Application Security In A Multi-Cloud World 2023

Executive Summary

The "great cloud migration" is looking different than how it was originally touted, with few organizations hosting all their applications exclusively on public cloud platforms. Almost all operate a hybrid infrastructure mixing public cloud, private cloud, and on-premises environments. While that mix continues to change and morph—a dynamic that raises security concerns by itself—security threats against applications are increasing in frequency and severity. Compounding these threats is alarmingly low organizational preparedness for multi-cloud security, poor visibility into security weaknesses of their own APIs (as well as third-party APIs and code), and insufficient protections against application DDoS attacks.

Comparative year-over-year data cited in this report is drawn from Radware's 2022 report entitled Application Security in a Multi-Cloud World 2022

Key Takeaways

Important findings from this research include:

- **Consolidation of public cloud environments**
  Last year, many organizations quickly expanded to three, four, and even five cloud environments. This year, many have scaled down their number of public cloud environments to a more manageable figure.
- **Increased concern about multi-cloud security**
  Organizations are increasingly concerned about the risks of multi-cloud security. Compared to the 2022 results, we see a sharp increase in concerns around multi-cloud consistency, visibility, and protection coverage.
- **Cyberattacks against applications happening more frequently**
  All types of attacks against applications have increased in frequency over the past 12 months, with an average of 41.5% of respondents seeing the four types of attacks daily or weekly. This is up from an average of 29% last year: a 43% increase.
- **APIs are more important and increasingly difficult to protect**
  Organizations are using internally developed APIs more, and these are increasingly important to the success of the company. However, organizations face growing gaps in documenting those APIs and have low confidence in the security of their APIs.
- **Third-party APIs and code represent a worsening threat vector**
  99% of organizations use web applications with third-party APIs and code that are executed directly in a browser. However, organizations lack visibility into what third-party code is used by their web applications, when it is updated, what threats exist, and whether the third-party code is taking malicious actions.

Attacks against applications have increased in frequency over the past 12 months, with an average of ***41.5%*** *of respondents seeing four types of attacks daily or weekly.*

About This Report

Radware commissioned Osterman Research to conduct a survey in multiple global markets to understand how organizations are navigating the challenges of application security in an environment spanning multiple public clouds, on-premises infrastructure, and private clouds. Details on the survey methodology are included at the end of this report.

Changing Multi-Cloud Dynamics

Organizations are using a changing mix of environments for hosting applications. In this section, we examine this mixture and the associated security posture, challenges, and threats.

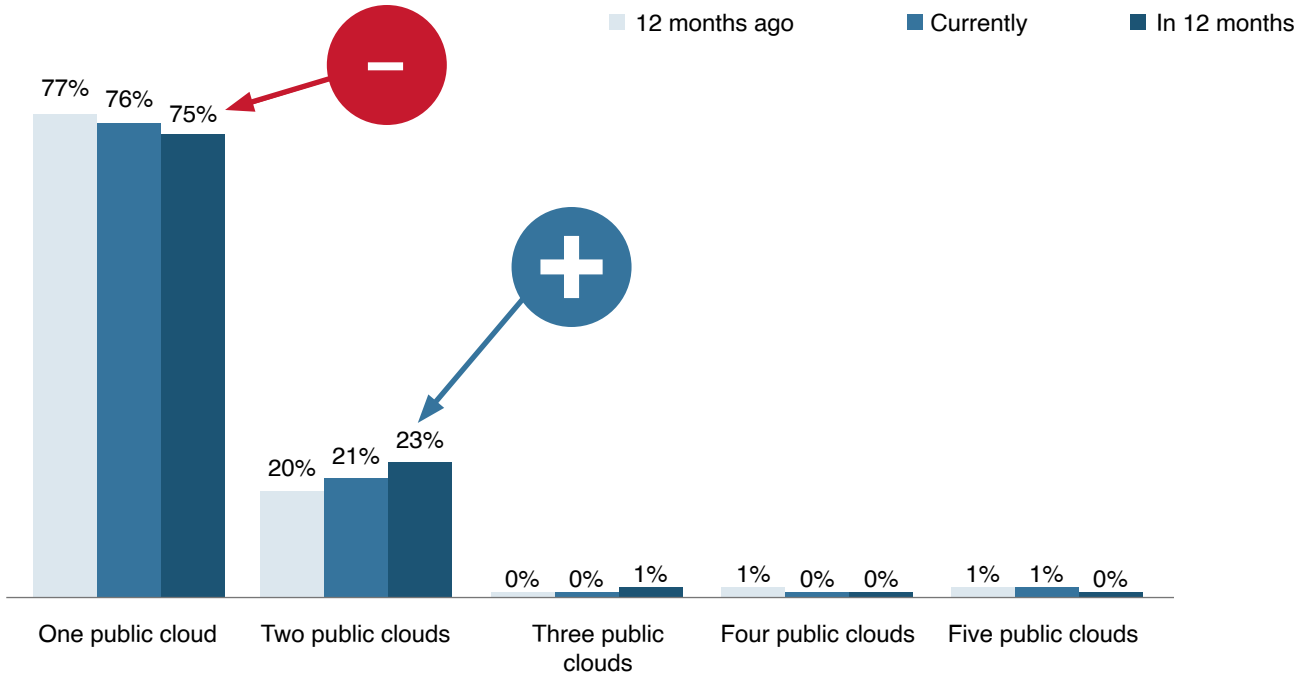
Public Clouds for Hosting Applications

Organizations are refactoring their public cloud strategy, retrenching from more to less for hosting applications. Virtually all organizations in this year's research are using only one or two public clouds, with only 1% using three or more. There is a shallow trend line between organizations using one public cloud and two, with the use of one public cloud declining year-over-year and the use of two public clouds rising.

Compared to last year's results, we see a clear trend of organizations consolidating around one or two public cloud environments, moving away from extensive usage of three, four or five clouds. From a numerical perspective, the drive to reduce cloud environments can be due to strategic vendor consolidation, as well as reducing unwanted variation introduced from earlier merger or acquisition activity. From a security point of view, relying on fewer public cloud services streamlines ongoing security considerations because the scope of the problem space is less. From a functionality perspective, on the other hand, consolidating to fewer platforms could result in innovations introduced on one platform being unavailable on another, hampering service delivery. If cloud platforms are easily interchangeable commodities, reliance on fewer is a strategically sound direction. But when this changes again, organizations finding themselves trailing their competitors will reengage afresh with multiple cloud platforms. Expect this to remain a dynamic situation.

99% of organizations are using one or two public cloud services; few use three or more.

Figure 1: Use of Public Clouds for Hosting Applications
Percentage of respondents



Source: Osterman Research (2023)

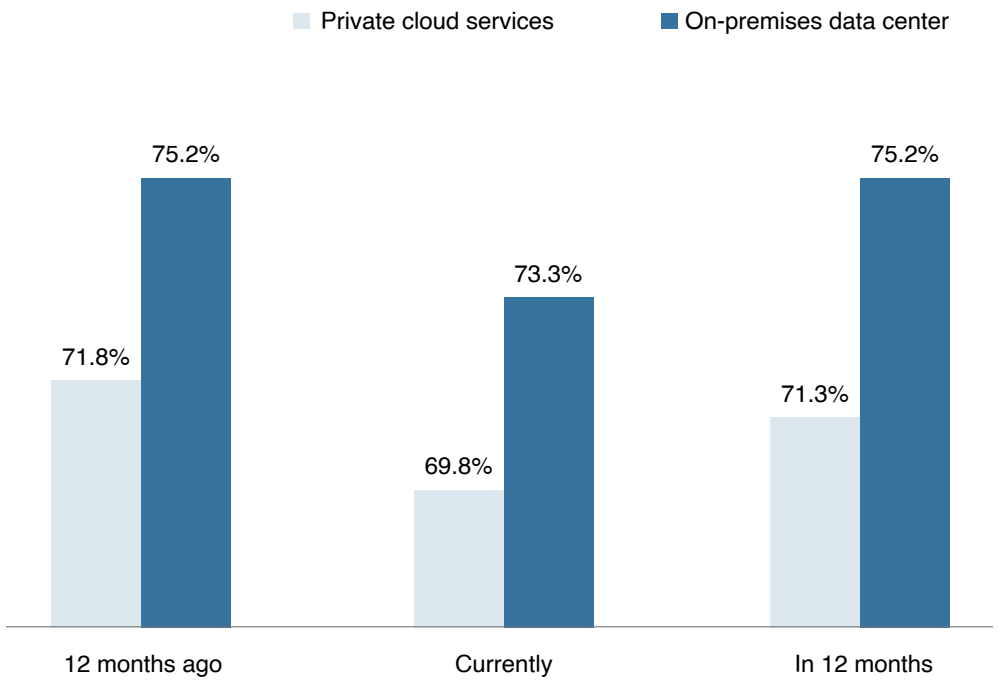
Organizations Still Reliant on Private Clouds and On-premises Data Centers

While every organization relies on at least one public cloud platform, around seven out of ten also use private cloud services and on-premises data centers for hosting applications. The ongoing reliance on more than public cloud services appears to be strategic, not tactical. There is a rebound evident for both types of environments for hosting applications (see Figure 2 below), with the declining usage over the previous 12 months for each expected to reverse over the upcoming 12 months. Organizations that have attempted to migrate away from private cloud services and on-premises data centers to the public cloud appear to have not met their objectives—and are reversing course.

This shows that while there is much talk about “the great cloud migration” and the abandonment of on-premises environments, not only do most organizations still use these environments but they expect usage to increase.

Organizations are embracing public cloud in combination with private cloud and on-premises data centers; it’s additive, not reductionist.

Figure 2: Hosting Applications on Other Environments
Percentage of respondents



Source: Osterman Research (2023)

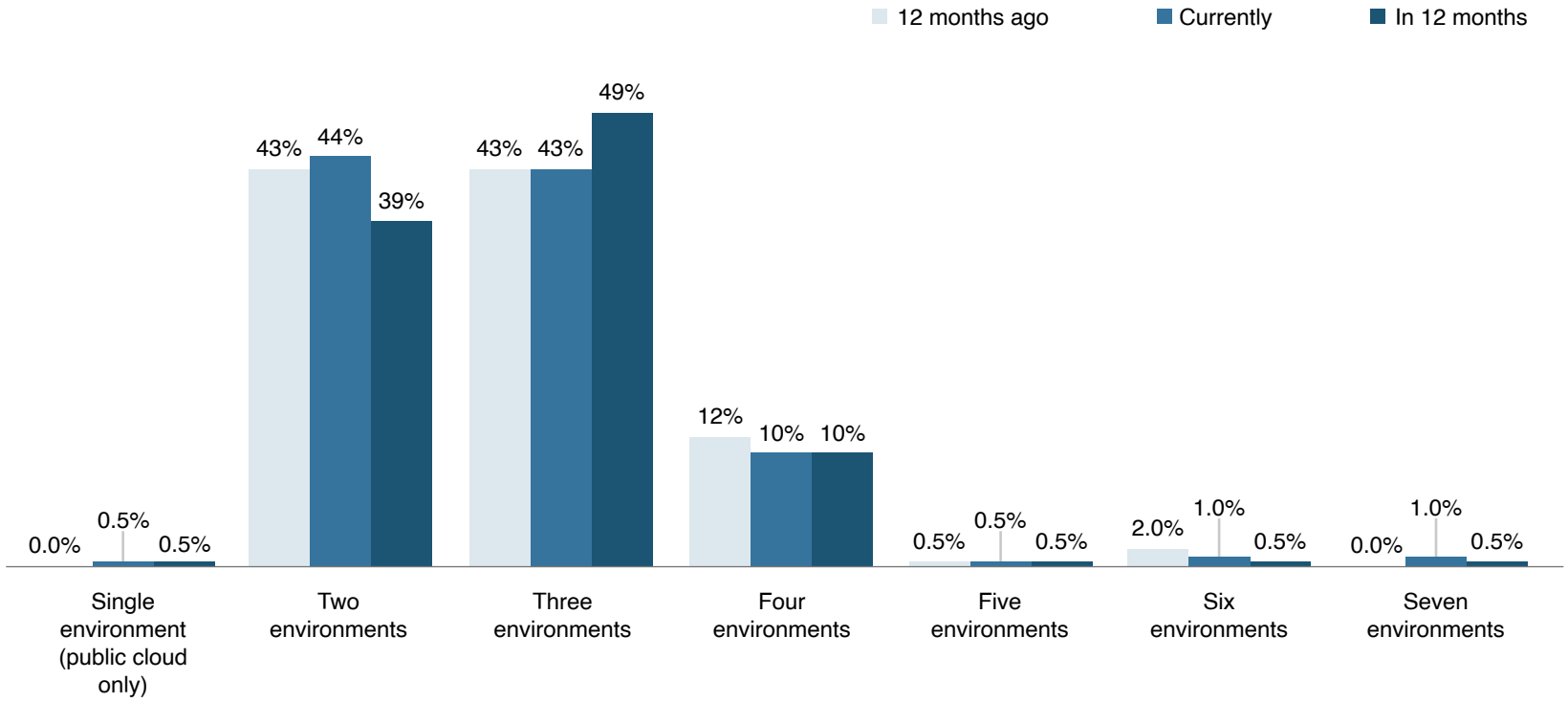
Combined Infrastructures in 2023

Most organizations use multiple disparate environments for hosting applications—after combining usage of public cloud, private cloud, and on-premises data centers.

- **Most use two or three environments, in various combinations**
  87% of organizations currently use any combination of two or three environments—public cloud (one or more), private cloud, and on-premises data centers. In 12 months, this will increase slightly to 88% of organizations, with the growth in three environments provided by the reduction in two.
- **Almost half use the triple infrastructure strategy**
  46.4% of organizations use all three environments in parallel, creating a complex situation where strong capabilities for cross-environment administration, management, and security are essential.
- **When it's only one, it's always public cloud**
  Less than 1% of organizations use a single environment for hosting applications. For those that do, it is always public cloud. This is an uncommon pattern, however.

87% of organizations currently use any combination of two or three environments—public clouds (one or more), private clouds, and on-premises data centers.

Figure 3: Multiple Environments for Hosting Applications
Percentage of respondents



Source: Osterman Research (2023)

Threats Against Apps on Public Cloud Platforms

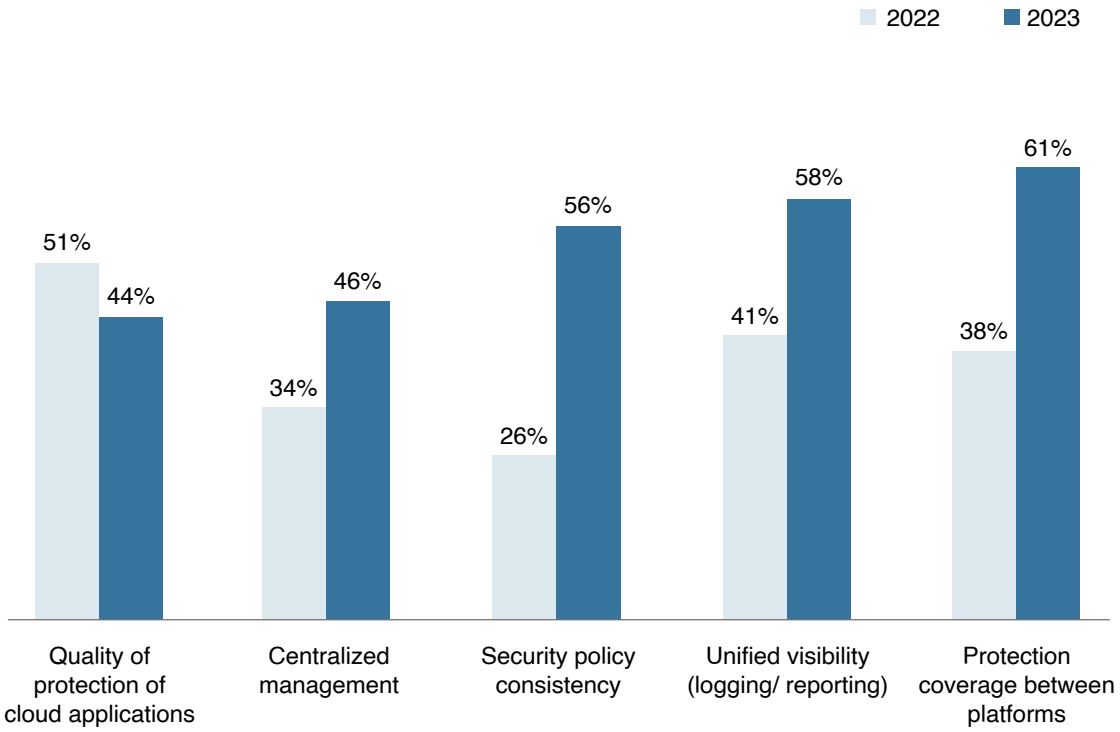
When organizations use multiple platforms for hosting applications, the capabilities available to them for securing applications are intensely important. And when available security capabilities are deficient, security posture is threatened.

Respondents assessed four out of five threats as getting progressively worse this year compared to last year, with the inability to achieve consistent security policies the problem that has grown the most. Inconsistent security policies increase the likelihood of data breaches and unauthorized exposure when threat actors probe for systemic differences to exploit across cloud services.

Compared to last year's results, we see a marked increase in concern over various aspects of public cloud security, particularly on the issues of security policy consistency, centralization, and unified logging and reporting (see Figure 4).

Compared to last year, the number of respondents who said inconsistent security policies are a big problem for applications on public cloud platforms grew by 112%

Figure 4: Assessing Threats Against Applications on Public Cloud Platforms
Percentage of respondents indicating “problem” or “extreme problem”



Source: Osterman Research (2023)

Web Application Protection

Attacks Against Applications are Happening More Often

The frequency of four types of attacks against applications—bot, application, API, and DDoS—has increased over the past 12 months, with an average of 42% of respondents experiencing attacks on a daily or weekly basis. This is up from an average of 29% in 2022—a 43% year on year increase.

Most of the growth in the daily and weekly attack cadence has been at the cost of the yearly and never-attacked cadence, which declined from an average of 30% for each of the four attack types in 2022 to an average of just 12% in this year's research.

Almost all organizations are regularly experiencing bot attacks, with only 2% of organizations this year claiming to experience a yearly or never-attacked cadence, down from 34% last year.

Bot attacks are the most frequently seen attack type on the daily, weekly, and monthly cadence. Over the past year, application attacks have become the most frequently occurring attack on the daily cadence—jumping from 4% in 2022 to 22.8% this year.

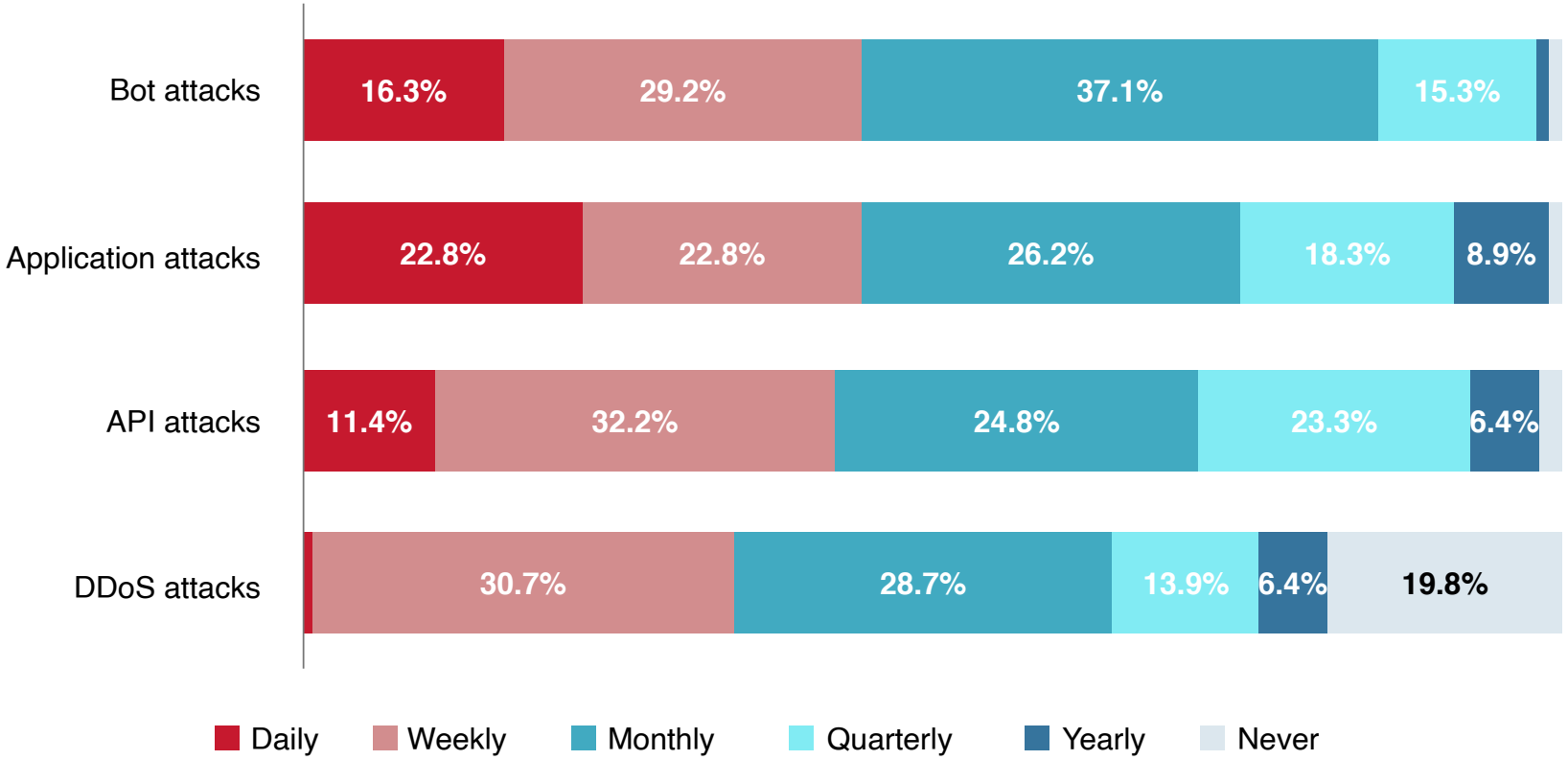
API attacks have also seen a sharp rise, with 68% of respondents seeing them on a daily, weekly, or monthly basis, compared to only 55% from last year. Moreover, last year 18% of respondents claimed to have never faced an API attack, whereas this year, less than 2% claimed to have never seen an attack on their APIs.

Another noticeable rise was in DDoS attacks, which saw 60% of respondents being attacked monthly or more frequently, compared to 53% last year.

22.8% of organizations experience application attacks every day, up from 4% last year.

< Prev Next >

Figure 5: Frequency of Attacks Against Applications
Percentage of respondents



Source: Osterman Research (2023)

API Protection

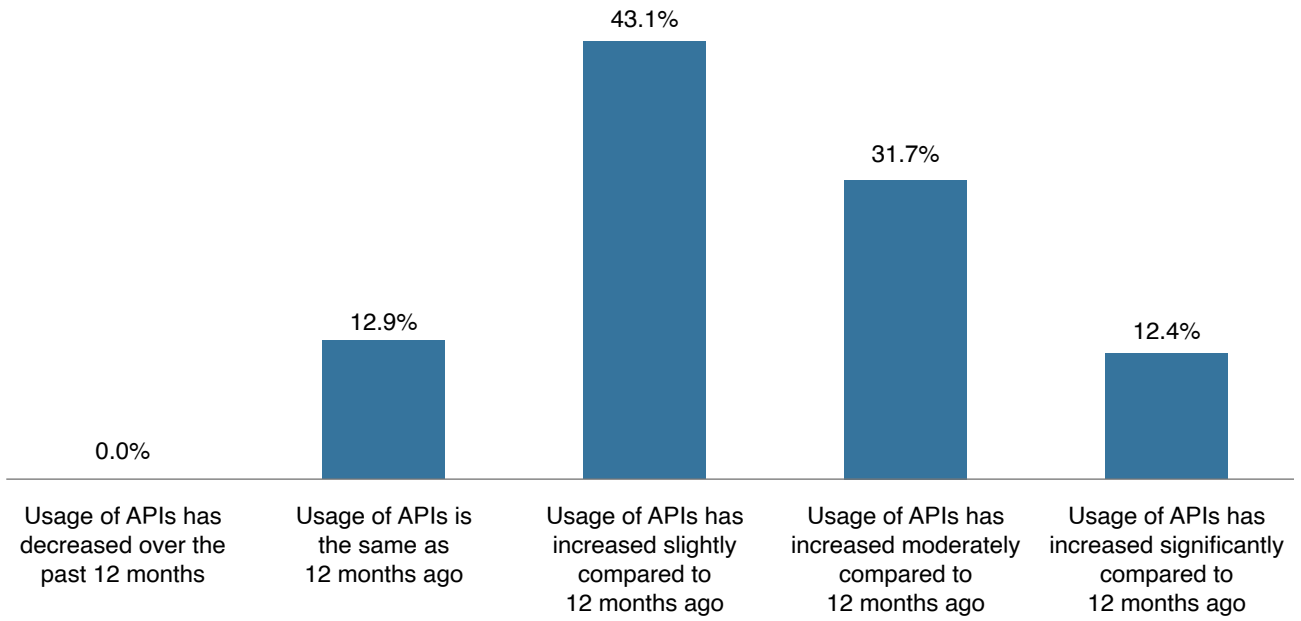
APIs are a fundamental design construct in modern web applications. We look at the usage, importance, and update cadence of APIs developed internally at organizations in this section, along with confidence in API security posture.

API Usage Continues to Climb

Over the past 12 months, more than 87% of the respondents in this research report increased usage of the APIs developed internally at their organization, with almost half (44.1%) reporting the two highest levels of increase. None have seen API usage decline over the previous 12 months. Ongoing dependence on modern application development strategies and methodologies—with an emphasis on microservices and cross-application integration—makes continual and increasing reliance on APIs an almost foregone conclusion.

87.2% of organizations are increasingly developing and using APIs as an essential element of their modern application strategy.

Figure 6: Change in API Usage Over the Past 12 Months
Percentage of respondents



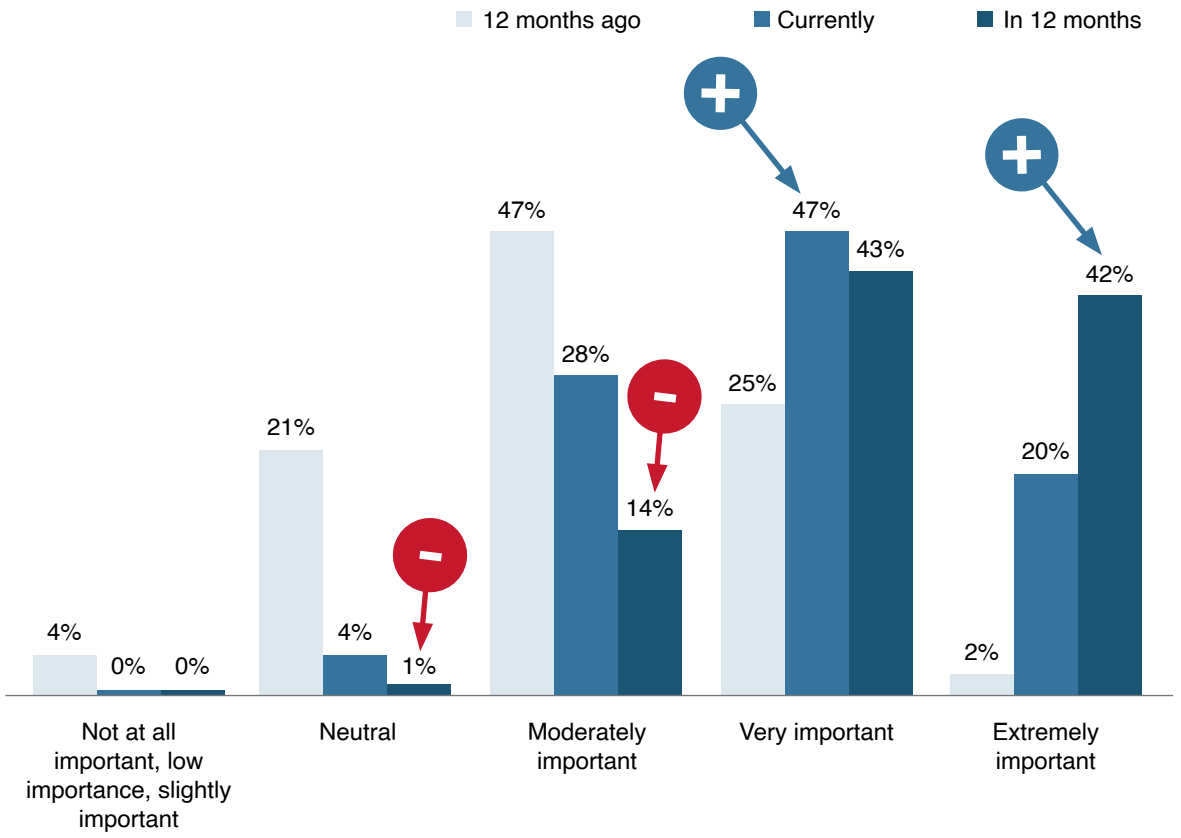
Source: Osterman Research (2023)

APIs Are Becoming More Important to Business Success

APIs have already become highly important to business success—with growth in the two highest levels of importance from 27% to 67% over the past 12 months. The intensity of importance is expected to swing even higher over the next 12 months, with respondents indicating the “extremely important” rating growing to 42%, a 1,580% increase over the 24-month timeframe we queried. With organizations building modern applications and service interfaces for access by internal apps, customers, and supply chain partners, API usage is inextricably tied to core business processes, outcomes, and thus measures of business success.

42% of organizations expect APIs to be inextricably linked to business success in a year—up from just 2% a year ago.

Figure 7: Importance of APIs to Business Success
Percentage of respondents



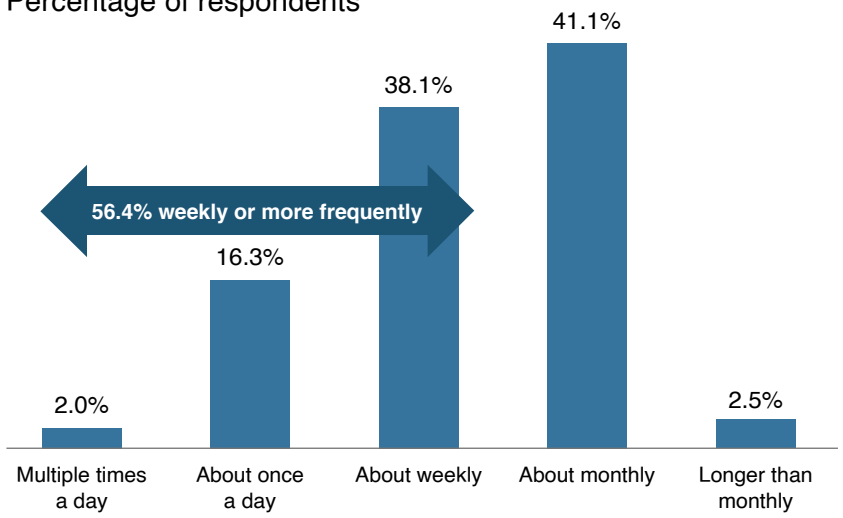
Source: Osterman Research (2023)

Most Organizations Update APIs at least Weekly

Developing APIs is a significant area of investment for organizations, with 56.4% updating internally developed APIs for production usage weekly or more frequently. While this rapid cadence of development and release is essential to stay at the forefront of changing customer demands and to deliver new features, the weekly or more frequently update cadence means new opportunities for data breach and exposure due to coding errors or conflicts between updated components at least 52 times per year. Protecting production APIs from attack is essential, but no less so than ensuring a secure and robust development process to minimize the potential attack scope as new updates to APIs are released.

56.4% of organizations update APIs weekly or more frequently.

Figure 8: Change Cadence for APIs Developed Internally
Percentage of respondents



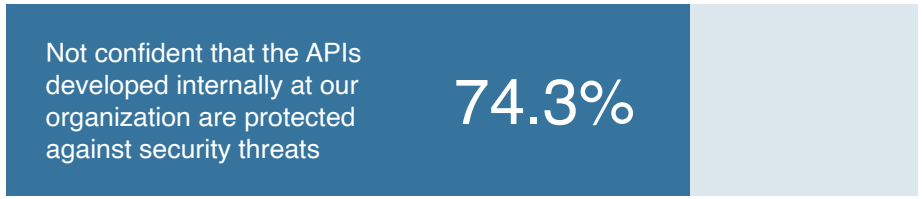
Source: Osterman Research (2023)

Low Confidence in Current API Protections

Three out of four respondents are not confident in how internally developed APIs are protected against security threats that lead to unauthorized data access, exposure of application logic, and data breach. Organizations that maintain up-to-date documentation on their APIs are somewhat more likely to be confident in current protections—because the discipline of maintaining documentation increases the likelihood of understanding the internals of their APIs and thus any unresolved weaknesses. For an application design construct that is increasingly important to business success, insufficient protections are a major warning signal.

74.3% of organizations are not confident that their APIs can withstand security threats.

Figure 9: Confidence in Protecting APIs from Security Threats
Percentage of respondents



Source: Osterman Research (2023)

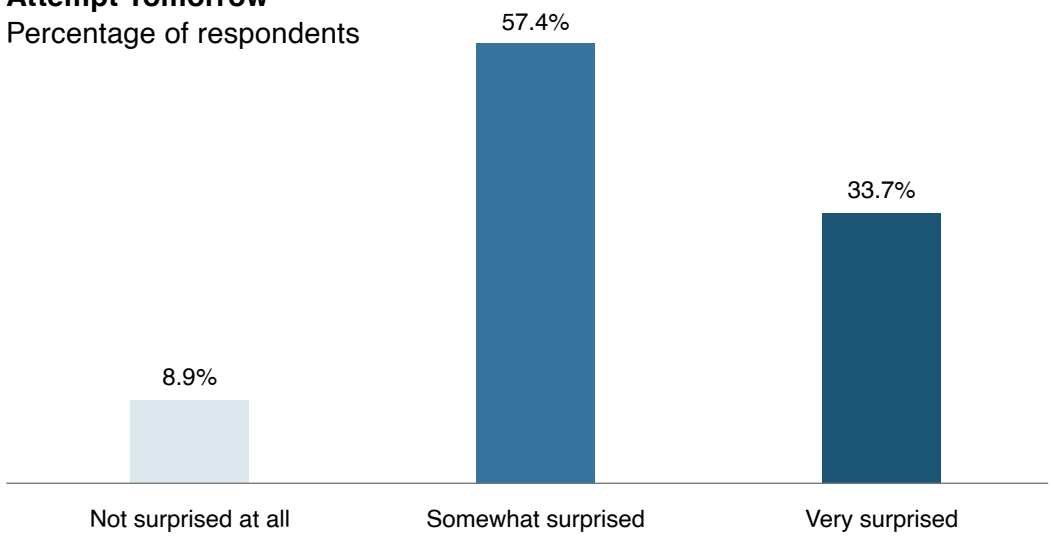
Most Wouldn't Be Surprised by an API Breach

Most respondents know their current protections for internally developed APIs are insufficient to withstand a data breach attempt "tomorrow": 66.3% of respondents would not be very surprised if their APIs suffered a data breach tomorrow.

Of these, most hope their current protections are sufficient but lack certainty (57.4% would be "somewhat surprised"), while some are certain of insufficiency and can only hope for the best (8.9% would be "not surprised at all").

Figure 10: Level of Surprise Due to a Hypothetical Data Breach Attempt Tomorrow

Percentage of respondents



Source: Osterman Research (2023)

66.3% of respondents would not be very surprised if their APIs suffered an imminent data breach.

Client-Side Protection

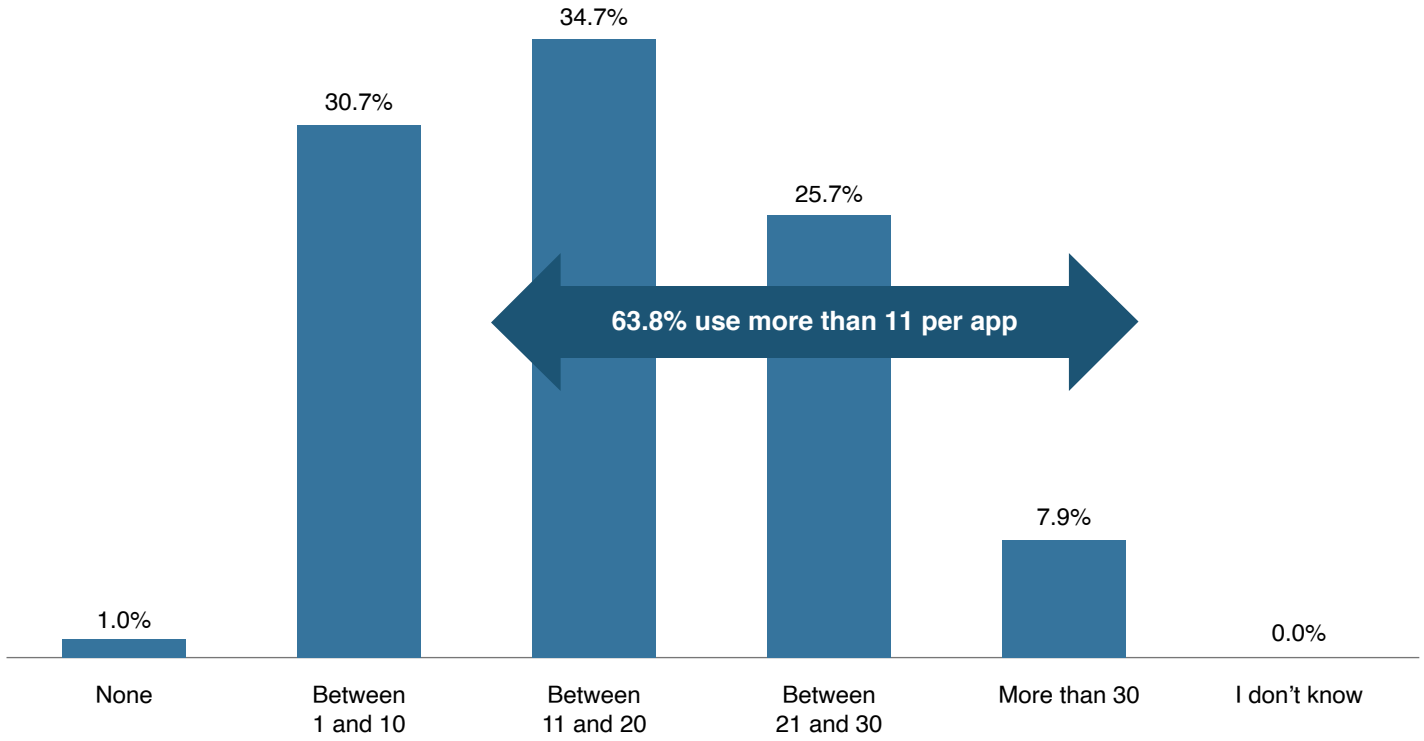
When building applications, organizations complement their internally developed APIs with APIs to third-party web applications. These third-party APIs are executed directly in the user's browser (hence also known as client-side APIs). In this section, we look at reliance on third-party APIs, concerns about exploits, and the efficacy of client-side security posture.

Organizations use an average of 15.9 third-party APIs in each of their web applications.

Number of Third-Party APIs in Each Web App

99% of organizations make extensive use of third-party APIs, with 68.3% of organizations using more than 11 third-party APIs for each of their web applications. On average, organizations use 15.9 third-party APIs that are executed directly in the user's browser in each of their web applications.

Figure 11: Number of Third-Party APIs Per Web Application
Percentage of respondents



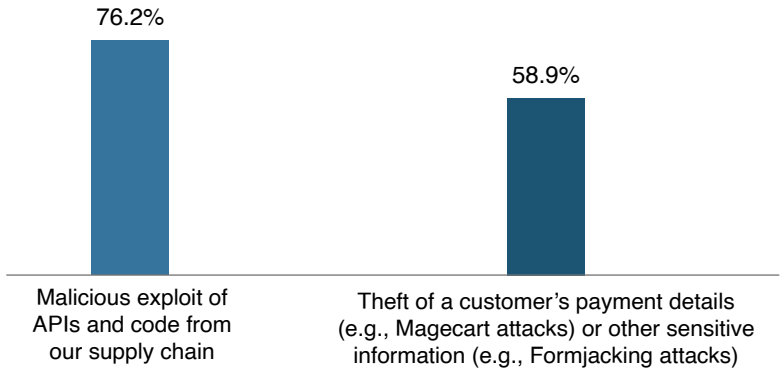
Source: Osterman Research (2023)

Concern About Types of Attacks

Building applications around third-party code and APIs means that while an organization reassigns responsibility for code development to another party, they retain full responsibility for anything bad that happens due to malicious exploit of that code and APIs. These software supply chain vulnerabilities have become a topic of hot concern over the past 24 months, with most organizations playing catchup to rectify low preparedness. Unsurprisingly, respondents indicate very high levels of concern about software supply chain threats (76.2%).

76.2% of organizations are highly concerned about software supply chain threats.

Figure 12: Concerns About Various Types of Malicious Exploits
Percentage of respondents indicating “concerned” or “extremely concerned”



Source: Osterman Research (2023)

By comparison, somewhat fewer respondents are highly concerned about other types of client-side attacks. Although still in the majority (58.9%), Magecart and Formjacking attacks that inject malicious JavaScript to steal payment details and sensitive information from customers trigger less concern than supply chain vulnerabilities.

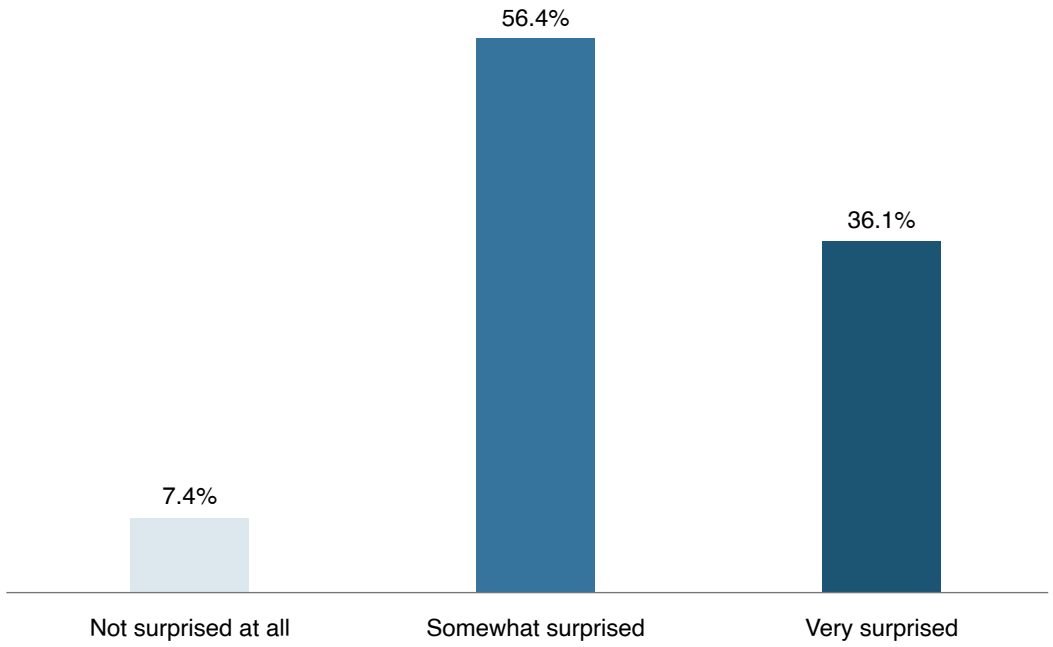
Most Wouldn't Be Surprised by a Breach of a Third-Party API

By a slim margin, respondents have higher confidence in the ability of third-party APIs to withstand security threats than they have for the APIs developed internally at their organization. 63.9% of respondents would not be very surprised if they suffered a supply-chain breach via third-party APIs or code tomorrow.

Concerns about external APIs and code track closely to concerns about internally developed APIs. For third-party APIs, 36.1% would be "very surprised" at a successful data breach "tomorrow" (see Figure 13 below), compared to 33.7% for a breach of an internally developed API (refer to Figure 10).

Regardless of the slim margin, however, is the overwhelming sense that even third-party APIs are a cause for anxiety and consternation at organizations, with most respondents uncertain of the efficacy of protections against data breach attempts against third-party APIs.

Figure 13: Level of Surprise Due to a Hypothetical Data Breach Attempt Tomorrow
Percentage of respondents



Source: Osterman Research (2023)

Application DDoS Protection

Application DDoS attacks (also known as Layer 7 DDoS and Web DDoS attacks) are unleashed to compromise the availability of an organization's website or another critical business web application. We look at business concerns about application DDoS attacks in this section, along with the business impacts of such attacks.

Concerns About Application DDoS Attacks

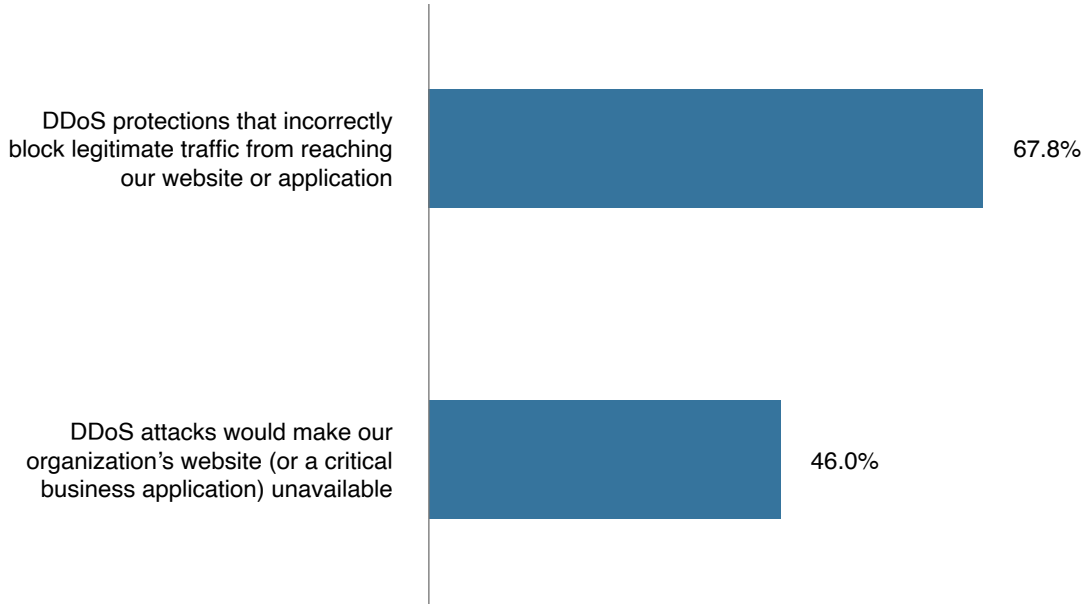
Application DDoS attacks raise two significant issues for organizations. The first is deploying the right level of protection to stop such attacks from compromising web applications. The second is having a web application taken offline due to such an attack.

Of the two, respondents were more concerned about getting the first one wrong, particularly when legitimate traffic is incorrectly blocked from reaching their website. This is the enduring, persistent, and perpetual threat that must be managed every minute of every day when protections are put in place.

By comparison, fewer respondents exhibited high levels of concern about an actual DDoS attack resulting in non-availability of their organization's website or a critical business application. This reflects either higher levels of confidence in the efficacy of current protections to stop attacks while minimizing false positives or complacency due to less frequent attacks (as noted in Figure 5 above).

67.8% of organizations are highly concerned that application DDoS protections will prevent legitimate traffic from reaching their website.

Figure 14: Concerns About Application DDoS Attacks
Percentage of respondents indicating “concerned” or “extremely concerned”



Source: Osterman Research (2023)

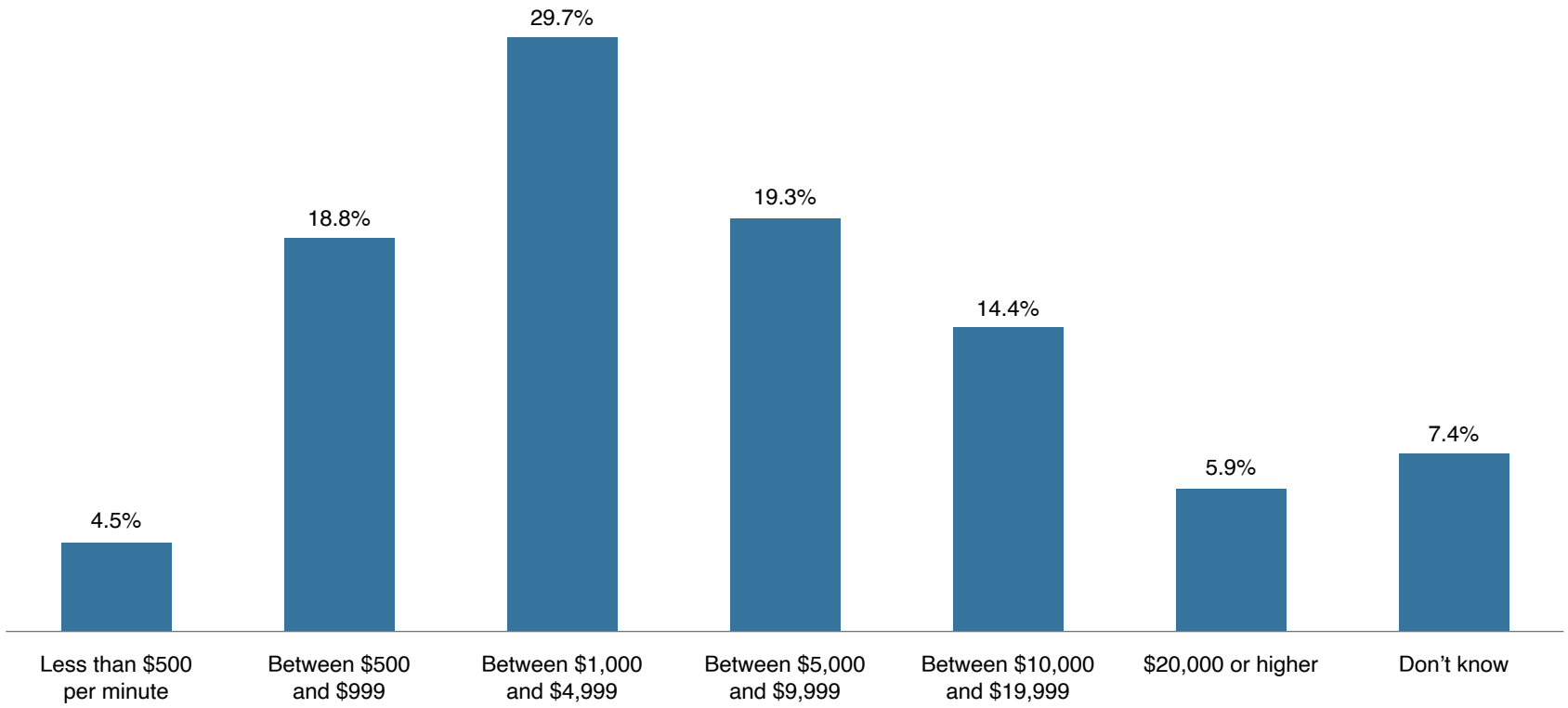
Financial Impacts of Application DDoS Attacks

The push of digital transformation and digital channels to engage with customers means that an organization's website and other business web applications are increasingly revenue-generating destinations. When these are unavailable—for whatever the reason—customers can't make purchases and revenue streams are compromised.

Almost all respondents in this research knew the cost of downtime to their organization due to an application DDoS attack. The two highest cost bands were $1,000 to $4,999 per minute (29.7% of respondents) and $5,000 to $9,999 per minute (19.3% of respondents). The overall average across all organizations was $6,130 per minute, or $367,797 per hour.

Downtime due to a successful application DDoS attack costs organizations an average of $6,130 per minute.

Figure 15: Per Minute Cost of Downtime of Successful Application DDoS Attacks
Percentage of respondents



Source: Osterman Research (2023)

Other Business Impacts of Application DDoS Attacks

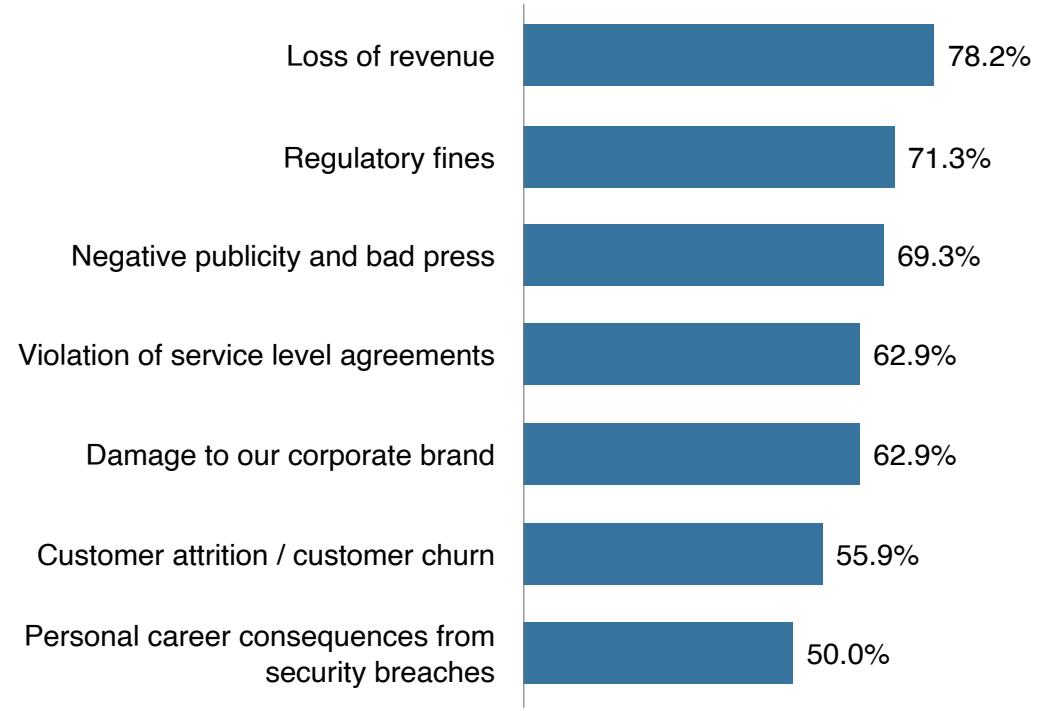
Loss of revenue due to an application DDoS attack inflicts a high cost on organizations, as we have just explored. When set in the context of six other potential business impacts, loss of revenue is rated as being most significant by 78.2% of respondents. Regulatory fines and negative publicity are in second and third place, respectively.

In sixth place overall, the lower ranking of customer attrition and churn signals that for many organizations these higher-ranked consequences—while costly in the short-term—are often resolved with time. Sales revenue takes an immediate hit and regulatory fines bite into this year's profits, but if appropriately addressed, the loss of customers is short-lived.

Beyond the organizational consequences we asked about, half of respondents indicated that a successful attack would have personal career consequences, e.g., loss of employment or reduced pathways for promotion.

78.2% of organizations see revenue loss as a highly significant business impact of application DDoS attacks.

Figure 16: Business Impacts of Application DDoS Attacks
Percentage of respondents indicating “significant” or “extremely significant”



Source: Osterman Research (2023)

Voices of the Survey

The final question of the survey—an open-ended question—asked respondents to write their greatest unaddressed challenge in securing applications over the next 12 months. The most mentioned unaddressed challenges are noted below, along with selected responses for each of the six groups:

- **Authentication**
  How to enhance or improve user authentication methods, and deal with broken and weak authentication mechanisms.
- **Identifying unknown vulnerabilities**
  How to adapt to new and sophisticated attacks that target application vulnerabilities, identifying unknown vulnerabilities and patching them ASAP, and mitigating vulnerabilities which are added when new technologies are adopted.
- **Various types of injection attacks**
  Several types of injection attacks were of concern to respondents, including code injection, random injections, SQL injection, and injection flaws.
- **Protecting against insider threats**
  Respondents noted issues with employees and authorized users who act with malicious intent. They said insider attacks are challenging to stop, hard to find, and take forever to clean up. Respondents said they don't have enough capability currently to mitigate the risk of malicious employees nor the ability to respond faster when insider threats are identified.
- **Driving security across the hybrid workforce**
  The shift to hybrid and remote working arrangements is challenging security teams. Respondents say they struggle to provide secure access to applications for both office-based and remote workers, and that the security issues associated with evolving remote work remain unaddressed.
- **Software supply chain security**
  Ensuring security of integrated third-party components is an unaddressed issue for many organizations. This is part of a wider insufficiency in the processes of risk mitigation when it comes to third parties.

Methodology

This white paper was commissioned by Radware and conducted by Osterman Research. Two hundred and two (202) respondents in security roles were surveyed in August 2023. To qualify, respondents had to work at organizations with at least 1,000 employees. The surveys were conducted in 10 countries in three regions, with the surveys in France, Germany, and China fielded in French, German, and Chinese, respectively. The survey was cross-industry, and no industries were excluded or restricted.

Job Role

Senior DevOps and/or DevSecOps admin	21.3%
Application security architect	16.3%
Cloud security architect	16.3%
Senior network security admin	16.3%
API architect or senior developer	14.9%
VP or senior manager of research and development	14.9%

Geography

North America (34.7%)	
Canada	17.3%
United States	17.3%
EMEA (35.6%)	
United Kingdom	11.9%
France	11.9%
Germany	11.9%
APAC/LATAM (29.7%)	
Australia or New Zealand	5.9%
Brazil	5.9%
China	5.9%
India	5.9%
Mexico	5.9%

Industry

Industrials (manufacturing, construction, etc.)	9.9%
Energy or utilities	9.4%
Healthcare	9.4%
Retail or ecommerce	9.4%
Financial services	7.9%
Transport or logistics	7.9%
Hospitality, food or leisure travel	6.9%
Professional services (law, consulting, etc.)	6.9%
Life sciences or pharmaceuticals	6.4%
Education	5.9%
Media or creative industries	5.9%
Computer hardware or computer software	5.0%
Data infrastructure or telecom	5.0%
Public service or social service	2.5%
Agriculture, forestry or mining	1.5%

About Radware

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

Radware encourages you to join our community and follow us on: Facebook, LinkedIn, Radware Blog, Twitter, YouTube, and Radware Mobile for iOS and Android.