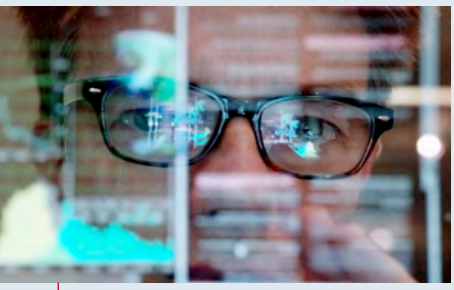
radware

# THE STATE OF WEB APPLICATION SECURITY

Protecting Applications in the Microservice Era


# Table of Contents



*The 2019 State of Web Application Security research was conducted on behalf of Radware by Enterprise Management Associates, Inc. (EMA). Look for **Analyst Notes** throughout the report for commentary from EMA's David Monahan, managing research director, security and risk management.*

# Across the globe, organizations are constantly searching for more efficient ways to connect with customers, business partners, suppliers and staff. The ability to adapt quickly to changing market conditions with new and updated web applications is critical to success.

To understand what strategies and solutions organizations employ to secure web applications, Radware sought the opinions of senior executives and IT professionals responsible for network security at companies with a global reach. What follows is a summary of current perceptions about the state of application attacks, security practices and the impact of the transition to microservice architectures.

In addition, Radware offers insights into the growing sophistication of bad bots formulated from an analysis of traffic passing through its customers' networks during a 12-month period.

# Executive Summary

Business moves fast. In a matter of milliseconds, transactions are made, trades are processed, and deals are done. If an organization's IT security is not up to the task of protecting the applications that enable today's e-commerce stream, debilitating data breaches can happen in the blink of an eye.

To better understand the state of web application security, Radware commissioned a third annual global survey of senior executives, security researchers, application developers and IT professionals at companies with worldwide operations. The goal of this year's survey was to understand how the adoption of microservice architectures affects:

- What types of application security solutions are being adopted by organizations;
- Who is responsible for ensuring application security within organizations;
- What business processes are in place — in and across departmental boundaries; and
- What types of threats are most prevalent, and what are the reasons why some cyberattacks still succeed.

Digital transformation is an evolutionary process. Organizations pursue digital transformation strategies to improve their ability to deliver excellent customer experiences on digital platforms. For example, moving to microservice architectures has proven both strategic and beneficial for many companies as a means to launch applications faster and simplify maintenance.

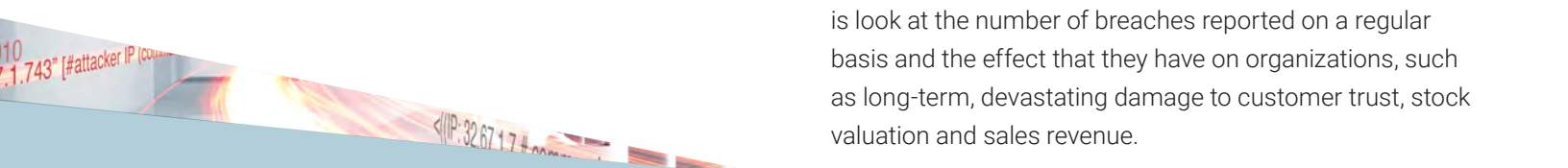
But technology advancements outpace infrastructure upgrades. Organizations are in constant motion trying to keep up. They want their customers to be able to take advantage of every opportunity available to interact meaningfully with their branded products and services. Agility equals success.

## CAN SECURITY RUN AT THE SPEED OF BUSINESS?

In general, the survey found that security did not run at the speed of business even though respondents felt good about the application security solutions they had deployed.

To keep pace, many organizations implemented multiple solutions to protect their applications, hoping that any vulnerabilities in their networks would be covered. Respondents also indicated that their organizations followed most of the recommended security practices, were keen to adopt emerging technologies and business processes, and were driven by new operational models focused on efficiency and competitiveness.

Although gathering an army of solutions may work in the short term, this approach is not optimal. All we need to do is look at the number of breaches reported on a regular basis and the effect that they have on organizations, such as long-term, devastating damage to customer trust, stock valuation and sales revenue.



## SECURITY PROFESSIONALS ARE SIDELINED

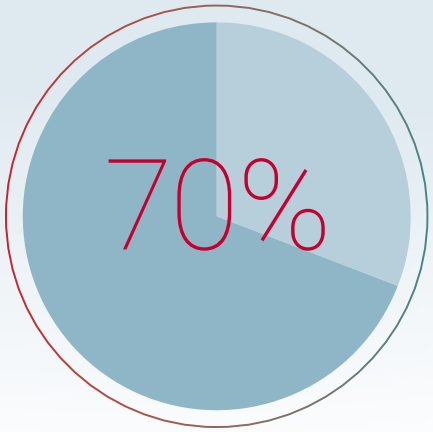
While the importance of securing applications was a stated goal of the majority of respondents, good intentions do not always result in the best outcome for a number of reasons:

- Security professionals are not always empowered to make decisions about application security. Survey respondents reported that 70% of chief information security officers (CISOs) did not have the final say over security choices.
- To cover all vulnerabilities, many organizations take on application security by deploying multiple solutions in a far-from-optimized manner.
- The wide range of application development tools and methodologies for running microservices has led to inconsistent implementations, deployments and business processes within organizations and loose adherence to best practices.
- Applications change frequently and are too loosely managed to appropriately secure.

## WHERE DO WE GO FROM HERE?

As the speed of business continues to quicken, application security solutions must protect valuable network assets and data. The critical questions are "Why are breaches still commonplace, and what can organizations do to optimize how they protect applications?"

The following sections dig deeper into the answers provided by survey respondents to offer useful insights and a faster path forward.




*Survey respondents reported that 70% of CISOs are not the key influencer of software security policy in their organizations.*


# One Goal, Many Approaches to Security

Organizations have one goal when it comes to protecting their applications: keep them secure. Radware's third annual global survey about the state of web security reveals that organizations around the globe are keenly aware of the threat that network security vulnerabilities pose to applications. But how companies go about attempting to protect applications is varied and lacks mature process controls.

As organizations pursue digital transformation goals, a common strategy is to purchase many solutions to protect applications without a clear overarching plan. By covering the network in broad strokes with multiple solutions, the hope is that any vulnerabilities get sealed.

The effectiveness of this approach is questionable, as 90% reported that they've had a data security breach in the past 12 months. In fact, only 56% of respondents were highly confident and 40% were only moderately confident that they could keep personally identifiable information (PII) — such as credit card data, medical records, transaction information and usernames/passwords — safe from breaches.

90%

REPORTED THAT THEY'VE HAD A DATA SECURITY BREACH IN THE PAST 12 MONTHS

ONLY

56%

OF RESPONDENTS WERE HIGHLY CONFIDENT THAT THEY COULD KEEP CUSTOMERS' PII SAFE.

## Strategies to Protect Applications

### TOP THREE CONSIDERATIONS FOR APPLICATION SECURITY SOLUTIONS


**FIGURE 1.** RESPONDENTS RANKED THE THREE MOST IMPORTANT FEATURES WHEN SELECTING APPLICATION SECURITY SOLUTIONS.

Despite some shortcomings, web application firewalls (WAFs) continue to be the most used protection for containerized solutions, likely because they have been in use for a number of years and have a large installed base.

## Strategies to Protect Microservices

Similar to last year's report, this year's respondents ranked data protection as the top security challenge (40%) related to the architecture of microservices. But the survey results revealed shifting concerns for other top issues (see Figure 2).

### TOP THREE SECURITY CHALLENGES — MICROSERVICE ARCHITECTURE

| 2018 | 2019 |
|---|---|
| 1. Data protection | 1. Data protection |
| 2. Availability assurance | 2. Visibility |
| 3. Policy enforcement | 3. Authentication |

**FIGURE 2.** RESPONDENTS RANKED THE TOP THREE SECURITY CHALLENGES IN A MICROSERVICE ARCHITECTURE.

***Analyst Note:*** *Organizations place a priority on maintaining consistent/persistent identities in applications and for entities visiting their sites.*

## Strategies to Protect Containers

### PROTECTIONS CURRENTLY IN USE TO SECURE CONTAINERIZED APPLICATIONS*

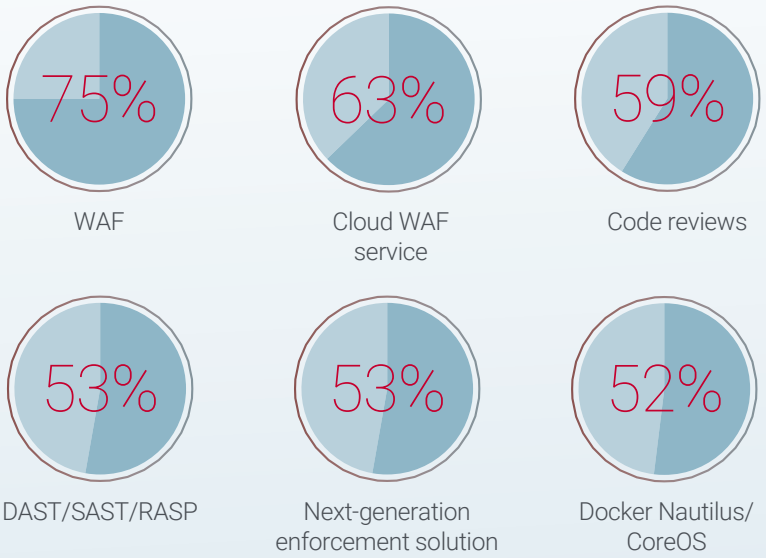



**FIGURE 3.** RESPONDENTS RANKED THE PROTECTIONS CURRENTLY USED TO SECURE CONTAINERIZED APPLICATIONS.

Top solutions respondents are considering for securing containerized applications:

1. DAST/SAST/RASP and Docker Nautilus/CoreOS (tied) — **40%**
2. Next-generation enforcement solution — **39%**

***Analyst Note:*** *It is likely that firms that already had WAF in place are now trying a variety of other solutions in a broad strokes approach without carefully evaluating results in efforts to secure applications and meet compliance requirements.*

* Data is based on those respondents that use microservices.

To protect containers, it is not surprising that organizations tended to rely on the tools offered by the cloud provider (see Figure 4).

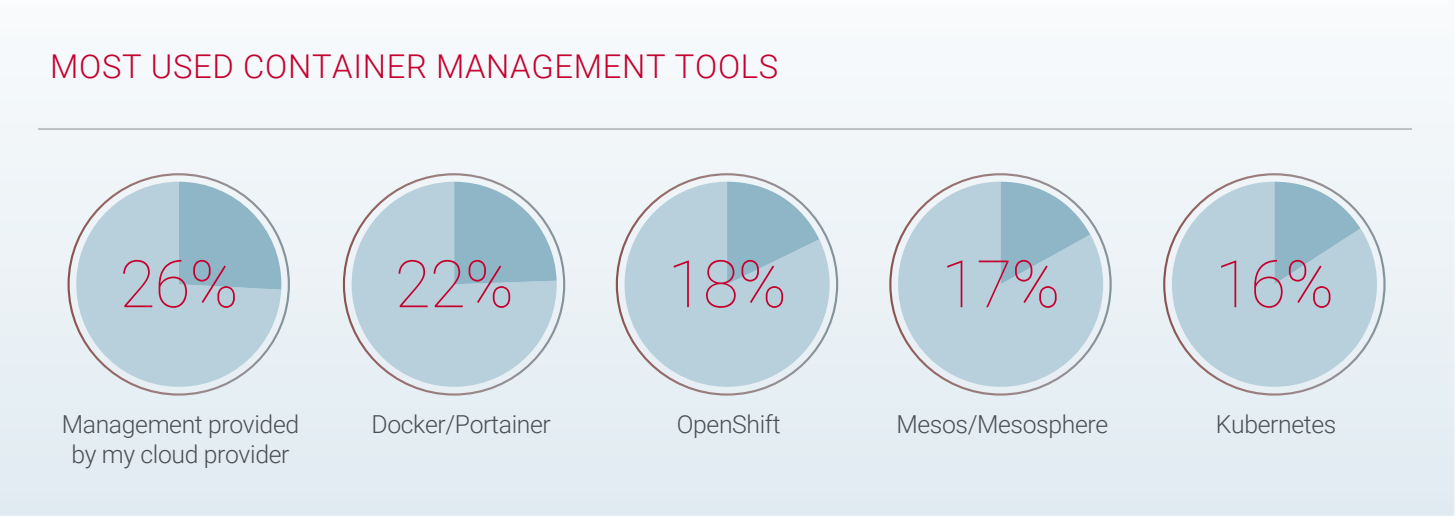



**FIGURE 4.** RESPONDENTS RANKED THE MOST USED CONTAINER MANAGEMENT TOOLS.

***Analyst Note:*** *Kubernetes is thought to have the highest adoption rate, yet it is ranked lowest in the survey. This result raises a question about how many cloud provider solutions are based on Kubernetes or other software.*

## Protecting Application Programming Interfaces (APIs)

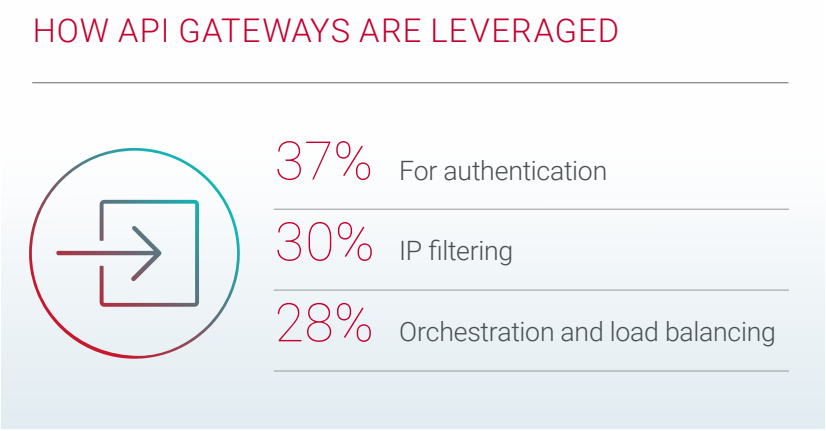



**FIGURE 5.** RESPONDENTS RANKED HOW THEIR ORGANIZATIONS LEVERAGED API GATEWAYS.

More than half of respondents said that their organizations interacted with APIs to share and consume data, while 17% only shared data, and 22% only consumed data via APIs. Results are consistent with how organizations interacted with APIs in last year's survey. Forty-eight percent both shared and consumed data; 15% only shared data, and 19% only consumed data.

***Analyst Note:*** *Sharing and consuming data with APIs is the path to the future for automation. The number of organizations that do this is expected to increase.*

## Managing Encrypted Traffic

Only 8% of organizations are not using SSL with their applications in some form, while 50% of organizations terminate their SSL tunnels before the host (gateway to gateway or host to gateway). This offloads overhead on the application servers and endpoints, but it also increases possible data exposures along the last hop.

***Analyst Note:*** *So long as the environment is well maintained, this approach to SSL management can be a reasonable performance compromise. If not, this is a significant exposure for the organization.*

## Dimming Perceptions of Cloud Service Providers

Organizations continued to look to service providers to host their applications; however, trust in the ability of cloud service providers to secure applications dropped 14 points from the 2018 survey (see Figure 6).

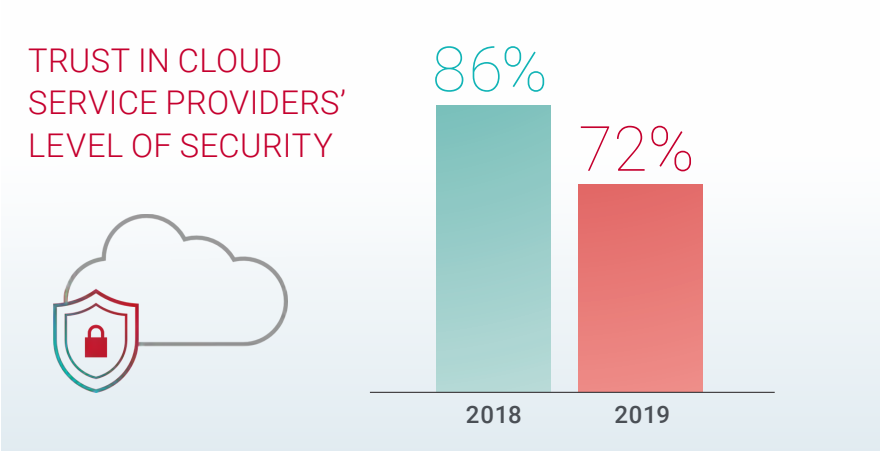



**FIGURE 6.** THE LEVEL OF TRUST IN CLOUD SERVICE PROVIDERS' APPLICATION SECURITY.

***Analyst Note:*** *A 14-point drop in confidence over one year of cloud service providers' ability to secure applications is significant and should be monitored.*

Respondents' confidence that applications were secure when hosted by a cloud service provider waned between 2018 and 2019 (see Figure 6).

According to respondents, only 35% of organizations that host applications in the cloud believed that the delineation of security responsibilities between them and their providers was clear. Almost 20% felt that there were serious misunderstandings.

# 53%

*of organizations with applications hosted in the cloud have experienced data exposure caused by misunderstandings as to which party was responsible to close security gaps.*

## Reliance on Open-Source Code

As part of their software development life cycle (SDLC) processes, respondents reported that 32% of the apps were composed of 50% or more open-source code.

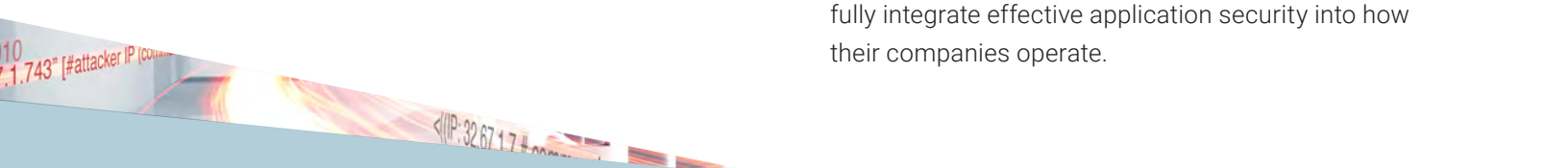
For developers, taking advantage of open-source code sped the process of delivering new or updated applications. The downside was that the organization sacrificed control over the software modules for agility. Unlike native code that is developed in-house, insight was limited into how open-source code was put through quality assurance testing or patched. Developers were in the dark about code vulnerabilities that hackers could exploit. Plus, if bugs were discovered, there was no party responsible for fixes.

***Analyst Note:*** *Survey responses are much higher than for the average percentage of open-source code users in commercial applications.*


# Enhancing Application Security Processes

Organizations are performing a balancing act pushing forward as quickly as possible with digital transformation strategies while at the same time seeking ways to optimize application security. Survey results revealed that no single best practice emerged as a way to guide enterprises in this effort. The process is still a journey of discovery.

The survey also revealed that organizations were, for the most part, following standard accepted security practices to implement security solutions. But in many ways, the non-technical part of digital transformation was the most difficult. Senior management needs to step back and consider larger organizational changes and process controls. Furthermore, decision-making responsibilities need to fully integrate effective application security into how their companies operate.



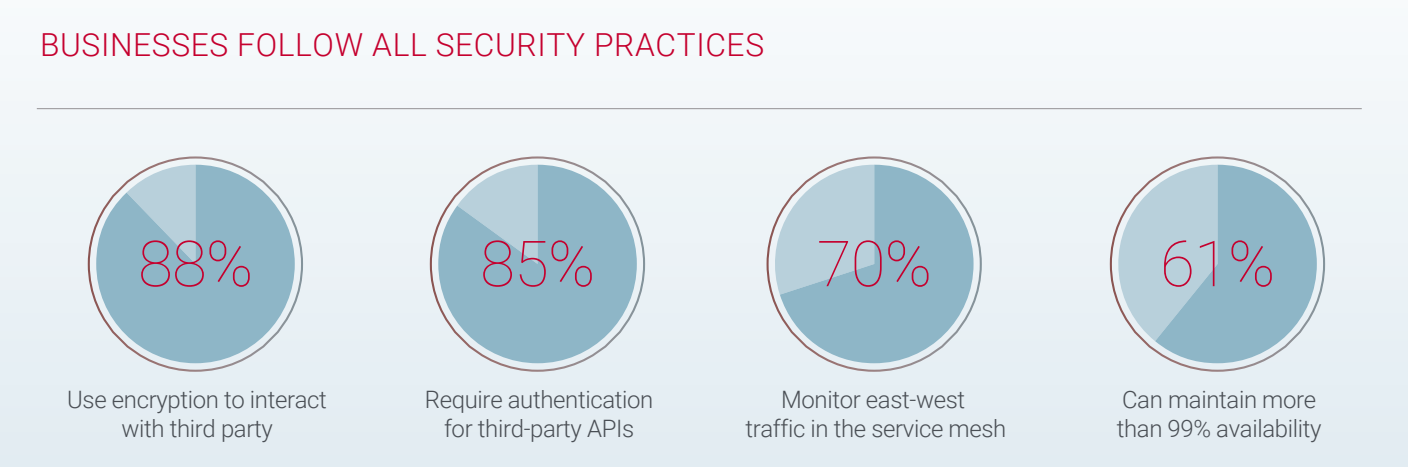



**FIGURE 7.** CURRENT APPLICATION SECURITY MEASURES USED BY RESPONDENTS.

## Microservice and Serverless Architectures

For organizations that develop applications, microservice architectures have grown in popularity in the past few years. This approach disperses loosely coupled services into distributed modules. That way, development teams working on one element of an application cannot break the entire application with their changes. Applications can be developed and updated more quickly in ways that work across multiple platforms.

In serverless or function-as-a-service (FaaS) architectures, applications are hosted by third parties. Developers do not need to manage server software or hardware. The process of scaling applications is simpler, and organizations only pay for the computing resources used because functions are called on instead of requiring always-on availability.

While development and operations (DevOps) automation tools are still the most prevalent, microservices gained traction over use of containers and serverless/FaaS.

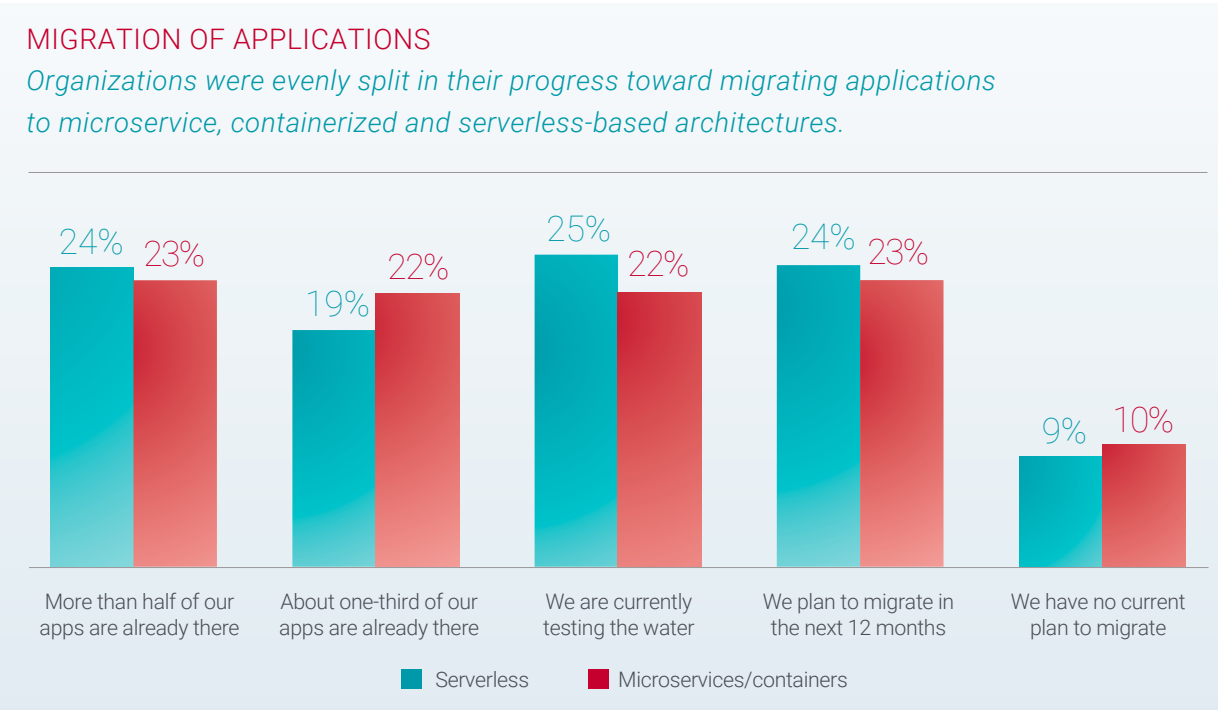



**FIGURE 8.** TEN PERCENT OF RESPONDENTS ARE NOT IN THESE ENVIRONMENTS AT ALL. ABOUT A QUARTER OF RESPONDENTS ALREADY HAVE HALF OF THEIR APPLICATIONS IN THESE ENVIRONMENTS, AND ANOTHER QUARTER OF THEM ARE CURRENTLY TESTING THE WATERS.

## Perceptions of These New Concepts

The benefits for those firms that have completed migrations were observable by respondents. Sixty-eight percent identified an increase in security effectiveness, and 61% recorded an increase in operational efficiency. Increases in operational costs were also realized by 52% of respondents.

In comparison to traditional server-based architectures, 57% of respondents said that the move to microservice/containerized architectures has increased their application risk profile.

*Serverless architectures improved confidence in security effectiveness but at the same time introduced a heightened sense of risk.*

***Analyst Note:*** *The perceived higher level of risks as organizations transition away from server-based architectures is likely because security professionals are still learning about the nuances of the new architectures. Improved application security was observable. Seventy-four percent of respondents identified a greater ability to proactively defend applications in a serverless architecture. However, future risks are unknown.*

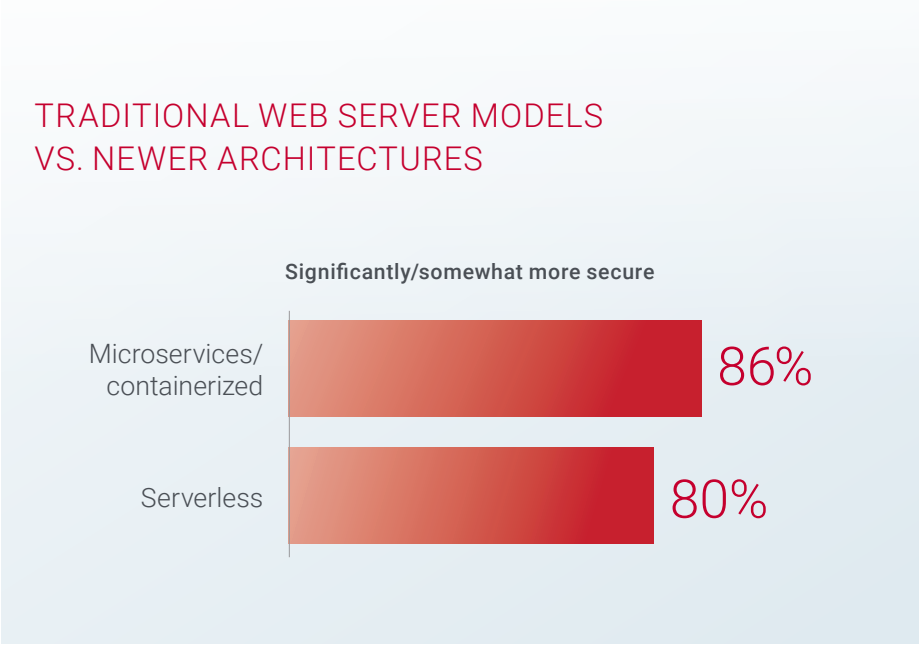



**FIGURE 9.** WHEN ASKED TO COMPARE THE SECURITY OF APPLICATIONS HOSTED ON TRADITIONAL WEB SERVERS, RESPONDENTS OVERWHELMINGLY SAW BETTER PROTECTIONS ON THE NEWER ARCHITECTURES.

## Collaboration in Action

As a result of the evolution of digital transformation, organizations are adjusting roles and responsibilities to try and cope with both the agility and security requirements that accompany these new environments. They are investing in talent to manage application security. More than 90% of respondents reported that their organizations have DevOps and/or development, security and operations (DevSecOps) teams. However, these teams are still relatively new and learning how best to work together.

When evaluating collaboration between DevOps and DevSecOps teams, 49% of respondents said that the groups were working together very closely, while 46% said that they managed to work together.

DevOps teams have been in place with a longevity of about six months (41%), with 28% of teams in place for 12 to 23 months and 21% for 24 months or longer. Fifty-seven percent of respondents said that the ratio of DevOps personnel to development personnel was between 1:6 and 1:10.

Thirty-eight percent of DevSecOps teams have been in place for 7 to 11 months, 35% for 12 to 23 months and 13% for more than two years. Fifty-eight percent said that the ratio of DevOps personnel to development personnel was between 1:11 and 1:20.

***Analyst Note:*** *These results are higher than expected and may indicate that integration of security within organizations' continuous delivery pipelines has matured more quickly than estimated.*

***Analyst Note:*** *The 1:11 to 1:20 ratio of DevOps personnel to development personnel is thin and may require bolstering depending upon how many applications are being supported per security person.*

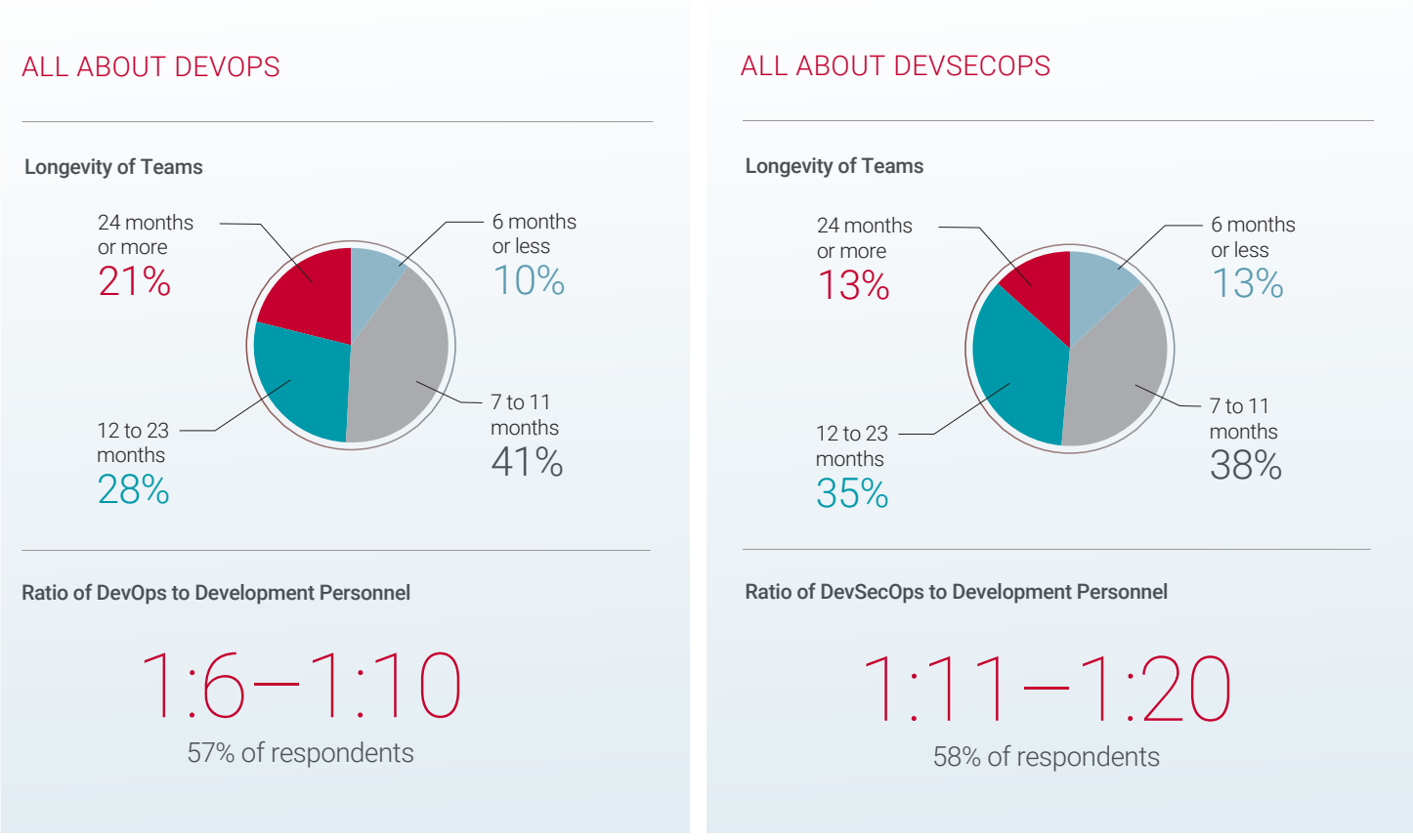



**FIGURE 10.** DEVOPS AND DEVSECOPS TEAMS ARE STILL FAIRLY NEW ADDITIONS FOR MOST ORGANIZATIONS.

Even with the establishment of tighter relationships between information security and app dev teams, only 9% of respondents believed that they achieved above three 9s (i.e., 99.9%) availability application services (see Figure 11). Three 9s is a very low availability bar, representing more than 500 minutes of downtime annually — almost nine hours of outages.

ESTIMATED AVAILABILITY OF APPLICATION SERVICES

*Only 9% of respondents said that their organizations achieved greater than 99.9% of availability for application services.*

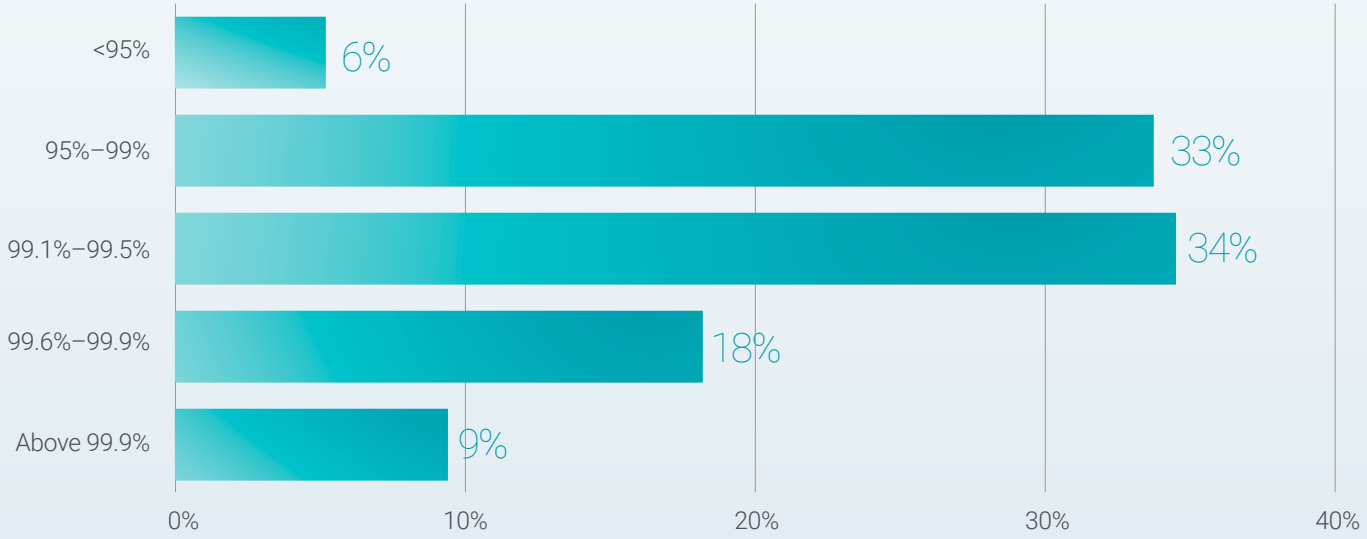



FIGURE 11.

***Analyst Note:*** *Considering consumer demand for always-on access, respondents' rankings of their organizations' application services availability are surprisingly low.*

## Managing APIs

APIs are central to enabling continuous integration of applications. As part of security protocols, 85% of respondents said that they required authentication or used a single sign-on (SSO) solution to interact with third-party APIs. Eighty-eight percent of survey participants used encryption when exposing data to third-party APIs, while 91% analyzed API vulnerabilities prior to integration. These high percentages demonstrate that businesses understand that APIs are a blind spot.

Gartner predicts that, by 2021, 90% of web-enabled applications will have more surface area for attack in the form of exposed APIs rather than the user interface (UI), up from 40% in 2019.[1]

[1] O'Neill, Mark; Zumerle, Dionisio; D'Hoinne, Jeremy, "API Security: What You Need To Do To Protect Your APIs," August 28, 2019, Gartner.

## Continuous Delivery

When asked about progress with continuous integration/continuous deployment (CI/CD), which is a critical step toward achieving digital transformation, 9% said that they have not yet begun, and 10% said that they are almost there but are stalled by security concerns. While 44% achieved CI, only a modest 37% said that they have achieved both CI and CD — but only for some of their applications.

More than half of survey respondents said that security was fully integrated with their CD pipeline, which indicates a maturation of the application delivery process in many organizations. The vast majority also said that security was integrated within the continuous delivery of web applications, APIs and mobile applications.

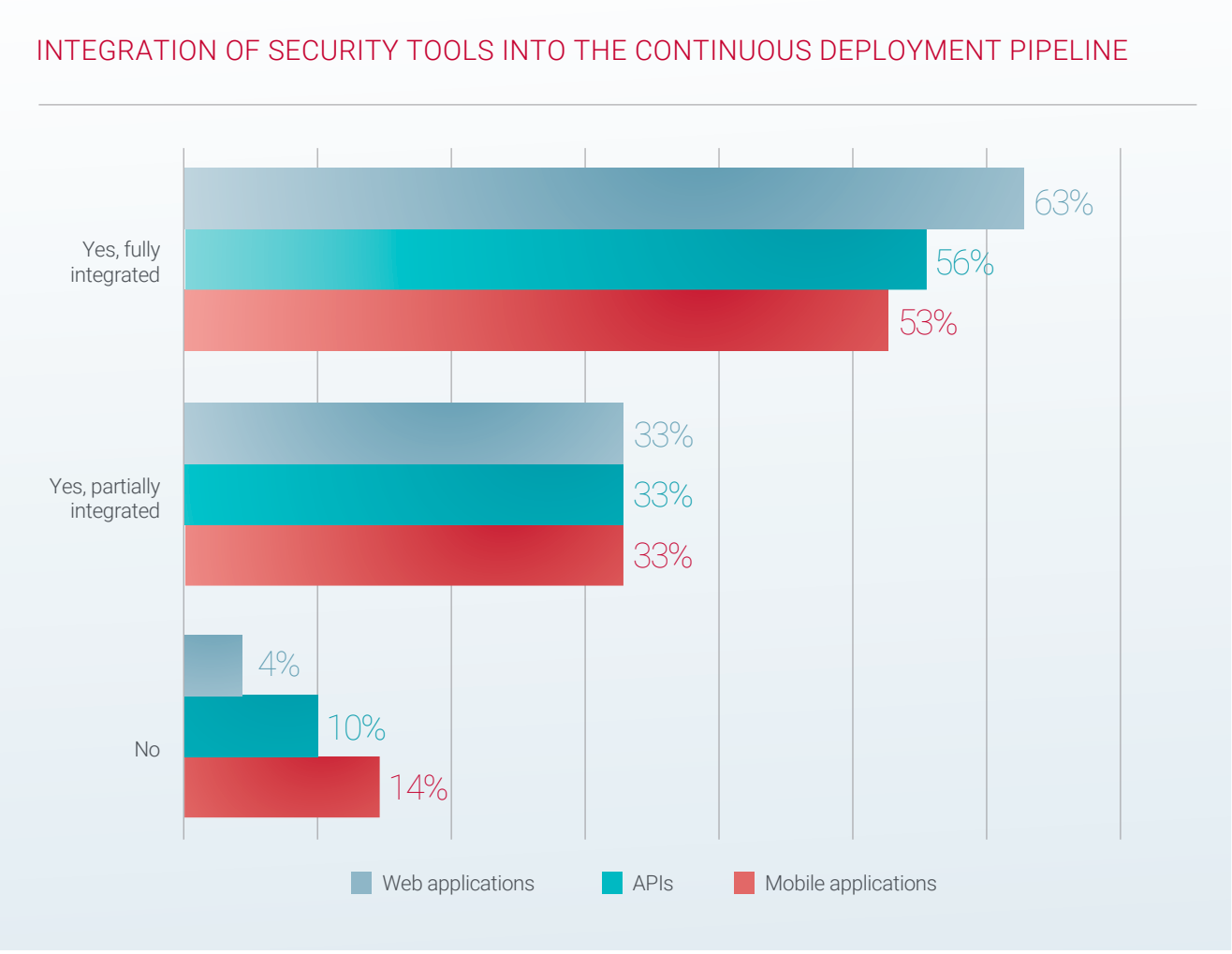



FIGURE 12.

## False Sense of Confidence

A staggering 95% of respondents felt that they were doing a good job distinguishing between good and bad bots on their networks, yet bad bots were a significant and evolving security threat. Forty-five percent said that bad bots accounted for more than 40% of the total traffic to applications on their networks.

FALSE SENSE OF CONFIDENCE

| | |
|---|---|
| Protecting PII | 96% |
| Good collaboration between security and development | 95% |
| Detect malicious bots | 85% |
| Controlling east-west traffic | 70% |
| Fully integrated into continuous delivery | 63% |
| 99% availability | 61% |

**FIGURE 13.** RESPONDENTS ARE CONFIDENT, YET ATTACKS STILL OCCUR.

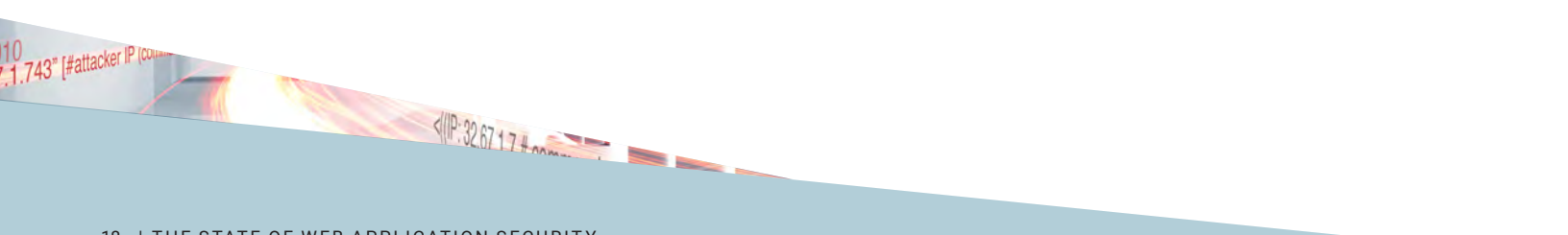
***Analyst Note:*** *Overconfidence in the ability to detect bad bots can be tied to using the wrong security tools to measure and mitigate. Radware estimates the average traffic flow of bad bots to be approximately 27%.*

Ninety percent of organizations that experienced a breach in the past 12 months believed that dwell time in their networks was one month or less. This time span is much shorter than what two recent large empirical studies determined was the average time that breaches were resident in networks before discovery.

IBM Security's *2019 Cost of a Data Breach* report found that the average time to identify and contain a breach was 279 days, or about nine months.[2] The Verizon *2019 Data Breach Investigations Report* stated that discovery of a breach was "likely to be months" and was "very dependent on the type of attack in question."[3]

[2] *"2019 Cost of a Data Breach,"* IBM Security/Ponemon Institute. *Retrieved from https://databreachcalculator.mybluemix.net/?cm_mc_uid=09674686157315681565684&cm_mc_sid_50200000=72371291568156568412&cm_mc_sid_52640000=46312901568156596761*

[3] *"2019 Data Breach Investigation Report," Verizon, May 8, 2019, Page 19.*



## ESTIMATED TIME BREACH WAS RESIDENT PRIOR TO DISCOVERY

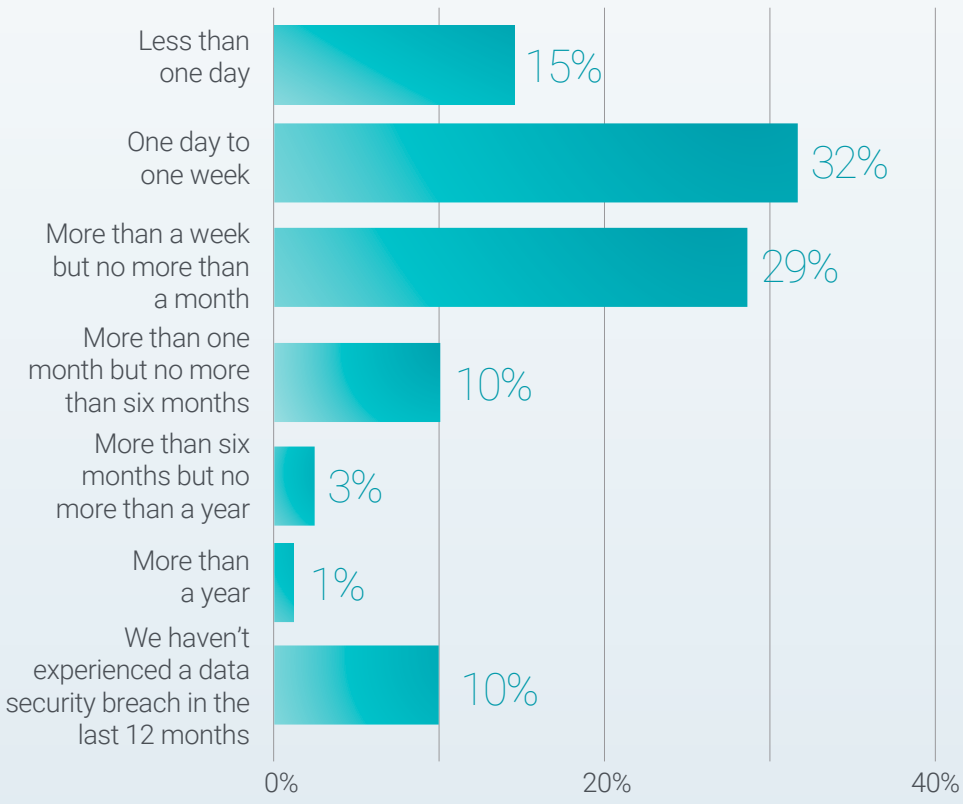



**FIGURE 14.** RESPONDENTS ESTIMATED HOW LONG DATA BREACHES IDENTIFIED IN THE PREVIOUS 12 MONTHS WERE RESIDENT IN THEIR NETWORKS PRIOR TO DISCOVERY.

***Analyst Note:*** *It is puzzling that most organizations underestimated the amount of time that breaches were in their networks. Is it poor log quality, lack of data or lack of context? Many organizations only kept one month's worth of log data on hand.*

Confidence also extended to organizations that employed multiple cloud providers. Seventy-one percent of respondents felt that they could enforce the same level of security across all hosted applications.


# Yet Attacks Still Find a Way

Even though the respondents expressed confidence in their organizations' capabilities to protect applications either on-premise or in hosted environments, attacks were still successful. Hackers seemed to love the challenge that new technologies introduced. They employed many tools to scan and map applications to identify vulnerabilities.

In addition to new and better ways to meet customer demand for relevant interactions with brands, emerging technologies also offered up a wider attack surface and new exposure to threats.

## The Threat Landscape

Threats to application security are part of doing business in a digital economy. Respondents indicated that they were under ongoing attacks on a variety of fronts.

### WEB APPLICATION ATTACKS

For many years, SQL injection (SQLi) and cross-site scripting (XSS) attacks have been the most prevalent attack types. Recently there was a rise in API manipulations and session cookie poisoning in both overall quantity and frequency. Access violations were the most common attack type overall.

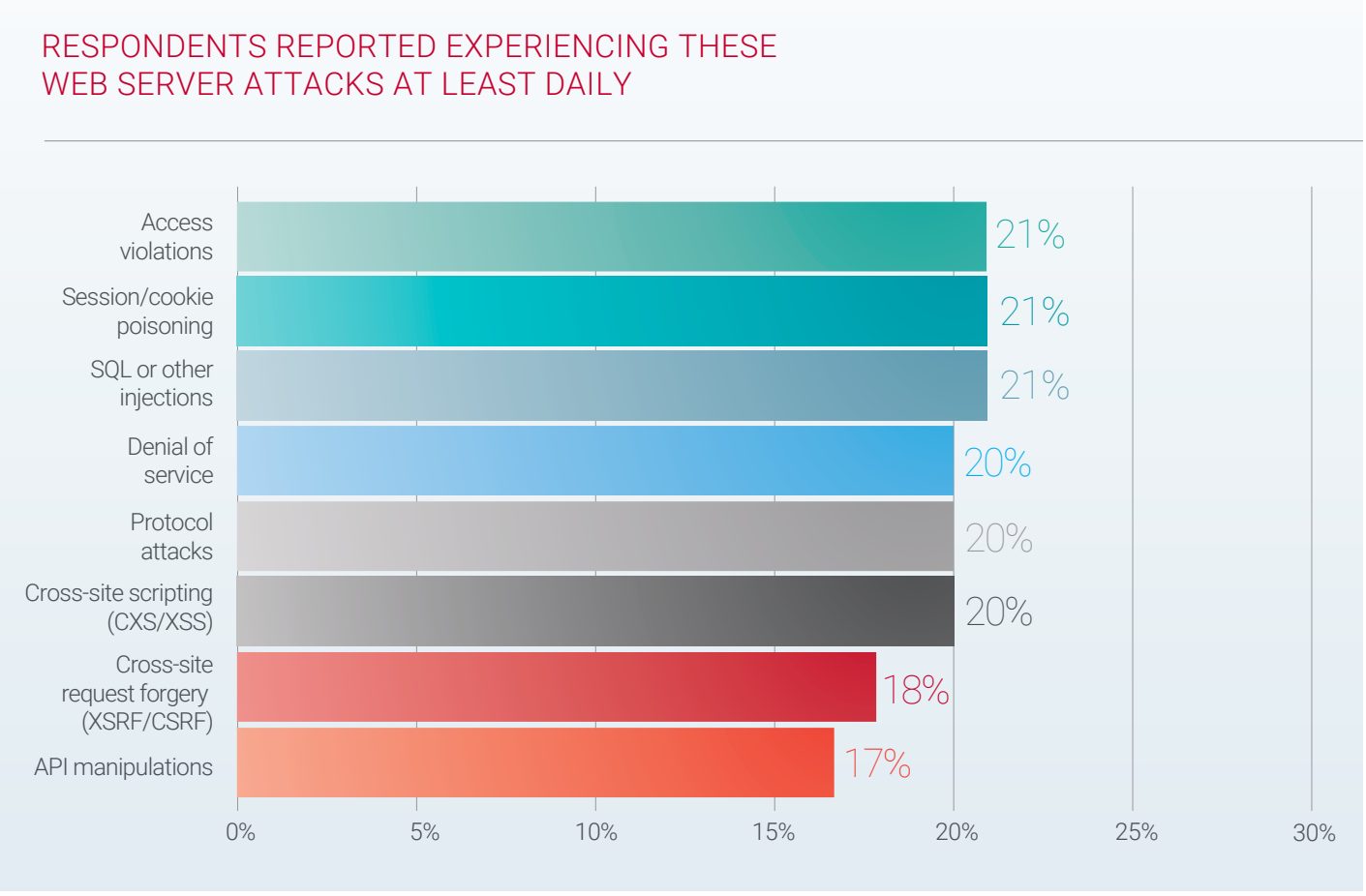



FIGURE 15.

### APIs

Access violations, which are the misuse of credentials, and denial of service (DoS) are the most common daily API attacks reported in the survey. Other threats included injections, data leakage, element attribute manipulations, irregular JSON/XML expressions, protocol attacks and Brute Force.

Gartner predicts that, by 2022, API abuses will move from an infrequent to the most frequent attack vector, resulting in data breaches for enterprise web applications.[4]

***Analyst Note:*** *Instances of data leakage attacks were significantly lower than other attack forms, indicating that data controls were proving successful to a large degree against attempts to infiltrate networks.*

## API ATTACKS THAT RESPONDENTS REPORTED EXPERIENCING AT LEAST DAILY

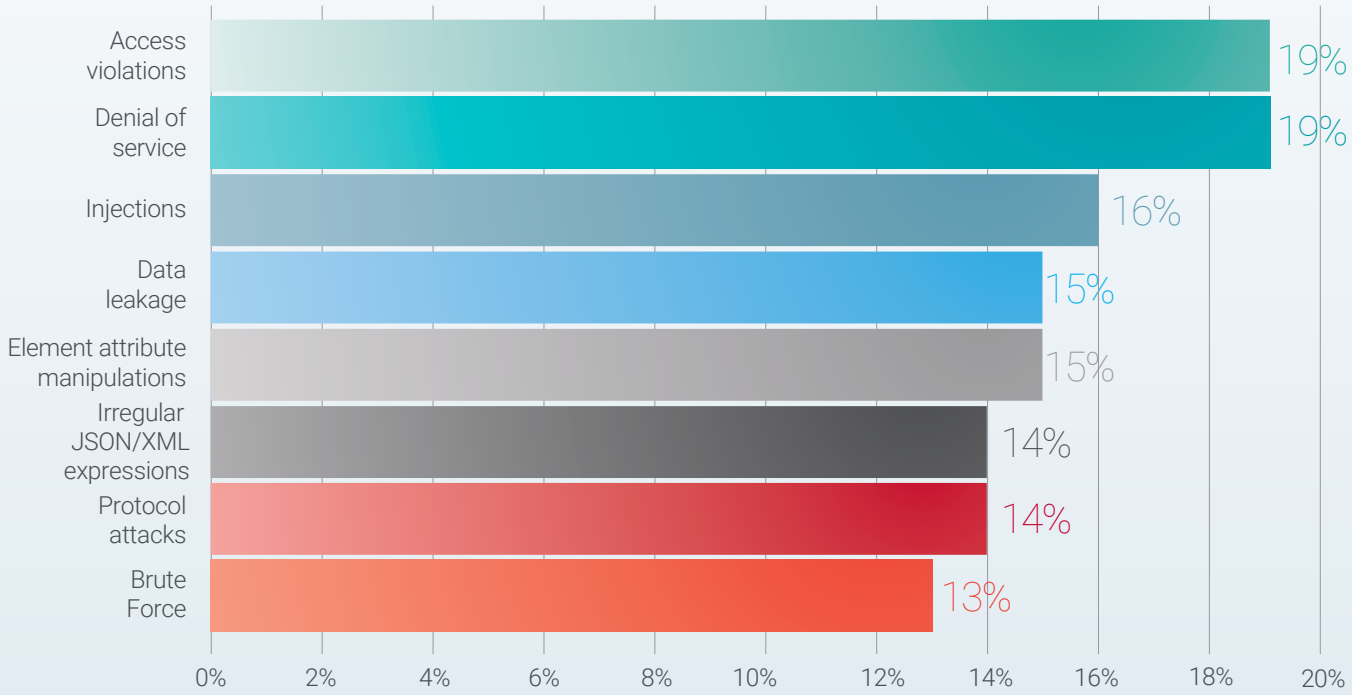



FIGURE 16.

[4]O'Neill, Mark; Zumerle, Dionisio; D'Hoinne, Jeremy, "API Security: What You Need To Do To Protect Your APIs," August 28, 2019, Gartner.

## BOT ATTACKS

Although web scraping is the most common attack overall, account takeover, DoS and payment abuse were the most common bot attacks and occurred daily.

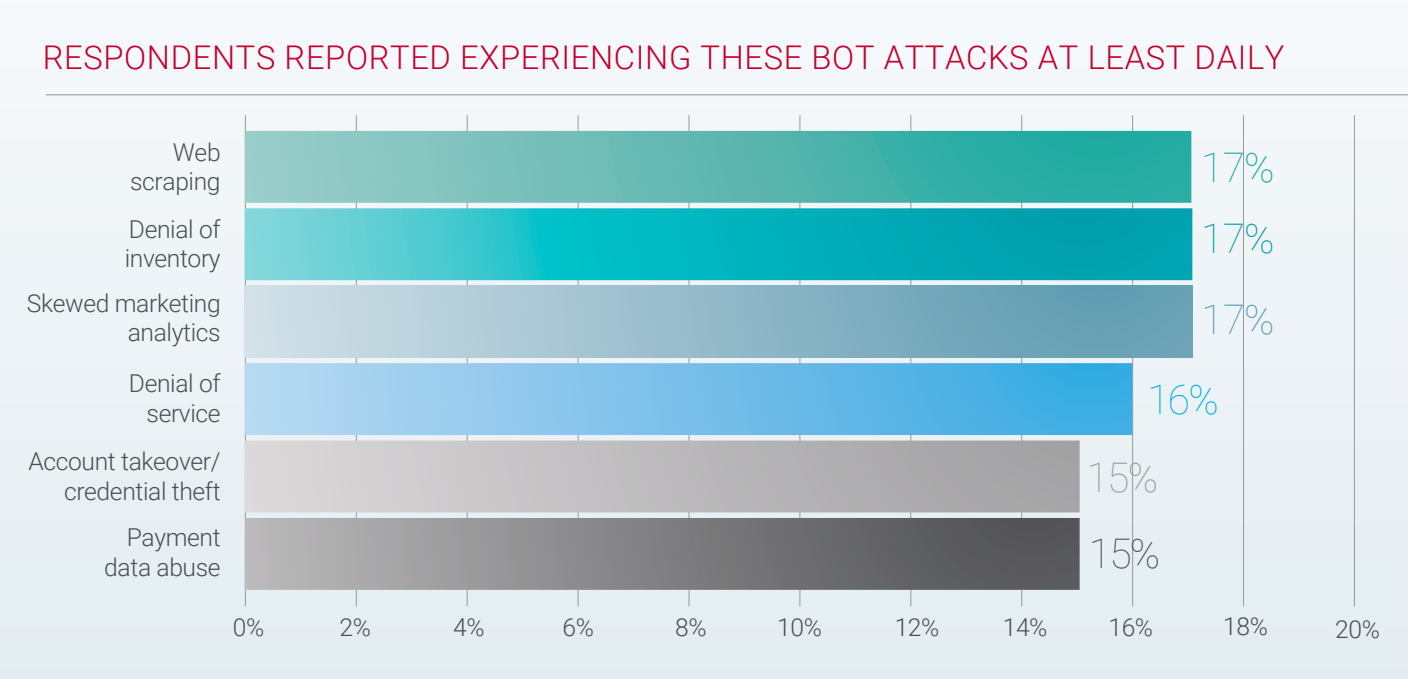



FIGURE 17.

## APPLICATION DENIAL-OF-SERVICE ATTACKS

Twenty percent of organizations experienced DoS attacks on their application services every day. Buffer overflow was the most common attack type.

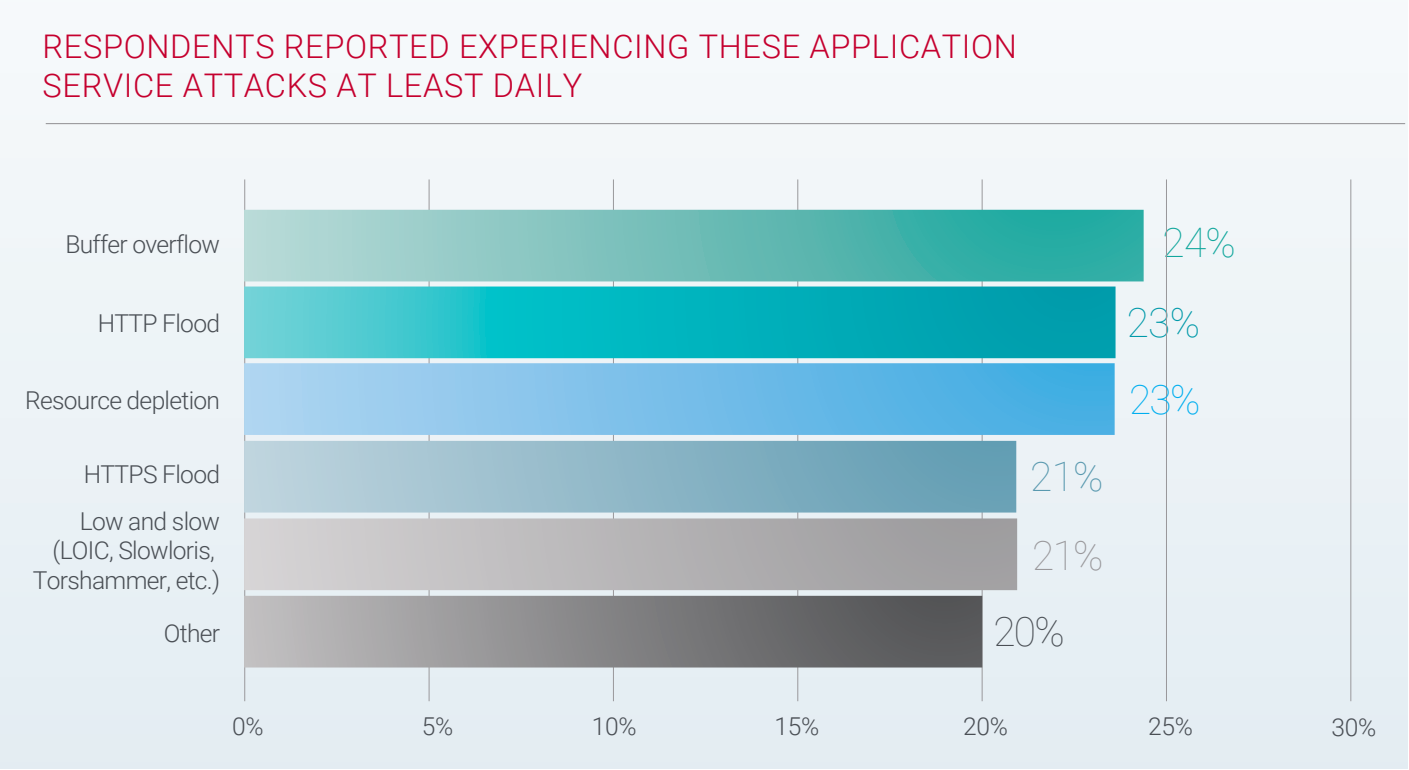



FIGURE 18.

## Conditions Are Friendly to Attacks

With the variety of solutions deployed across organizations, better relationships between information security and application development teams and a heightened focus on the importance of protecting applications, why are attacks still getting through?

One contributing factor was that the final responsibility for application security does not necessarily reside with the CISO. When asked to rank the top three influencers on software security policy, respondents listed IT leadership (CIO, VP, director) and business owners higher than CISOs (see Figure 19).

| | TOP THREE INFLUENCERS ON SECURITY POLICY | TOP THREE INFLUENCERS ON IMPLEMENTATION | TOP THREE INFLUENCERS ON SECURITY TOOLS |
|---|---|---|---|
| 1 | IT Leadership | IT Leadership | Business Owner |
| 2 | Business Owner | Business Owner | IT |
| 3 | CISO | Application Development (AppDev) | DevOps |

**FIGURE 19.** RESPONDENTS LOOKED PAST CISOs WHEN RANKING THE TOP THREE INFLUENCERS IN THEIR ORGANIZATION ON SOFTWARE SECURITY POLICY AS WELL AS ON IMPLEMENTATION.

The *2019 Executive Application & Network Security Report* from Radware found that 72% of executives discussed cybersecurity at every boardroom meeting. The severity of the threat landscape, the mounting cost of attacks and the potential long-term negative impact on business operations weighed heavily on high-ranking management.

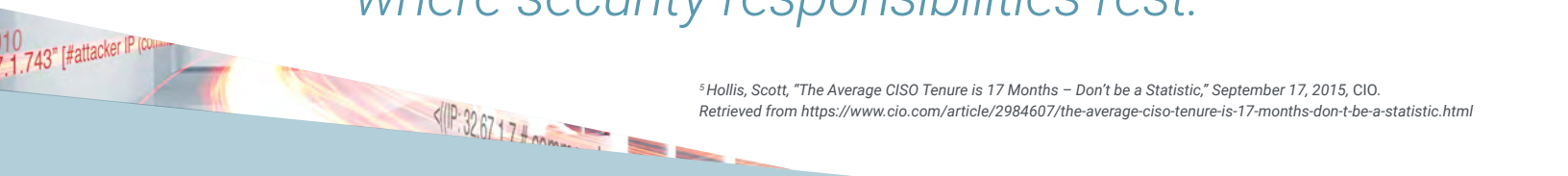
CISOs were under intense pressure from the C-suite to safeguard the customer experience, yet responses to this survey revealed that they had little financial decision-making authority for the security technologies that were deployed. So while they were increasingly accountable for results, there was not a corresponding uptick in authority over how applications were secured.

Perhaps that is why the average tenure for most CISOs was only 17 months.[5]

There was also some confusion about where cloud providers' responsibilities for security end. Only 35% of organizations using the cloud believed that the delineation of security responsibilities between them and their providers was clear. ***Fifty-three percent experienced data exposures due to misunderstandings.***

***Analyst Note:*** *There was ongoing confusion about which entity was responsible for application security, which seemed nonexistent and was not acceptable in an on-premise scenario.*

*More than one-half of the organizations hosting applications in the cloud reported a security gap caused by misunderstandings with service providers about where security responsibilities rest.*



[5] *Hollis, Scott, "The Average CISO Tenure is 17 Months – Don't be a Statistic," September 17, 2015,* CIO. *Retrieved from https://www.cio.com/article/2984607/the-average-ciso-tenure-is-17-months-don-t-be-a-statistic.html*

The rate at which applications underwent change was also a contributing factor to the success of attacks. On average, 22% of organizations reported making updates to web, cloud, in-house and third-party applications on a daily or more frequent basis. Even with CI/CD security processes in place, the dynamic nature of these environments created new risks (see Figure 20).

## RESPONDENTS REPORTED UPDATING WEB, CLOUD, IN-HOUSE AND THIRD-PARTY APPLICATIONS ON A DAILY OR MORE FREQUENT BASIS

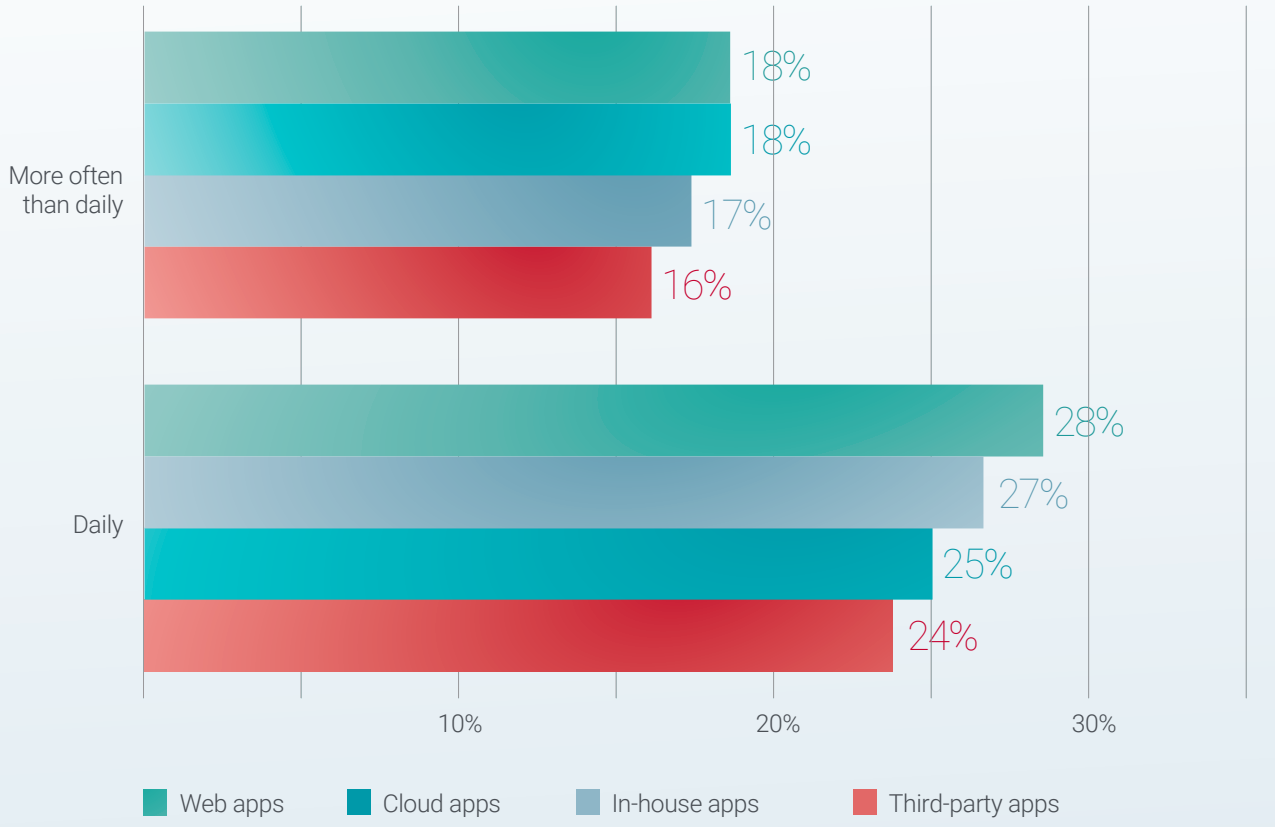



**FIGURE 20.**

## Implications of Cyberattacks

When application attacks are successful, organizations are likely to experience consequences that can cause long-term damage. Customers expect the organizations with which they associate to protect their data and provide always-on access to applications. When a data breach is revealed, the trust between customers and the organization is broken. The process of repairing a company's reputation is long and not always successful.

Respondents listed a variety of negative outcomes that their organizations experienced after attacks (see Figure 21).

CONSEQUENCES OF APPLICATION ATTACKS

*Successful attacks can produce a variety of negative consequences for organizations.*

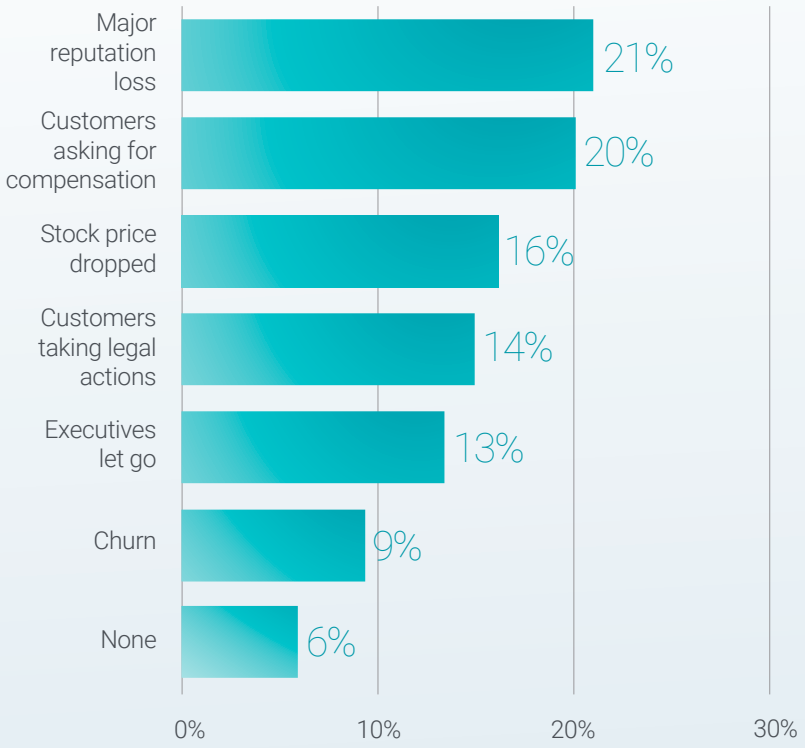



FIGURE 21.

## Car Makers Feel the Heat

Breaches at two car makers are good examples of the damage that organizations can incur for failing to protect consumers' data and safety.

In 2015, Fiat Chrysler Automobiles (FCA) recalled 1.4 million Jeep Cherokee vehicles to fix a software glitch that enabled hackers to wirelessly access some vehicles and control crucial electronic functions. Jeep owners have since filed a lawsuit seeking $70 billion USD ($50,000 per impacted vehicle). The case is still working its way through the court system.[6]

In 2018, an employee at Tesla was discovered to have used falsified credentials to make changes to the Tesla Manufacturing Operating System and export large amounts of sensitive data to third parties.[7] The company filed a lawsuit against the alleged perpetrator, but the damage to the company's brand cannot be completely repaired. How does Tesla prove that it has proper security protocols in place?

## Conclusion

The state of web application security was somewhat scattered as organizations deployed multiple solutions without a clear strategy to determine who was ultimately responsible to drive decision-making.

In many cases, CISOs did not have the final say about security choices. Each business unit or function may have pursued its own strategies and implemented different solutions without a holistic approach for securing applications across the enterprise.

Surprisingly, organizations did not recognize that this scattered approach still left their organizations vulnerable to attack. Confidence remained high among respondents' ability to recognize bad bot traffic and detect threats in their networks. There was a bit of decline in the perception that cloud service providers could securely host web applications, but organizations still said that they relied on third-party security measures.

As more applications are transitioned to microservice architectures, new security challenges will emerge. Now is the time for organizations to more fully understand what changes need to be made across all business functions to shore up security strategy, planning, implementation and process controls.

[6] *McCarthy, Kieren, "Jeep hacking lawsuit shifts into gear for trial after US Supremes refuse to hit the brakes," January 8, 2019,* The Register. *Retrieved from https://www.theregister.co.uk/2019/01/08/jeep_hacking_supreme_court/*

[7] *Townsend, Kevin, "Tesla Breach: Malicious Insider Revenge or Whistleblowing?" June 22, 2018,* SecurityWeek. *Retrieved from https://www.securityweek.com/tesla-breach-malicious-insider-revenge-or-whistleblowing*

# RADWARE INSIGHTS: APPLICATIONS FACE AUTOMATED THREATS

## 12-MONTH ANALYSIS OF CUSTOMER TRAFFIC

## RADWARE CUSTOMERS' NETWORKS TRAFFIC PROFILE

12-Month Analysis

As part of its service offerings, Radware's Bot Manager monitors the traffic passing through its customers' networks. Analysis of this aggregate traffic reveals real-world trends that counter some of the assumptions made by survey respondents.

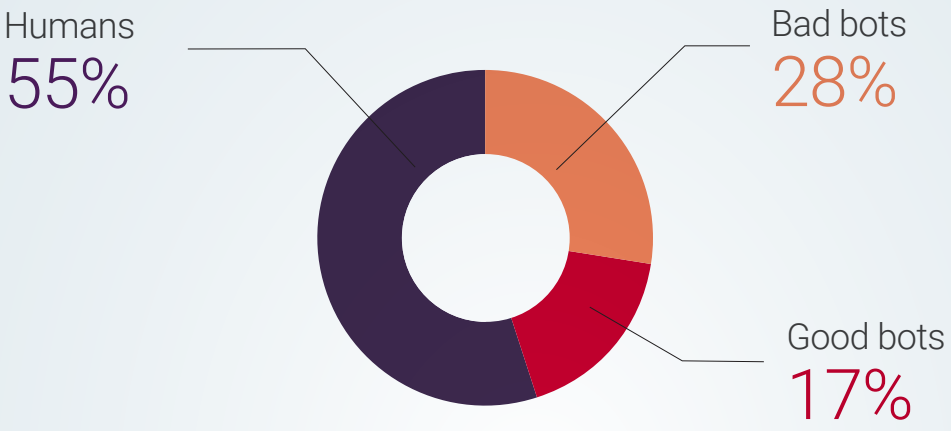
As the amount of bot traffic grows, the challenge for all organizations is to understand the difference between good and bad bots. In the survey, an unlikely 95% of respondents said that they felt that their organizations were doing a good job distinguishing between good and bad bots on their networks.

As bots get more sophisticated, they do a better job mimicking human behavior such as keystrokes and mouse movements to trick security screening. Other sophisticated bots can generate different device IDs to bypass challenges to get into networks, take over user accounts, scrape data and/or disrupt services.

On the other hand, security solutions — in an effort to block bad bots — also produce false positives, identifying good traffic as bad bots. Valid users are blocked from accessing services, and good bots such as Google could be denied access.

# ALMOST HALF OF ALL TRAFFIC **IS GENERATED BY BOTS**

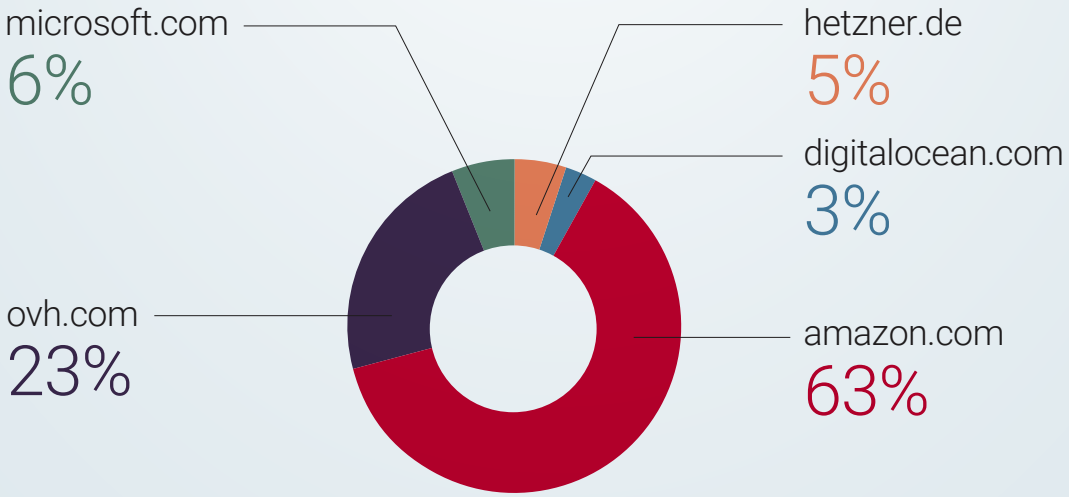
FIGURE 22.




# TOP 5 HOSTS **ORIGINATING BOT TRAFFIC**

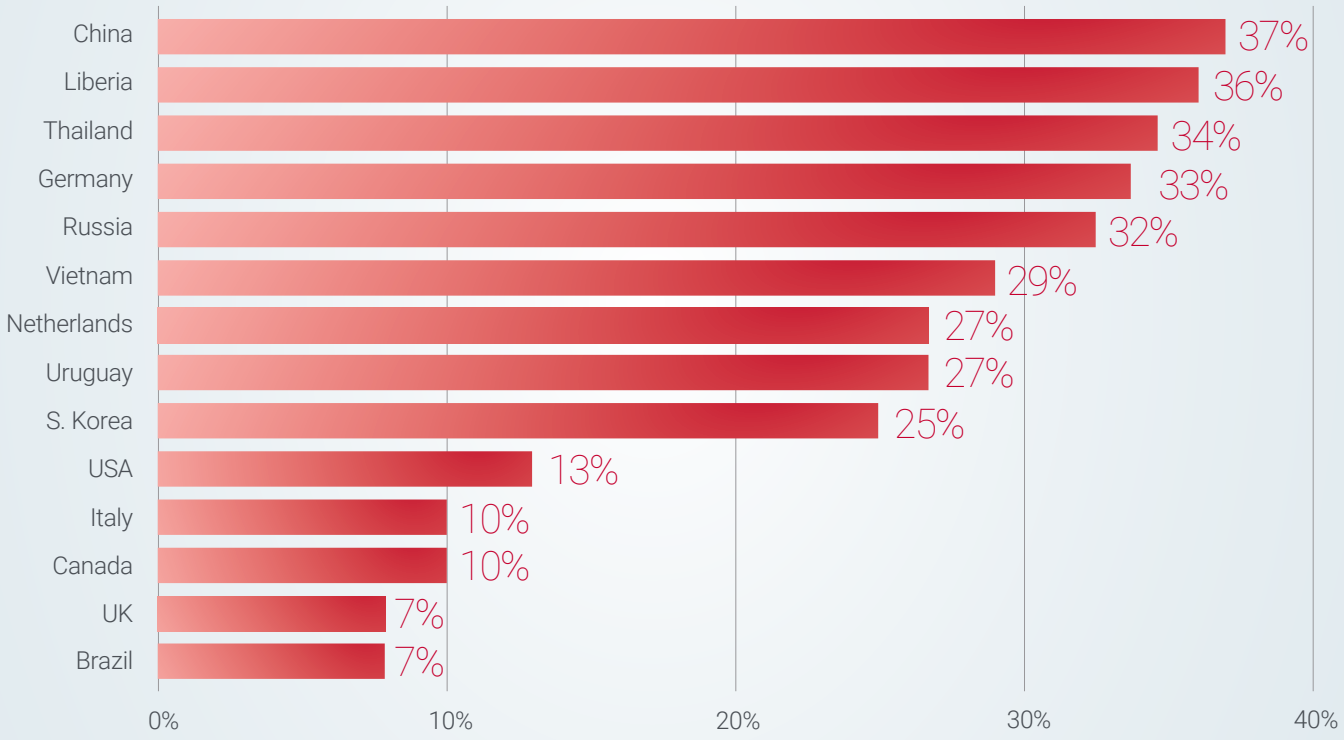
Two-thirds of bot traffic originates from Amazon. In addition to enterprises, cyberattackers benefit from the advantages of public cloud services to leverage the scalable infrastructure and infinite computer power to run programs and launch attacks.

FIGURE 23.



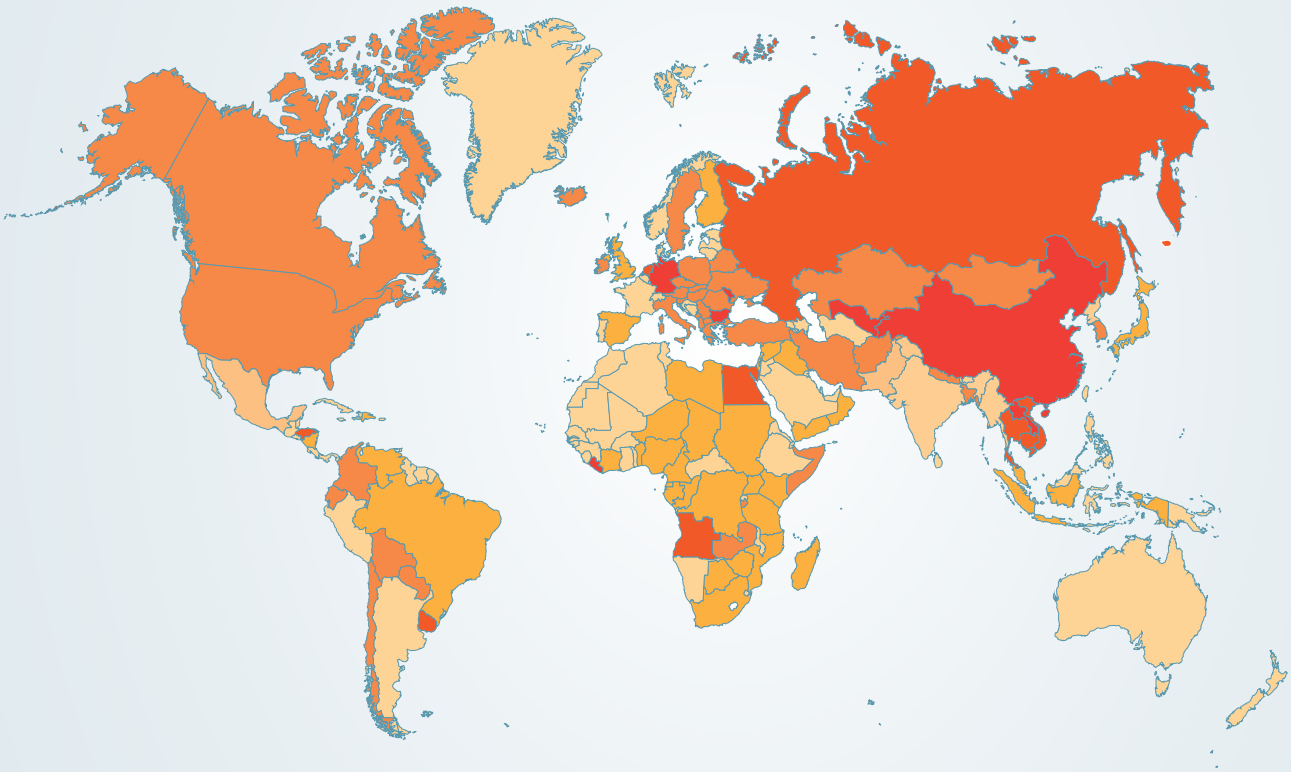
# GEOGRAPHIC BREAKDOWN PERCENTAGE OF BOT TRAFFIC GENERATION BY COUNTRY

FIGURE 24.



# GEOGRAPHIC BREAKDOWN WORLDWIDE HEAT MAP OF BOT TRAFFIC

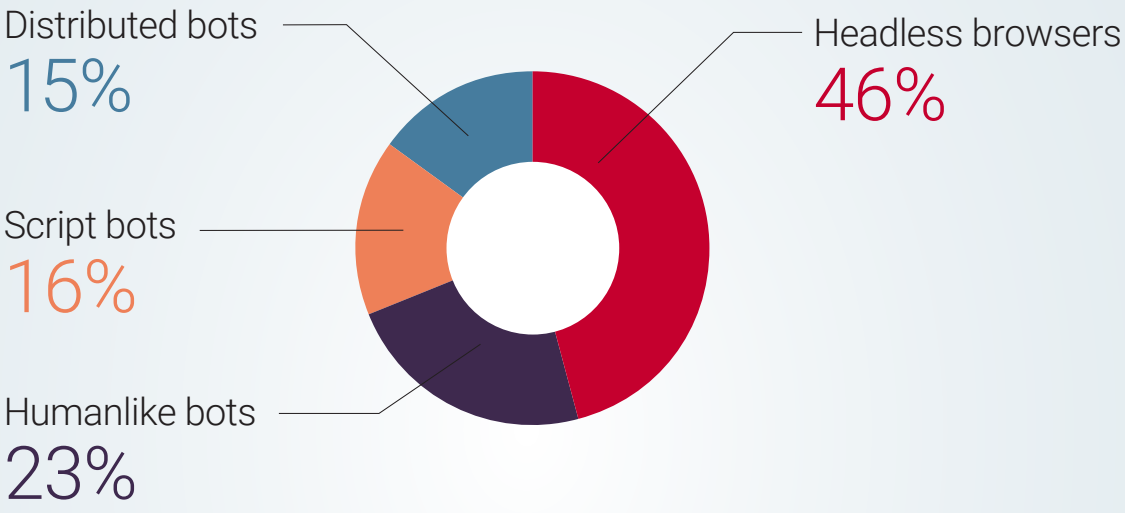
FIGURE 25.



# CLASSIFICATION OF BAD BOTS BOT TRAFFIC BY GENERATION

**FIGURE 26.** PERCENTAGE OF BAD BOT GENERATIONS IN NETWORK TRAFFIC.

Over time, bots have become more sophisticated. Each generation adds capabilities in an effort to thwart security solutions by mimicking human behavior.




**Script Bots** — First-generation bots were built with basic scripting tools and make cURL-like requests to websites using a small number of IP addresses (often just one or two). They do not have the ability to store cookies or execute JavaScript, so they do not possess the capabilities of a real web browser.

**Headless Browsers** — Second-generation bots operate through website development and testing tools known as "headless" browsers as well as later versions of Chrome and Firefox, which allow for operation in headless mode. Unlike first-generation bots, they can maintain cookies and execute JavaScript. Botmasters began using headless browsers in response to the growing use of JavaScript challenges in websites and applications.

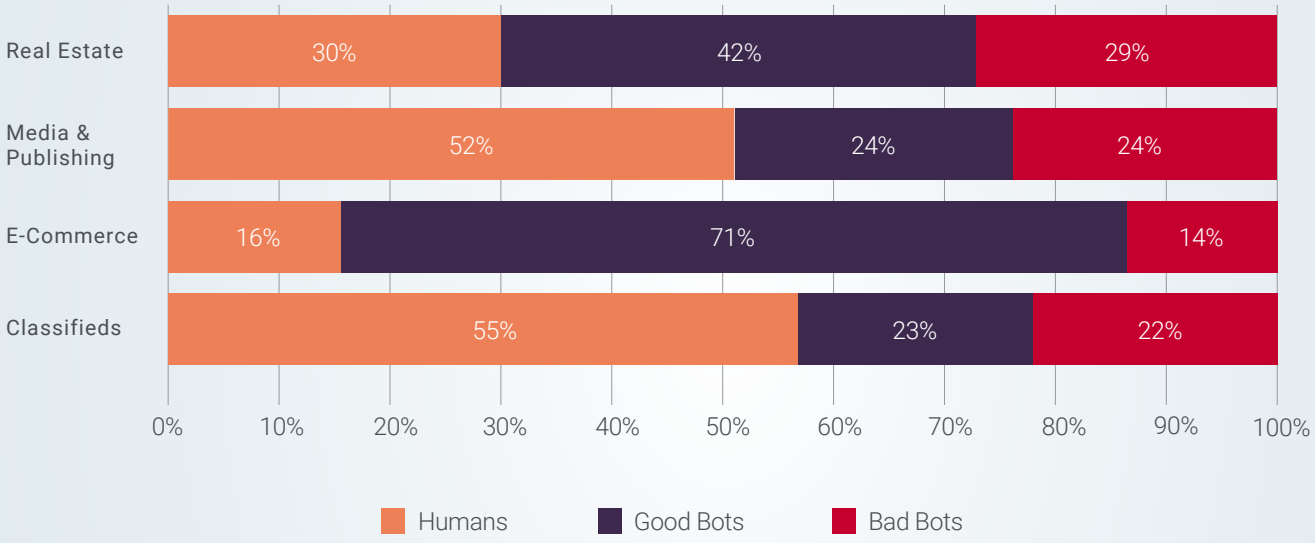
**Humanlike Bots** — Third-generation bots use full-fledged browsers — dedicated or hijacked by malware — for their operations. They can simulate basic humanlike interactions such as simple mouse movements and keystrokes. However, they may fail to demonstrate humanlike randomness in their behavior.

**Distributed Bots** — The latest generation of bots has advanced humanlike interaction characteristics, including moving the mouse pointer in a random, humanlike pattern instead of in straight lines. These bots also can change their user agents (UAs) while rotating through thousands of IP addresses. There is growing evidence that points to bot developers carrying out "behavior hijacking" — recording the way in which real users touch and swipe on hijacked mobile apps to more closely mimic human behavior on a website or app. Behavior hijacking makes them much harder to detect because their activities cannot easily be differentiated from those of real users. What's more, their wide distribution is attributable to the large number of users whose browsers and devices have been hijacked.

# VERTICAL TRENDS: WHERE BOTS ATTACK

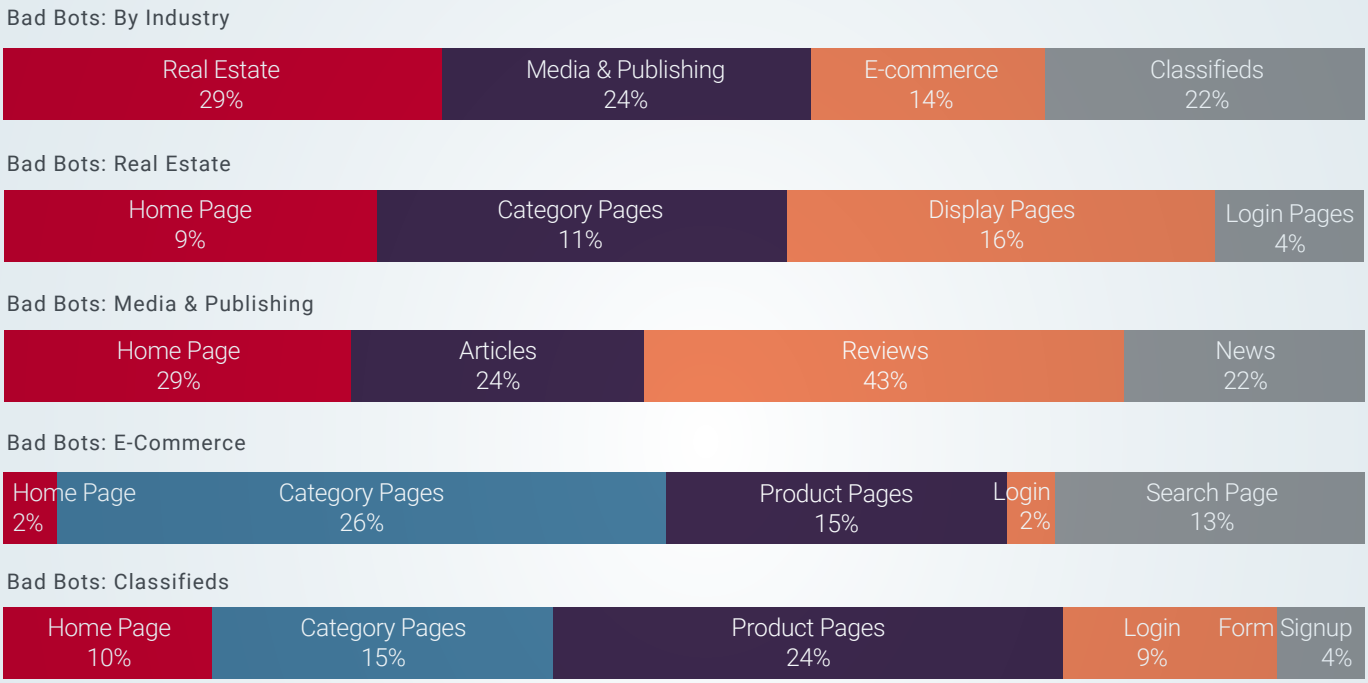
**FIGURE 27.** OVERVIEW OF TRAFFIC ON NETWORKS BROKEN OUT BY VERTICAL INDUSTRIES.

Analysis of network traffic uncovers interesting data about what type of traffic crosses the networks of organizations broken out by vertical industries.



# CLASSIFICATION OF BAD BOTS BOT TRAFFIC BY GENERATION

**FIGURE 28.** BREAKDOWN OF BAD BOT TRAFFIC BY PAGE ACROSS ALL INDUSTRIES.




Every industry is subject to different attack types. Hackers are selective in what they target depending on what bounty they think they can extract.

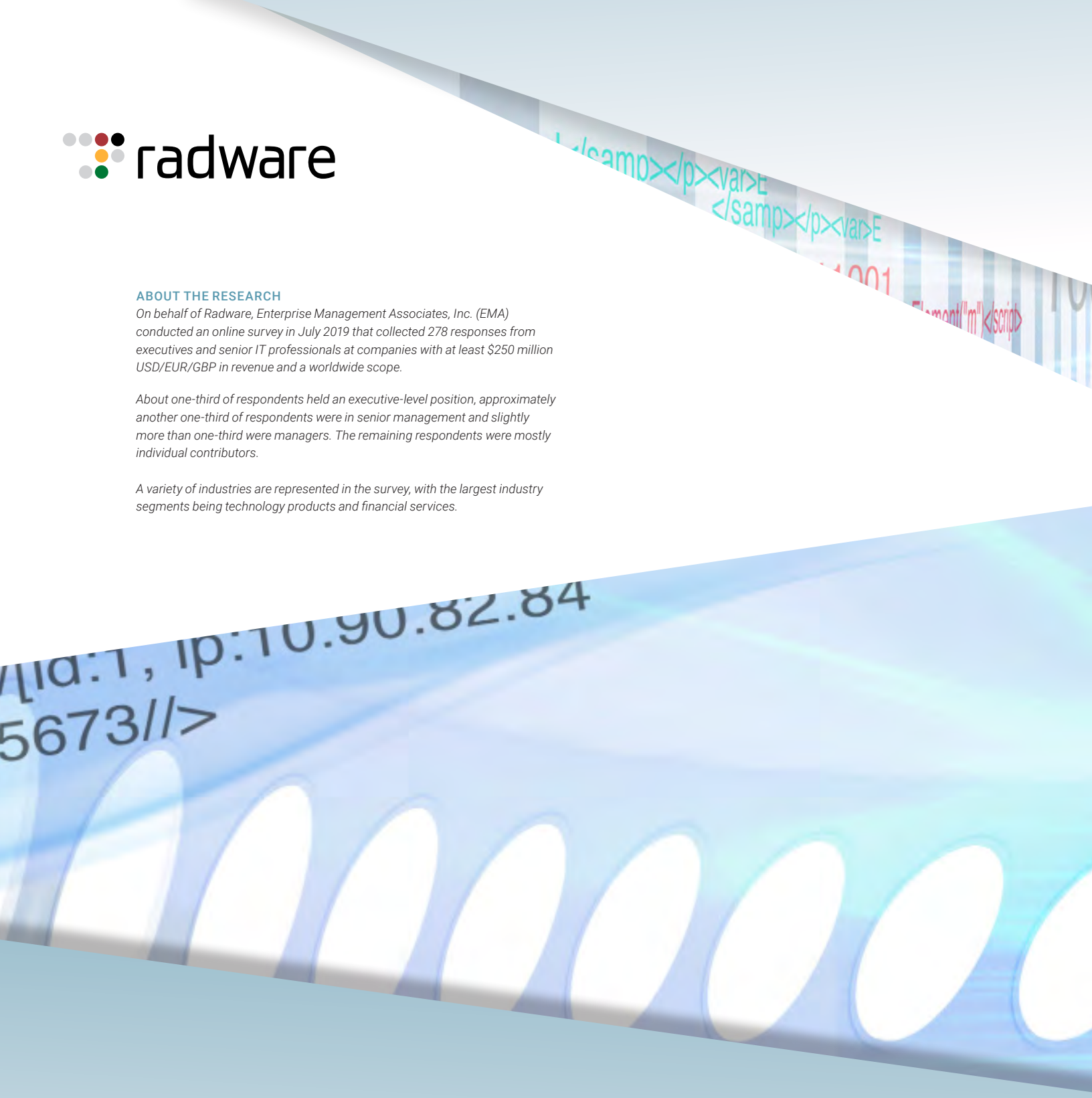
For both real estate and classifieds portals, bot herders target the display pages, likely culling relevant information from the listed ads, such as prices, photos and locations. The data could be used by competitors to adjust their own prices or monitor market changes.

The media & publishing industry suffers from high volumes of bad bots copying proprietary content. This practice affects the business models of these sites that rely heavily on affiliate programs and advertising for revenue. Besides illegally copying data, bot traffic skews website analytics for decision-makers.

The expectation for e-commerce is that bots are programmed to take over accounts to make fraudulent purchases. Instead, results show that category pages are targeted — mostly by web scrapers — to copy information. A U.S. appeals court recently ruled that web scraping is not a violation of the Computer Fraud and Abuse Act.[8]

[8] *Lee, Timothy B., "Web scraping doesn't violate anti-hacking law, appeals court rules," September 9, 2019,* Ars Technica. *Retrieved from https://arstechnica.com/tech-policy/2019/09/web-scraping-doesnt-violate-anti-hacking-law-appeals-court-rules/*


shell exe
1000101111010001
<shell execution>_split_[0]_quit =socket. close >><error!:. _split_[0]_qui
0111000101



## ABOUT THE RESEARCH

*On behalf of Radware, Enterprise Management Associates, Inc. (EMA) conducted an online survey in July 2019 that collected 278 responses from executives and senior IT professionals at companies with at least $250 million USD/EUR/GBP in revenue and a worldwide scope.*

*About one-third of respondents held an executive-level position, approximately another one-third of respondents were in senior management and slightly more than one-third were managers. The remaining respondents were mostly individual contributors.*

*A variety of industries are represented in the survey, with the largest industry segments being technology products and financial services.*

*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.*