radware

THE STATE OF WEB APPLICATION SECURITY

Global organizations face constant evolving threats but feel optimistic about their ability to manage attacks despite contradictory evidence

RADWARE 2018 STATE OF APPLICATION SECURITY RESEARCH

Table of Contents

To compete more effectively, companies are examining how best to manage and secure applications and data. As the complexity of cloud and on-premises networks increases, new vulnerabilities are introduced that leave applications open to constant attacks.

What is the current threat landscape like for multinational organizations? How is exposure to application attacks affecting how companies secure their networks against data breaches?

To find out, 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 global perceptions on the state of application attacks and insights on how to best identify and mitigate threats in the future.

Executive Summary

Applications run the world.

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

To better understand the challenges that organizations face to protect web applications, Radware commissioned a second annual global survey of senior executives and IT professionals at companies with worldwide operations. The goal of the survey was to find out how security breaches have affected respondents' organizations in the past 12 months and the impact of application attacks on plans for cybersecurity protection measures. The results painted a picture of what is common to companies around the world, as well as in three regions: Asia-Pacific (APAC), the Americas (AMER) and Europe/Middle East/Africa (EMEA).

In general, organizations reported a contradictory combination of inputs between the frequency and severity of attacks and confidence in their abilities to manage the impact.

While most respondents said that hackers were able to access their networks, the vast majority of respondents said that they were certain their organizations could keep up with the growing rate of application-layer attacks, even though many did not secure APIs or felt that their WAFs were not stopping all attacks.

KEY FINDINGS:
THE SURVEY REVEALED INSIGHTS IN FOUR KEY CATEGORIES:

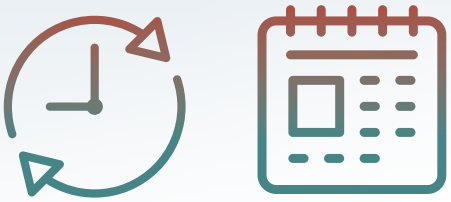
1. The State of Application Security
2. Protecting Sensitive Data
3. The Emergence of Bot Traffic
4. Securing Applications Across the Network Ecosystem

THE STATE OF APPLICATION SECURITY

Threats to application security are a growing problem, but respondents had conflicting thoughts about the seriousness of the threat landscape and their ability to manage it.

- More than 25% of organizations experienced attacks on a daily basis, with the majority experiencing attacks weekly.
- The most common types of application/web server attacks were encrypted web attacks and data security breaches.
- 70% of respondents reported attacks against their applications over IPv6, with one-third of the attacks targeting application programming interfaces (APIs).
- 80% of respondents from APAC believed that they were vulnerable to hackers compared to about 60% in both AMER and EMEA.
- 90% of respondents across all regions said that they were confident that their organizations could keep up with the growing rate of application-layer attacks.
- About half of the organizations surveyed indicated that some of their customers asked for compensation or their own reputations suffered because of application/web server attacks.
- Respondents said that data security breaches were the most difficult type of application attack to detect and mitigate.

Respondents estimated that it takes hours (43%) or days (42%) to discover data breaches.



HOURS DAYS

PROTECTING SENSITIVE DATA

As the number and severity of application attacks continue to grow, organizations are paying close attention to what information they collect, how many attacks they experience and how hackers access applications.

- 30% of companies collected and shared customer data about behavior, preferences and analytics.
- Over the past 12 months, respondents from APAC (55%) reported experiencing the most encrypted attacks, similar to EMEA (53%) and higher than AMER (41%).
- Across all regions, respondents estimated that it took hours (43%) or days (42%) for them to discover data breaches. Only a small number of organizations were alerted to data breaches by a third party.
- Anomaly detection tools were the most common method identified to discover data breaches.
- APIs were a major point of vulnerability. 62% of respondents did not encrypt data sent by API, 70% did not require authentication, and 33% allowed third parties to perform actions.
- The most common attacks targeting APIs were protocol attacks, access violations, brute force and denial of service that occurred on a weekly basis at 56% of the organizations.

THE EMERGENCE OF BOT TRAFFIC

Bot traffic, both good and bad, continues to grow as a percentage of overall internet traffic.

- Almost all (98%) felt that their organizations were capable of distinguishing between good and bad bots.
- The most common technique used to identify real users versus bots is CAPTCHA (which has already proven to be prone to bots that know how to bypass it), followed closely by dedicated anti-bot/anti-scraping solutions, IP rate-based detection and in-session detection and termination.
- Web scraping was viewed as a significant issue by most respondents who indicated experiencing these types of attacks on a regular basis, be it daily, weekly or monthly.

SECURING APPLICATIONS ACROSS THE NETWORK ECOSYSTEM

As more applications move to the cloud, organizations are addressing application security on their own networks and with cloud providers.

- Most respondents said that they incorporated web application firewalls (WAFs) in their application security strategies, but only one-third said that their WAF blocked all attacks.
- At the same time, nine out of 10 respondents were confident their security model was effective at mitigating most or all attacks.
- Organizations updated applications much more frequently than reported in previous reports, which introduced new security concerns. About one-third of all application types were updated on an hourly or daily basis, with about one-fourth updated weekly and another one-fourth updated monthly.
- 87% of respondents reported using a bug bounty program.
- In data centers, 60% said that they used DevOps automation tools to update applications.
- Respondents overwhelmingly (86%) placed their trust in cloud services providers' ability to provide high levels of application security. They were also confident (83%) in their own abilities to enforce security levels across multiple cloud platforms.

The State of Application Security

In application attacks, hackers exploit application vulnerabilities to cause service slowdowns and disruptions or gain access to digital assets. As network technologies evolve, the complexity of threats is keeping pace.

Hackers employ a number of tools to scan and map applications and look for vulnerabilities. The emergence of the internet of things (IoT) and artificial intelligence and the explosion of web, mobile and cloud-based apps create a treasure trove of entry points from which to launch attacks. Plus applications often undergo constant changes to support dynamic business requirements and may not go through rigorous security screening before being made publicly available.

How are organizations responding to the heightened need for application security defenses that safeguard their digital operations?

THE THREAT LANDSCAPE

Threats to application security are just part of doing business in a digital economy. That's the reality survey respondents indicated when asked how often their organizations' applications or web servers are attacked. Most said attacks happened weekly, and at least a quarter of the organizations reported attacks on a daily basis.

Encrypting data is no longer enough to stop hackers. In the last 12 months, respondents said that the most common types of application/web server attacks they experienced were encrypted web attacks and data security breaches. About half of respondents noted both of these attack types as most common (see Figure 1).

MOST COMMON APPLICATION ATTACKS IN THE LAST 12 MONTHS

FIGURE 1.

ORGANIZATIONS FACED A NUMBER OF ATTACK TYPES ON A REGULAR BASIS. THE MOST COMMON REPORTED THREATS WERE ENCRYPTED WEB ATTACKS AND DATA BREACHES.

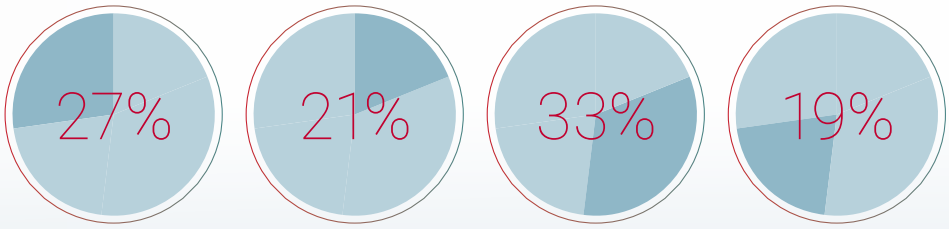
50%	Encrypted web attacks (SSL/TLS based)
46%	Data security breaches
39%	Web scraping
34%	HTTP/Layer 7 DDoS
34%	API manipulations
34%	SQL injections
32%	Cross-site scripting
24%	Credential stuffing/credential cracking
11%	None of these/no attacks experienced

IPv6 is an internet protocol that was developed in anticipation of the need to be able to generate unique IP addresses for the ever-growing number of network-connected devices. Seventy percent of respondents reported attacks against their applications over IPv6, while one-third of the attacks targeted application programming interfaces (APIs) (see Figure 2).

ATTACKS AGAINST APPLICATIONS OVER IPV6

FIGURE 2.

ACROSS ALL REGIONS, RESPONDENTS REPORTED THAT THEY HAVE SUFFERED APPLICATION ATTACKS OVER IPV6.



THE ISSUE WITH DENIAL OF SERVICE

According to Radware's *2017–2018 Global Application and Network Security Report*, denial-of-service (DoS) attacks shift from the network layer to the application layer, making them harder to detect and mitigate.[2] DoS attacks on applications render them inoperable. There are many techniques to exhaust the application resources. The most common ones are overwhelming application servers with session requests and buffer overflow, which involves writing more data to a fixed-length block of memory than can be accepted. Generally, their goal is to prevent legitimate users from accessing the applications. Respondents indicated that they experienced in the past 12 months a fairly equal distribution of the types of DoS attacks disrupting application services (see Figure 3).

MOST COMMON DENIAL-OF-SERVICE (DOS) ATTACKS IN THE LAST 12 MONTHS

38%	BUFFER OVERFLOW
37%	HTTP FLOOD
36%	HTTPS FLOOD
34%	LOW AND SLOW (SUCH AS LOIC, SLOWLORIS, TORSHAMMER)
34%	RESOURCE DEPLETION
15%	WE DIDN'T SUFFER ANY DENIAL-OF-SERVICE ATTACKS AGAINST OUR APPLICATIONS

FIGURE 3.
ORGANIZATIONS FACE A NUMBER OF DOS ATTACKS ON A REGULAR BASIS.

REGIONAL DIFFERENCES: **APAC SEES MORE APPLICATION-LAYER DDOS**

Denial-of-service (DoS) attacks on the application layer often target applications in ways that mimic legitimate user requests to exhaustion of the application resources or other limiting actions. The purpose of DoS attacks is to disrupt service. The survey revealed that buffer overflow and HTTP flood attacks were the most common types of DoS attacks, especially in APAC, versus AMER and EMEA.

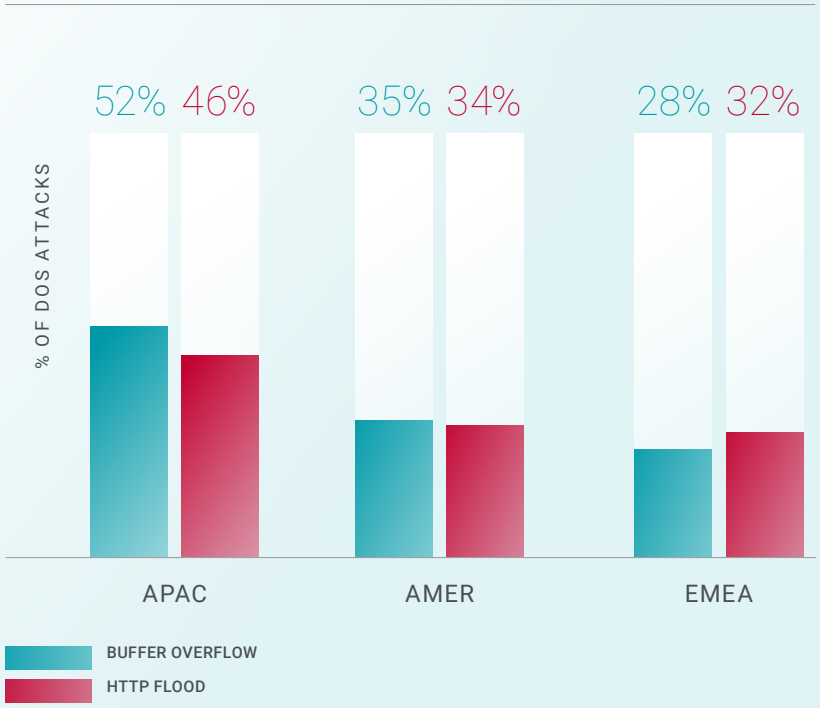


FIGURE 4.

2 *Radware's 2017–2018 Global Application and Network Security Report*

KEY FINDING:

CONFLICTING OUTLOOKS

When asked if hackers can penetrate the applications in their organizations' networks, two-thirds of respondents said yes. About 80% of respondents from APAC believed that they were vulnerable compared to about 60% in both AMER and EMEA (see Figure 5).

REGIONAL DIFFERENCES: **APAC SEES HIGHER RISK OF NETWORK PENETRATION**

PERCENTAGE WHO BELIEVE A HACKER CAN PENETRATE THEIR NETWORK

FIGURE 5.

80%

APAC RESPONDENTS

60%

AMER AND EMEA RESPONDENTS

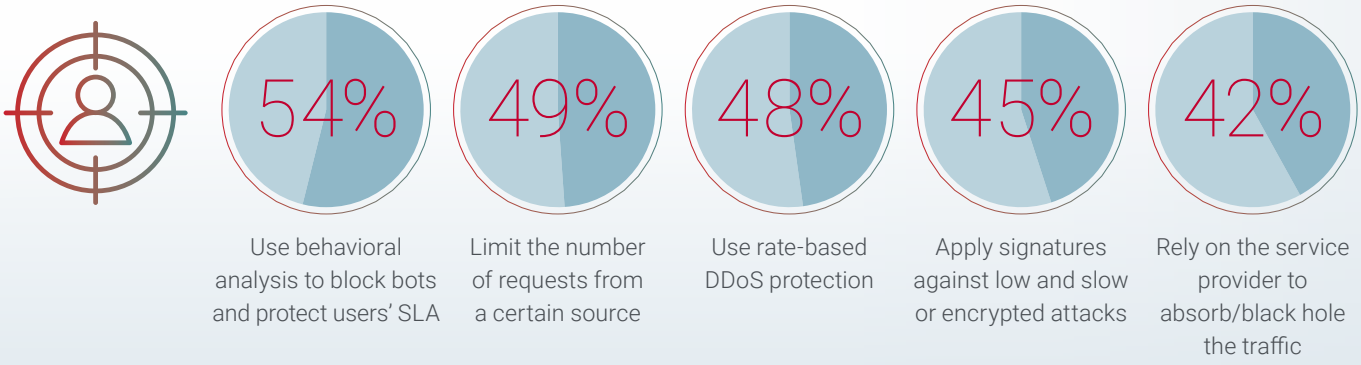
At the same time, 90% of all respondents across all regions said that they were confident that their organizations can keep up with the growing rate and complexity of application-layer attacks.

The conflicting outlook matches a key finding in Radware's *2018 C-Suite Perspectives* report that found that the majority of respondents across all regions (65%–81%) felt that their internal security resources were sufficient to handle their security needs. Yet 66% believed that hackers could penetrate their networks.[1]

1 Radware. *C-Suite Perspectives: Trends in the Cyberattack Landscape, Security Threats and Business Impacts; 2018 Executive Application & Network Security Report.*

STEPS ORGANIZATIONS TAKE TO PROTECT WEB APPLICATIONS

FIGURE 6.



WHY THE DISCREPANCY?

There are likely two main reasons to consider. First, it's difficult for organizations to keep up with the fast pace of evolving threats. New application exploit kits are released almost daily, and most organizations refresh security practices perhaps once a year and security solutions every three or four years. Consistent action is undertaken that can generate a false sense of security because critical solutions based on aged heuristics do not address the current threat landscape.

Second, cybersecurity issues can be a blind spot for senior management. Based on internal reviews, executives are led to believe that the issue is "taken care of" by the responsible department. They may not know what questions to ask to identify application security vulnerabilities. Attacks may even be happening that are not reported at the executive level.

For example, survey respondents felt that their organizations were taking proactive measures to protect web applications. Across all regions, organizations reported using behavioral analysis to block bots, limiting the number of requests from certain sources, and rate-based DDoS protection (see Figure 6).

Compared to a similar survey in 2017, respondents were also more confident that they were able to achieve 100% availability of application services. In this year's survey, on a scale of one to five, most scored their organization's ability at four (see Figure 7).

CONFIDENCE IN AN ORGANIZATION'S ABILITY TO ACHIEVE 100% APPLICATION SERVICES AVAILABILITY

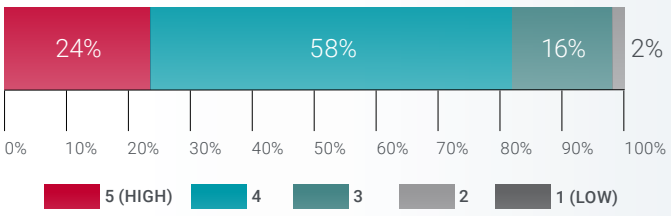
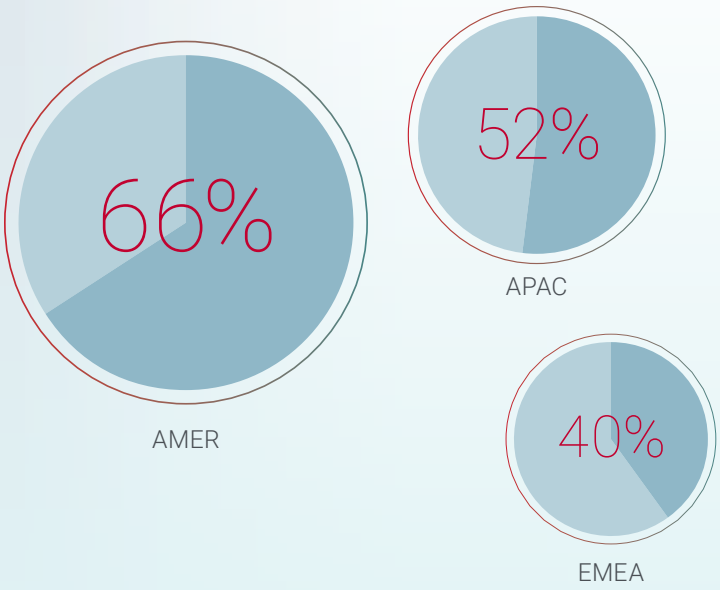


FIGURE 7.

WHEN ASKED TO RANK ON A FIVE-POINT SCALE, WITH FIVE BEING THE MOST CONFIDENT, THEIR ORGANIZATION'S ABILITY TO ACHIEVE NEARLY 100% AVAILABILITY FOR APPLICATION SERVICES, 82% OF RESPONDENTS SELECTED FOUR OR FIVE.

REGIONAL DIFFERENCES: **AMER FELT MOST CONFIDENT IN THEIR SECURITY MODEL** FIGURE 8.



Respondents from AMER felt the most confident that they were able to keep personally identifiable information (PII) about customers safe from breaches. It's likely that General Data Protection Regulation (GDPR) requirements in Europe impacted respondents' confidence levels in that region. Similar results for AMER and APAC may be revealed in future surveys after similar regulations are implemented.

Data security breaches

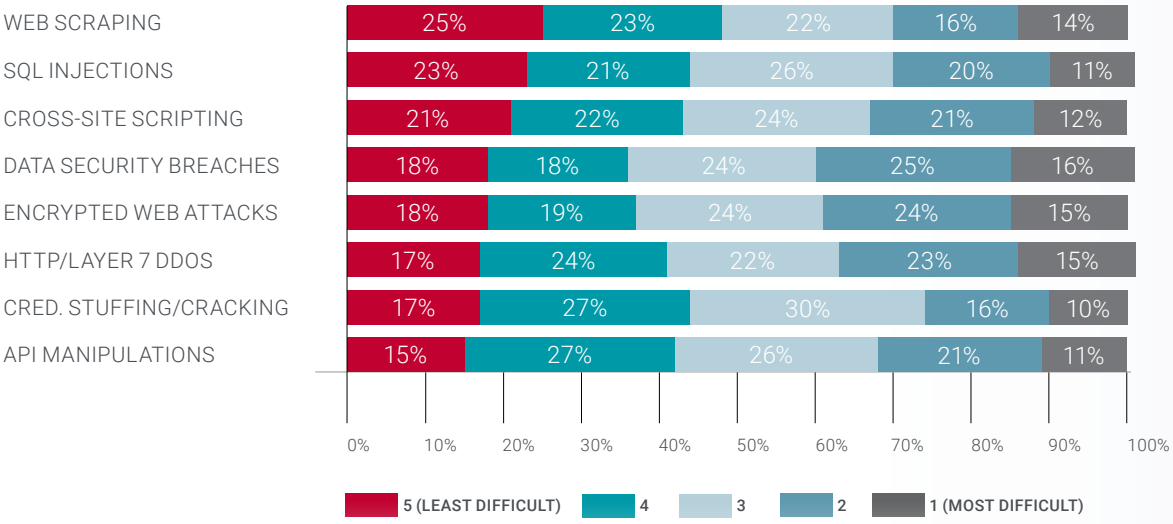
Respondents said that data security breaches were the most difficult type of application attack to detect and mitigate likely because more sophisticated attacks may happen for months (or years) before detection; multiple incidents may not be connected; and companies only discover compromised data after the fact.

Detection: When it comes to detecting attacks, 41% said that data security breaches were the most difficult to identify while web scraping (48%) and SQL injection (44%) were the least difficult. Respondents were almost equally split in their rating of the difficulty of detecting encrypted web attacks and HTTP/DDoS attacks, as about the same percentages rated them most or least difficult (see Figure 9).

Mitigation: Across all regions, respondents said that cross-site scripting (44%), SQL injections (40%) and credential stuffing/cracking (40%) were the least difficult to mitigate. Data security breaches (40%) were ranked the most difficult to mitigate (see Figure 10).

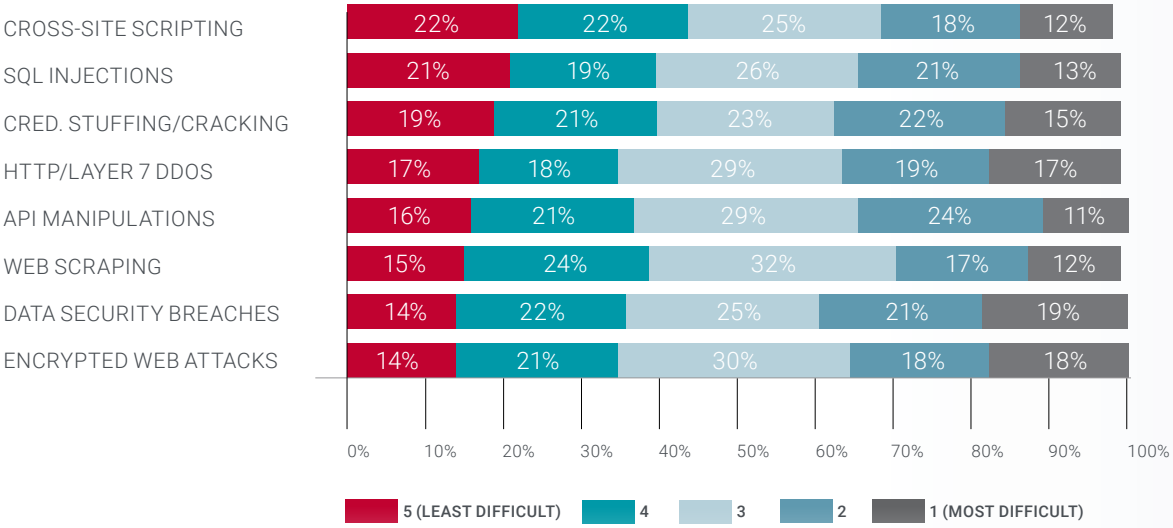
DIFFICULTY DETECTING ATTACKS

FIGURE 9.



DIFFICULTY MITIGATING ATTACKS

FIGURE 10.



IMPACT OF ATTACKS

When application attacks are successful, organizations can experience many negative consequences, including loss of reputation, customer requests for compensation, churn, stock price drops and executive job losses, among other impacts. Customers expect the organizations with which they associate to protect their data. When a data breach is revealed, trust between customers and the organization is broken. The process of repairing a company's reputation is long and not always successful.

About half of the organizations surveyed indicated that some of their customers asked for compensation or their own reputations suffered because of application/web server attacks.

Cultural differences may play a role in the consequences that each region faces after a security breach. In AMER, and more specifically the United States, the stock market is more sensitive compared to EMEA. In EMEA, the most likely impact is for customers to seek recompense through requests for compensation and legal action. In APAC, some customers are more likely to churn (see Figure 11).

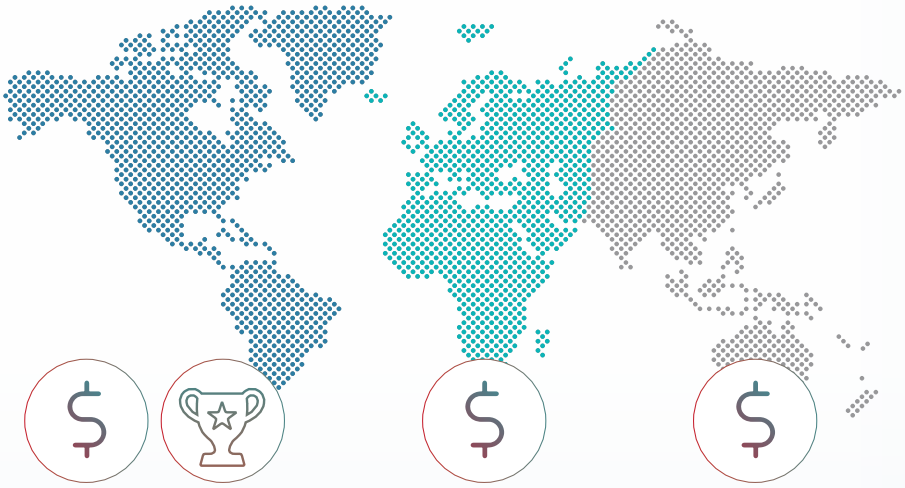
Organizations work very hard to capture and retain customers with targeted marketing programs, service-level agreements and privacy assurances. Security breaches can cause lasting damage to customer loyalty.

Senior executives can also pay the price for security breaches. Across all regions, 23% of respondents reported executive firings related to application attacks. This data matches recent news about several chief executive officers of major companies losing their positions about six months after a data breach.

APPLICATION ATTACK IMPACTS BY REGION

FIGURE 11.

Respondents from each region ranked the same top two major impacts of application attacks, with variance further down the list.



CUSTOMER REQUESTS FOR COMPENSATION AND LOSS OF REPUTATION IS A TIE

CUSTOMER REQUESTS FOR COMPENSATION

CUSTOMER REQUESTS FOR COMPENSATION

AMER

1. (Tie) Customer requests for compensation — 43%
1. (Tie) Loss of reputation — 43%
2. Stock price drop — 41%

EMEA

1. Customer requests for compensation — 54%
2. Loss of reputation — 44%
3. Legal action by customers — 34%

APAC

1. Customer requests for compensation — 59%
2. Loss of reputation — 53%
3. Churn — 49%

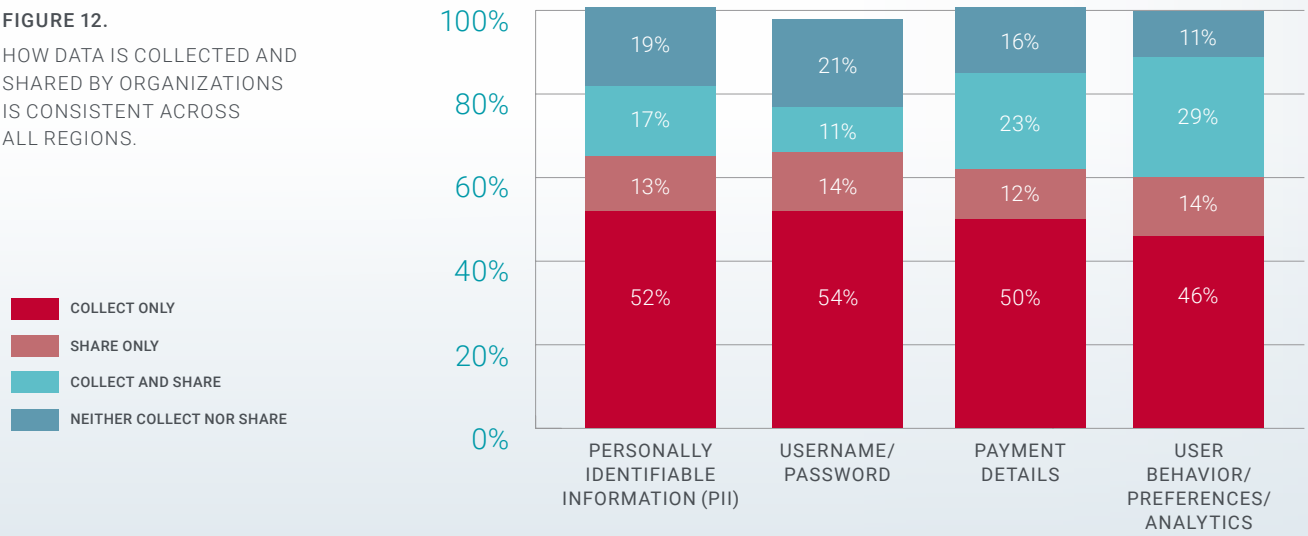
Protecting Sensitive Data

Major data breaches now occur on a monthly basis. Here are some extreme application attacks at major companies across a variety of industries:

- **Air Canada** — According to an email, which the airline sent customers, attackers breached the company's mobile app to gain access to sensitive data, including passport numbers.
- **McDonald's** — A leaky API exposed personal information of users in India who ordered food via the company's McDelivery mobile app.
- **Facebook** — Company CEO Mark Zuckerberg was in the hot seat after the social media company confirmed that political data firm Cambridge Analytica scraped details about 87 million users in an effort to influence the American election process.

DATA COLLECTION AND SHARING

FIGURE 12.
HOW DATA IS COLLECTED AND SHARED BY ORGANIZATIONS IS CONSISTENT ACROSS ALL REGIONS.



- **Under Armour** — The company owns MyFitnessPal, a popular app to track diet and exercise. A data breach was estimated to have compromised the personal information of about 150 million users, although payment data was stored in a separate system.
- **Panera Bread** — A security researcher discovered that the popular eatery had leaked customer records from its website in plaintext. The company didn't address the issue until an information security journalist exposed the details of the breach on his blog. The number of customers affected could be as high as 37 million.
- **Kmart and Sears** — The companies were victims of a data breach at an online support partner, which resulted in the exposure of payment information for hundreds of thousands of people. Bad news for the struggling companies.

Hackers don't care where an organization is located or what services it provides. They are happy to grab whatever sensitive data they can from wherever they spot an opening. All kinds of data, including personally identifiable information (PII), government identification numbers, medical records — the list is long — have value as a commodity for sale on the darknet.

No company wants its data compromised. The rollout of the GDPR in the European Union (EU) in May 2018 required organizations around the world that do business in this region to meet stricter data privacy laws. Any company that offers goods or services, monitors personal behavior or handles the personal data of EU residents is impacted by the law. Failure to comply can result in hefty fines.

DATA COLLECTION AND SHARING PRACTICES

Multinational organizations keep close tabs on what kinds of data they collect and share. About half of survey respondents said that they only collected various types of customer data for internal use, but did not share it. Forty-three percent of respondents shared data about user behavior, preferences and analytics (see Figure 13). When extrapolated across the number of websites that most people interact with every day, the possible exposure of sensitive data is massive.

DISCOVERING DATA BREACHES

When considering attack experiences in the past 12 months, most respondents estimated that it took hours or days to discover a breach (see Figure 13).

Of the respondents who reported experiencing a data breach in the past 12 months, anomaly detection tools were the most common method of discovery (69%). About half of all respondents said that an information leak to the public or a darknet monitoring service led to discovering one or more security issues (see Figure 14).

Discovery of a data breach via a ransom demand was more common in AMER than in APAC where information leaks and detection tools rank higher.

TIME TO DISCOVER DATA BREACHES

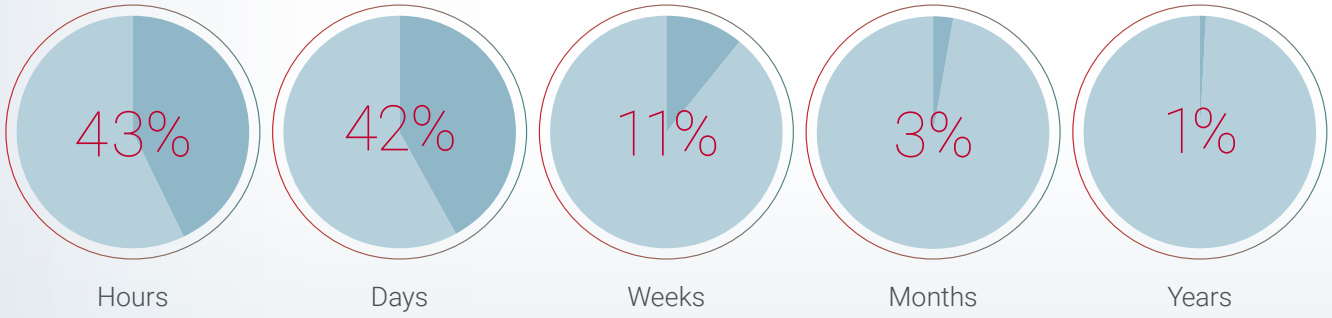


FIGURE 13.

A SIMILAR PERCENTAGE OF RESPONDENTS REPORTED DISCOVERING SECURITY BREACHES WITHIN HOURS OR DAYS.

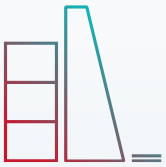
DISCOVERING DATA BREACHES

69%

ANOMALY DETECTION TOOLS/SIEM

51%

DARKNET MONITORING SERVICE



45%

INFORMATION WAS LEAKED PUBLICLY (NET)

Information leaked publicly ONLY: 5%
Leak and another method: 40%

27%

RANSOM DEMAND (NET)

Ransom demand ONLY: 3%
Ransom demand and some other way: 24%

FIGURE 14.

MOST DATA BREACHES ARE DISCOVERED THROUGH THE USE OF ANOMALY DETECTION TOOLS.

REGIONAL DIFFERENCES: **AMER HAD LOWEST NUMBER OF DATA BREACHES**

Respondents from AMER reported the lowest average number of breaches in the past 12 months. APAC experienced the most attacks.

AVERAGE NUMBER OF ATTACKS IN PAST 12 MONTHS

AMER 4.65

EMEA 8.65

APAC 36.24

FIGURE 15.

Data Breach Discovery by Vertical Industry

FIGURE 16.

Anomaly detection tools are the main way that organizations across all represented verticals discover data breaches. It's significant that a sizable portion of data breaches are discovered via reactive notifications from darknet monitoring (57%) and ransom demands (40%).

	TOTAL (N=242)	TECHNOLOGY (N=47)	MANUFACTURING (N=41)	FIN. SVCS./INS. (N=35)	RETAIL (N=32)
ANOMALY DETECTION TOOLS/SIEM	69%	66%	66%	74%	72%
DARKNET MONITORING SERVICE	51%	68%	34%	57%	56%
INFORMATION WAS LEAKED PUBLICLY (NET)	45%	47%	51%	51%	44%
Information leaked publicly ONLY	5%	6%	12%	3%	0%
Leak and another method	40%	40%	39%	48%	44%
RANSOM DEMAND (NET)	27%	30%	12%	40%	22%
Ransom demand	3%	2%	0%	3%	3%
Ransom demand and another source	24%	28%	12%	37%	19%

KEY FINDINGS:

APIs — AN INVITATION TO ATTACK

62% of respondents did not encrypt data sent via API

70% of respondents did not require authentication

33% allowed third parties to perform actions

THE ISSUE WITH APIs

Application programming interfaces (APIs) simplify the architecture and delivery of application services and make possible the digital interactions that users have with applications. But they also introduce a wide range of risks and vulnerabilities as a backdoor for hackers to break into networks. Through APIs, data is exchanged in HTTP where both parties receive, process and share information. A third party is theoretically able to insert, modify, delete and retrieve content from applications via API gateways.

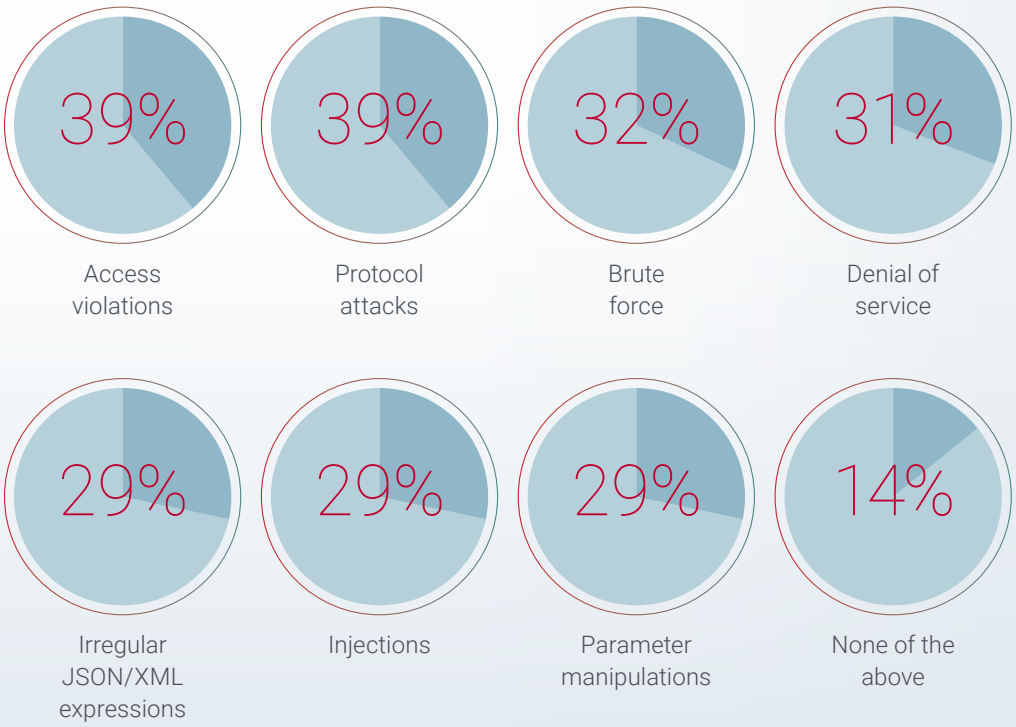
API gateways are used by 60% of respondents for security purposes, as well as orchestration and load balancing.

Half of survey respondents said that they both shared and consumed data with APIs. Forty percent said that their organizations use encryption when exposing data to third-party APIs, while one-third allowed third-party APIs to perform actions.

7 COMMON ATTACKS AGAINST APIs

FIGURE 17.

ACCESS VIOLATIONS AND PROTOCOL ATTACKS LED THE LIST AMONG ORGANIZATIONS THAT HAVE EXPERIENCED API ATTACKS IN THE PAST 12 MONTHS.



Of the respondents who used API gateways, the most common types of attacks against APIs in the last 12 months were access violations and protocol attacks, with both types experienced by about 40% of organizations (see Figure 17).

On a weekly basis, access violations (58%) were the most common attack type reported by organizations that experienced attacks against APIs in the past 12 months, followed by denial of service (57%) and irregular JSON/XML expressions (56%). Other attacks reported include protocol attacks, brute force, parameter manipulations and injections.

REGIONAL DIFFERENCES: **APAC HIGHER RATIO OF API ATTACKS**

Organizations in APAC (42%) were more likely to experience denial-of-service API attacks than companies in AMER and EMEA (both 25%).

FIGURE 18.

Bots: Friend and Foe

Internet robots — more commonly referred to as bots — were created to automate repetitive tasks and facilitate interactions between clients and servers across the web. A few examples include search engines, chatbots and pricing scrapers that are heavily used in e-commerce.

Hackers also use bots for malicious purposes. Bad bot traffic is used for attacks on networks, servers, smartphones and connected devices to cause damage, steal data, exploit intellectual property and purge inventory in online shops and ticketing systems.

BOT TRAFFIC IN THE NETWORK

The amount of both good and bad bot traffic is growing. In response, organizations are forced to increase network capacity. It's important for organizations to be able to accurately identify legitimate, human-generated traffic and distinguish between good and bad bots, but it's not easy.

Malicious bots attempt to fool applications and servers into thinking they are real users. The designs that bot developers use to bypass standard detection tools are growing increasingly sophisticated. Hackers try to reverse-engineer their way around security measures by spoofing the system into thinking that the bot is a real user by mimicking key strokes, mouse movements and other humanlike behaviors.

DETERMINING REAL USERS VS. BOTS

The most common technique used by respondents to distinguish between real users and bots on their networks is CAPTCHA, which stands for Completely Automated Public Turing Test to Tell Computers and Humans Apart. The challenge-response test requires users to enter a randomly generated sequence of letters and numbers in a text box. Sixty-two percent use CAPTCHA followed closely by dedicated anti-bot/anti-scraping solutions and IP rate-based detection (both 57%), and in-session detection and termination (49%). There are bots that have proven to be up to 90% effective at bypassing CAPTCHAs by mimicking human behavior as well as other challenges that businesses typically use. In addition, dynamic IP attacks render the good ol' IP-based protection school ineffective.

KEY FINDING:

Surprisingly, almost all (98%) said that their organizations were capable of distinguishing between good and bad bots (see Figure 19). Respondents in AMER and APAC were most likely to say that they can make the distinction with certainty, while more in EMEA were able to distinguish by approximation. Across all regions, 30% of distinguishable bot traffic was bad.

ABILITY TO DISTINGUISH BETWEEN GOOD AND BAD BOTS

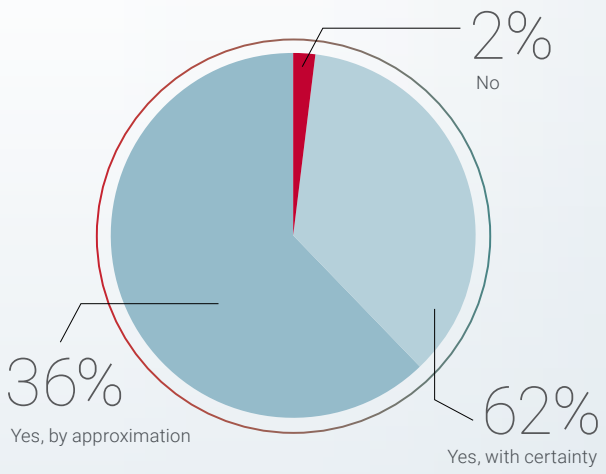


FIGURE 19.

THE VAST MAJORITY OF ORGANIZATIONS REPORTED THE CAPABILITY TO DISTINGUISH BETWEEN GOOD AND BAD BOT TRAFFIC ON THEIR NETWORKS.

REGIONAL DIFFERENCES: **AMER EXPERIENCES MORE WEB SCRAPING**

Organizations in AMER (50%) were more likely to view the risk of web scraping as very significant versus companies in APAC (35%) and EMEA (29%). But the gathering of price information and website copying was reported as more prevalent in APAC than in the other regions.

FIGURE 20.

THE ISSUE WITH WEB SCRAPING

Web scraping is an example of an attack technique that uses a bot to extract data from websites for analysis. Web-scraping attacks are most commonly used to maliciously gather pricing information, copy websites and steal intellectual property.

Almost two in five respondents indicated that the risk of web scraping was very significant, and half rated it as significant (see Figure 21).

RISK OF WEB-SCRAPING ATTACKS

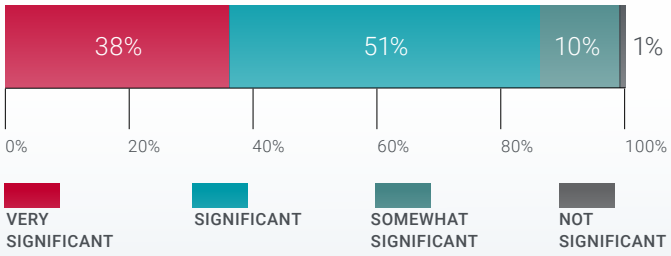


FIGURE 21.

THE VAST MAJORITY OF RESPONDENTS SAID THAT WEB SCRAPING POSED A RISK TO THE SECURITY OF THEIR ORGANIZATIONS' INTELLECTUAL PROPERTY.

Across all regions, almost two in five respondents indicated that their organizations experienced weekly web-scraping attacks, while half said that the attacks were monthly or yearly (see Figure 22).

BUSINESS IMPLICATIONS ARE SIGNIFICANT

In an effort to weed out bad traffic, organizations run the risk of classifying good traffic as bad. "False positives," when real users are identified as bots, can result in bad user experiences and poor customer service. Security measures that are too aggressive frustrate real customers, causing a negative financial impact. But security measures that are too lax open up applications to data breaches. Organizations must find the right balance.

FREQUENCY OF WEB-SCRAPING ATTACKS

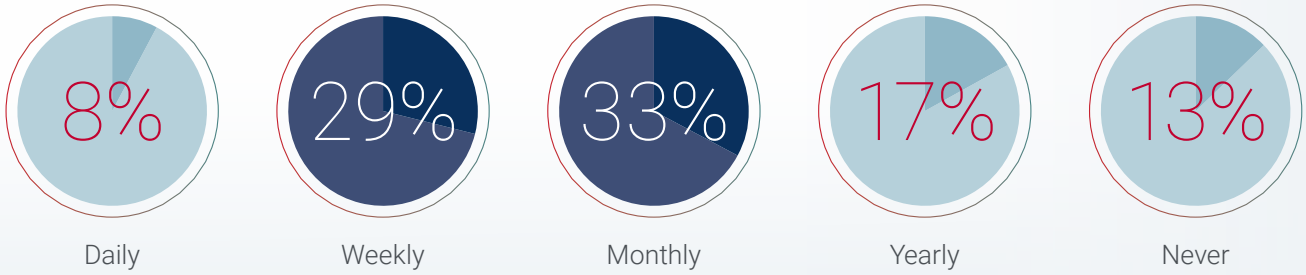


FIGURE 22.

EIGHTY-SEVEN PERCENT OF RESPONDENTS REPORTED THAT WEB-SCRAPING ATTACKS IMPACTED THEIR ORGANIZATIONS AT SOME POINT DURING THE PAST 12 MONTHS.

One method is to track the bot activity over time with a violation scoring system. The process helps minimize false positives and maximize user experiences.

For example, bot attacks often generate huge amounts of traffic in an effort to disrupt application service performance or bring down servers. It's a known anomaly for which organizations employ detection tools, but history shows that bots are often successful in DoS attacks, or organizations are forced to deploy additional capacity to manage the traffic bursts.

On some occasions, the spike in network traffic is genuine. The flash-crowd visits could be the result of marketing campaigns, such as Amazon's Prime Day when shoppers flood that site and other retailers' sites looking for deals.

The vast majority of survey respondents (84%) across all regions said that they can tell the difference between flash-crowd visits and bot attacks. Surprisingly, respondents from retail, where the impact of marketing activities on site visits and sales was closely monitored, were the least likely to be able to make the distinction versus other verticals (see Figure 23).

FIGURE 23.

CONFIDENCE IN ABILITY TO DISTINGUISH BETWEEN FLASH-CROWD VISITS AND BOT ATTACKS BY VERTICAL

58% RETAIL

83% MANUFACTURING

90% TECHNOLOGY

93% FINANCIAL SERVICES

Securing Applications Across the Network Ecosystem

Applications are like living, breathing organisms. They are in a constant state of development. In the rush to bring new customer experiences to market or address business needs, organizations may skip critical security checks, leaving them open to vulnerabilities that could have been mitigated.

As the network ecosystem grows more complex with applications running in the cloud and businesses offering and consuming software as a service (SaaS) and relying on third-party data centers to secure data, how can organizations ensure that their applications are protected on their own networks and across multiple clouds?

APPLICATION PROTECTION STRATEGIES

Survey respondents indicated that web application firewalls (WAFs) were incorporated into their application security strategies. Almost half of all organizations, particularly those in the AMER region (57%), employed a positive WAF model, which defined on a whitelist what traffic was allowed, and rejected all other traffic. One-third of respondents said that they used both positive and negative (a blacklist of traffic that is not allowed) models.

KEY FINDING:

Contradictions Abound

9 out of 10

respondents said that their security model was effective at mitigating most or all attacks, but only one in three respondents said that their WAF mitigated all attacks.

Bug bounty programs are also an indication that organizations acknowledge their limitations in identifying all flaws and vulnerabilities themselves. They are a proven way to tap the power of crowdsourcing to reward individuals who discover and report bugs after applications have been released or updated. Across all regions, 87% of respondents reported using a bug bounty program to find vulnerabilities in their application services.

POSITIVE AND NEGATIVE SECURITY MODELS

POSITIVE:

- Learns legitimate traffic behavior
- Detects anomalies and blocks unauthorized access
- Protects against zero-day attacks and unknown exploits

NEGATIVE:

- Blocks known attacks via known signatures and rules
- Cannot protect against unknown vulnerabilities such as zero-day attacks
- Cannot provide full OWASP Top 10 protection

FIGURE 24.

FREQUENCY OF APPLICATION CHANGES

FIGURE 25.

ACROSS ALL APPLICATION TYPES, AT LEAST 30% OF APPLICATIONS WERE UPDATED ON AN HOURLY OR WEEKLY CYCLE.

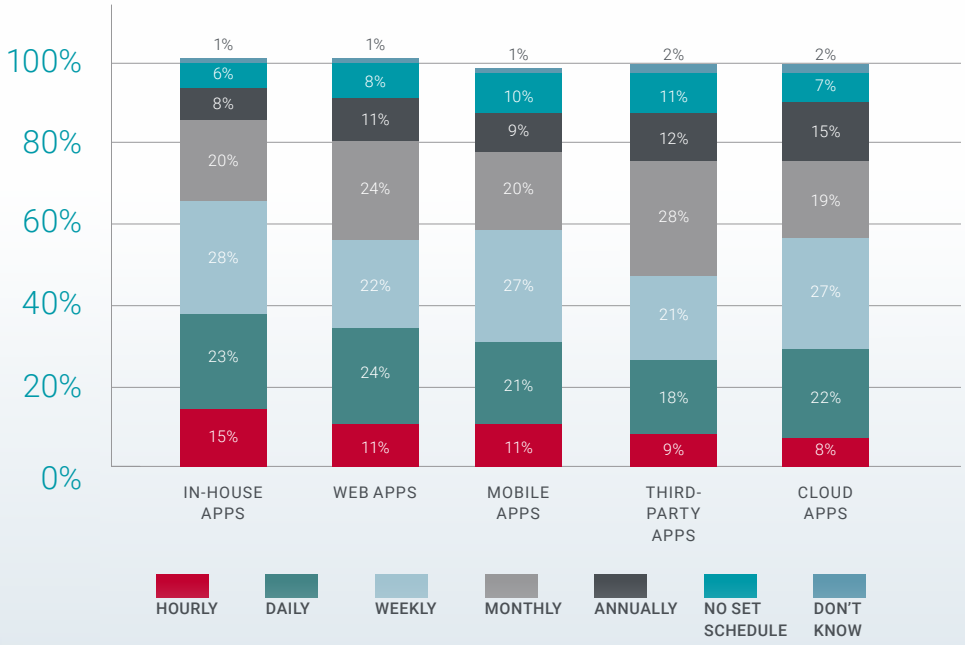


FIGURE 26.

TECHNOLOGIES USED IN DATA CENTERS

63% DEVOPS AUTOMATION TOOLS

48% CONTAINERS AND DELIVERY (3 IN 5 USE ORCHESTRATION)

44% SERVERLESS/ FAAS

37% MICROSERVICES

THE DYNAMIC APPLICATION ENVIRONMENT

Organizations manage a wide variety of application types. The frequency with which the applications change varies depending on their functionality (see Figure 25). At least 30% of all applications, regardless of type, are u pdated on an hourly or daily basis, indicating the need for a constant refresh of protective security measures.

More than 60% of respondents indicated that they used DevOps automation tools to update applications. Containers and delivery, serverless/function as a service (FaaS) and microservices are also becoming popular strategies to the point where more than one in three organizations has already adopted them (see Figure 26). Among those using containers and delivery, three in five said that they use orchestration.

Among the 37% of respondents that used microservices, one-half rated data protection as the biggest challenge, followed by availability assurance, policy enforcement, authentication and visibility.

CLOUD PROVIDER TRUST FACTOR

Organizations appear eager to have cloud services providers take responsibility for securing their applications, likely because it's a convenience to add it to the bundle of services that they are already purchasing. Across all regions, respondents had a very high level of trust in their cloud providers' level of security (see Figure 27). They were also very confident that they were able to enforce the same level of security across multiple cloud platforms (see Figure 28).

Cloud providers can see this as an opportunity to monetize security services by adding multiple security options at different price points to their service options.

Organizations should be somewhat wary of outsourcing all security measures to cloud providers with the assumption that ideal security levels will be maintained on every platform. While it may seem like a way to simplify management of application security, giving up too much control to partners can backfire. The example cited earlier about Kmart and Sears both falling victim to a data breach at the same online support partner is a cautionary tale of the potential impact of signing away too much responsibility.

Additionally, cloud services providers' offerings are broad. They cannot be expected to maintain the specialized application security knowledge available from native information security vendors.

REGIONAL DIFFERENCES:
APAC MICROSERVICES

Microservices were more common in APAC (48%) than in AMER (34%) or in EMEA (30%).

FIGURE 29.

TRUST IN CLOUD PROVIDER'S LEVEL OF SECURITY

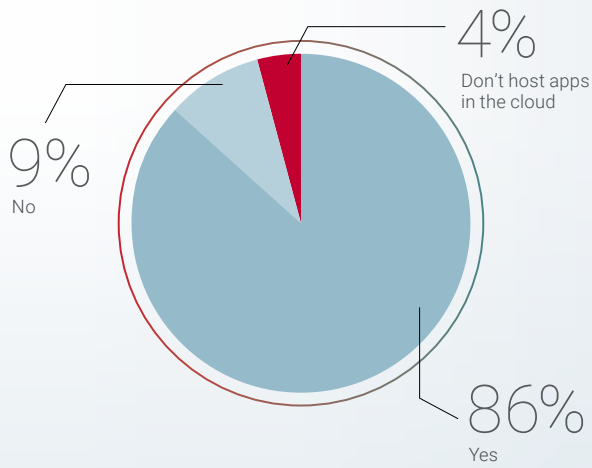


FIGURE 27.

RESPONDENTS WERE VERY SURE THAT THEIR APPLICATIONS WERE SECURE WHEN HOSTED BY A CLOUD PROVIDER.

ABILITY TO ENFORCE SECURITY LEVELS ACROSS MULTIPLE CLOUD PLATFORMS

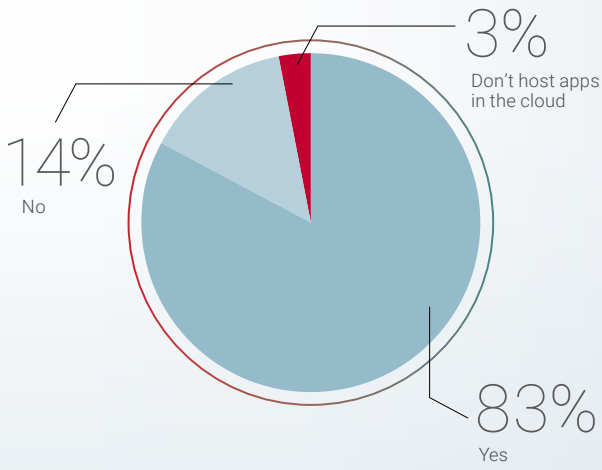


FIGURE 28.

RESPONDENTS WERE VERY CONFIDENT IN THEIR ABILITIES TO ENFORCE CONSISTENT SECURITY LEVELS ACROSS MULTIPLE CLOUD PLATFORMS.

Summary and Recommendations

Why do organizations have a false sense of confidence about their ability to detect and mitigate attacks and protect application services?

Survey results indicated that respondents understood that attacks were constant and evolving and their security protocols were not foolproof. At the same time, they overwhelmingly conveyed confidence in their ability to manage the growing rate of application-layer attacks.

False sense of security: Application threats evolve at a mind-blowing pace. Organizations that have application security tools and processes in place may be under the impression they are in control but are likely not keeping up with the daily barrage. Other organizations may not even know that their application services are under attack. It's just a matter of time before a significant data breach happens.

Executive blinders: Senior management — correctly — looks to their internal teams tasked with application security to manage the issue. "No news equals good news" may be clouding their perceptions of the effectiveness of their organizations' application security strategies, especially when applications are hosted by cloud services providers.

What should organizations do to secure their critical applications?

RECOMMENDATIONS FROM RADWARE:

1. USE IT OR LOSE IT

Encryption is an accepted, proven method to secure data traveling on private and public networks. Yet this study reveals that half of the organizations suffered attacks disguised in encrypted traffic. As the information ecosystem grows, less than half of respondents use encryption when exposing data to third-party APIs.

For encryption to be effective, it must be implemented hand in hand with security controls. Audit which APIs are active in your organization and make sure encryption is used.

Seventy percent also identified attacks against applications over IPv6, which in fact features capabilities like end-to-end encryption and Secure Neighbor Discovery (SEND).

Make sure that data is secure at rest and in transit. Don't rely blindly on encryption or third-party APIs or services, even from cloud providers.

2. LEARN AND PROTECT

DevOps and agile development practices are great at creating new applications quickly and efficiently. More than 60% of respondents said that they used DevOps automation tools to update applications. Unfortunately, the fluidity of these environments also creates a bevy of unintended security risks. Ensure that your WAF solution can automatically detect and protect applications and APIs as they are added to the network by automatically creating new policies and procedures.

3. MINIMIZE FALSE POSITIVES

False positives translate to blocked users, which can result in lower conversion rates and hits to a company's reputation. Unfortunately, automated services and applications adhere to some common behaviors and make it difficult for organizations to tell a malicious user from a legitimate one. That puts companies on the offensive to scour all their traffic looking for imposters. In addition, the frequency of changes to applications makes it difficult for security solutions to keep up, resulting in frustrated customers who are trying to access their data or services. It's important to keep false positives to a minimum to provide seamless customer experiences.

4. COVER THAT TOP 10 LIST

Industry pundits and experts at security consortiums and communities continue to categorize and identify the greatest web application security risks facing organizations. A WAF solution should provide complete coverage, including all OWASP Top 10 vulnerabilities.

5. GRAB THE BOT BY ITS SOURCE

Bots, crawlers and spammers, using new techniques to disguise malicious traffic, can exhaust resources and scrape sensitive information from websites or cloud-based assets. A good WAF needs to sniff out these clandestine cyber assaulters. Device fingerprinting identifies, blacklists and blocks the source machines that are used for attacks regardless of the IP they hide behind. This fingerprint — a unique identification of the source — enables you to track its activity over time and make educated decisions regarding whether it is a good or bad bot.

6. NEGATIVE + POSITIVE = ZERO-DAY PROTECTION

There are many known application attack vectors and exploit kits out there, which every solution should block. Zero-day assaults swiftly exploit newly discovered vulnerabilities. Negative and positive security models that automatically detect application domains, analyze potential vulnerabilities and assign optimal protection policies are critical.

7. PROTECTION VIA UNIFICATION

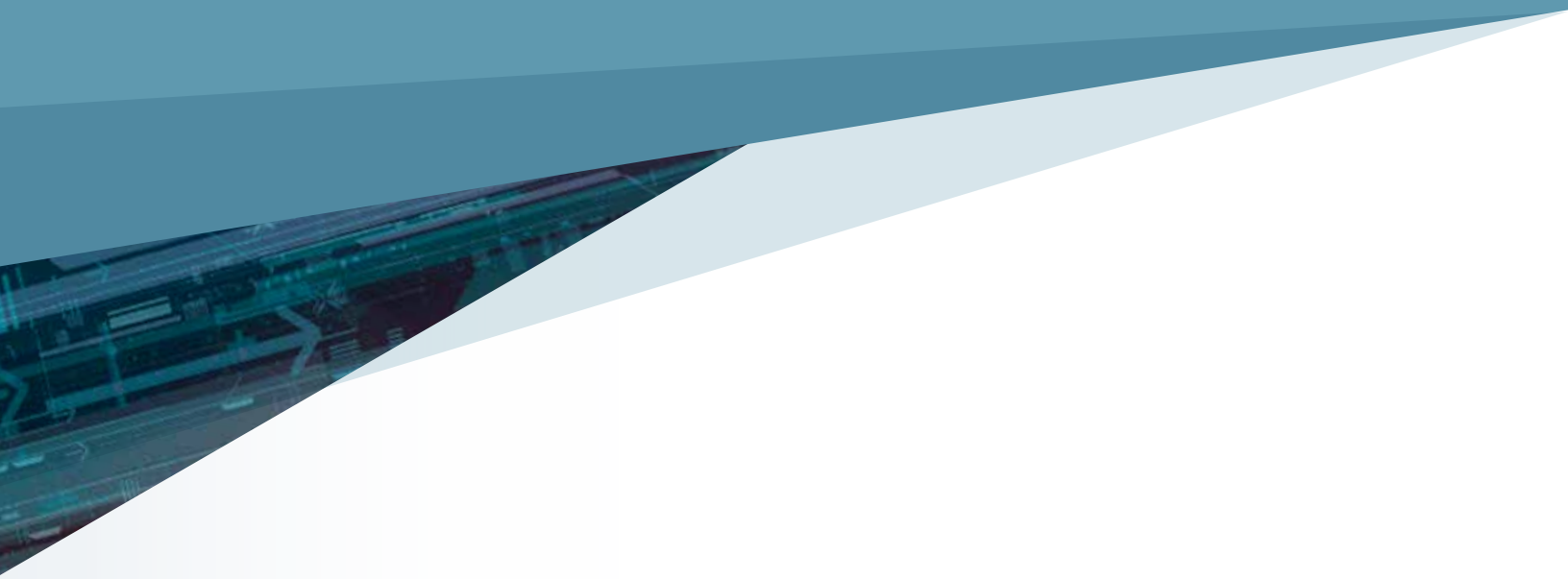
Companies face a wide range of security challenges, such as OWASP vulnerabilities, bot management, securing APIs and protecting against DoS. A synchronized attack-mitigation system that provides secure application protection against all the above threats, across all platforms and at all times is the way to go. It provides comprehensive security and a single view of application security events for quick incident response and a minimum impact on the business.

ABOUT THE RESEARCH

On behalf of Radware, Merrill Research conducted an online survey in April 2018 that collected 301 responses from executives and senior IT professionals at companies with at least 250 million USD/EUR/GBP in revenue and a worldwide scope. Responses are analyzed in total and by three regions: Asia-Pacific (APAC), the Americas (AMER) and Europe/Middle East/Africa (EMEA).

About one-third of the participants reported directly to the chief executive officer/executive committee, one-fourth reported to the chief information officer, and one-fifth reported to the chief information security officer.

A wide variety of industries are represented in the survey, with the largest industry segments being technology products and manufacturing/production/distribution.



radware

www.radware.com

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.