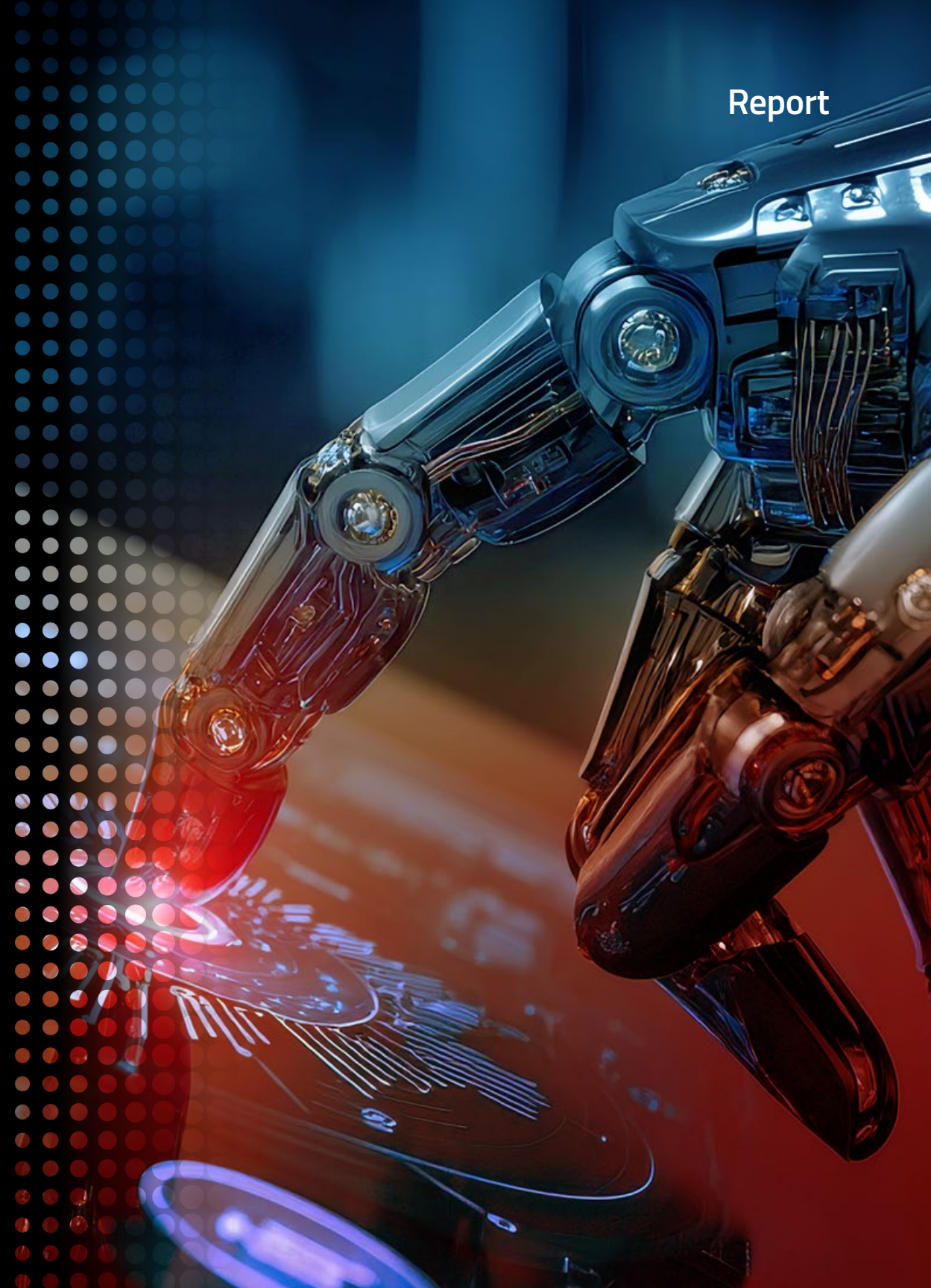
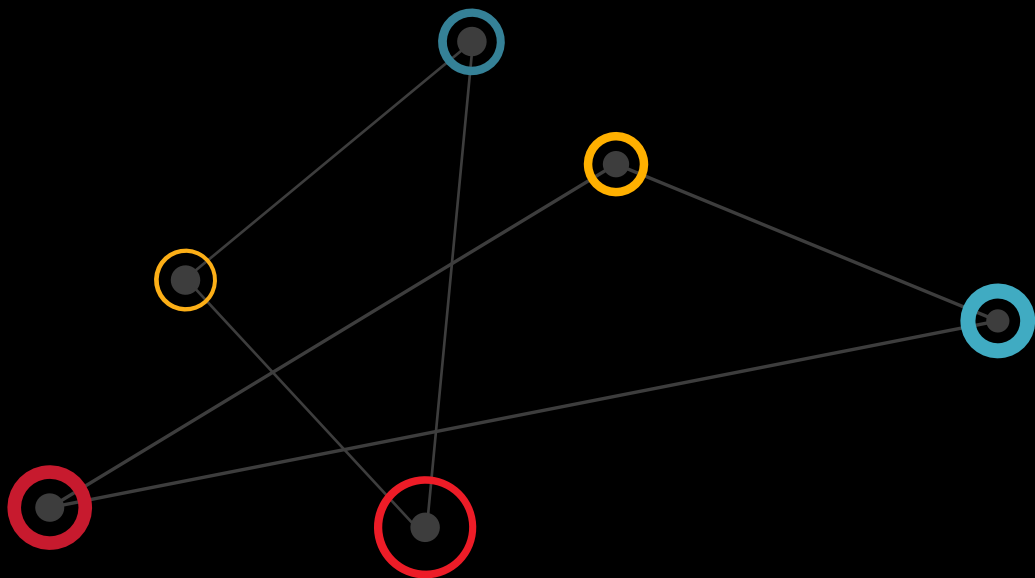





Report

2025 Cyber Survey:

Application Security at a
Breaking Point



Executive Summary



The rising menace of AI weaponized by threat actors has stormed onto the scene, dampening confidence in application security protections and threatening a renewed onslaught of attacks against applications. Indispensable application design constructs developed internally and across the supply chain remain ill-protected, even as usage relentlessly increases and threats multiply. Visibility into threats and security weaknesses is too low, and many organizations lack sufficient protections against new AI threats and business logic attacks, among others.

Comparative year-over-year data cited in this report is drawn from Radware's 2023 report entitled [Application Security in a Multi-Cloud World 2023](#).

Key Takeaways

The essential insights from this research are:



AI-powered cyberthreats spark high concern, rapid response

The emergence of AI-powered cyberthreats is highly concerning. Specific concerns include the use of AI to rapidly develop new threats, inadequate technical protections against new threats, and shortened attack timelines. To counteract the growing threat of AI, most organizations are planning to implement AI-based cybersecurity solutions within the next 12 months.



Applications are under attack from all directions

More than half of organizations already experience a range of attacks against their applications monthly or more frequently, led by bot, API, and application attacks. Increased usage of AI by threat actors to develop sophisticated and polymorphic attacks is most likely to drive a faster attack cadence.



New attacks against APIs exploit logic vulnerabilities

APIs are in a constant state of fluctuation, and only a few organizations maintain up to date documentation on their APIs. This conceals the threats posed by and to the organization's API inventory, which is alarming given the rapid emergence of new threats against APIs, e.g., business logic attacks.



Use of third-party service APIs is widespread, but not fully understood

More organizations are taking advantage of extra third-party services' APIs in their applications, but fewer have anything approaching sufficient visibility into active threats, malicious scripts, and untrusted connections due to these APIs. Concerns about the theft of customer data through these APIs is increasing.



Application DDoS attacks are disruptive and costly

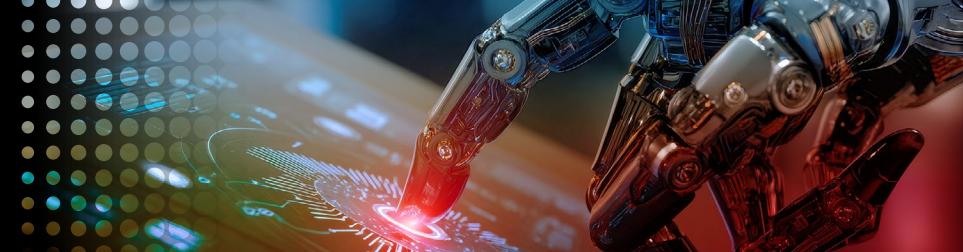
Applications can be disrupted due to DDoS protection failures and DDoS attacks, although organizations are increasingly concerned about disruptions caused by attacks. On average, downtime due to an application DDoS attack costs \$6,106 per minute.

The rising menace of AI weaponized by threat actors has stormed onto the scene, dampening confidence in application security protections and threatening a renewed onslaught of attacks against applications.

About This White Paper

The survey and white paper were commissioned by Radware. Information about Radware and details on the survey methodology are provided at the end of the paper.

High Concerns About Offensive AI Threats



Threat of AI Being Used to Intensify Hacking Tradecraft

The use of AI to improve and intensify hacking tradecraft is of high concern to the organizations in this research. Specific high-rated concerns are attack tools getting better, cyberattacks becoming more voluminous, and the introduction of previously unseen attacks, among others. See Figure 1.

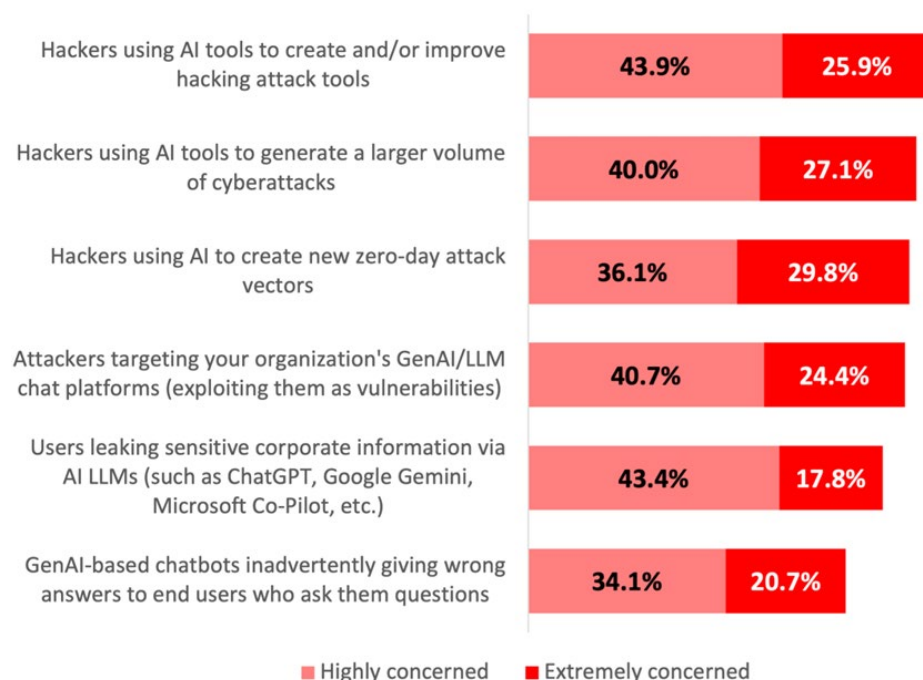


Figure 1: Concerns about how AI could change cyberthreats and introduce new risks

We asked respondents about the challenges they face in defending against AI-driven threats. After grouping the open-ended responses, the top challenges were:

- **Lack of expertise on AI cyberthreats**, e.g., “Artificial intelligence is becoming more and more powerful, and there are fewer [people with] talent of this type.”
- **AI threats evolve faster than defenses**, e.g., “AI threats are always evolving, making it difficult to stay up to date.”
- **AI threats are difficult to detect**, e.g., “AI can generate convincing fake images, videos, and text, making phishing and misinformation campaigns harder to detect.”
- **AI threats are emergent**, e.g., “AI can generate polymorphic malware that changes its code to evade detection.”
- **AI threats are complicated to defend against**, e.g., “AI-powered threats evolve in real-time, bypassing traditional, static defenses.”
- **AI threats include diverse attack types**, e.g., “AI-driven threats can be so complex and diverse that they are difficult to counter with a single strategy.”

Organizations are concerned about hackers using AI to create better hacking tools, run more attack campaigns, and develop new types of attacks.

Concern Regarding Inadequate Defenses Against AI Cyberthreats

Concerns regarding actions by threat actors to embrace AI to intensify hacking tradecraft are amplified by the overwhelming sense of lack of preparation to meet these new types of attacks. From an overall perspective, organizations are highly concerned about the potential for threat actors to use AI to generate attacks in nature and cadence that the organization is ill-prepared to defend against. See Figure 2.



Figure 2: Concerns about how AI cyberthreats affect organizations

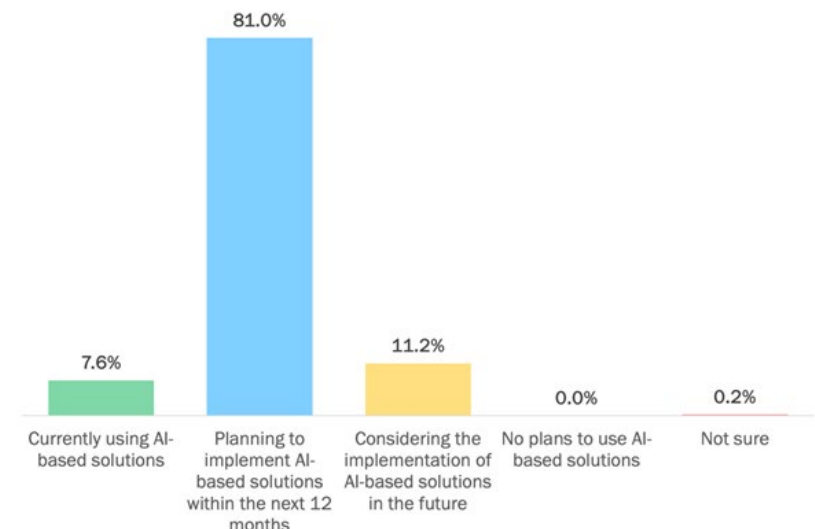
In recent years, organizations have invested in cybersecurity to defend against attacks that seek to compromise applications, such as bot and API attacks. There are significant implications of the rising adoption of AI by threat actors for use in offensive campaigns, including new attacks that bypass existing defenses, are easier to launch and at a faster cadence, and drive compromise in areas that were previously too difficult to attack.

In the hands of threat actors, AI means new types of attacks on a faster cadence that organizations lack the ability to defend against.

Organizations are Planning to Embrace New AI-Based Cybersecurity Solutions

Most organizations are planning to implement AI-based cybersecurity solutions within the next 12 months to defend against the rising threat of offensive AI campaigns. While a small proportion of organizations have already implemented AI-based cybersecurity solutions (7.6%) and some haven't yet committed to a timeframe (11.2%), most view this as an immediate priority. See Figure 3.

Figure 3: Intent to use AI-based cybersecurity solutions



81% of organizations are planning to implement AI-based cybersecurity solutions within the next 12 months.

Applications Are Under Attack

Attacks Happen Frequently, and Business Logic Attacks Have Increased Rapidly

The applications used by the organizations in this research are under attack—relentlessly. Bot attacks and API attacks happen most frequently (on the combined cadence of daily, weekly, and monthly), followed closely by application and API business logic attacks. API business logic attacks are a new class of threat, and while this is the first time we have asked for cadence data, already 55% of organizations experience such attacks daily, weekly, or monthly. For 15% of organizations, bot attacks happen every day. Across the five attack types, threat actors seek to disrupt normal application functioning, corrupt application safeguards to bypass normal authorization requirements, and harness business logic structures for unintended and malicious purposes. See Figure 4.

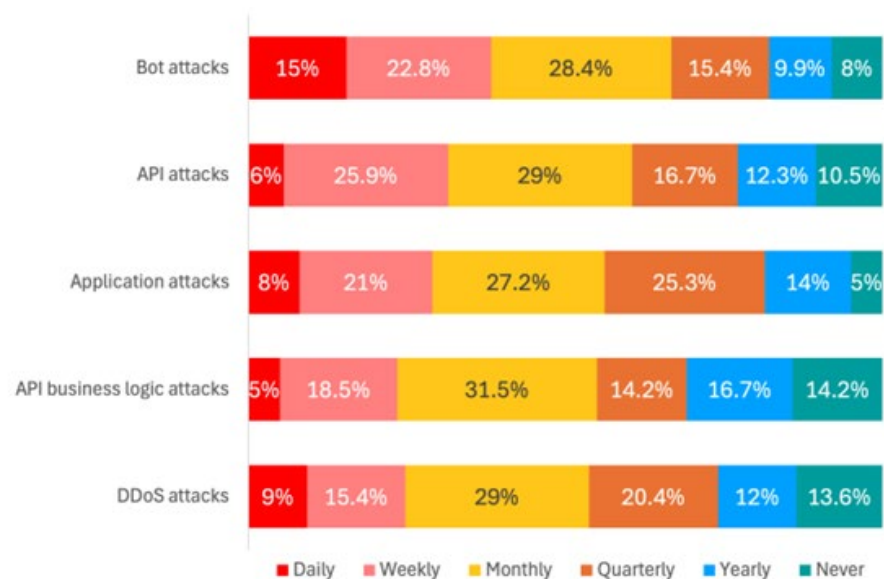


Figure 4: Frequency of attacks against applications

Compared to our data from 2023, the average cadence of attacks is lower, with more organizations this year indicating a quarterly, yearly, or never cadence. With the continued expansion of threat types on the offensive side, and in particular the amplification of threat actor capabilities via AI, it is most likely that attack cadence will increase over the next 12 months—not slow further.

For the financial services organizations in this research, the most frequently occurring attacks are bot attacks and API business logic attacks. For the healthcare organizations in this research, bot attacks are in first place on the combined daily, weekly, and monthly cadence. Along with API business logic attacks, both types happen twice as frequently on the daily cadence compared to the other three. Organizations in both the financial services and healthcare industries that are not taking proactive measures against bot attacks and API business logic attacks are poorly positioned to counteract the most frequently seen threats.

API business logic attacks are a new class of threats, and although this is the first time we asked for cadence data, they are already experienced with high frequency.

API Usage Increasing as Controls Weaken

API Usage Is Increasing, as Is the Update Cadence

The usage of APIs developed internally is increasing for most respondents (70.2%). Compared to the 2023 data, those who selected the highest rate of usage growth rose by 42%.

In conjunction with an increased level of usage, organizations are updating APIs on a faster cadence. In this research, 72.7% of respondents indicated that both third-party and internal APIs are updated at least weekly. APIs change dynamically and regularly to address new customer demands and market opportunities; they are not static. Minimizing coding errors on the front end, rapidly identifying development vulnerabilities in pre-release testing cycles, and having the capability to detect attacks against API are all essential.

Compared to the 2023 data, many more organizations in 2025 are updating APIs at least weekly. In 2023, 56.4% did so. The most startling change is those indicating a cadence of “multiple times a day,” which increased 6X from 2% in 2023 to 12.4% in 2025. See Figure 5.

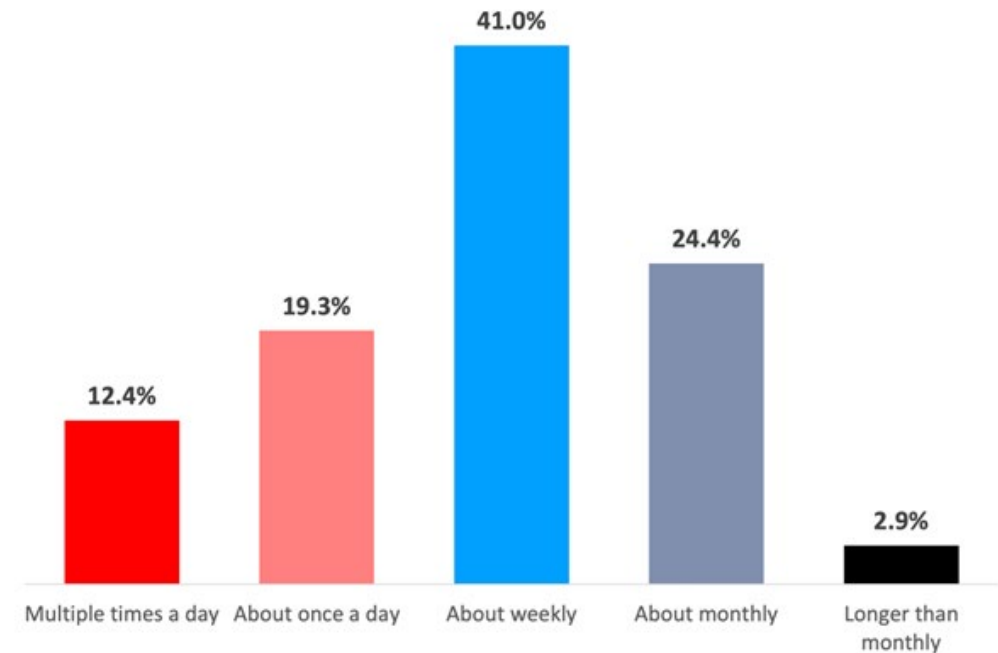


Figure 5: Cadence of updating APIs

At financial services organizations, 80.2% update third party and internal APIs at least weekly, including 10.3% daily. None of the financial services organizations in this research are updating on a cadence of longer than monthly.

At healthcare organizations, 64.8% update APIs at least weekly, with 15.6% updating on the daily cadence.

72.7% of respondents are updating third-party and internal APIs at least weekly.

Documentation Is Incomplete for Most

On average, only 6.1% of respondents say they have full documentation for all their APIs. It is lower at the financial services organizations in this research (3.2%) and higher at healthcare organizations (7.4%). When documentation is lacking and incomplete, some APIs are unknown entirely and others are only partially documented. The problem with this stance is that it conceals the threats posed by and to the organization's API inventory. See Figure 6.

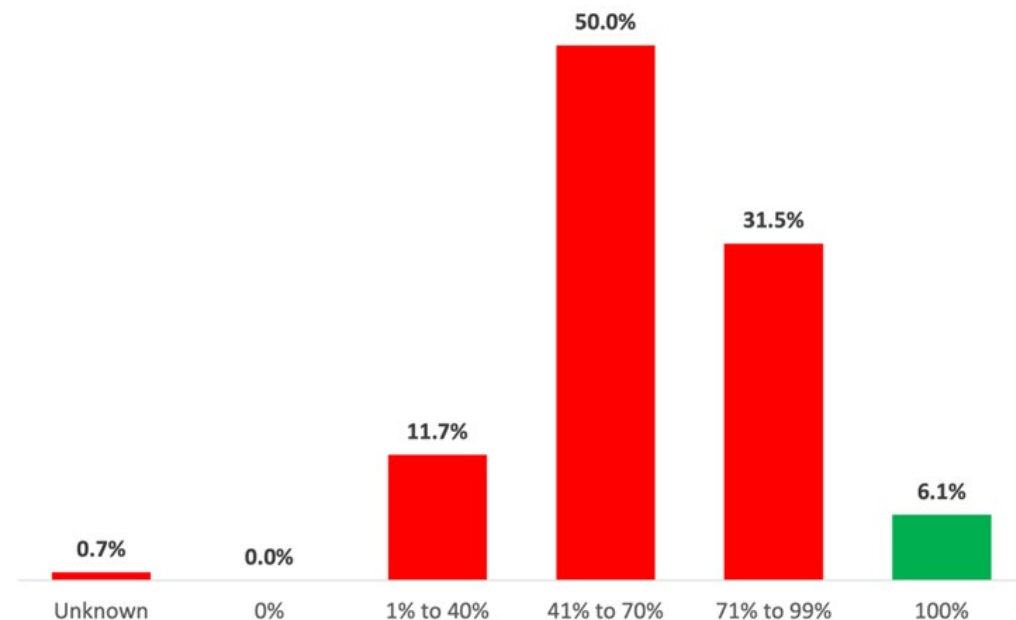


Figure 6: Distribution of API documentation rates

Documentation makes a difference to the level of confidence organizations have in their API security posture. Overall, 38.3% are not confident in the API protections they are currently using. When correlated with documentation rates, higher rates show higher confidence. For instance, among those that are confident in their API security protections, 47% have documented 71% or more of their APIs. Among the not confident cohort, only 22.3% have done so.

Rates of confidence in protection of APIs from threats differs by industry. The financial services organizations in this research have the highest rate of not being confident—at 40.5%. Given how attractive threat actors view the data held by financial services organizations, it is concerning that so few have the required confidence in their API protection posture.

Only 6.1% of respondents have fully documented all their APIs.



Business Logic Attacks Have Increased Rapidly, but Mitigations Are Lagging

Business logic attacks (BLAs) represent a threat area of rapidly growing concern to the organizations in this research. Such attacks happen when threat actors manipulate normal application logic flows to achieve outcomes that are unintended from the application, such as the ability to exfiltrate data, stack or reuse coupons, and steal funds. Most respondents to this research have seen API business logic attacks over the previous 12 months (85.8%). Only 14.2% of respondents say such attacks never occur at their organization. See Figure 7.

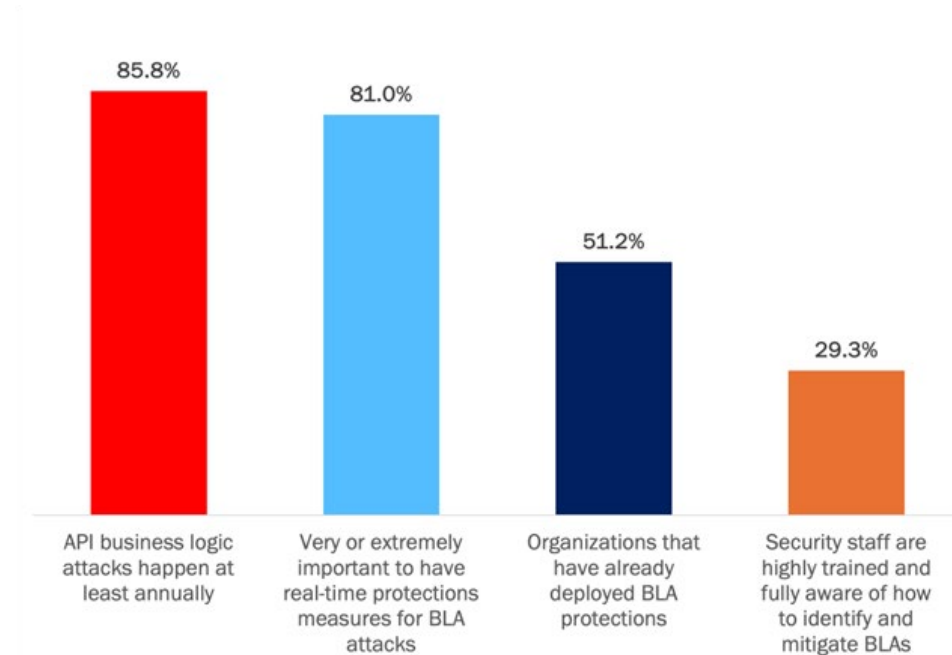
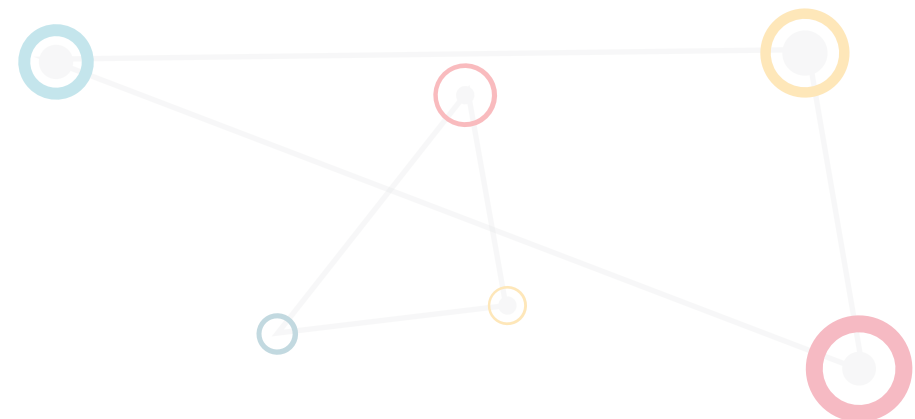


Figure 7: Concerns and responses to business logic attacks

The organizations in this research are trailing behind their assessment of the importance of real-time protections for business logic attacks. While 81% say it is very or extremely important to have real-time protection measures in place, only 51.2% have already deployed runtime business logic protections, and only 29.3% indicate that their security staff is highly trained and fully aware on the identification and mitigation of BLAs.

Business logic attacks present an ideal opportunity for threat actors to use emerging offensive AI capabilities. For example, AI agents can automate the malicious exploration of API sequencing, looking for unexpected logic vulnerabilities and loopholes to exploit. Organizations should expect hackers to develop and share newly crafted playbooks to amplify threat opportunities.

Business logic attacks are a new threat vector for applications, and many organizations are ill-prepared.



Growing Use of Third-Party Services Without Safeguards and Visibility

Organizations Are Using More APIs per Web App

Ninety-nine percent of organizations use third-party service APIs embedded in their applications. This percentage remains constant from our 2023 data. What has changed, however, is the number of third-party services APIs used by organizations. The percentage using 11 or more third-party APIs per web application has increased from 68.3% in 2023 to 86.1% currently. On average, organizations are using 18.6 third-party APIs per app, up from 15.9% in 2023. More organizations are integrating their applications with third-party services, with APIs acting as the conduit for data sharing. See Figure 8.

Third-party service APIs enrich applications with capabilities, insights, and application functioning the organization hasn't had to develop themselves—and hence it is entirely unsurprising that they are so widely embraced. On the positive side, this allows organizations to leverage best in class services to speed time to market and elevate application quality. On the negative side, it introduces new types of threats around data compromise that the organization cannot mitigate at a coding level.

86.1% of organizations use 11 or more third-party service APIs in their web applications.

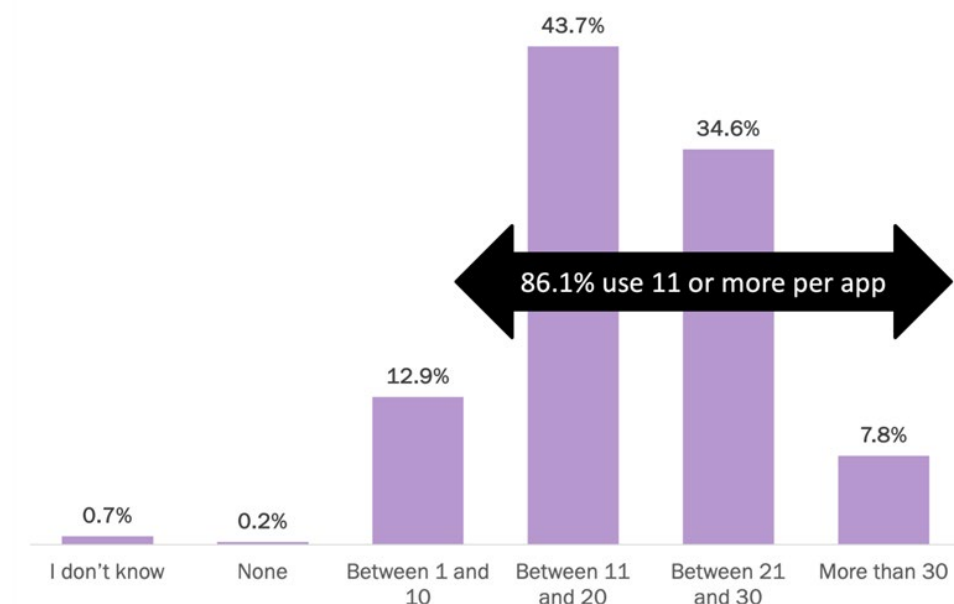


Figure 8: Number of third-party APIs in web applications



Reduced Visibility Into Third-Party Client (Browser)-Side Code

More organizations lack visibility into the third-party code used by their web applications that may compromise customer data and activity. In our 2023 data, an average of 38.6% of organizations had visibility of 50% or less across a range of aspects related to third-party code usage. The number in this year's data has risen to 47.7%. In other words, roughly half of respondents don't know what code is being used, what threats are active, and when malicious scripts and services are introduced by the third-party code and APIs used by their applications.

When visibility into browser-side outbound activity is lacking, organizations have only a partial and incomplete understanding of how customer data and activity could be compromised. Without the foundation of full visibility across the range of likely threats, attempts at proactive mitigations are flawed. See Figure 9.

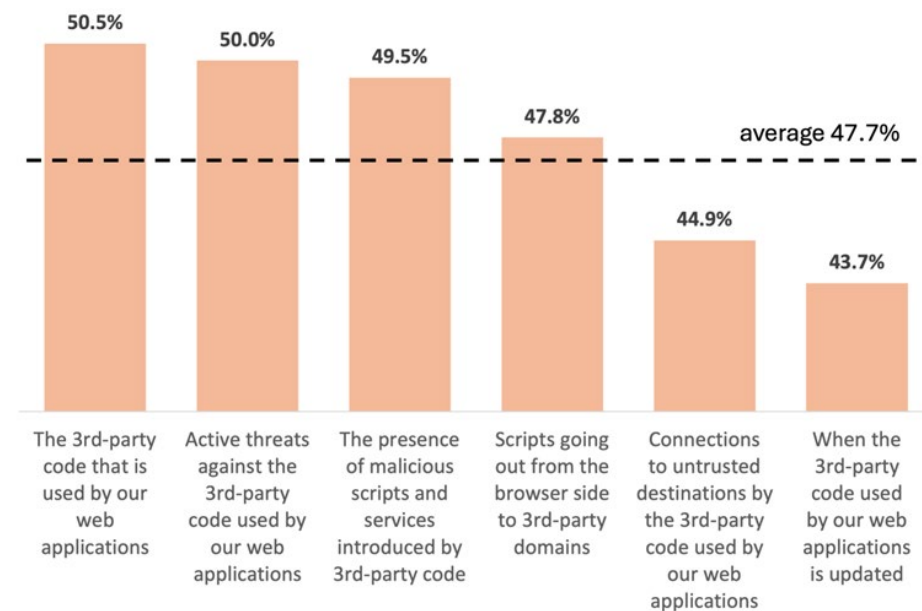
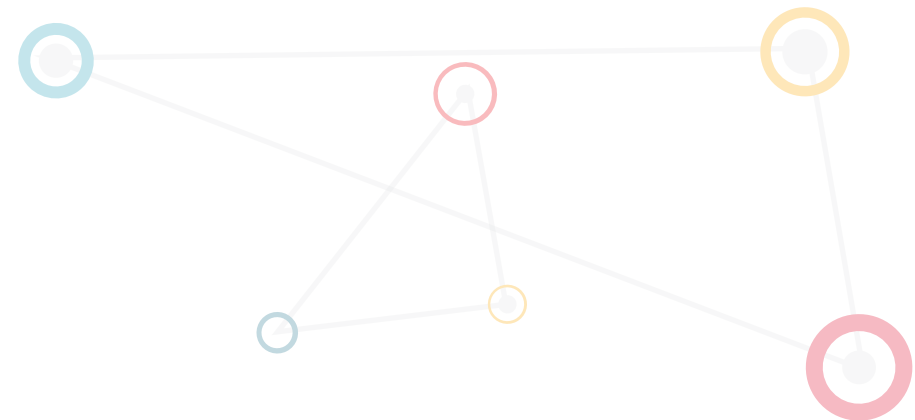


Figure 9: Organizations lacking visibility into third-party code used by their web applications

Half of respondents don't know what third-party code is being used by their web applications, which data is being leaked to third-party services, and when malicious scripts and services are introduced.



Growing Concern About Theft of Customer Data and Payment Details

The compromise of third-party APIs and code running on an organization's web applications can lead to data breaches, theft of customer payment details, and other types of unintended application interactions. For the respondents in this research, around two in three have significant concerns about how their organization is protecting against malicious software supply chain exploits and theft of customer payment details. Among other aspects of a defensive posture against these threats, lack of visibility into what third-party code is being used is a fundamental problem, as discussed above.

Respondents have a growing sense of concern about how their organization protects against the theft of customer payment details; this has increased from 58.9% highly or extremely concerned in our 2023 data to 64.9% currently. See Figure 10.

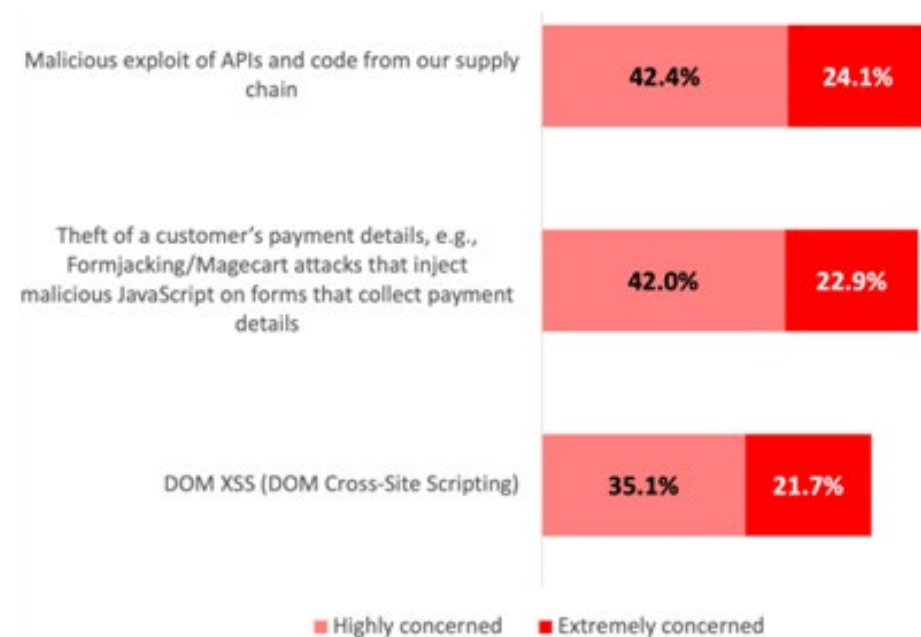


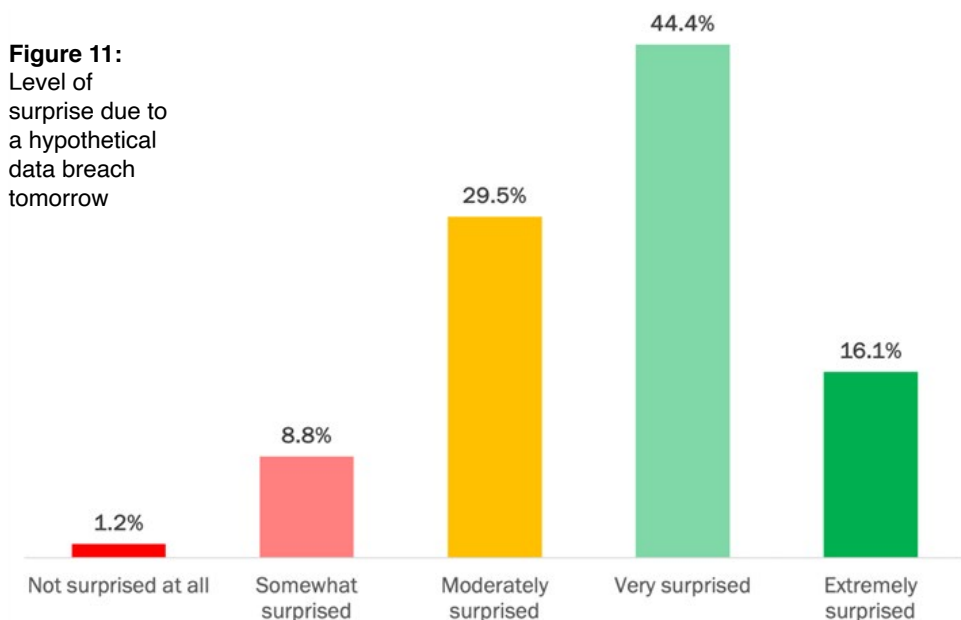
Figure 10: Concerns about protection posture against attacks on third-party APIs and code

64.9% of respondents are concerned about how their organization protects against attacks that seek to steal customer payment details.

Few Are Fully Confident in Their Data Breach Protections

Only 16.1% of respondents have full confidence that their current protections for third-party services could withstand a data breach attempt. They would be “extremely surprised” at a successful hypothetical breach that happened “tomorrow.” The vast majority do not hold this highest rating, however, indicating that most have a range of concerns about the efficacy of their current protections against data breach attempts. See Figure 11.

Figure 11:
Level of surprise due to a hypothetical data breach tomorrow



Only 16.1% of respondents are fully confident in their current protections against data breach attempts of third-party services code running on their web applications.

Application DDoS Attacks Are Disruptive and Costly

Growing Concern About the Disruptive Consequences of Application DDoS Attacks

Respondents are almost equally concerned about two types of disruption due to application DDoS attacks against their organization. The significant trend line is for DDoS attacks that make an organization's website or critical business application unavailable, which has increased in intensity compared to our 2023 research—from 46% with the two highest levels of concern then to 68.6% now. There are significant and costly consequences in having a website offline due to an attack. See Figure 12.

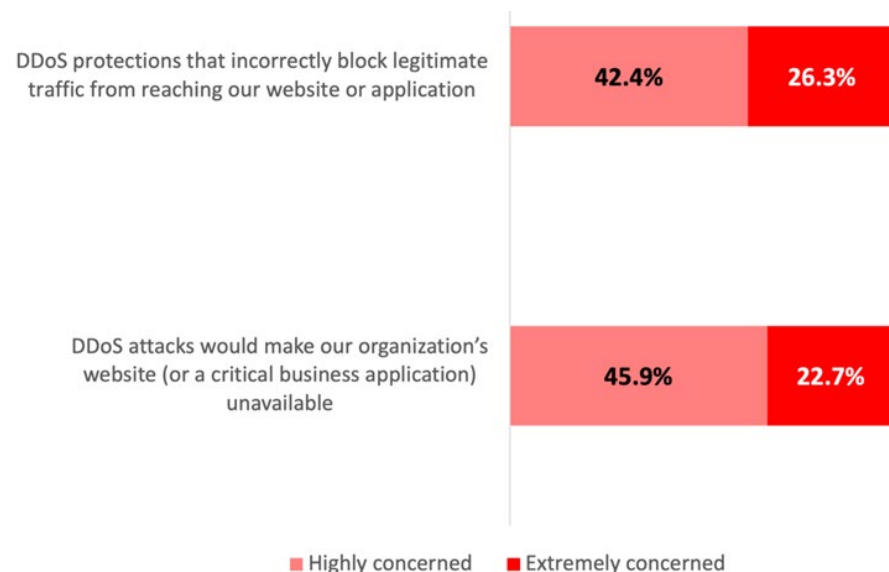


Figure 12: Concerns about disruptions from application DDoS attacks

68.6% of respondents express significant concern about DDoS attacks that would make their web applications unavailable.

Cost of Downtime Due to an Application DDoS Attack

When an application DDoS attack takes a website or critical business application offline, there are immediate financial consequences that most organizations have quantified or risk-modelled in advance. These accrue from negative publicity, loss of revenue, and brand damage due to downtime from an application DDoS attack.

The cost of downtime ranges significantly for the respondents to this research, with 20% indicating a cost of less than \$500 per minute and 13.4% saying at least \$20,000 per minute. Across the bands in Figure 13 below, the average cost per minute is \$6,106—or \$366,345 per hour.

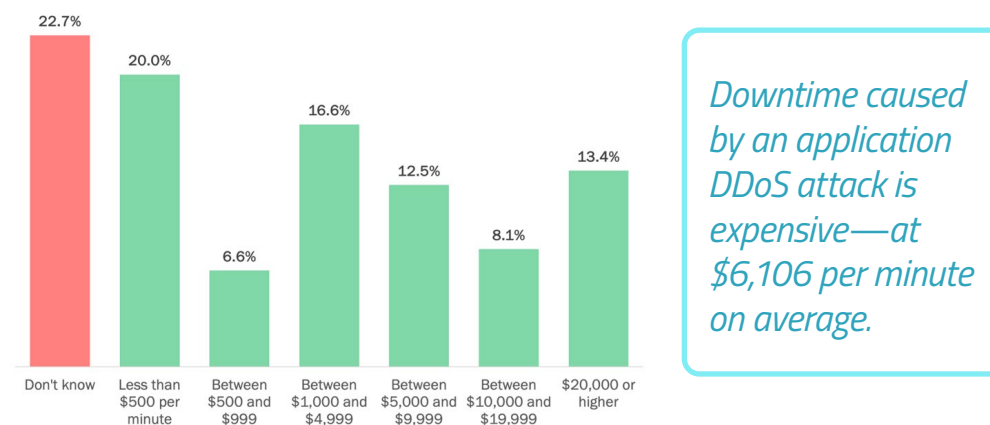


Figure 13: Per minute cost of downtime due to a successful application DDoS attack

Downtime costs vary substantially by type of organization. When split by industry, organizations in the healthcare sector report the highest average per minute cost of downtime at \$8,130, compared to \$5,540 for the financial services organizations in this research. The likelihood of life and death consequences for organizations in the healthcare sector is an immediate and pressing concern that many other industries don't face, including those in financial services.

Environments for Hosting Applications

Most organizations use public cloud services, with the dominant approach being the use of two or more for redundancy and optimization of technical capabilities. Multiple public cloud services are used by 81.7% of respondents in this research, while 11% use only one, and 7.3% use none. Over the past 12 months, the use of multiple public cloud services has increased at the expense of the other public cloud cohorts.

In parallel, there is also high use of private cloud services and on-premises data centers. By implication, the vast majority of organizations must manage application security considerations across not only multiple clouds but also multiple disparate environments. See Figure 14.

Among the financial services organizations in this research, the shift to multiple public cloud services at the expense of only one public cloud is more dramatic. 89.7% of respondents at a financial services organization indicate the use of multiple public cloud services, compared to 81.7% overall.

For the healthcare industry, the most notable feature in this research is a greater proclivity to use private cloud services (91.8%) and on-premises data centers (91%) than the average. Some healthcare organizations have pulled back from using public cloud services over the past 12 months, with growth from 4.9% 12 months ago to 9% currently not using public cloud services at all.

Most organizations are managing application security considerations across multiple clouds and multiple disparate environments.

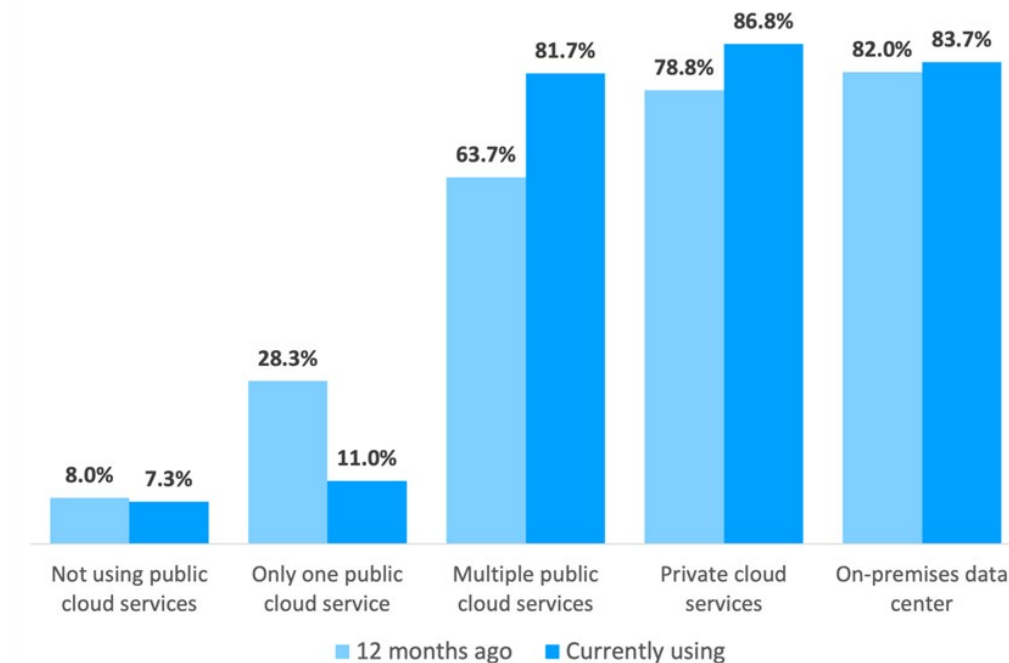
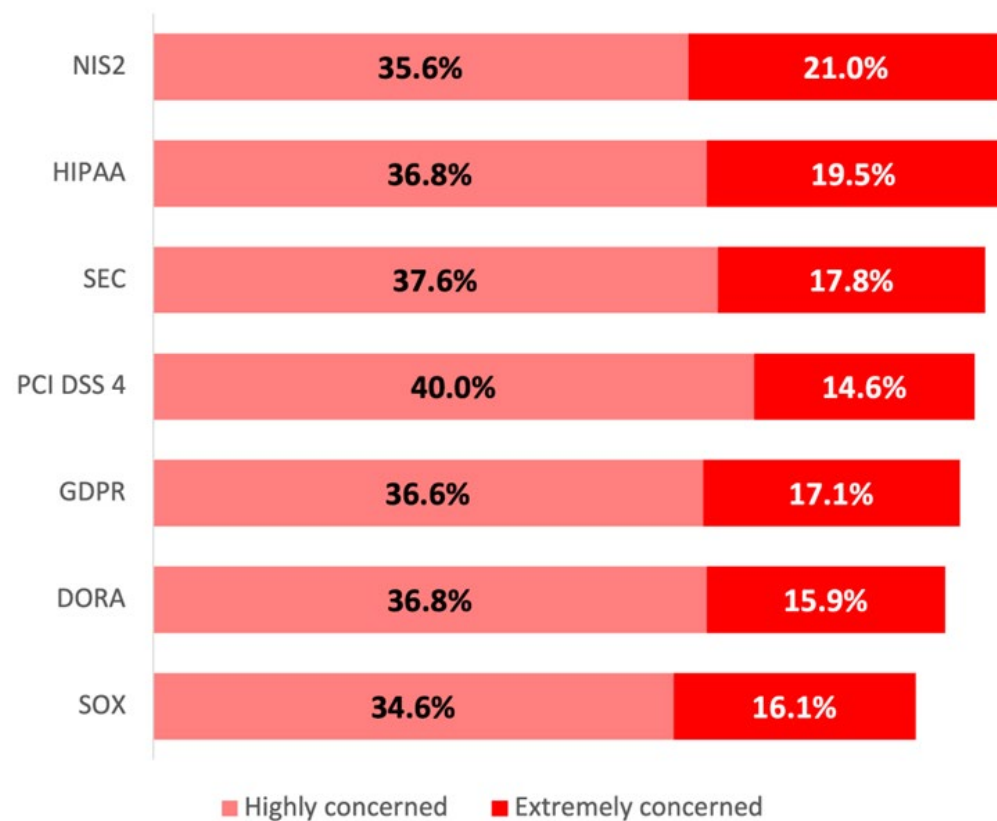


Figure14: Environments for hosting applications

Compliance

Compliance Requirements Weigh Heavily

An average of 54.3% of respondents express high or extreme concern about a range of regulations and the compliance posture at their organization. This indicates that achieving compliance—fully—remains a work-in-progress at most organizations. See Figure 15.



Achieving compliance with key regulations remains a work-in-progress at most organizations.



Figure15: Concern about regulations

Methodology

This white paper was commissioned by Radware and conducted by Osterman Research. In March and April 2025, 410 respondents were surveyed. To qualify, respondents had to work at organizations with at least 1,000 employees. The surveys were conducted in nine countries across three regions, with the surveys in France, Germany, Mexico, and Brazil fielded in French, German, Spanish, and Portuguese, respectively. Participants represented a diverse range of senior technical and security leadership roles, including those responsible for compliance, risk, development, network and cloud architecture, as well as application and API security. The organizations they work for span a broad spectrum of sectors, with strong representation from technology, services, and critical infrastructure industries.

JOB ROLE

Cybersecurity Compliance Officer (CCO), Chief Risk Officer (CRO),
Data Privacy Officer (DPO), Chief Privacy Officer (CPO)
VP or senior manager of research and development
Senior network security admin
Senior DevOps and/or DevSecOps admin
Cloud security architect
API architect or senior developer
Application security architect

GEOGRAPHY

North America

United States
Canada

EMEA

United Kingdom
France
Germany

APAC/LATAM/South America

Brazil
Mexico
Australia/New Zealand
India

INDUSTRY

Agriculture, forestry or mining
Computer hardware or computer software
Data infrastructure or telecom
Education
Energy or utilities
Financial services
Government
Healthcare
Hospitality, food or leisure travel
Industrials (manufacturing, construction, etc.)
Information technology
Life sciences or pharmaceuticals
Media or creative industries
Professional services (law, consulting, etc.)
Public service or social service
Retail or ecommerce
Transport or logistics

About Radware

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

THIS REPORT CONTAINS ONLY PUBLICLY AVAILABLE INFORMATION, WHICH IS PROVIDED FOR GENERAL INFORMATION PURPOSES ONLY. ALL INFORMATION IS PROVIDED "AS IS" WITHOUT ANY REPRESENTATION OR WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES THAT THIS REPORT IS ERROR-FREE OR ANY IMPLIED WARRANTIES REGARDING THE ACCURACY, VALIDITY, ADEQUACY, RELIABILITY, AVAILABILITY, COMPLETENESS, FITNESS FOR ANY PARTICULAR PURPOSE OR NON-INFRINGEMENT. USE OF THIS REPORT, IN WHOLE OR IN PART, IS AT USER'S SOLE RISK. RADWARE AND/OR ANYONE ON ITS BEHALF SPECIFICALLY DISCLAIMS ANY LIABILITY IN RELATION TO THIS REPORT, INCLUDING WITHOUT LIMITATION, FOR ANY DIRECT, SPECIAL, INDIRECT, INCIDENTAL, CONSEQUENTIAL, OR EXEMPLARY DAMAGES, LOSSES AND EXPENSES ARISING FROM OR IN ANY WAY RELATED TO THIS REPORT, HOWEVER CAUSED, AND WHETHER BASED ON CONTRACT, TORT (INCLUDING NEGLIGENCE) OR OTHER THEORY OF LIABILITY, EVEN IF IT WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, LOSSES OR EXPENSES. CHARTS USED OR REPRODUCED SHOULD BE CREDITED TO RADWARE.

© 2025 Osterman Research. All rights reserved.

No part of this document may be reproduced in any form by any means, nor may it be distributed without the permission of Osterman Research, nor may it be resold or distributed by any entity other than Osterman Research, without prior written authorization of Osterman Research.

Osterman Research does not provide legal advice. Nothing in this document constitutes legal advice, nor shall this document or any software product or other offering referenced herein serve as a substitute for the reader's compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, administrative order, executive order, etc. (collectively, "Laws") referenced in this document. If necessary, the reader should consult with competent legal counsel regarding any Laws referenced herein. Osterman Research makes no representation or warranty regarding the completeness or accuracy of the information contained in this document.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.