radware

PROTECTING WHAT YOU CAN'T SEE

Eliminating Security Blind Spots in an Age of Technological Change

Table of Contents

Executive Summary

The need for speed is at the heart of decisions that organizations need to make about how to implement digital transformation strategies. By fostering faster time to market for revenue-generating services and applications, companies know that they can gain competitive advantages. But at what cost to network and application security?

For many corporations, the security risks of moving forward quickly with new information technologies are worth the rewards of improved customer experiences. Security is not an afterthought, but it also shouldn't stand in the way of progress.

The professionals charged with protecting their organizations' digital assets felt the pressure to keep up with the speed of business. They also discovered that moving fast introduces challenges and uncertainties about where attacks/vulnerabilities are hiding in networks and applications. Limited visibility across their entire network ecosystems proved to be an issue. How do you protect what you can't see?

To provide insight into the complex challenges faced by organizations as they seek to balance business agility and security requirements, Radware produces an annual *Global Application & Network Security Report*. This ninth annual version of the report combines Radware's organic research, real attack data and analyses of developing trends and technologies with the findings from a global industry survey.

In 2019, the quickest path to productivity was via migration to the public cloud. In fact, more than 75% of organizations have done so. In addition, companies continue to adopt new technologies that allow them to improve upon continuous development and deployment, such as the rapid adoption of microservices. Enterprises and service providers also kept an eye on how emerging 5G network technologies and internet of things (IoT) devices might fit into their operational strategies.

These environments greatly expand the attack surface and introduce new vulnerabilities to exploit. Security teams were hampered by a lack of visibility into attack vectors in siloed public cloud environments and microservice architectures. Hackers, including those affiliated with governments, were only too happy to respond with new tactics that take advantage of blind spots.

KEY FINDINGS

- Only 6% claimed not to have experienced an attack.
- Nation-state attacks were an issue as respondents indicated a substantial increase in the percentage of cyberattacks attributed to cyberwar, up from 19% in 2018 to 27% in 2019.
- Only 10% of respondents felt that their data is more secure in a public cloud environment. But 30% felt that the benefits of the cloud, such as agility and lower costs, outweigh the security risks.
- Web and application intrusions (27%) were seen as the biggest threat to their companies' cloud environments, similar to the percentage in previous years' surveys.
- Companies with revenues of more than 1 billion USD/EUR/GBP reported an average cost of 1.7 million USD/EUR/GBP per cyberattack. Companies with revenues lower than 1 billion USD/EUR/GBP estimated the cost of a cyberattack at 480,000 USD/EUR/GBP.

ADDITIONAL FINDINGS

- Visibility was identified as a growing issue by 46% of respondents who said that they don't know if they have experienced SSL- or TLS-based attacks on encrypted traffic. Three of five indicated that more than half of their traffic is encrypted — with the average at 62%.
- About one-third of respondents experienced a distributed denial-of-service (DDoS) attack in the past year. Of those who were attacked, 91% experienced application-layer attacks, primarily domain name system (DNS) or HTTP/HTTPS Flood attacks.
- Almost three-quarters of respondents used a public cloud environment, while two of five used multiple public cloud environments. Large and worldwide companies were most likely to use three or more public cloud environments.
- The majority of respondents indicated that they are not prepared to safeguard 5G network rollouts in their countries. Companies in Asia-Pacific (APAC) and Europe/Middle East/Africa (EMEA) were more likely to say that they are at least somewhat prepared compared to organizations in Latin America. Service provider/telecom companies were more likely than any other vertical to say that they are prepared to handle 5G rollouts (58% vs. 16%–34%), although 13% said that they won't address 5G before 2022.
- The biggest concern that respondents identified if their organizations were faced with cyberattacks is data leakage/information loss (30%), consistent with rankings from the three previous years' surveys.
- Seven of 10 organizations that suffered a cyberattack in the past year had a malware/bot attack, two-thirds had an attack related to phishing or fraud, and half experienced DDoS or web application attacks.

The Visibility Issue

Survey respondents acknowledged the complexity of keeping up with quickly changing network environments. Lack of visibility into what is happening in their networks means that many just don't recognize the full impact of the attacks or why they are targeted.

22%	don't even know if they were attacked
27%	of those who were attacked don't know the hackers' motivations
38%	aren't sure whether an IoT botnet hit their networks
46%	aren't sure if they suffered an SSL-based DDoS attack
13%	don't know how a cyberattack impacted their business
30%	do not monitor east-west traffic[1]

[1] *2019 State of Web Application Security Report*

Methodology & Sources

The *2019–2020 Global Application & Network Security Report* combines statistical research and frontline experience to identify cybersecurity trends that are important to organizations as they determine long-term growth strategies.

Global Industry Survey

The quantitative data source is a cross-industry survey conducted by Radware. This year's survey included 561 individual respondents who represented a wide variety of organizations around the world. The study was built on prior years' research collecting vendor-neutral information about issues that organizations faced in preparation and combat of cyberattacks.

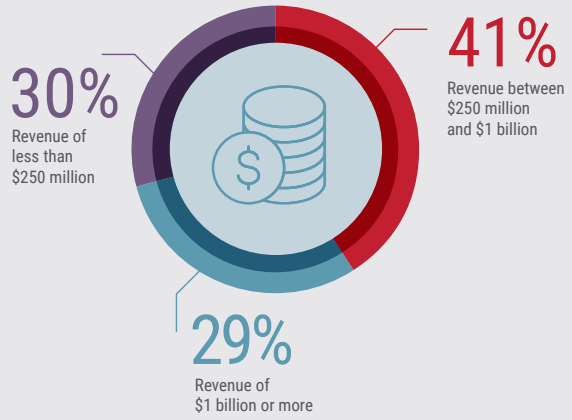


Figure 1. Respondent breakdown by revenue.

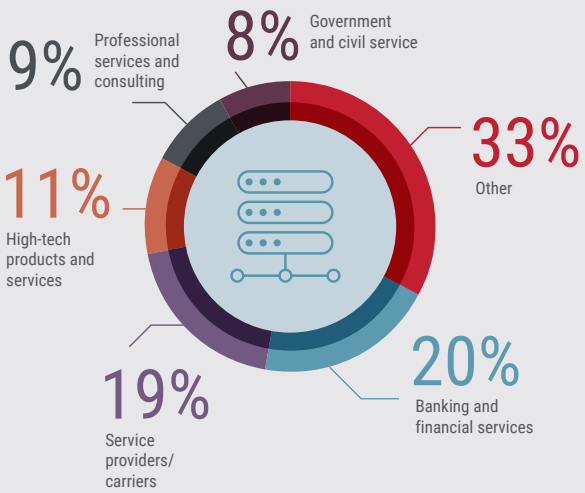


Figure 2. Respondent breakdown by industry.

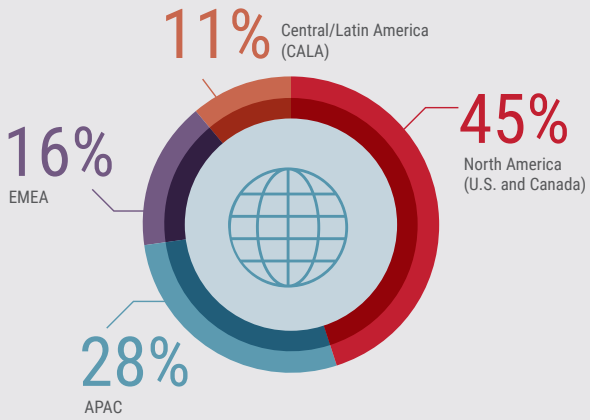


Figure 3. Respondent breakdown by geography.

Radware's Emergency Response Team (ERT)

The team is composed of dedicated security consultants providing 24x7 security services. In the event of cyberattacks, ERT members serve as the first line of defense. They have successfully dealt with some of the industry's most notable episodes of cyber and other attacks. This report shares their insight from frontline experiences, providing deeper forensic analysis than surveys or academic research alone.

Radware's Global Deception Network

The Deception Network is a global network of honeypots and detection agents that trap network and application attack campaigns as they emerge. Every hour, the agents communicate with thousands of IPs performing suspicious or malicious activities such as DDoS and web application attacks, scanners, IoT botnets and more. Radware's advanced algorithms learn threat patterns and intentions, qualify them and feed them in real time to Radware's security solutions for preemptive protection.

The 2019 Threat Landscape

In 2019, the threat landscape showed signs of where cyberattackers will focus their efforts going forward. Hackers figured out how to take advantage of blind spots in public clouds and private networks to launch headline-grabbing cyberattacks. Notable incidents reveal that data is vulnerable in the gaps between enterprises and public cloud providers. Other attacks reveal the limitations of humans who can unknowingly fall prey to traps and trigger widespread damage.

Radware's 2019 Global Industry Survey

Radware's global industry survey revealed what businesses were up against as they fought to take advantage of digital transformation strategies while securing their networks and applications.

Respondents shared a sense of confidence when dealing with known threat vectors. But as businesses transition to public cloud environments, microservice architectures and 5G networks, security professionals do not have the visibility and, in some cases, the right solutions. Support is needed to protect their enterprises with assurance across several domains.

How Often Were Businesses Attacked?

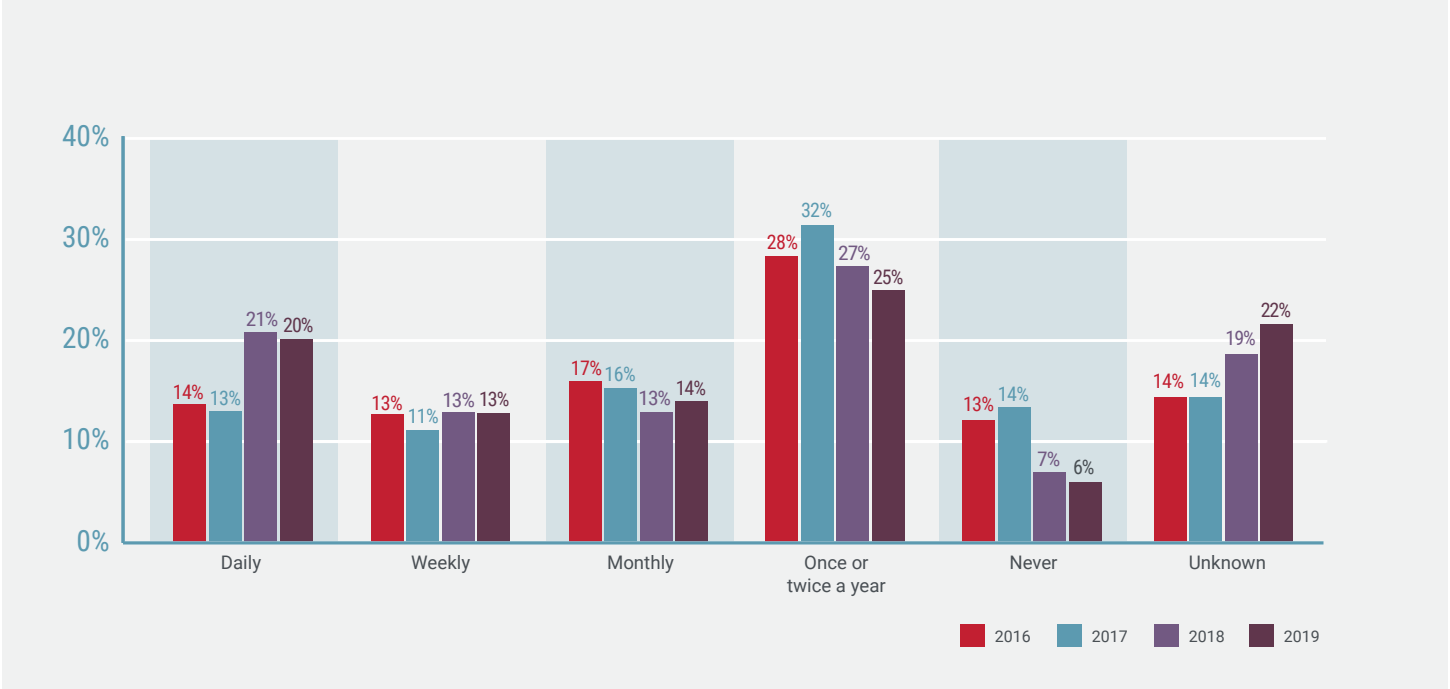


Figure 4. Frequency of cyberattacks during the year (2016–2019).

Dealing with relentless cyberattacks is just part of the job for survey respondents. Ninety-four percent reported a cyberattack in the past 12 months; only 6% claimed not to have experienced an attack. As in 2018, about one-third of respondents said that their organizations experience cyberattacks either daily or weekly. Of concern are the 22% of respondents who said that they were not aware if attacks occurred. Lack of visibility into what is happening in their networks is likely a contributing factor.

Vertical Focus: Experience Daily Attacks

1. Education	45%
2. Retail	39%
3. Banking and financial services	37%

Figure 5. Segments that reported experiencing daily cyberattacks.

The industries that indicated the highest frequency of daily cyberattacks were education, banking and financial services and service providers.

Why Were Businesses Attacked?

Among respondents who experienced cyberattacks, about one-third said that the primary goal of hackers was financial gain or service disruption. As organizations adopt more dynamic network environments to enable more agile responses to business opportunities, new blind spots in the attack surface emerge for cybercriminals to leverage.

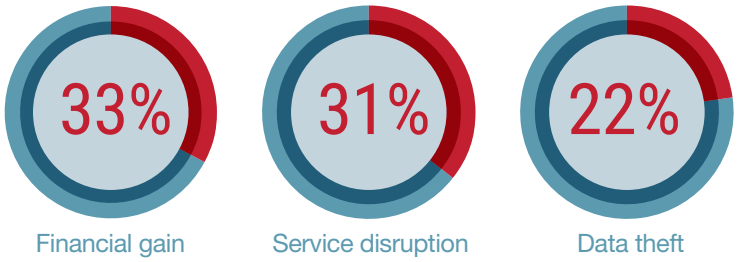


Figure 6. Primary goals of hackers (2019).

		REGION			
	Total	USA/Canada	APAC	EMEA	CALA
Financial/ransom	**59%**	70%	52%	59%	30%
Insider threat	**29%**	26%	28%	31%	39%
Political/hacktivism/social	**28%**	30%	23%	38%	20%
Cyberwar/geopolitical conflict related	**27%**	36%	27%	20%	7%
Competition/espionage	**25%**	23%	22%	34%	26%
Angry users	**20%**	21%	12%	23%	30%
Motive unknown/other	**27%**	28%	27%	27%	26%
Have not experienced any cyberattacks	**1%**	0%	2%	1%	2%

Figure 7. Motives for cyberattacks vary by region.

Ransom

Of the respondents who reported experiencing cyberattacks sometime during the previous year, ransom remained the primary motivation, with a 16% year-over-year increase from 2018 and back to the level reported in 2017. North American companies ranked ransom as the highest motivation for cyberattacks — at 70%.

In 2019, hackers launched cyber-extortion campaigns directed at enterprises and government agencies, often targeting employees with phishing emails that included links that, once clicked, enabled attackers to enter the networks.

2019: **CASE IN POINT**

Johannesburg, South Africa — The Shadow Kill Hackers group locked down the city's infrastructure demanding four bitcoins.[2]

Arizona Beverages — Hackers leveraged iEncrypt ransomware to attack outdated back-end servers in the company's network.[3]

[2]https://www.newsbtc.com/2019/10/30/johannesburg-city-infrastructure-locked-down-due-to-bitcoin-ransom/
[3]https://www.scmagazine.com/home/security-news/ransomware/arizona-beverages-ransomware-attack-exacerbated-by-unpatched-servers-poorly-configured-back-up-system/

Nation-State Attacks

Another phenomenon in 2019 is the 42% increase in attacks reported by respondents who said that their organizations were attacked and attributed the attacks to foreign governments. In nation-state attacks, government entities launch attacks to gain user information and tamper with the operations of companies or other nations. Hacktivism is more prevalent in EMEA at 38% than in the total respondents' average of 28%. In APAC, angry users retaliated with cyberattacks, according to 30% of respondents, compared to 20% of total respondents.

2019: **CASE IN POINT**

DNS hijacking campaign — Iranian hackers are suspected of a wave of DNS hijacking attempts against domains around the globe belonging to government, telecom and internet infrastructure organizations.[4]

Operation Soft Cell — Hackers compromised the IT infrastructures of 10 telecom companies, setting up VPNs with administrator privileges to gain access to customer data, with specific interest in about 20 high-value targets.[5]

Operation ShadowHammer — Using the ASUS Live Update utility, hackers installed back doors on ASUS computers around the globe to target a pool of users identified by their network adapters' MAC addresses.[6] This example is a supply chain attack where cybercriminals target a popular service intending for the damage to trickle down to the user base for maximum impact.

What Kinds of Attacks Did Businesses Experience?

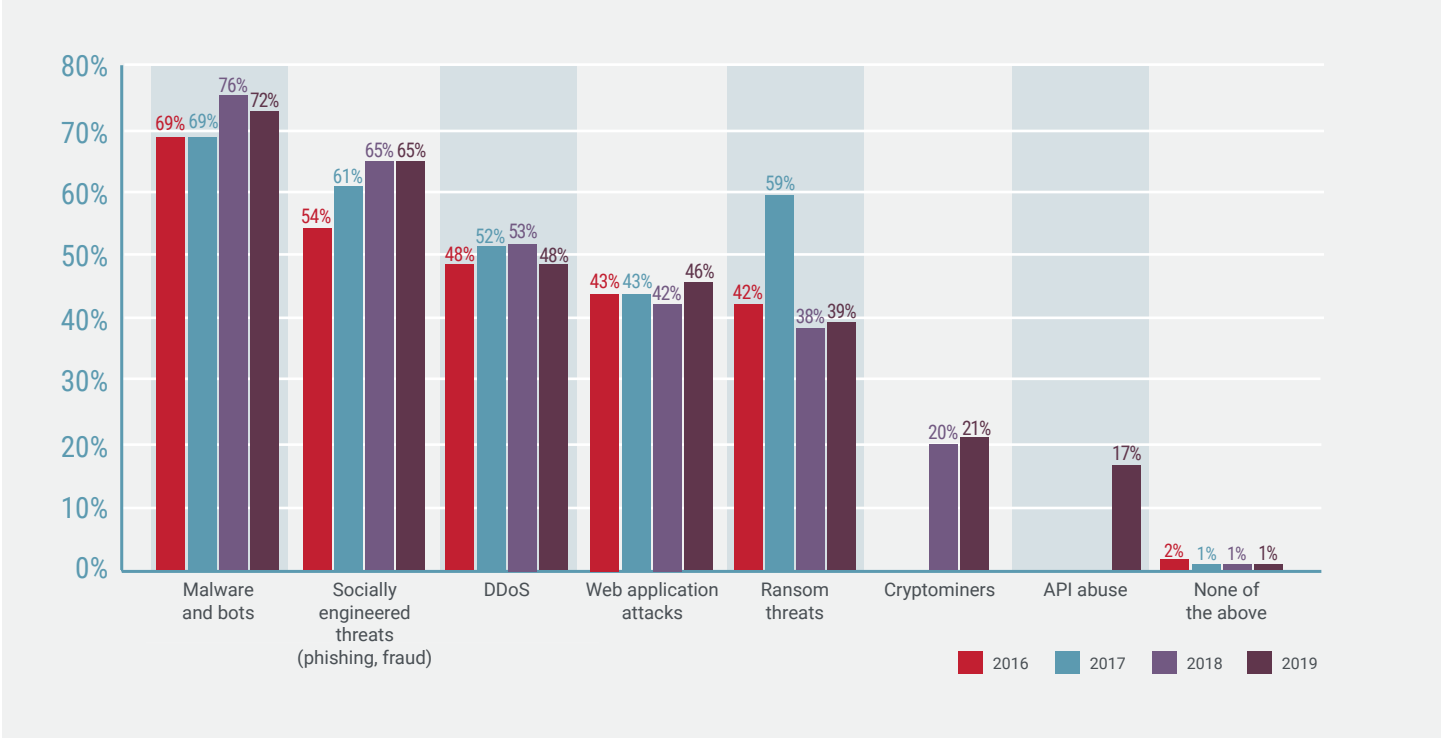


Figure 8. Types of attacks experienced (2016–2019).

There were no major developments in the threat landscape identified by survey respondents. The types of cyberattacks that businesses experienced remained fairly consistent with results from 2018. Malware attacks were the most prevalent, hitting seven of 10 organizations. The change in DDoS attacks was minor with only a 10% decline year over year, as well as for web application attacks, which only saw an increase of 10%.

[4]https://www.fireeye.com/blog/threat-research/2019/01/global-dns-hijacking-campaign-dns-record-manipulation-at-scale.html
[5]https://www.scmagazine.com/home/security-news/apts-cyberespionage/operation-soft-cell-campaign-targets-cellular-telecom-providers-points-to-chinas-apt10/
[6]https://securelist.com/operation-shadowhammer/89992/

Brute Force	53%
Basic query flood	46%
Recursive flood	34%
Reflective amplification attack	37%
Cache poisoning	45%

Figure 9. Attack vectors experienced against DNS servers.

Of those who experienced attacks against a DNS server, half experienced a Brute Force attack, and another two-fifths indicated a basic query flood. Brute Force attacks are more common in North America and CALA than in the APAC region. Cache poisoning attacks increased significantly for the second year in a row (to 45%, up from 31% in 2018).

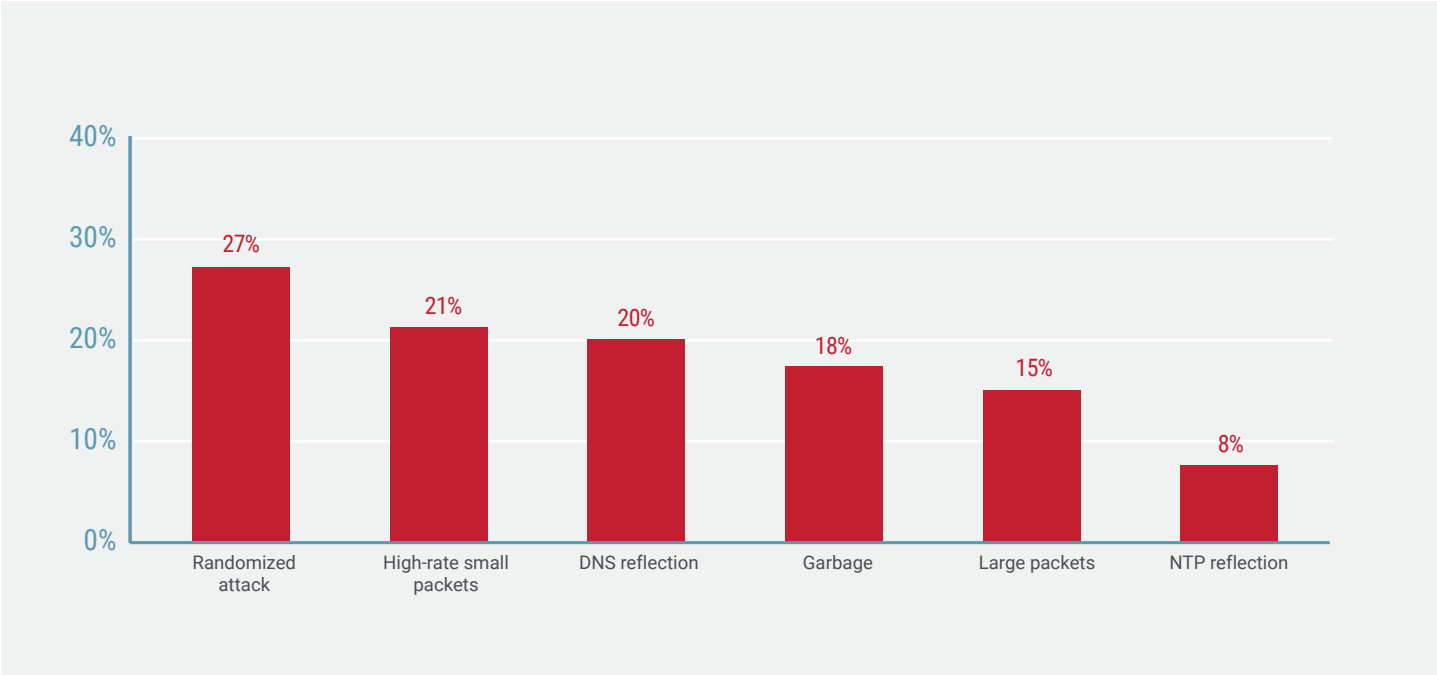


Figure 10. Types of UDP DDoS attacks incurred.

Respondents in two of five organizations said that they did not incur any user datagram protocol (UDP) DDoS attacks in the past year. Companies that were hit by UDP DDoS attacks reported a variety of types, including randomized attacks, high-rate small packets, DNS reflection, garbage, large packets and network time protocol (NTP) reflection.

Focus on DDoS Attacks

In general, cyberattacks did not differ greatly based on industry, except for DDoS attacks that were most common to service provider/telecom companies at 64% compared to 48% for all respondents.

Key characteristics of DDoS attacks in this year's report include:

- 10% of DDoS attacks were above 10Gbps
- The average packets-per-second (PPS) rate declined
- 42% lasted less than one hour
- Burst attacks were shorter and lasted only a few minutes

Three of four DDoS attacks impacted respondents' infrastructure with partial service degradation or a complete outage. Advances in DDoS protection technologies have proved effective against simple network floods. Over time, DDoS attacks have moved to the application layer. Nearly all (91%) of the respondents who incurred a DDoS attack indicated that the application layer was the preferred vector.

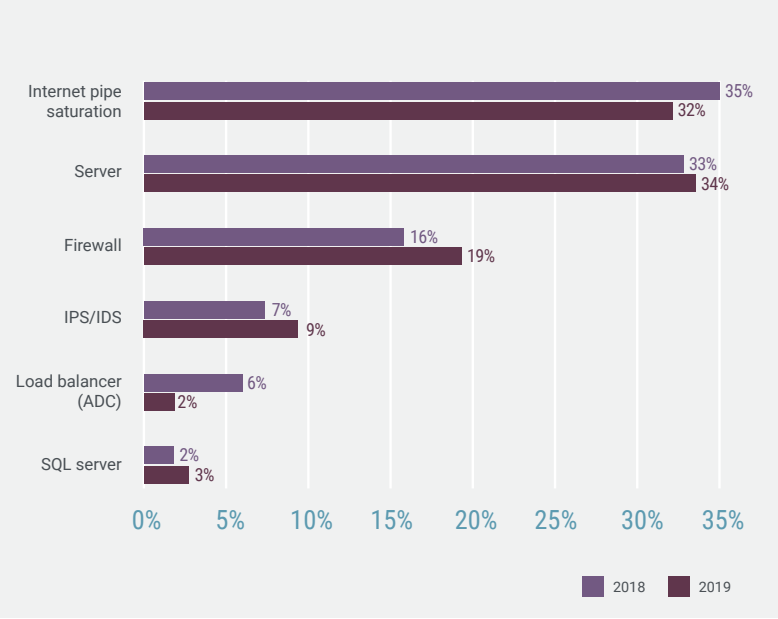


Figure 11. Components impacted by DDoS attacks.

Infrastructure upgrades and investments in capacity contributed to a 9% reduction in internet pipe saturation situations as a result of DDoS attacks, compared to 2018.

A New Version of an Age-Old Attack

The Radware Threat Research Center (TRC) and ERT monitor clients' network traffic to defend against known and emerging attacks. During the last two years, the TRC and ERT identified a steady growth in attackers leveraging TCP reflection attacks and recently issued a *Radware Threat Alert — TCP Reflection Attacks*.[7]

In a TCP SYN-ACK reflection attack, an attacker sends a spoofed SYN packet (with the original source IP replaced by the victim's IP address) to a wide range of random or preselected reflection IP addresses. The services at the reflection addresses reply with a SYN-ACK packet to the victim of the spoofed attack. Although the typical three-way handshake might assume that a single SYN-ACK packet will be delivered to the victim, when the victim does not respond to the last ACK packet, the reflection service will continue to retransmit the SYN-ACK packet, resulting in amplification.

The alert outlines the genesis, profile, impacts and protection recommendations for this type of attack.

[7]https://blog.radware.com/security/2019/11/threat-alert-tcp-reflection-attacks/

New Attack Vectors

In 2019, two new DDoS attack vectors came to light that leverage amplification attacks, a favorite vector in the DDoS-for-hire industry. Amplification attacks query information from a service, such as the DNS or NTP, with spoof requests that make their way to the targets.

IoT Threats

IoT threats continued at a rapid pace in 2019. Hackers successfully used timeworn strategies to gain access to vulnerable connected devices.

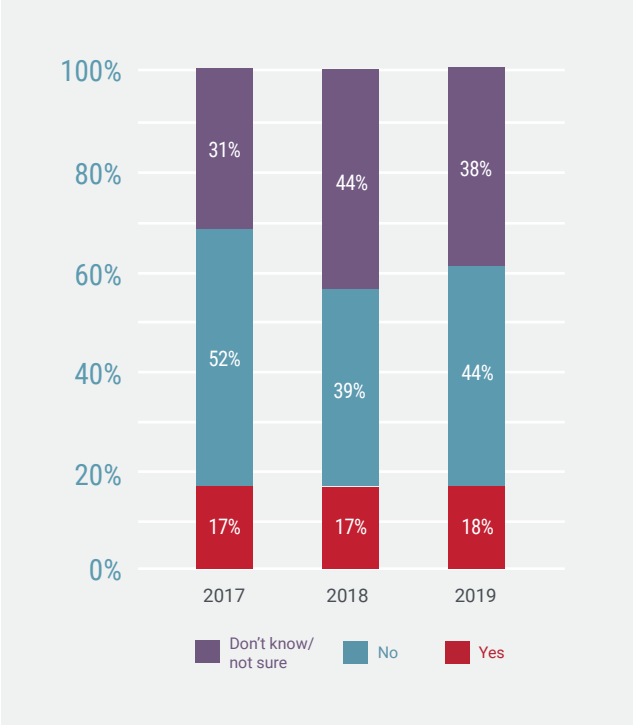


Figure 12. Knowledge of DDoS attacks originated with an IoT botnet.

Visibility into IoT botnet attack traffic continues to be an issue for organizations. Although down from 2018 responses, 38% of respondents still said that they do not know or are not sure if they experienced any DDoS attacks originated by an IoT botnet during the past year.

2019: CASE IN POINT

WS-Discovery — A multicast protocol launched that discovers nearby connected devices, such as printers or security cameras, and directs them to amplify DDoS attacks over the internet.[8]

MacOS ARMS — Attacks leverage the Apple remote management service (ARMS) of the macOS on computers connected to the internet without firewall or local network protection to amplify DDoS attack traffic.[9]

2019: CASE IN POINT

Silex malware — This malware goes after the firmware of IoT devices, a practice known as "bricking," by logging in with known default credentials. The author of the malware is purportedly a 14-year-old male who was inspired by the BrickerBot malware attack in 2017.[10]

D-Link router attacks — A hacker group hijacks DNS traffic on D-Link routers to direct it to malicious clones of legitimate websites.[11] The strategy is similar to attacks at Brazilian banks tracked by the Radware TRC dating back as far as 2015.[12]

[8]https://www.csoonline.com/article/3439442/misconfigured-ws-discovery-in-devices-enable-massive-ddos-amplification.html
[9]https://www.zdnet.com/article/macos-systems-abused-in-ddos-attacks/
[10]https://www.zdnet.com/article/new-silex-malware-is-bricking-iot-devices-has-scary-plans/
[11]https://www.zdnet.com/article/hacker-group-has-been-hijacking-dns-traffic-on-d-link-routers-for-three-months/
[12]https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/dns-hijacking-brazil-banks/

Bot Attacks

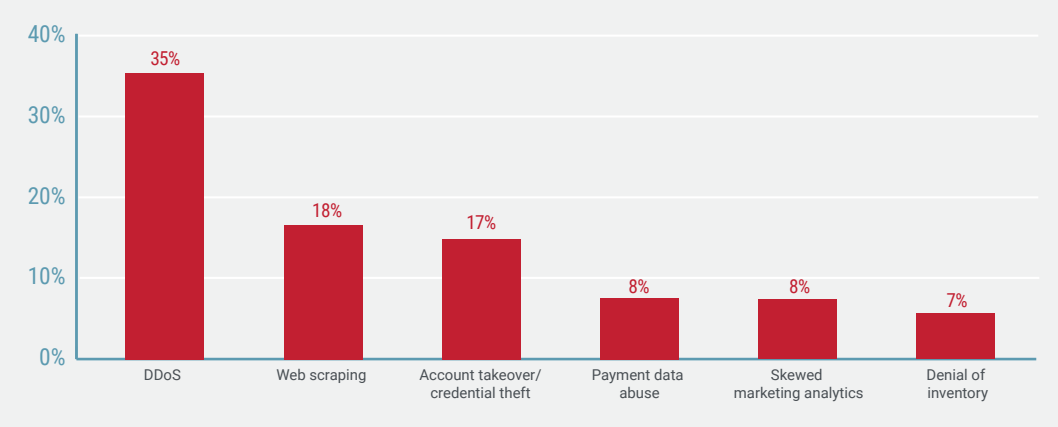


Figure 13. Bot attacks experienced in 2019.

Bot attacks were experienced by 56% of respondents, and DDoS was the most prevalent at 35%. Thirty-eight percent of respondents did not know if their organizations were hit by IoT botnets.

A heat map shows where bot traffic is generated, with hot spots in China, Russia and countries in Africa.

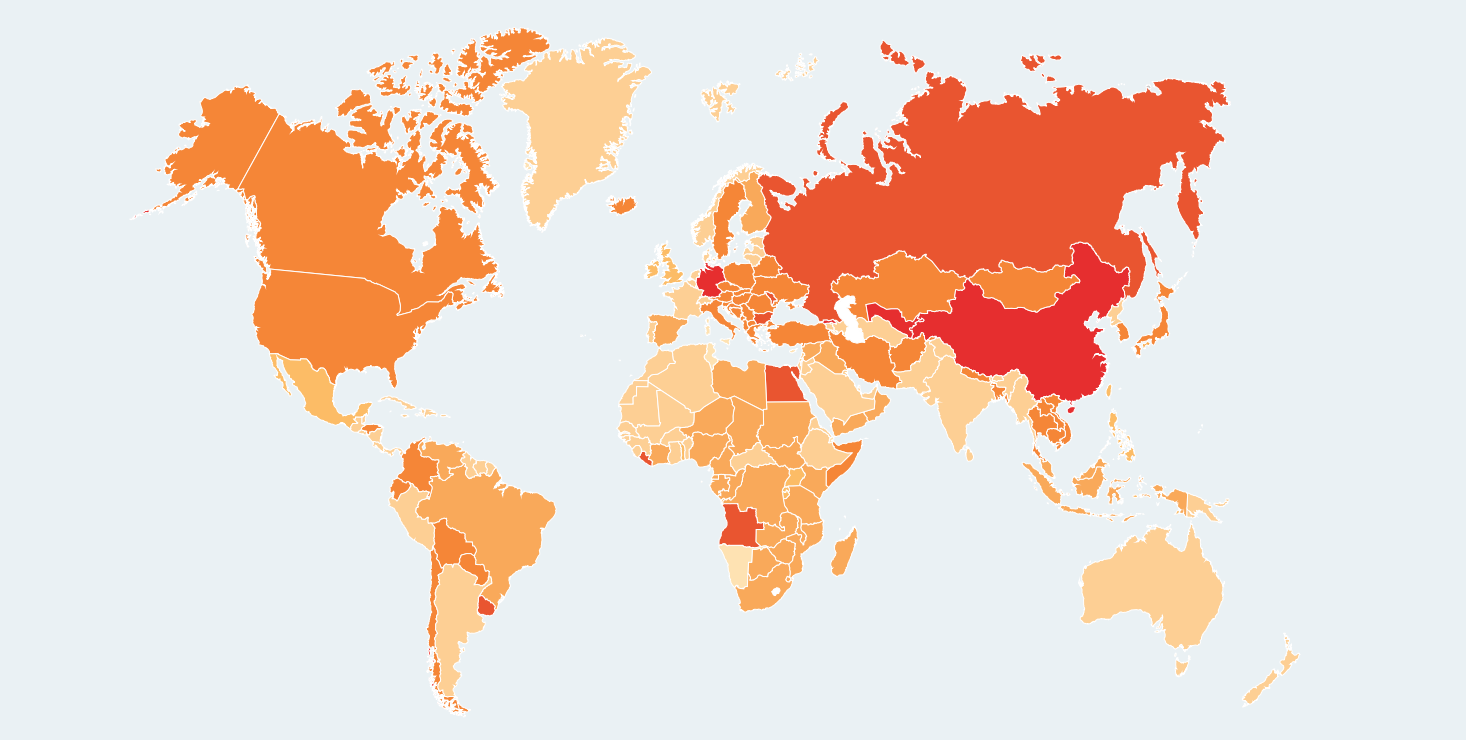


Figure 14. Worldwide heat map of bot traffic, August 2018 to August 2019.

As bots get more sophisticated, they do a better job of mimicking human behavior by using 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 disrupt services.

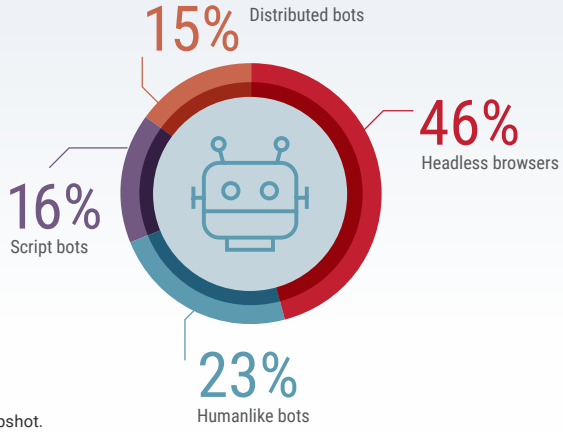


Figure 15.
Bad bot traffic
by generation,
12-month snapshot.

Business Concerns About Cyberattacks

Data leakage continued to be the biggest business concern related to a cyberattack, although to a lesser extent than in 2018 (down to 30% from 35%). A secondary concern is a service outage.

Data leakage/information loss	30%
Service outage	23%
Reputation loss	16%
Revenue loss	11%
Customer/partner loss	8%
Productivity loss	7%
Losing my job	6%

Figure 16. Business concerns if faced with a cyberattack.

Cost of Cyberattacks

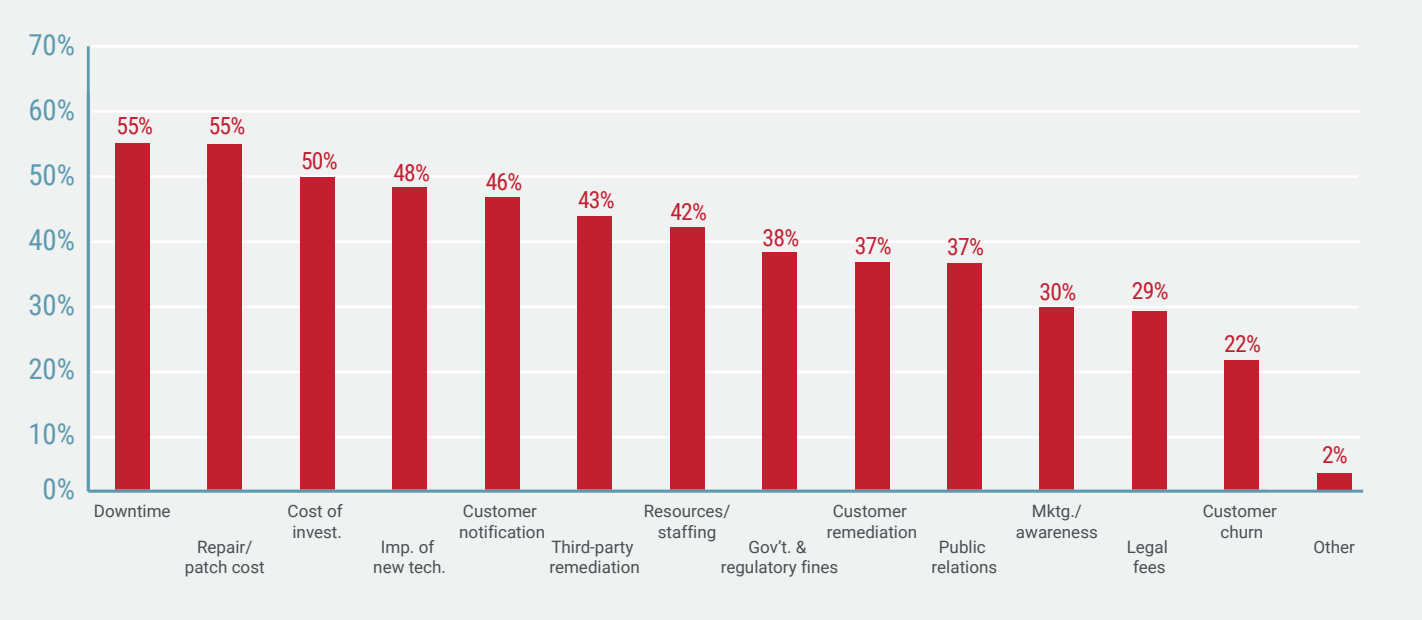


Figure 17. Factors included when calculating the cost of cyberattacks.

Only about one-quarter of survey respondents said that their organizations had tried to calculate the cost of a cyberattack. At least half of those who calculated the cost of an attack included factors associated with downtime, repair/patching and investigation.

COMPANY SIZE BY REVENUE	AVERAGE COST OF A CYBERATTACK
>1 billion USD/EUR/GBP	1.7 million USD/EUR/GBP
<1 billion USD/EUR/GBP	480,000 USD/EUR/GBP

Figure 18. Estimated cost of a cyberattack by company revenue.

Similar to 2018, two of five respondents estimated that a cyberattack cost their organization less than 100,000 USD/EUR/GBP. But cost estimates varied depending on the organization's size. Companies with revenues of more than 1 billion USD/EUR/GBP reported an average cost of 1.7 million USD/EUR/GBP per cyberattack. Companies with revenues of less than 1 billion USD/EUR/GBP estimated the cost of a cyberattack at 480,000 USD/EUR/GBP.

Companies with revenue below 1 billion USD/EUR/GBP were most likely to say that an attack would cost them less than 100,000 USD/EUR/GBP (48%) vs. 23% of companies with revenue of 1 billion USD/EUR/GBP or higher. Those with revenue of at least 1 billion were more likely to incur at least 500,000 USD/EUR/GBP in related expenses.

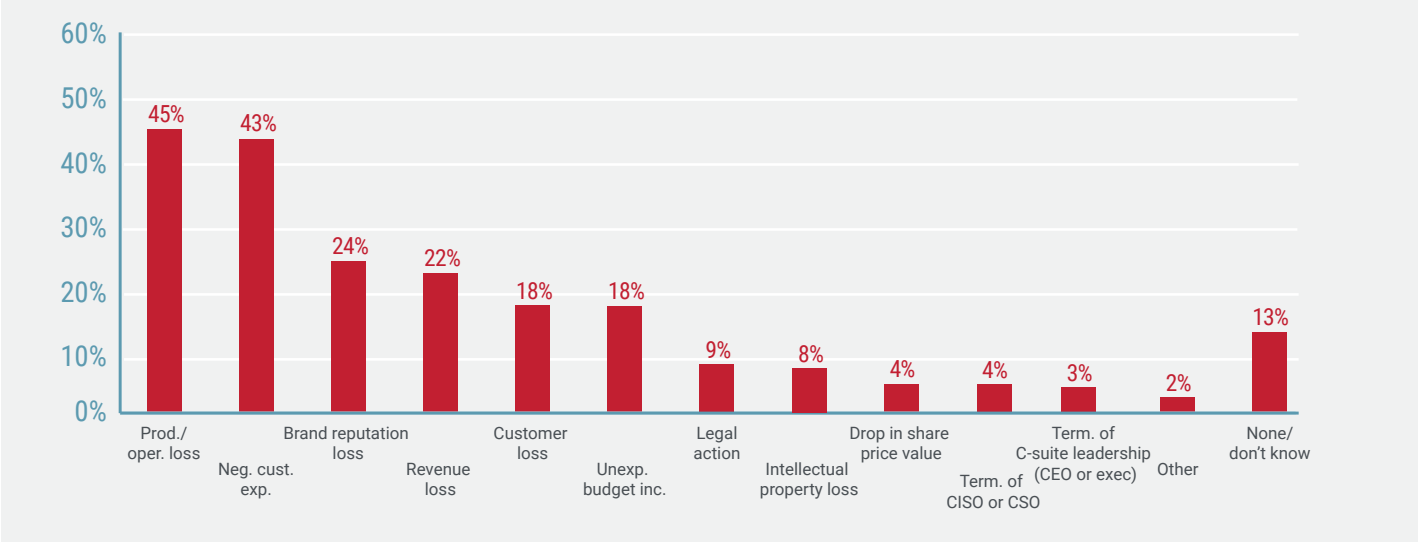


Figure 19. Repercussions of successful attacks.

Successful attacks most often resulted in productivity or operational loss or negative customer experience. The most common losses are consistent across all regions.

What Security Strategies Did Businesses Use?

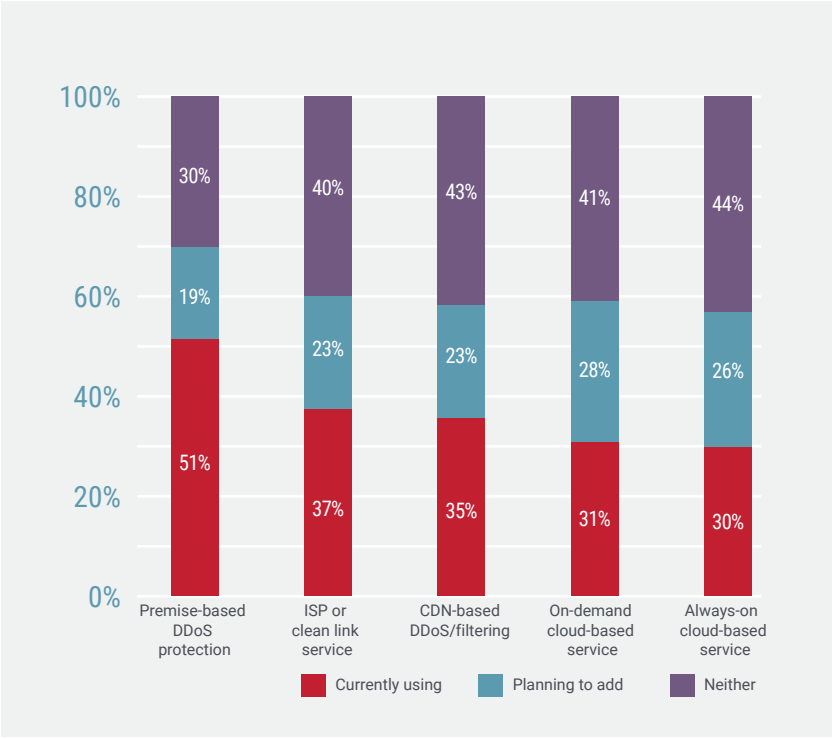


Figure 20. Solutions used to protect against cyberattacks.

Half of the respondents reported having used premise-based DDoS protection to guard against cyberattacks. One-third used an internet service provider (ISP) or clean link service or content delivery network (CDN)-based DDoS/filtering. More than half used multiple solutions, but one-fourth utilized only one solution against cyberattacks.

The Move to Multiple Public Clouds Creates Security Silos

Although security professionals have better visibility into what is happening on their networks when computing resources are managed on-premise, the benefits of a public cloud environment are compelling. As expected, enterprises continued to transition more applications and data to public cloud environments in 2019.

Organizations look to public cloud service providers for network infrastructures that enable more agile responses to customer needs and deliver high availability and network performance while reducing operational costs.

The next step in this migration is the concurrent use of multiple public cloud environments for a number of reasons:

- **Cost optimization** — Every public cloud service provider offers different services and pricing packages. Organizations have more negotiating power when they are not tied to only one service provider.
- **Service redundancy** — If all digital assets reside in one public cloud environment, there is too much risk for network downtime. Using multiple public cloud environments enables strategic planning for backup protection.
- **Best-of-breed functionality** — Each public cloud provider has its strengths and weaknesses when it comes to certain capabilities such as computing power, automation, big data processing, etc.
- **Acquisitions/mergers** — When companies combine operations, it is common practice to maintain applications and services on multiple public cloud environments.
- **Shadow IT teams** — Development and operations (DevOps) and other teams, which cannot wait for a central IT organization to allocate network resources, often secure their own arrangements with public cloud service providers.

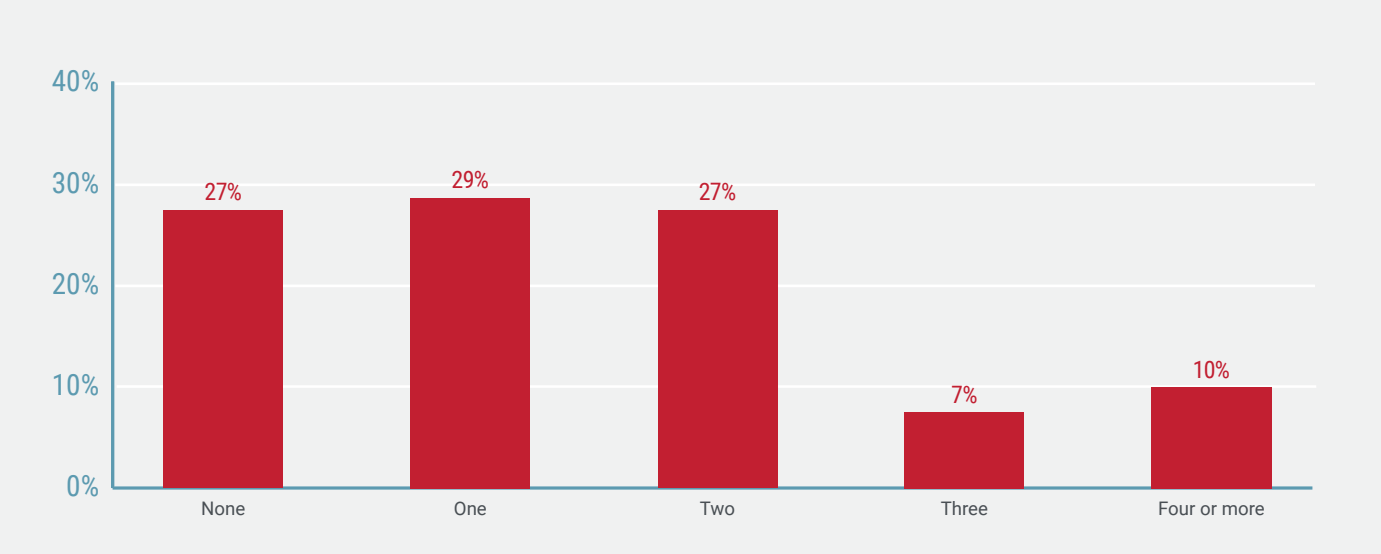


Figure 21. Use of public cloud environments.

Three-fourths of survey respondents said that their organizations used at least one public cloud, and more than two of five used two or more public clouds. Large and worldwide companies were most likely to have used three or more public cloud environments. Amazon Web Services (AWS) (44%) and Microsoft Azure (43%) were the two most used public cloud vendors. Only about one-quarter of respondents said that they have not used public clouds.

Balancing Business Challenges

The strategic use of multiple public cloud environments introduces new business challenges. Although organizations are better able to respond rapidly to market opportunities, the decentralized nature of this model adds complexity to how applications and computing resources are secured.

Organizations — whether via chief information security officers (CISOs) or other security teams — need to stay abreast of the technological and environmental changes in their public clouds. There is a need for visibility across all the different platforms from one holistic solution that enables management of the security posture by utilizing one common language. The goal is to be able to:

- Prevent attacks by reducing the size of the attack surface
- Detect and identify evolving threats
- Respond with accurate and effective mitigation

Security professionals weighed the benefits of having used a public cloud against the risks. Although only 10% of respondents felt that their data was more secure in a public cloud environment, 30% felt that the benefits of the cloud, such as agility and lower costs, justified the security risks.

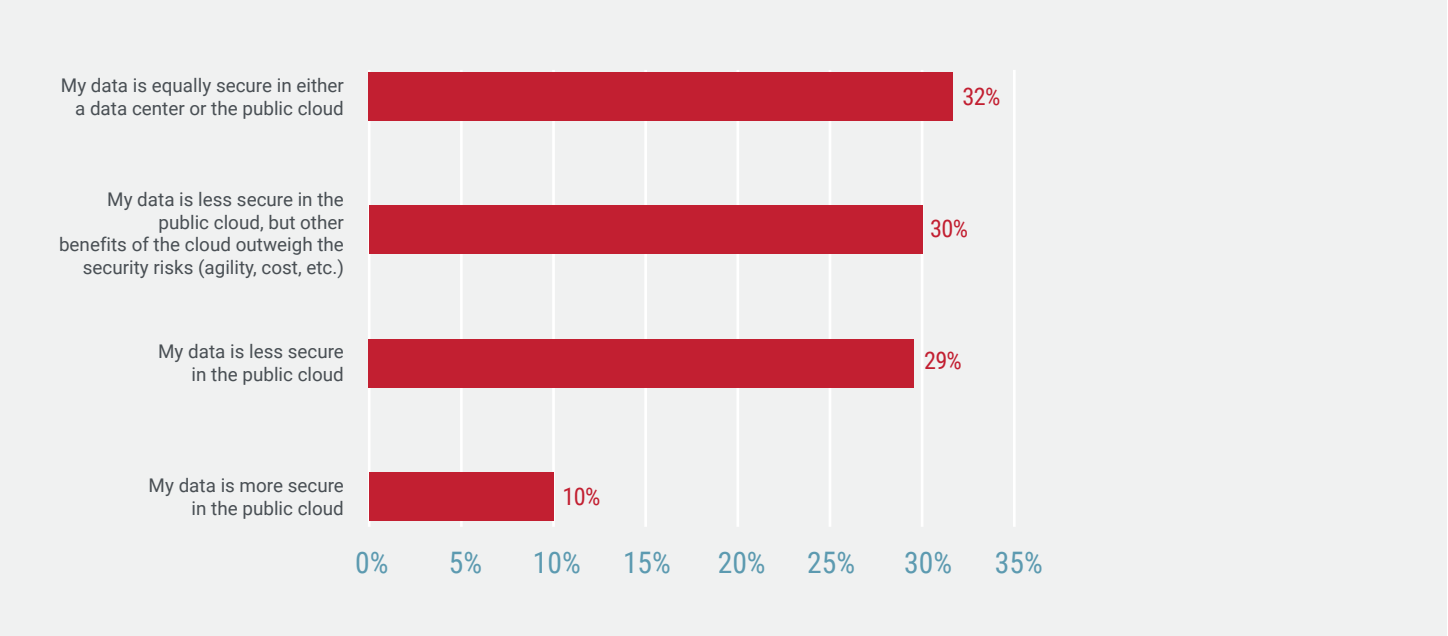


Figure 22. Lack of confidence in public cloud security.

But lack of visibility about which entity — the organization or the public cloud service provider — is responsible for specific elements of network security caused security breaches. In Radware's *2019 State of Web Application Security Research* report, 65% said that they aren't clear about security boundaries, and 53% of respondents experienced data exposure as a result of misunderstandings with the public cloud provider regarding security responsibilities.

65% aren't clear where the boundaries of responsibility are

53% have experienced data exposure caused by misunderstandings

Figure 23. Misunderstandings about responsibilities for public cloud security.

In the public cloud environment, web and application intrusion (27%) was seen as the biggest threat to their companies' cloud environments, similar to previous years' surveys.

The Need to Rethink Security Strategies

Often when organizations migrate from on-premise to public cloud environments, security teams want to continue to use the same approach for protecting applications and data. But use of a public cloud, especially multiple public clouds, introduces new attack vectors that require better visibility into what is happening across the entire ecosystem. Security tools offered by public cloud vendors are often a popular choice to fill the gap following migration.

Web and application intrusion	27%
Credential threat	20%
Malware	15%
DDoS	14%
Insider threat	11%
Other	2%
None/don't know/don't use the cloud	11%

Figure 24. Security threats to the public cloud environment.

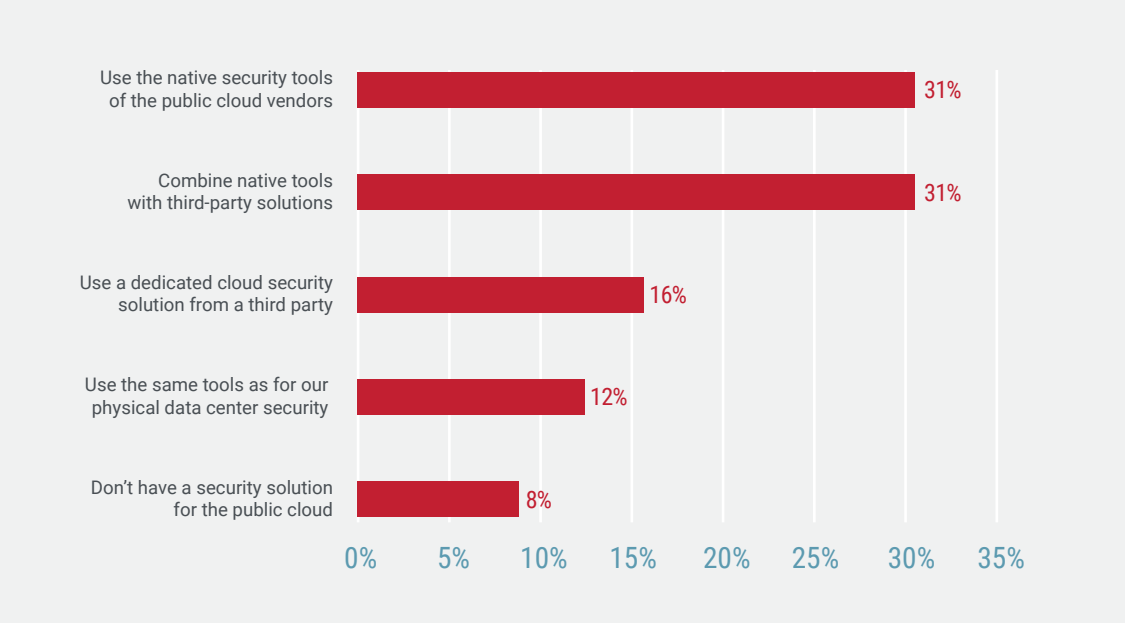


Figure 25. Main approaches to secure the public cloud.

The majority of respondents who said that their organizations used public cloud environments indicate that they selected native security tools or a combination of native tools with third-party solutions to secure their public cloud.

Possible reasons for organizations adopting a heterogeneous approach to securing public clouds might be because public cloud vendors are not cybersecurity experts and typically provide best-of-breed security tools vs. a 360-degree holistic security solution. Many organizations recognize the risks associated with relying solely on a public cloud vendor for security and opt to include a dedicated cybersecurity/DDoS vendor.

Fortifying the Public Cloud

SundaySky's video marketing platform provides marketers and customer experience professionals with video-powered content to provide consumers with an exceptional digital experience. Founded in 2006, the company is headquartered in New York City with additional offices in Tel Aviv and Tokyo.

Network elasticity and scalability have always been critical to SundaySky's business. With customers leveraging the network more during business hours than in the evening, using a cloud-based platform for SundaySky's network infrastructure benefits the company immensely. SundaySky uses AWS, which provides the ability to scale network capacity to meet spikes in demand and offers a pay-as-you-go pricing model.

But with progress comes new challenges — and new security threats. SundaySky had to comply with various regulations, including HIPAA, regarding the handling and security of data. Multiple AWS environments and accounts meant that SundaySky required a single workload security solution that would:

- Assist with managing access permissions to AWS services and data
- Reduce obsolete/excessive permissions across multiple AWS environments
- Provide a centralized console for management of account updates and timely identification of insecure misconfigurations and compliance assurance
- Protect against data breaches, account takeovers and other attacks while eliminating false positives

To protect its AWS environment and attain improved visibility into account updates and insecure misconfigurations, SundaySky implemented Radware's Cloud Workload Protection Service (CWPS), an agentless, cloud-native workload security solution.

"Radware's Cloud Workload Protection provides us with the single pane of glass to manage the permissions and workloads that we were looking for. Being concerned about misconfigurations and potential risks has become a thing of the past. It's fortified our cloud-based network."

— Shay Reshef, Director of Security, SundaySky

SundaySky's operation and security teams now leverage CWPS for a single view of accounts and workloads running across their network, in addition to account updates and associated permissions. Previously unidentified workloads and/or outdated accounts have been pinpointed and secured, and CWPS monitors account updates and configuration changes for misconfigurations and excessive permissions, ensuring that SundaySky meets compliance regulations regarding the handling of customer data.

Keeping Permissions Tight

Threats have evolved dramatically over the past few years, and hackers have devised methods to leverage cloud technologies. When data and applications are hosted in the cloud, the number of entry points to the network increases dramatically. Controlling who has permission to access network elements and data is very important.

Organizations need to find the right balance between too excessive and restrictive permission policies. Excessive permissions leave environments open to malicious activity. Permissions that are too restrictive block DevOps teams from being able to do their jobs.

Twenty percent of survey respondents ranked credential threats as the biggest threat to their company's cloud environment, slightly behind web and application intrusion.

Diffusion of Staff Responsibilities

Part of the problem is that IT administrators are generally no longer part of a centralized team controlling and administering the entire computing environment. As the role of DevOps grows, DevOps teams are spread across development Scrum teams, small groups with members representing the different functions needed to accomplish the goals at hand. No one entity controls the granting of permissions, but developers, DevOps, compliance and others should only receive the permissions they need.

Aggressive governance policies might harden organizations' environments but could limit the ability of development teams to react quickly to update applications or access data as needed to address changing business requirements.

Skills Shortage Affects Security Tactics

Competition for qualified employees is high, as are salaries. Constant turnover makes it difficult to maintain qualified knowledge transfer. Cybersecurity Ventures predicts that 3.5 million cybersecurity jobs around the globe will go unfilled by 2021.[13] CISO respondents to the Radware global survey indicated that they struggle to find and hire skilled IT security staff.

The role of the CISO is also evolving. As different security and developer roles in organizations gain prominence, such as DevOps, management of relationships with public cloud vendors might not reside directly with the CISO. It is quite possible that multiple groups have relationships with each public cloud vendor. This arrangement can add complexity and potentially conflict with departments and working groups regarding how security policies should be applied.

Threat propagation in public cloud environments and the shortage of qualified security professionals necessitate the need for greater automation in security solutions. In the Radware global survey, CISOs indicated that there was a greater reliance on automation to detect and mitigate threats.

Strategies to Secure Multiple Public Cloud Environments

Applying security protocols that were successful for on-premise environments will not work as applications and data migrate to public cloud environments. Security teams need to adopt new strategies to harden security across their entire public cloud ecosystem by:

- **Adopting third-party security solutions**
  The public cloud service providers' core competencies are not network security. Rather, network protection is generally a proprietary add-on to their service offerings that operate in a silo. Instead, select a security solution from a vendor with proven expertise and thought leadership. Choose a holistic approach that can protect multiple public cloud environments with consistent implementation and maintenance of security protocols while automating prevention, detection and response.

- **Engaging a fully managed security service**
  To overcome staff and skills shortages, take advantage of an outside team focused on securing your public cloud network security environments.

- **Centralizing management of network security**
  With a security solution in place that provides visibility and control of security policies across all virtual public clouds and clouds, it is possible to achieve tighter regulation of user credentials and permissions from a centralized dashboard.

[13] https://cybersecurityventures.com/jobs/

Situation Analysis

Cloud-native attack foils defenses at public cloud service provider

Public cloud environments broaden the attack surface from which hackers can try to gain access to enterprises' data and applications.

In 2019, one of the largest financial institutions in the United States announced that it was the victim of a data breach, which exposed the personally identifiable information (PII) of more than 100 million customers who had applied for credit card products. This global banking institution is a respected and experienced company that prioritizes the security of its customers' data. Let's take a look at how a hacker launched a cloud-native attack to gain access to the data stored in a public cloud environment managed by AWS.

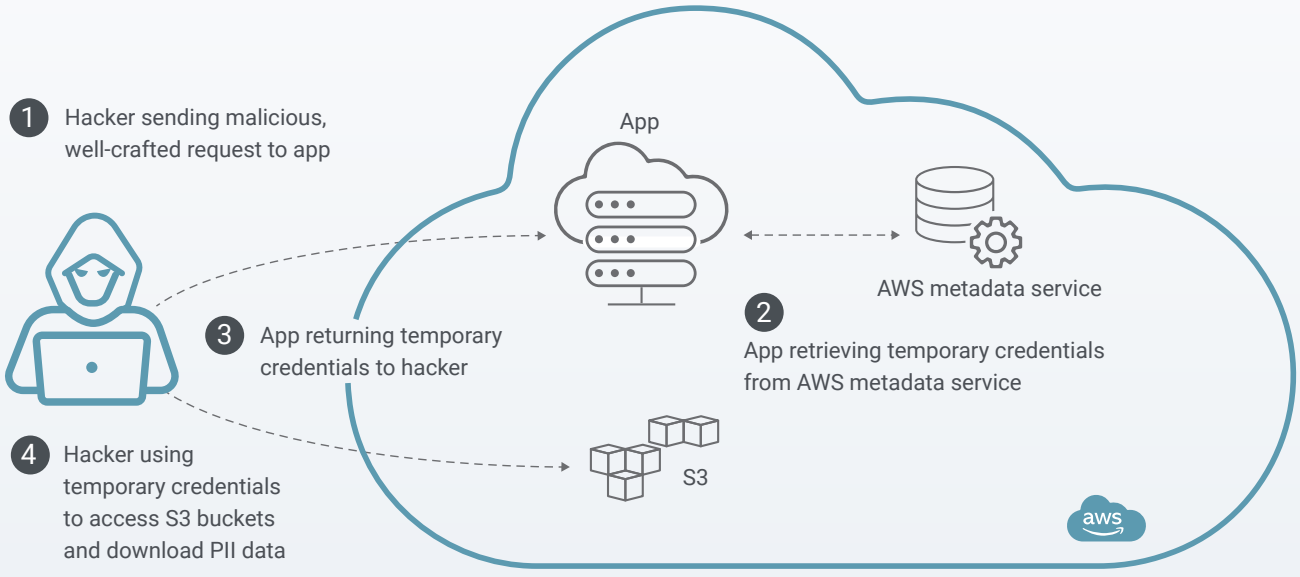


Figure 26. Multifaceted threat example.

How the Hacker Attacked

A hacker used leaked credentials to attack a public-facing web application server hosted by AWS. The hacker exploited a server side request forgery (SSRF) vulnerability to target the hosting web application.

By using the machine role of the web application firewall (WAF), the hacker queried the AWS metadata service and obtained temporary identity and access management (IAM) credentials. With these credentials in hand, the hacker was able to perform reconnaissance activities in the AWS environment to access S3 storage buckets and download PII data, which was later uploaded to GitHub.

Because the financial institution did not have visibility into the activity, it wasn't until weeks later that the breach was discovered after the hacker bragged about the attack on social media and published links to the stolen data. An anonymous tip alerted the bank to the attack.

Why the Attack Worked

External-facing applications are susceptible to web vulnerabilities, which cannot always be handled in time either by patching the application or via the web server. A security solution should be able to prevent and detect data leakage activity.

In this scenario, the following anomalies could have been detected in time to avoid data leakage and illegal access:

- WAF-Role had excessive permissions with no business need
- EC2 role was used outside of the machine and cloud, and the activity went undetected
- Anomalous source — a nontypical source IP used the WAF to access the data
- Anomalous S3 destination — S3 destinations aren't typically accessed
- Anomalous S3 operations — nontypical S3 activity performed by WAF-Role
- Anomalous intensive access — transferring large amounts of files out of the cloud

Lessons Learned

1. Public cloud environments require cloud-specific protections.
2. All attack surfaces — application and infrastructure — need to be covered.
3. Detection is important, but correlation of individual malicious steps is critical.

Moving Forward

The global industry survey results shine a mirror on industry trends regarding the impact of cyberattacks on organizations. As security professionals evaluate strategies to support their companies' digital transformation goals, the need to gain visibility into changing network environments is heightened.

Although confidence in their ability to handle known attack vendors slightly improved, the increase in "don't know" responses as to whether their organizations have been attacked is troubling. Is the rapid pace at which organizations are embracing digital transformation to blame? As the transition to more agile network infrastructures continues, how will an organization know when the next "holes" emerge, which hackers will exploit with new and creative tactics, if that organization's visibility is limited?

Solutions that enable security professionals to gain systemwide views of what is happening — combined with automated detection and mitigation — are necessary to keep up with the speed of business in our digital world.

Microservice Architectures Challenge Traditional Security Practices

How fast is fast enough? When it comes to creating and maintaining great customer experiences, organizations don't have time to wait for traditional security reviews before rolling out or enhancing applications. The first priority is that applications meet customer needs. Application security is critical, but for businesses to maintain competitive advantages, it can't stand in the way of progress.

The cycle of planned update release schedules is outmoded and impractical. Instead, businesses have embraced agile workflows to be able to fix bugs, incorporate feedback from customers and implement new features on a daily or even hourly basis.

Enterprises are also making fundamental changes in their choice of environments where applications are developed and hosted. They are moving away from monolithic applications housed on-premise to microservice architectures hosted in public clouds. This shift is in response to the need for ecosystems that are flexible and scalable enough to support rapidly changing business requirements. How can security practices keep up?

The Conflicting Concepts of Agility and Security

When speed of delivery is the aim of continuous application deployment models, the demands of traditional security processes can be roadblocks. IT security teams see themselves as gatekeepers, implementing rigorous processes to reduce the risk of application attacks. Mistakes are not good for job security, but the investment in requirements refining, prototype testing, traffic inspection and policy reviews takes precious time.

Application DevOps teams have emerged as the designers and overseers of the agile network ecosystems that enable the automated continuous delivery processes. But these teams have different priorities that conflict with conventional, deliberative security practices. Their charge is to quickly deliver applications that support business needs. Building in time for exhaustive security reviews just isn't possible. As a result, traditional IT teams may find themselves uninvited from the process.

Distributed Architectures Introduce New Security Challenges

To accelerate development and better utilize resources and budgets, DevOps teams are breaking computing infrastructures down into containers and applications down to microservices running in these containers. This approach provides the flexibility, scalability and efficiencies that they seek by employing a variety of off-the-shelf tools for automation, independent development processes of each microservice, etc.

Microservice architectures encourage the use of application programming interfaces (APIs), a set of tools and protocols used to develop application software, for different use cases. The most common API formats in modern architectures are REST/JSON.

In the microservice architecture, the operational communication between the different tools used in the application development and delivery environment is done via APIs. This interface is a predefined request–response message system that exposes reliable content and operation negotiation.

Publicly available APIs are commonly being used for machine-to-machine communication, mobile apps and IoT devices, and others allow sharing of content and data openly between communities and applications. DevOps environments with the ever-increasing demand for continuous delivery require complete process automation utilizing APIs across the board:

- Service provisioning and management
- Platform management apps
- Continuous delivery process automation

API vulnerabilities are hard to detect and do not stand out. Traditional application security assessment tools do not work well with APIs or are simply irrelevant in this case. When planning for API security infrastructure, authentication and authorization must be taken into account, yet these are often not addressed properly.

All the different types of injection, authentication, access control, encryption, configuration and other issues can exist in APIs just like in a traditional application.

According to Radware's 2019 web application security study, 81% of respondents reported hacking attempts targeting APIs.

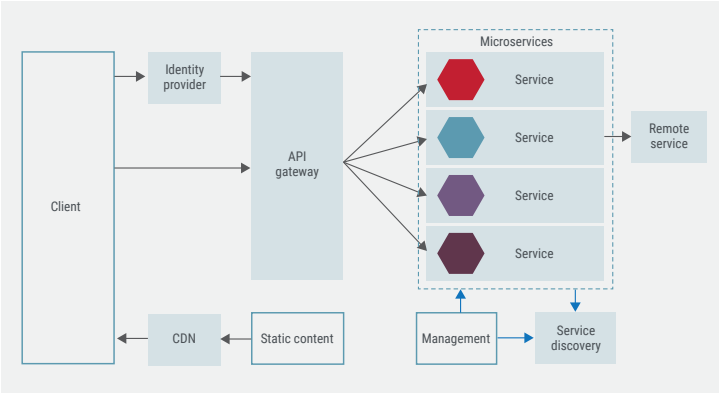


Figure 27. Example of microservice architecture diagram.

The move is great for flexibility because applications can be updated in an iterative fashion. Each module performs its own unique function that can be modified by developers without impacting other parts of the application provisioned in separate containers.

For example, Netflix is an early adopter of the microservice architecture.[14] The company is able to deploy new code multiple times per day without affecting customers' viewing experiences.[15]

Microservice architectures meet organizations' need for speed, but the tradeoff is the introduction of new security challenges.

Cloud-native applications running in microservice architectures leverage and consume public cloud services such as workloads, storage, Kubernetes orchestration services and CDNs. These services provide simple delivery while using industry standard open-source projects or public cloud technology.

Each container requires its own security profile because of the type of data transferred or the technology it is based on, which increases the attack surface and complicates the management of protection protocols across thousands of containers that are likely housed in multiple, geographically dispersed public cloud environments. Traffic flows also change to east-west to facilitate communication between containers.

The distributed nature of the architecture also means that there is no central point of visibility for organizations to monitor what is happening across all the environments where their applications are housed.

In this distributed environment, access to applications is no longer well defined. East-west traffic flows feed multiple entry points to applications that must be secured, but it is likely that this traffic is not currently being inspected. The Kubernetes orchestration platform may already be vulnerable and requires its own security measures against API attacks.

Evolving Responsibilities for Application Security

In addition to new security challenges, organizations need to figure out consistent roles and responsibilities to define who has the power, budget and backing of the management team to secure data and applications in the microservice architecture. Figuring out how to transition security from a business agility blocker to that of an enabler requires a mastery of traffic flows, inspection and enforcement points and automated incident-severity measures, to name just a few considerations. Only then will organizations be able to redefine roles and responsibilities.

There is no one practice that is common in organizations. As the application development process evolves, the business division or team that manages application security varies.

- **CISOs/IT security teams** — If applications are compromised, these are the teams that will likely take the brunt of the blame from management. It seems logical that they should be held accountable for network and application security. But shifts in business drivers mean that traditional IT security is not necessarily involved in how applications are secured.
- **DevOps** — Development teams drive the pace of application delivery and typically do not report to the CISO. Their work is driven by operational requirements, and meeting customer needs is their priority.
- **Development, security and operations (DevSecOps)** — Many organizations are implementing DevSecOps teams to work in conjunction with DevOps. These professionals focus on integrating security practices within the DevOps process, which support the continuous delivery pipeline. In the interest of speed, "good enough" security policies may be acceptable.

[14]https://dzone.com/articles/microservices-journey-from-netflix-oss-to-istio-se
[15]https://www.netsolutions.com/insights/why-do-great-product-companies-release-software-to-production-multiple-times-a-day/

In Radware's *2019 State of Application Security Research* report, organizations indicated an adjustment of roles and responsibilities to cope with both the agility and security requirements of the microservice architecture. However, defining and refining processes and practices are far from optimized, which is good news only for hackers.

The positive sentiment about the security of microservice and serverless environments by their nature — especially for DevOps — leads to an "after the fact" approach, allowing for unmonitored east-west traffic, redundant distribution of SSL certificates and conventional security solutions that fall behind the velocity of changes that applications undergo.

Security Professionals Feel the Heat

Respondents to the Radware global survey generally understand that the move to public cloud environments brings added security concerns. Only one of 10 feels that the data is more secure in the public cloud environment. Two of five respondents said that they use multiple cloud environments. Forty-two percent indicated that they feel somewhat prepared to safeguard data and applications running in the public cloud. Yet 59% also said that their data is less secure in the public cloud (with 30% willing to take the risk because other benefits, such as agility, outweigh the security issues).

Gaining Visibility Going Forward

Expect the move to public cloud environments and the use of distributed architectures to continue for the development and hosting of applications. What can security professionals do now to both align their function with business priorities and ensure that data and applications are secure in the microservice architecture?

1. **Adopt a risk management mindset that prioritizes business drivers to shape security mitigation policies.** A "security at all costs" approach is likely to generate an unacceptable level of false positives and erroneously impact customers' experiences with the applications. Security should follow the same development timeline as product development.

2. **Establish clarity about roles for application security.** Clear accountability empowers the right teams to take responsibility for decisions about the acceptable level of risk and strategies to protect applications.

3. **Focus on implementing a security solution that provides one consistent point of visibility across all network environments, both public and private.** Reliance on solutions offered by public cloud vendors leaves blind spots in the security posture, which attackers can exploit.

4. **Select a security solution that fits the ecosystem already in place without requiring adjustments, such as changing how traffic is routed, the submission of SSL certificates or the alteration of IP addresses.**

5. **Take advantage of the open-source nature of cloud-native applications to aggregate telemetry information about traffic volumes, consumption of applications, performance issues, geographic distribution of users and the nature of data being processed.** Use the information to analyze behavior to get better visibility about what is happening across all platforms.

6. **Secure the channels through which the applications are being delivered.** That means protecting APIs and web and mobile services from attack vectors such as protocol manipulation, data manipulation in servers, and session and credential attacks.

7. **Deliver a security posture that is scalable and elastic to adapt to changing business needs.** Automate the monitoring and mitigation of attacks everywhere in the ecosystem to support the continuous deployment process for applications.

Balancing Business Needs and Security Demands

When applications are the heart of a business, reacting quickly to market opportunities and maintaining the right security posture become a balancing act. Microservice architectures are desirable because they enable more agile continuous deployment models. At the same time, they introduce new security challenges.

Security solutions, which flexibly adapt to their organizations' need for speed in the continuous delivery of applications, are required.

Getting Ready for 5G & IoT

It was the best of times, it was the worst of times, it was the age of 5G networks, it was the beginning of a new threat landscape the likes of which have never been faced before.

The commercial rollouts of 5G networks beginning in 2020 set up a tale of two prospects, a story full of twists and turns that would surely delight Charles Dickens.

1. The promise of blazing fast data speeds and lower latency services on mobile networks that enable large-scale deployment of IoT devices

2. The certainty of new attack vectors launched through the vastly expanded number of access points in 5G networks' distributed architecture

5G technology forever changes expectations for the mobile network experience. All traffic is in the cloud, and computing elements and services are closer to the edge of the network, which improves performance and makes it easier for service providers to scale services. The 5G infrastructure is ideal for the deployment of IoT devices because it can handle massive amounts of data with very low latency from mobile connections.

Network performance improvements and IoT capabilities promise to help businesses move even faster to create value for customers by taking advantage of productivity gains and new market opportunities. Yet uncertainty about this new technology is prevalent.

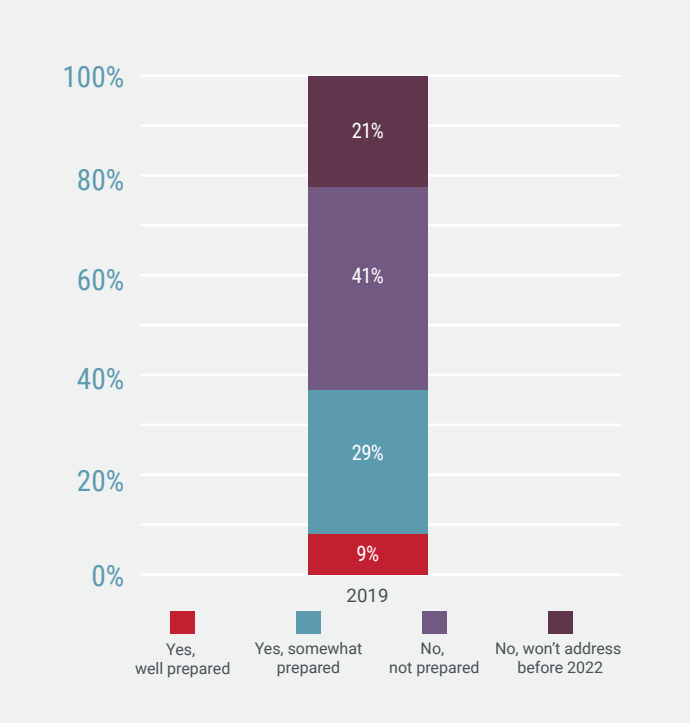


Figure 28. Enterprises' preparation for 5G network rollouts.

The majority of respondents indicated that they are not prepared for 5G network rollouts in their countries. Companies in APAC and EMEA were more likely to say that they are at least somewhat prepared compared to organizations in Latin America. Service provider/telecom companies were more likely than any other vertical to say that they are prepared to handle 5G rollouts (58% vs. 16%–34%), although 13% said that they won't address 5G before 2022.

The distributed architecture of 5G networks introduces a whole new set of security threats. In particular, IoT devices typically have low security measures embedded at endpoints, making them ideal launch points for coordinated malware attacks by botnets within and outside networks.

Thirty-eight percent of respondents said that they don't know if they have experienced DDoS attacks originated by IoT botnets. Lack of visibility by enterprises into attack surfaces could spell trouble in the future when 5G networks are more prevalent.

Ready or Not

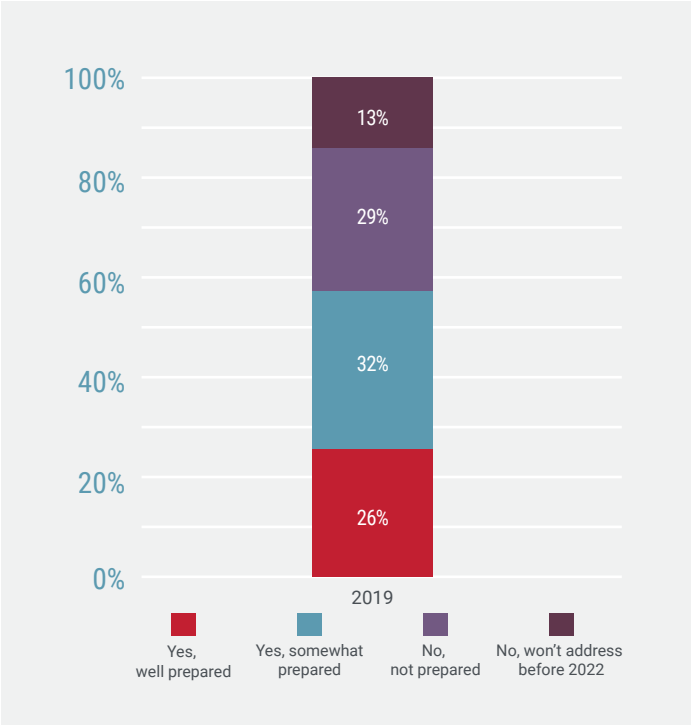


Figure 29. Service providers' preparation for 5G network rollouts.

Service providers are further along in their preparations for 5G than enterprises. Fifty-eight percent of service provider respondents indicated that they feel prepared for the 5G rollout, compared to 38% of total respondents. Since service providers are the entities that are actually deploying 5G networks, it makes sense that respondents from this group are further ahead in their comfort level with the changes that the technology will bring.

The difference in confidence levels points to an opportunity for service providers to educate enterprise customers about the benefits of 5G as well as what the changing threat landscape means for their businesses.

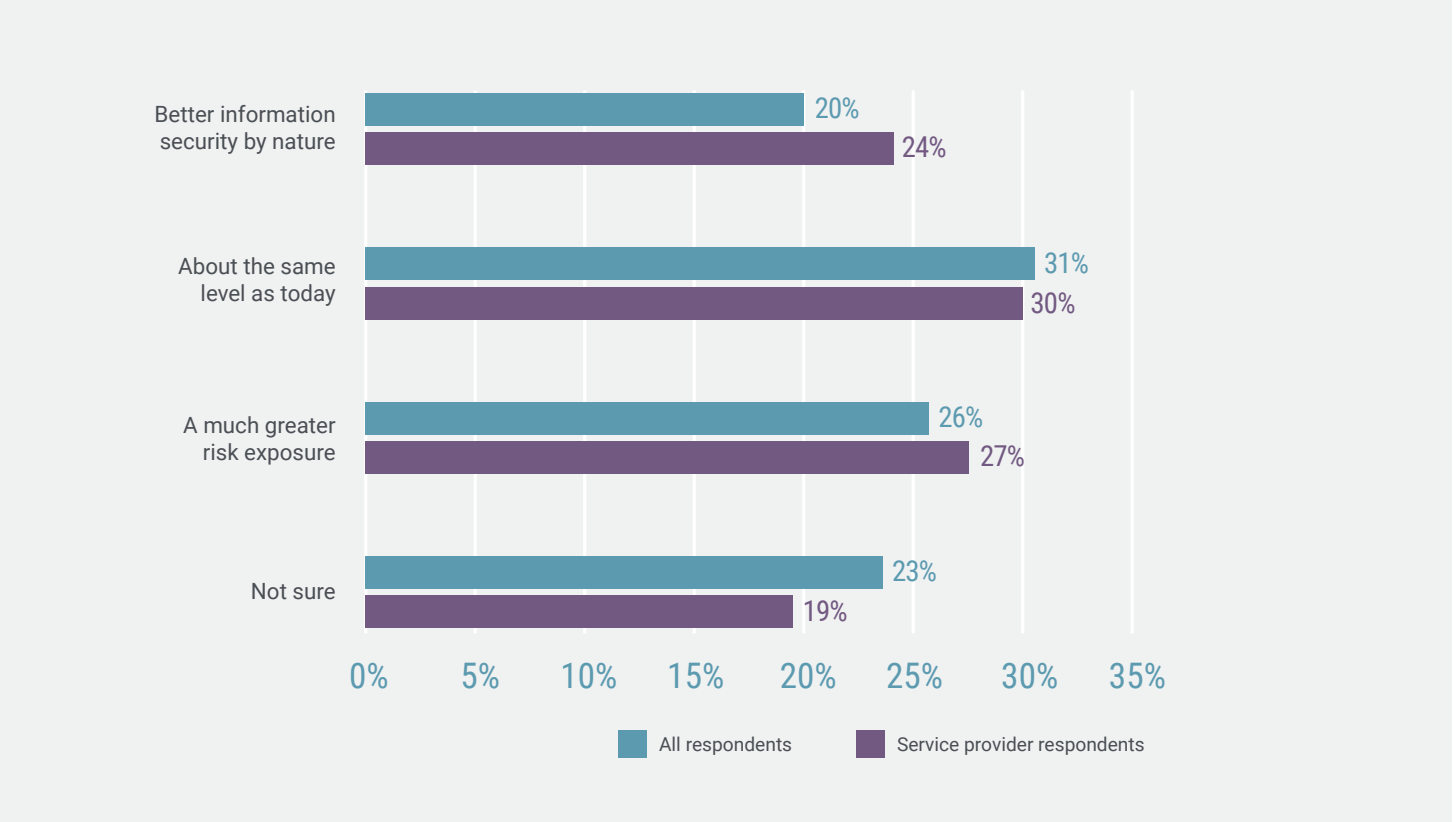


Figure 30. Anticipation of 5G security levels.

Respondents understand that the distributed nature of 5G networks changes the threat landscape but are fairly evenly split about the level of risk that the new technology introduces. Service providers' answers about the impact of 5G on security levels are similar to the overall survey results from all respondents.

The Impact of IoT Devices

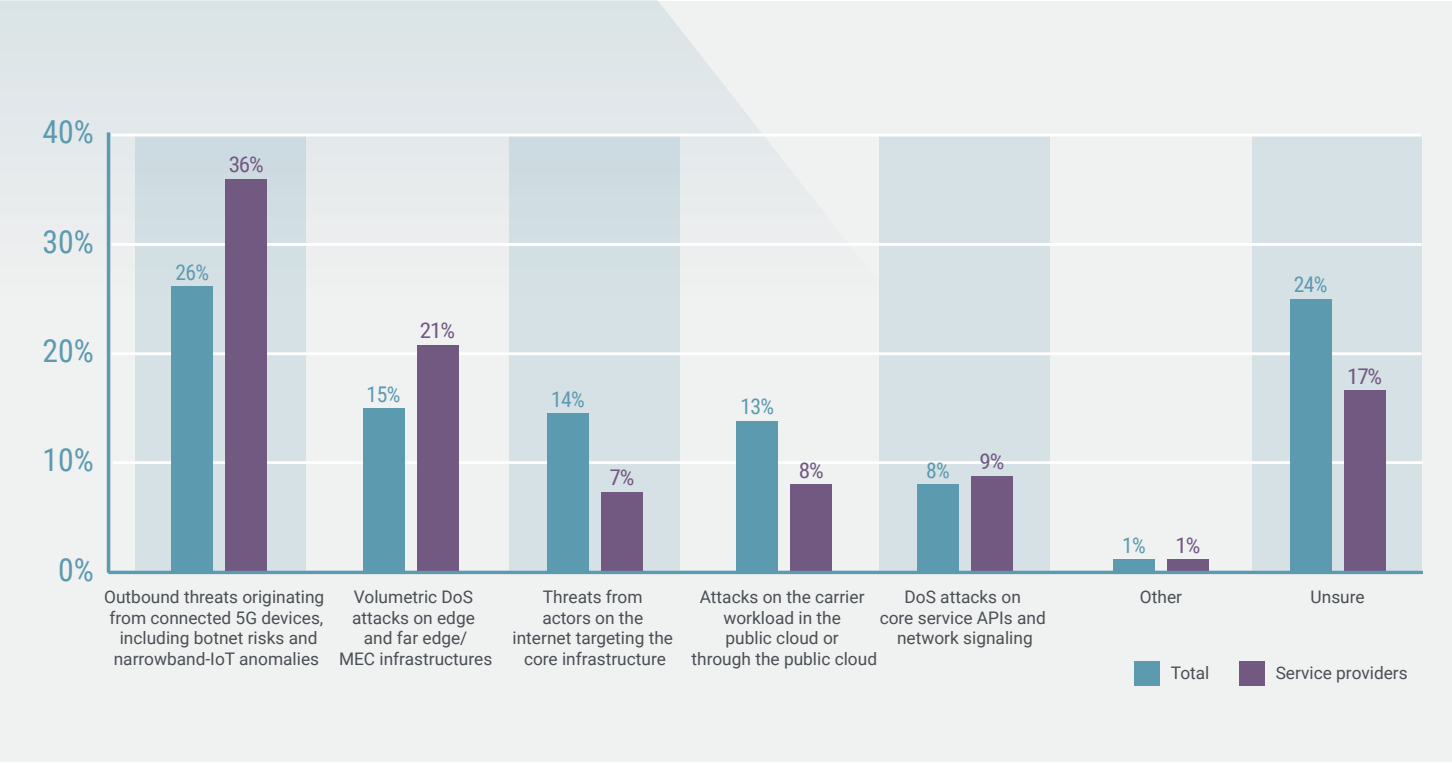


Figure 31. Perception of the greatest IoT threats.

Enterprises are concerned about outbound traffic generated by connected devices as well as network elements at the edge of the network. In the global industry survey, 36% more service provider respondents vs. all respondents see outbound threats originating from connected 5G devices as the greatest risk of 5G technology.

Yet organizations are eager to take advantage of IoT devices. International Data Corporation (IDC) estimates that, by 2025, there will be 41.6 billion connected IoT devices generating 79.4 zettabytes (ZB) of data.[16]

[16]https://www.idc.com/getdoc.jsp?containerId=prUS45213219

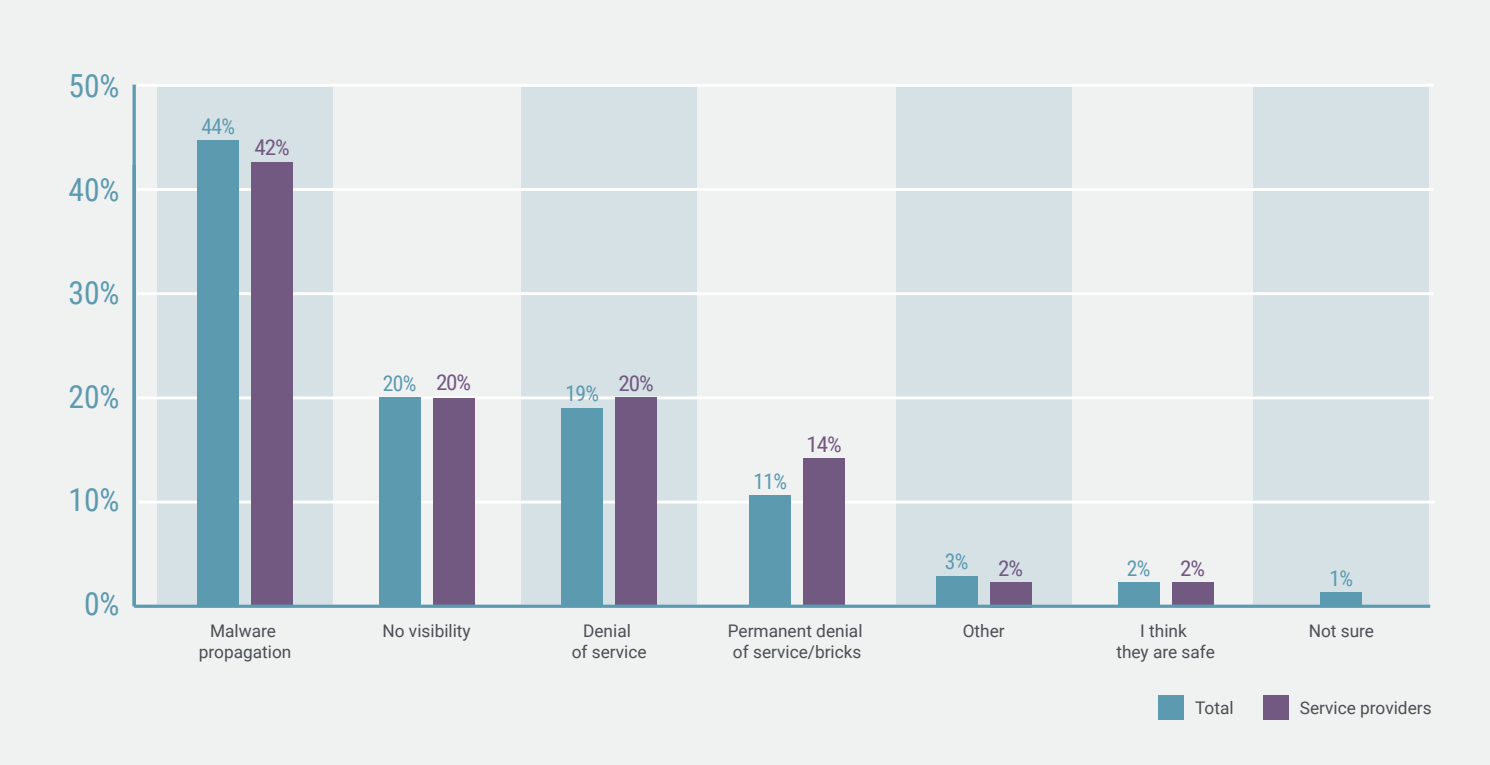


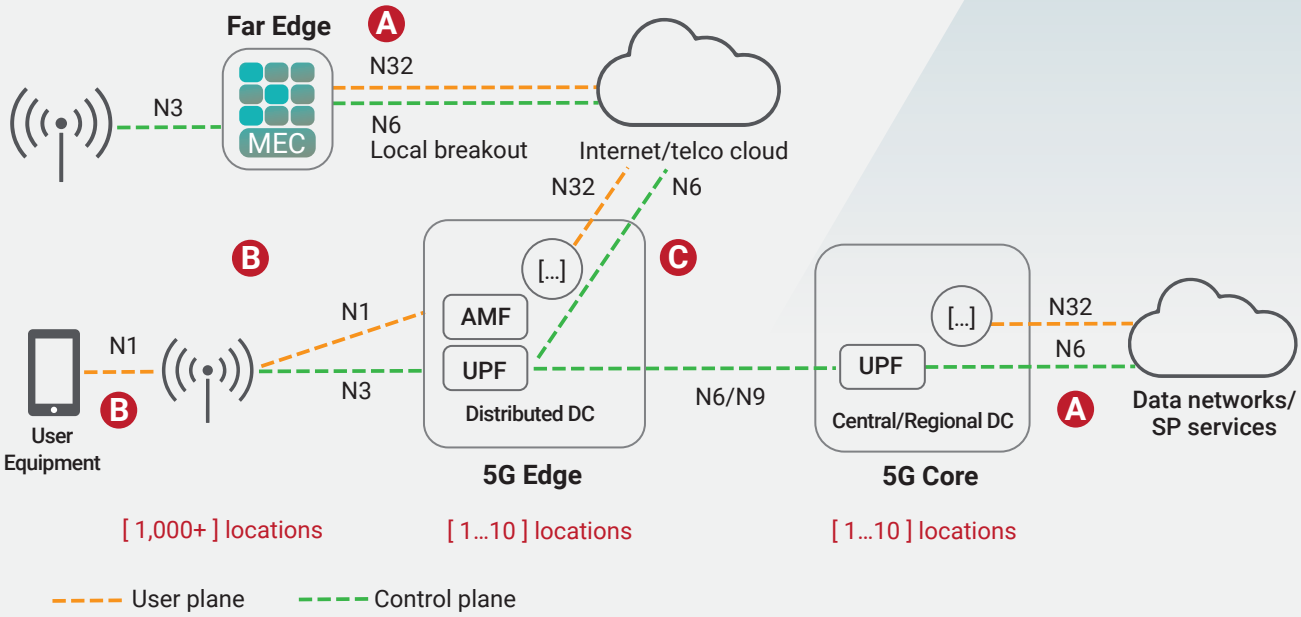
Figure 32. Perception of the greatest IoT security risks.

When it comes to IoT connected devices, respondents are most worried about malware propagation (44%), followed by no visibility (20%), denial of service (19%) and permanent denial of service/bricks (11%).

These concerns are warranted. IoT devices have no standard of security built in. The emphases in the development of this equipment are data collection and price sensitivity for production and sales. The burden of the security vulnerabilities is something that enterprises have never had to deal with before.

Enterprises may assume that service providers will provide protections for IoT device security in the network.

For service providers that already need to protect their own network assets against threats launched from IoT devices, offering 5G security as a managed service is a possible incremental revenue opportunity.



- A Inbound attacks from the internet targeting the core network
- B Distributed applications and APIs on the mobile edge from third parties or other service providers
- C The core network from the access network where infected mobile and IoT devices can be harnessed into a large-scale bot attack entering the network from the radio access network (RAN)

Figure 33. Network infrastructure protection plan.

Taking the Good With the Bad

To protect against 5G security threats, service providers must implement solutions to safeguard these protection points in the network infrastructure.

Because of its distributed nature, the deployment of 5G networking infrastructures is dramatically different than that of previous generations of mobile networks. Network functions are virtualized, so services can expand beyond service providers' networks to external network domains to be physically closer to connected devices for more efficient delivery. Faster data speeds and lower latency combine to enable a whole new world of possibilities for service providers and enterprises.

But the increased size of the attack surface and susceptibility of IoT connected devices will require both service providers and enterprises to quickly get up to speed on new security requirements. Gaining visibility into what is happening at all access points is critical for protecting 5G networks.

In an already tight labor market for security professionals, finding talent that has the expertise to lead 5G-related initiatives is challenging. Instead, enterprises will likely turn to service providers to offer security measures for inbound traffic from the internet.

2020 Cybersecurity Predictions

Organizations are eager to accelerate the pace of digital transformation as a means to boost their abilities to adapt to rapidly evolving market opportunities. Every step forward seems to add to the complexity of securing networks, data and applications.

Radware network security experts predict what to expect in 2020.

1.THREAT LANDSCAPE:

The Resurgence of Amplification Attack Vectors

As cyberdefenses improve, attackers respond in kind. We have reached a point where volumetric attacks are required to critically impact most targets. In 2020, expect to see cybercriminals refine tactics, techniques and procedures (TTPs) to generate amplification effects that result in volumetric attacks.

2. MASSIVE SOPHISTICATED BOTNETS ARE COMING TO THWART ELECTIONS AND E-COMMERCE:

With APIs becoming the main information corridor between applications, threat actors will use bots to target APIs. Bots will get smarter and be able to sense mitigation techniques automatically and then shift techniques between attack vectors. The rapid proliferation of IoT devices will continue to fuel the formation of massive botnets, which are often used by malicious groups such as nation-states (for example, in social networks for espionage and propaganda) and organized crime (theft/financial gain). Furthermore, threat actors will have greater access to these tools as they become less expensive and more commonly available.

3. PUBLIC CLOUD:

Multicloud Strategies Grow Even as Threats Increase

Enterprises will continue to move their applications to the public cloud but do not want to be locked in with one vendor. Instead, they will use multiple cloud service providers to negotiate better fee structures and reduce the risk of service outages affecting business operations. This strategy exponentially increases the size of the attack surfaces in which hackers can search for vulnerabilities, knowing that organizations are challenged to maintain consistent security across multiple public cloud environments. We expect news of major application breaches to make headlines in 2020, but the benefits of this approach outweigh the risks and will not slow adoption of the public cloud.

4. APPLICATION SECURITY:

Microservices and Speed of Business Reduce Visibility Into the Attack Landscape

As more organizations employ microservices for application development and hosting, new vulnerabilities and threats will emerge. Because applications are disaggregated across a distributed architecture, protecting east-west traffic flows inside the network will become a larger concern than defending north-south traffic flows from external entities. In 2020, we expect a rash of hacks on applications via east-west flows, attacks on APIs and testing of vulnerabilities in Kubernetes. The priority for continuous deployment of applications will continue to take precedence over traditional IT security protocols in the interest of faster time to market. DevSecOps will take a higher profile as the function responsible for successful attacks and data breaches as both its authority and budget for application security increase. New privacy legislation will also reduce visibility into data transactions.

5. 5G ROLLOUTS:

Progress Showcases IoT Device Vulnerabilities

Commercial rollouts of 5G networks in 2020 will finally enable the organizations to take advantage of IoT devices that leverage the network performance improvements and lower latency of the new technology. Expect to see a successful takedown of a high-profile network and applications with an attack launched through IoT devices connected to a 5G network.

6. AUTOMATION:

Fighting Fire With Fire

Artificial intelligence (AI) and machine learning are reaching a tipping point where we will see these technologies underpinning many other technologies and solutions that automate some business operations. Hackers will continue to look for ways to poison the decision-making algorithms that guide AI and machine learning to create new attack surfaces. From a security perspective, we expect machine learning to move beyond identification of new threatening behaviors to the automated tuning of security policies to reduce human errors and enable organizations to redeploy security engineers from production networks to DevSecOps. Enterprises will also seek one holistic view of their security posture across multicloud environments.

Respondents Profile

In fall 2019, Radware conducted a survey of the global security community and collected 561 responses. The survey was sent to a wide variety of organizations globally and was designed to collect objective, vendor-neutral data about issues that organizations face while preparing for and combating cyberattacks. Respondents' profile information is listed below.

What Is the Scope of Your Organization's Business?

Worldwide	43%
Regional	12%
Country	45%

Figure 34. Geographic scope of business.

In Total, How Many Employees Work in Your Organization?

# OF EMPLOYEES	% OF RESPONDENTS
50–499	29%
500–999	12%
1,000–2,999	16%
3,000–9,999	16%
10,000 or more	27%

Figure 35. Number of employees in the organizations surveyed.

Which Best Describes Your Organization's Industry?

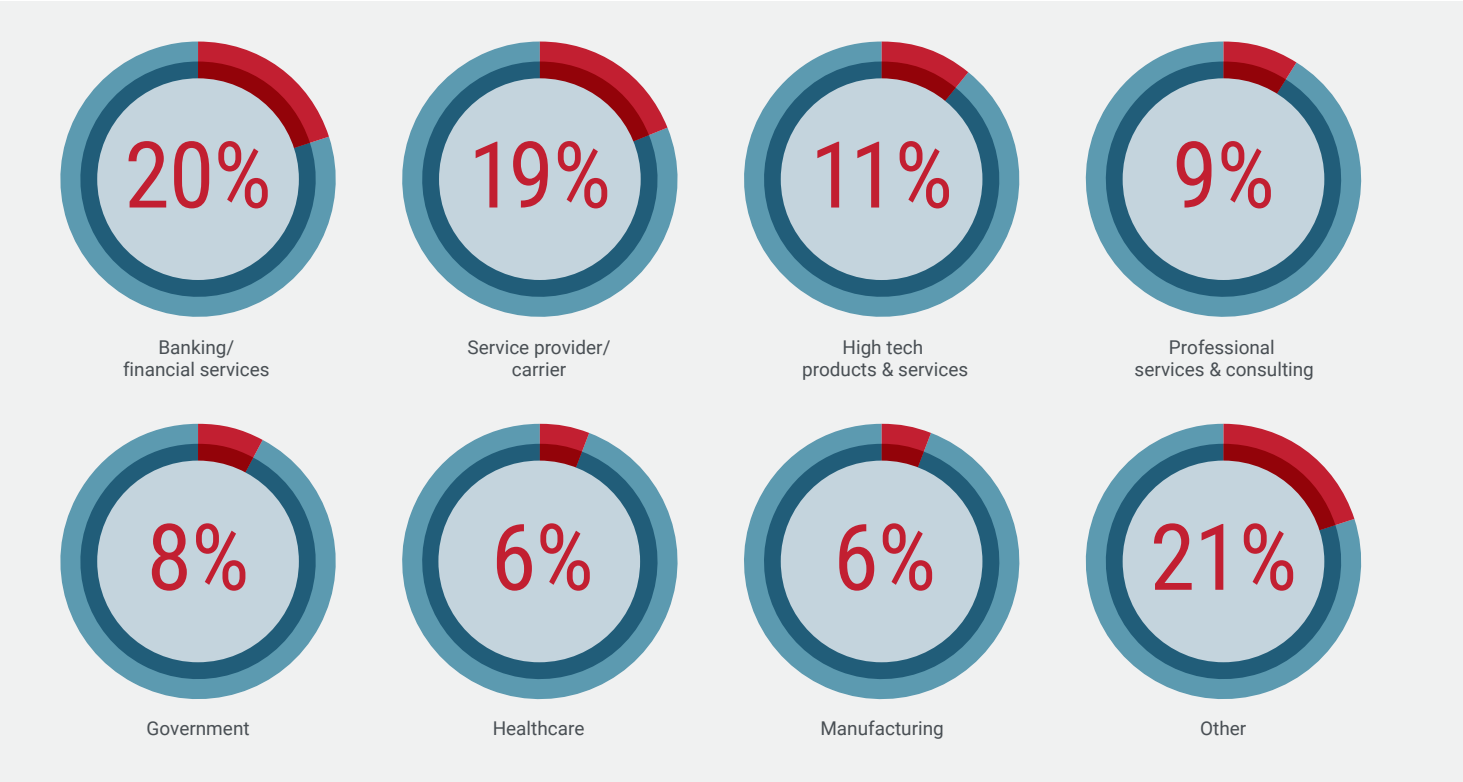


Figure 36. Industries represented.

Which Best Describes Your Rank Within Your Organization?

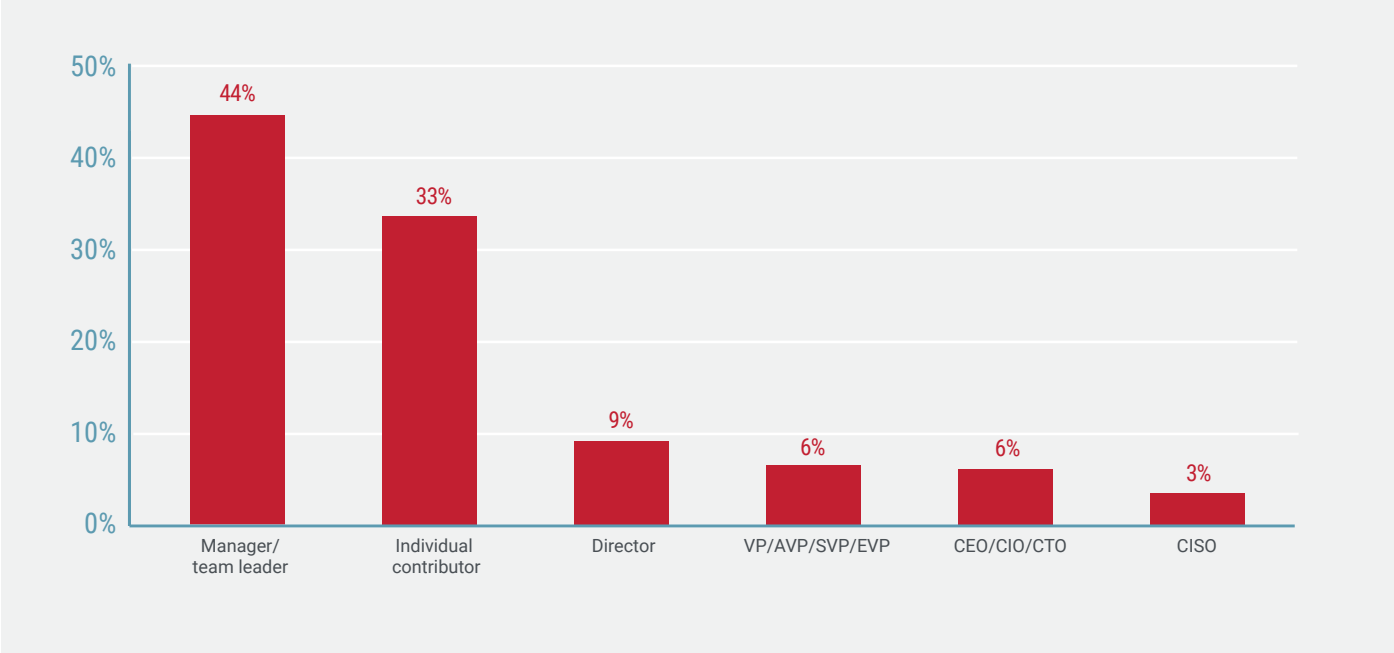


Figure 37. Respondents' rank within their organizations.

Credits

CONTRIBUTORS

Michael Groskop
VP, Portfolio Management
Radware

Nissim Pariente
VP, Security Analytics
Radware

Louis Scialabba
Director, Carrier Solutions Marketing
Radware

Eyal Arazi
Manager, Security Product Marketing
Radware

Daniel Smith
Security Researcher
Radware

PROJECT MANAGEMENT

Carolyn Muzyka
Director, Marketing Communications
Radware

Laura Ann Tillotson
Manager, Marketing Communications
Radware

Colin Beasty
Manager, Global Strategic Marketing
Radware

EDITORS

Deborah Szajngarten
Director, Public Relations
Radware

Ben Zilberman
Manager, Security Product Marketing
Radware

EXECUTIVE SPONSORS

Michael O'Malley
VP, Corporate and Strategic Marketing
Radware

Shira Sagiv
Head of Portfolio Marketing
Radware

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

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