance.

Figure 24 **Extent to which organizations see their application infrastructure evolving in 2021**

(percentage responding "high" or "very high" priority)



The key to application security in 2021 will rest on the ability of app development and product teams balancing the need to secure infrastructures while migrating apps to public clouds via automation and governance.

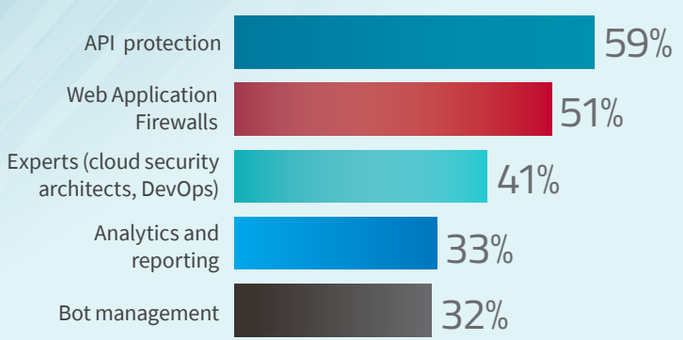
API Protection Will Be the First Area for Investment

About three in five organizations recognize the risk associated with the increased use of APIs and the challenge to secure them and are very likely or definitely likely to invest heavily in API protection through most of 2021. This concern is even greater with the non-security respondents, many of which are Application Development and Delivery (AD&D) professionals who build, introduce and connect the APIs., Respondents indicated the need for API protection is driven by non-security roles, not security staff (65% vs. 51%). Slightly more than one-half will invest to this extent in web application firewalls, (see figure 25). Interestingly, only about one-third of organizations plan to invest or invest heavily in bot management capabilities.

IMPACT: While web application firewalls offer important defensive capabilities to detect and prevent attacks against APIs, bot management tools offer a robust defense against sophisticated bot attacks. And, as shown previously, they give security teams a better grasp on dealing with a variety of threats and attacks.

Figure 25 **Where organizations will invest to improve application security during the next 12 months**

(percentage responding "very likely" or "will be" investing heavily)



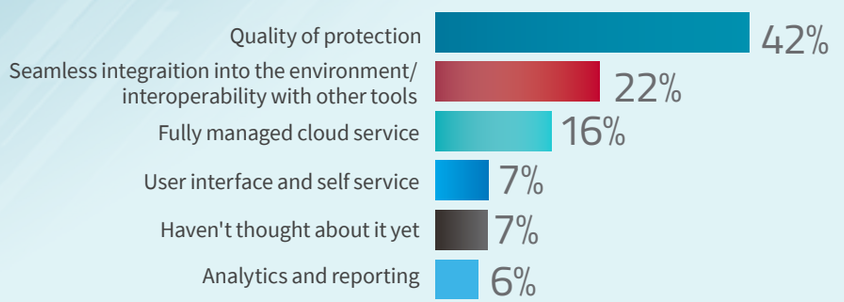
Quality of Protection is a Priority in Solution Selection

When procuring web application and API protection technologies, more than two in five respondents report that the quality of the protection in the solution is their primary consideration (see figure 26). Twenty-two percent of respondents say that the ability to seamlessly integrate the solution into their environment and with other tools already being used is their primary consideration.

Respondents in non-security roles surprisingly rank the need for quality of protection higher than their counterparts in security roles. Non-senior management respondents are twice as likely as senior management to prefer more access to analytics (8% vs. 4%) and the use of managed services (21% to 10%). We speculate this has to do with their day to day experience, and might point at skill-shorted IT security staff or simply too full of a plate.

IMPACT: Integrating security controls and checks can slow down the delivery of apps. Higher inspection levels takes time, which can impact performance and user experience on one hand, or make for longer development cycles. As such, development teams express different priorities than security teams. As we see in the survey, fewer than one-half of respondents prioritize the quality of app protection.

Figure 26 **Primary consideration when procuring web application and API protection technology**



A Need for Consistency and Visibility

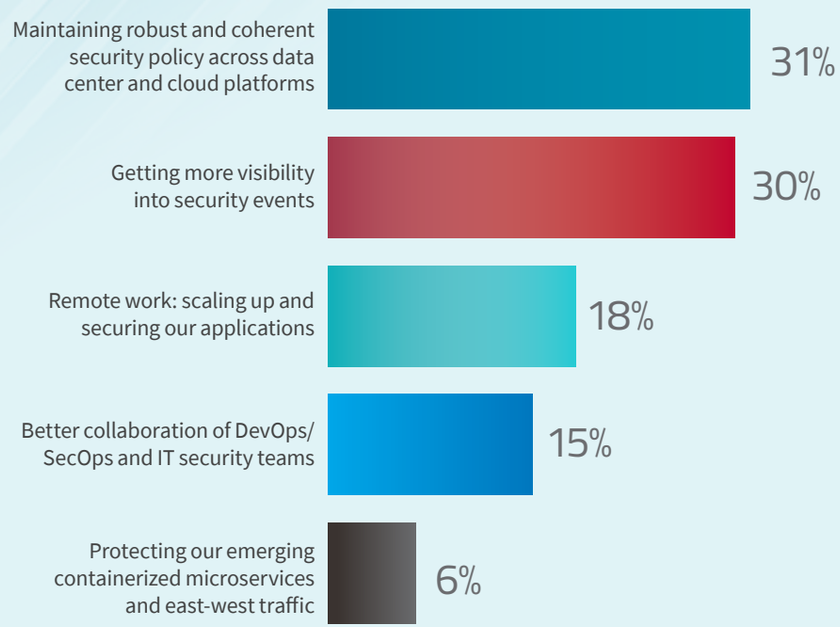
Thirty-one percent of respondents anticipate that their organization's most significant application security concerns over the next two years will be maintaining a coherent security policy across their data centers and the cloud platforms that they use or will be using (see figure 27). Nearly as many respondents believe that their most significant concern will be gaining visibility into the security events impacting their organization.

These statistics underscore one of the key overarching issues of application security: that despite the implementation of new security technologies, organizations continue to struggle maintaining visibility and consistency of security policies across new platforms, architectures and technologies (APIs).

IMPACT: Despite the fact that about two-thirds of employees were still working from home or in other remote locations at the time of the survey, only 18% of respondents told us that scaling up and securing their applications for remote work would be their most significant concern over the next few years. It is likely that organizations had either mostly or completely addressed this issue by the time of the survey (conducted eight months into the pandemic) or they believe that the vast majority of their workforce will have returned primarily to in-office work within the next year or so.

One of the key overarching issues of application security is maintaining visibility and consistency of security policies across different platforms and technologies

Figure 27 **Most significant application security management concerns anticipated during the next two years**



Concern About Visibility into Events — by Role

34% Senior management

25% Other

Radware Predictions

The Mad Dash to The Cloud Will Undermine Application Security In 2021

"As organizations shift to the hybrid work model, implementing new strategies is critical to protecting digital assets and guarding against cyberthreats. The Covid-19 pandemic triggered an accelerated migration of business applications and infrastructure into the cloud, which unintentionally increased attack surfaces and created security gaps for hackers. We expect to see the consequences of this error-prone reality in 2021"

Anna Convery-Pelletier, CMO

Automation and Orchestration to The Rescue

"Remote work accelerated by COVID-19 will lead toward a zero-trust environment to ensure that the applications are accessed by the right users who are authorized and authentic. Improved automation and orchestration tools will emerge to scale application security across multiple clouds"

Prakash Sinha, Senior Director, Application Delivery

The Internet Becomes One Interconnected Service Factory

"APIs running in the backend of the core network or the edge cloud (MEC) are powering web and mobile applications, and there's no single, cross-environments comprehensive solution. The risk is greater – if one component fails it means either the whole system or application is down, or simply everything becomes inaccessible."

Pascal Geenens, Director, Threat Intelligence

APIs Become the Achilles Heel of Application Security

"We see customers using more functional, home-grown APIs - rather than standard web or mobile – and face a challenge of observability and control over them. These undocumented APIs are the sweet spot for more sophisticated attacks – by hackers or bots – that will use it as an entry point where unauthorized, unauthenticated access will lead to an escalation of privileges, resulting in data theft"

Michael Groskop, VP Portfolio Management

Human Errors Will Become More Frequent; More Costly

"The more amorphic, dispersed, and diverse business applications are becoming, the harder it is for organizations to provide hermetic protection. Grocery shopping security solutions is easy, but how does one manage them over multiple cloud infrastructures, with CI/CD automation, API adoption, microservices and serverless architectures, all add blind spots exponentially. In today's development cycles with incessant changes, human errors will become more frequent and more costly."

Ben Zilberman, Product Marketing Director, Application Security

RADWARE CASE STUDY: BANKING

U.S. Credit Union Relies on Cloud-Based Protection to Ensure a Superior Banking Experience

This credit union has been serving customers throughout the Southeastern United States for over 75 years. With 300,000 members and $4 billion in assets, it is one of the largest credit unions in the region.

Like most financial service organizations, it is heavily dependent on various online platforms, including its website and customer banking portal, to provide a superior digital experience for its customers.

The Challenges

Several years ago, the credit union's online platforms came under attack and customers were unable to access the portal and/or complete banking transactions, resulting in dissatisfied customers. This necessitated the implementation of a cloud-based web application firewall (WAF). The credit union selected Imperva's Cloud WAF.

Unfortunately, several months later, the credit union was still suffering from various application-based attacks, including a series of new bot-based, account takeover attacks. While Imperva's WAF proved successful in blocking these attacks, it came at an unacceptable cost. Imperva was reactionary and manual-driven, requiring the credit union's security team to identify attack traffic themselves. This cost the team time when under attack and tied up limited security resources.

The credit union contacted Radware to review application protection solutions. Radware and Cisco, a Radware alliance partner, presented a joint solution to provide comprehensive protection against an array of network and application attack vectors.

The Solution

The solution comprises several Radware security solutions, starting with its Cloud WAF Service for protection against OWASP Top-10, zero-day assaults and other attack application-layer attacks. The credit union particularly values the automatic policy generation capabilities of the Cloud WAF Service, which adapts security policies to new threats and changes to applications and websites, saving the security team time and operational costs.

It also includes Radware Bot Manager, which safeguards the credit union's web and mobile applications and APIs from automated threats by distinguishing malicious bots from legitimate traffic.

Lastly, DDoS attack protection will be provided by leveraging a hybrid implementation that includes DefensePro, Radware's on-premise DDoS mitigation appliance, and Radware's Cloud DDoS Protection Service for protection against distributed denial-of-service attacks, network Layer 3/Layer 4 and application-Layer 7 attacks and SSL protection.

Staying In Business While Under Attack

In October 2020, the credit union was the target of advanced application and bot attacks which nearly crippled their application and network infrastructure. From October 17-21, the credit union experienced access control violations of their websites, followed by website application attacks which peaked at 2.5 MPPS on October 24th. A series of malicious bot attacks against the credit union websites, totaling 57.43 million hits, started on October 25th (See Figure 2).

At the time of these assaults, the credit union was still using Imperva Cloud WAF, which was incapable of fully mitigating the attacks. This resulted in high call volumes since many users were unable to access their accounts via the mobile application.

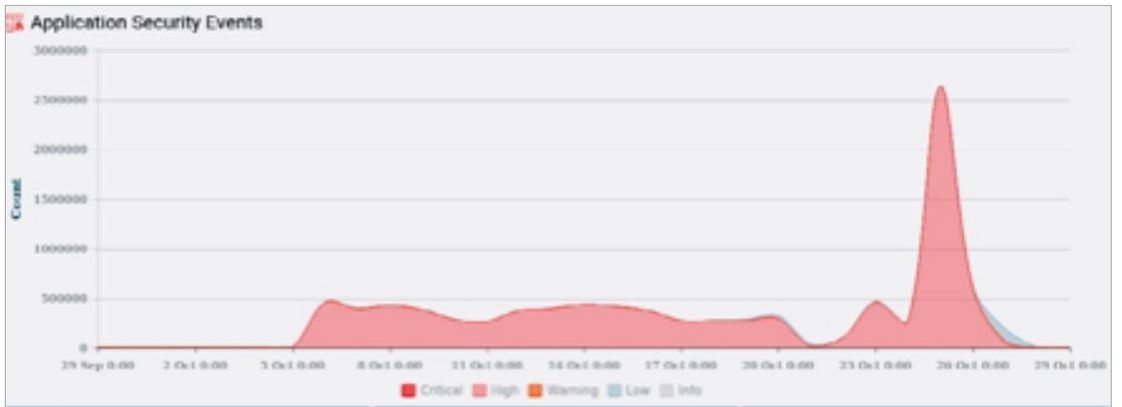
Radware expedited the implementation and onboarding of Radware Cloud WAF Service and Bot Manager. Both solutions mitigated the assaults and restored availability and security for the credit union's mobile and web applications. The VP of IT stated that the credit union's security team was impressed with speed and effort of the implementation and the ability of Radware professional services to address the credit union's issues.

Moving Forward

Radware's Cloud WAF Service and Bot Manager have successfully safeguarded the credit union's application from a series of high-volume application and bot attacks, allowing the company to guarantee uninterrupted service for its customers.

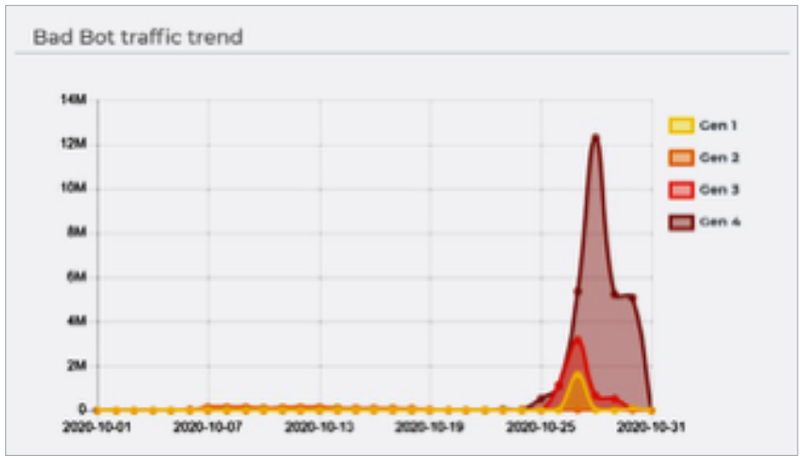
Because Radware's application security tools use automation and behavioral learning to adapt to new threats, the credit union security team has more time to do proactive planning for the next evolution of threats.

Figure 1 **Application Security Events Experienced (Oct. 1 - Nov. 1)**



Severity	Daily Average	Daily Peak
Critical	0	0
High	313,139.4	2,623,283
Warning	381.2	10,162
Low	6,291.6	127,297
Info	0	0
Total Count	319,812.3	2,760,742

Figure 2 **Bad Bot Traffic by Generation (Oct.1- Oct. 31).**



***Gen 1**-Basic script bots mitigated through blacklists.*
***Gen 2**-Headless browser bots blocked via fingerprint.*
***Gen 3**-Bots simulating basic human like interactions blocked by keystroke or mouse movement analysis. Gen 4-Bots simulating advanced human like interactions blocked using Radware's intent-based deep behavioral analysis.*

About the Research

On behalf of Radware, Osterman Research surveyed 205 decision-makers and influencers in organizations that have a minimum of 1,000 employees during November 2020. The median number of employees at the organizations surveyed was 2,200.

The primary job functions of the individuals surveyed included network security (24%), DevOps/DevSecOps (20%), network operations and related roles (15%), application development (14%) application security (9%) and various other IT and related roles (16%). The majority (70%) of those surveyed are either in senior management or management roles, with another 16% in executive positions.

The organizations surveyed are in a wide range of industries, including manufacturing (15%), technology products (10%), retail/wholesale (9%), financial services (9%), biotech/pharma (8%), business services (7%) and automotive (7%), among several other industries.

Of the 205 surveys, 70 were conducted in North America (US and Canada), 67 were conducted in Europe (Germany, France and the United Kingdom) and 68 were conducted in other countries (China, India, Brazil, Australia, Chile and New Zealand).

About Radware

Radware® (NASDAQ: RDWR) is a global leader of cybersecurity and application delivery solutions for physical, cloud and software-defined data centers. Its award-winning solutions portfolio secures the digital experience by providing infrastructure, application and corporate IT protection and availability services to enterprises globally. Radware's solutions empower more than 12,500 enterprise and carrier customers worldwide to adapt quickly to market challenges, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit www.radware.com.

Radware encourages you to join our community and follow us on: Radware Blog, LinkedIn, Facebook, Twitter, SlideShare, YouTube, Radware Connect app for iPhone® and our security center DDoSWarriors.com that provides a comprehensive analysis of DDoS attack tools, trends and threats.