radware

Report: Application Security In A Multi-Cloud World

Executive Summary

Organizations are no longer moving to the cloud; they are already there. The research shows that only a negligible percentage of organizations, less than 0.5%, do not deploy applications in the public cloud at all. However, organizations are increasingly shifting into the next iteration of the cloud movement: the multi-cloud. The research shows that 95% of the organizations use at least two types of infrastructure, and nearly half of the organizations deploy applications on four or more different platforms. As a result, deploying applications across multi-cloud and hybrid cloud environments has become the new normal.

The growing number and diversity of environments for hosting applications raises the bar on what is required from security tools, with consistency in security policy and cross-environment visibility key requirements. Many organizations are struggling to achieve high-quality protection and centralized, cross-cloud visibility, and 69% of organizations can trace data breaches or data exposures to inconsistent application security configurations across the different public cloud platforms that they currently use. The trust in native public cloud security capabilities is declining, and more than half of the organizations cannot trust their security staff to configure and maintain a strong application security posture, across the public cloud platforms that they currently use for hosting applications.

> *Increased reliance on multi-cloud for hosting applications demands urgent action to assure application security, irrespective of where the applications are hosted.*

Key Takeaways

The key takeaways from this research are:

- **Multi-Cloud Usage is Rapidly Scaling**
  58% of organizations currently deploy applications on two or more public cloud environments, and this figure is expected to rise to 63% within the next 12 months.
- **On-Premises Data Centers Aren't Going Away**
  While the usage of on-premise hardware data centers is gradually declining, over 80% of organizations still use it for at least some of their applications, and 75% of the organizations are expected to continue to do so in the next 12 months.
- **Almost All Organizations are Hybrid**
  95% of the organizations use at least two types of infrastructure (for example, on-premises data center, private cloud, public cloud), and 45% of the organizations deploy applications in a hardware data center, on a private cloud, AND on at *least two* public clouds.
- **Proliferation of Security Tools**
  Given the number of different environments that applications are deployed to, it is no surprise that organizations must rely on multiple security tools: 49% of organizations use more than one application security tool, and it is expected that the numbers will rise to 51% of organizations within 12 months.
- **Quality of Protection and Visibility are Biggest Concerns for Multi-Cloud**
  51% of organizations define the quality of application protection achieved as a “problem” or “an extreme problem,” and 41% of organizations say the same for centralized cross-cloud visibility.
- **The Consequences**
  70% of organizations are not confident in their ability to apply cross-platform application security, and 69% indicate they had data breached or exposed as a result of discrepancies in multi-cloud security configurations.

< Prev   Next >

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.

< Prev Next >

Growth Dynamics with Multi-Cloud

This section provides information about the growth in the adoption of multi-cloud platforms, as well as its continued reliance on on-premise infrastructure and private cloud services.

Growing Adoption of Multi-Cloud

Organizations are increasingly reliant on a multi-cloud strategy for hosting applications. The significant trend line is the growth in reliance on three and four public clouds combined with decreasing reliance on only one or two public clouds. Only outliers are not using any public cloud services for hosting applications; in 12 months, 0.4% of the organizations are expected to use no public cloud services, down from 1% currently.

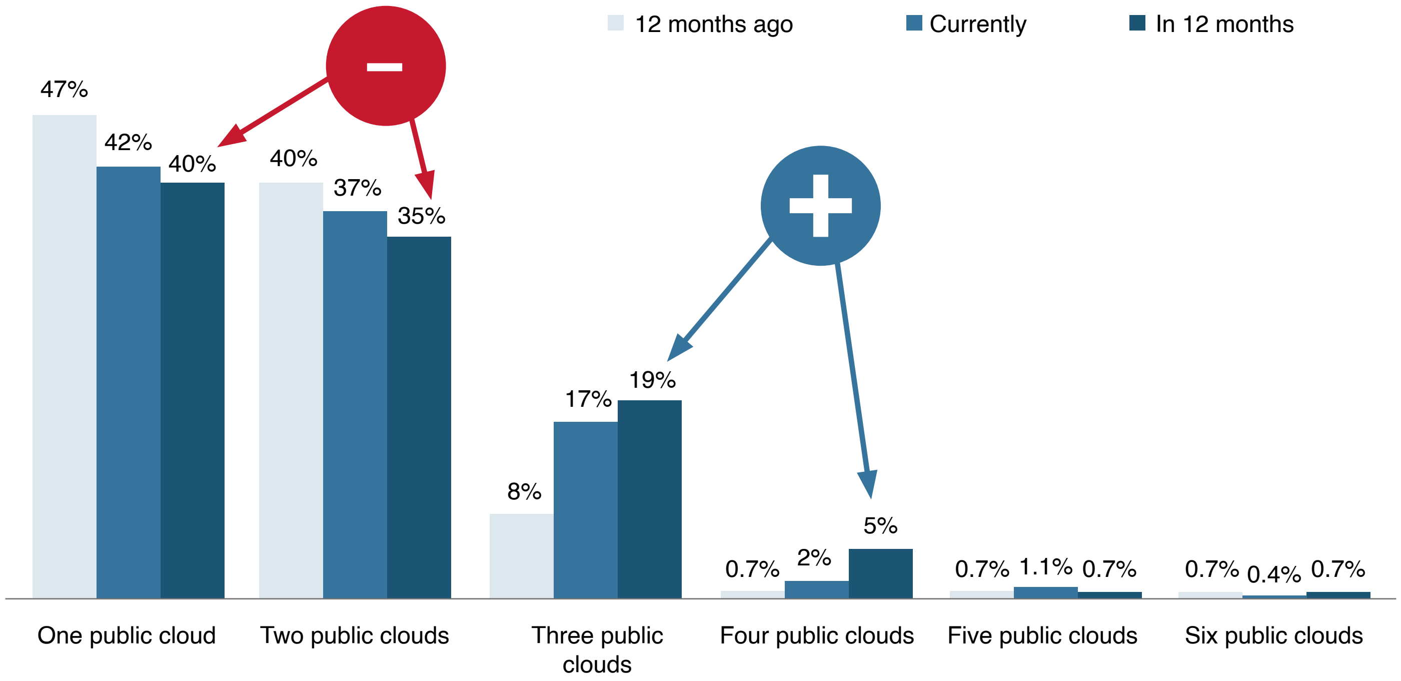
Organizations are increasingly reliant on a multi-cloud strategy for hosting applications.

< Prev Next >

See Figure 1.

Figure 1: Count of Public Clouds for Hosting Applications

Percentage of respondents



Source: Osterman Research (2022)

As organizations adopt multiple cloud platforms, the requirement for cloud security tools that offer consistent controls, policy, and visibility across a changing mix of cloud platforms becomes increasingly important.

Executive Summary

Growth Dynamics with Multi-Cloud

Attacks and Incidents in Multi-Cloud

Conclusion

Methodology

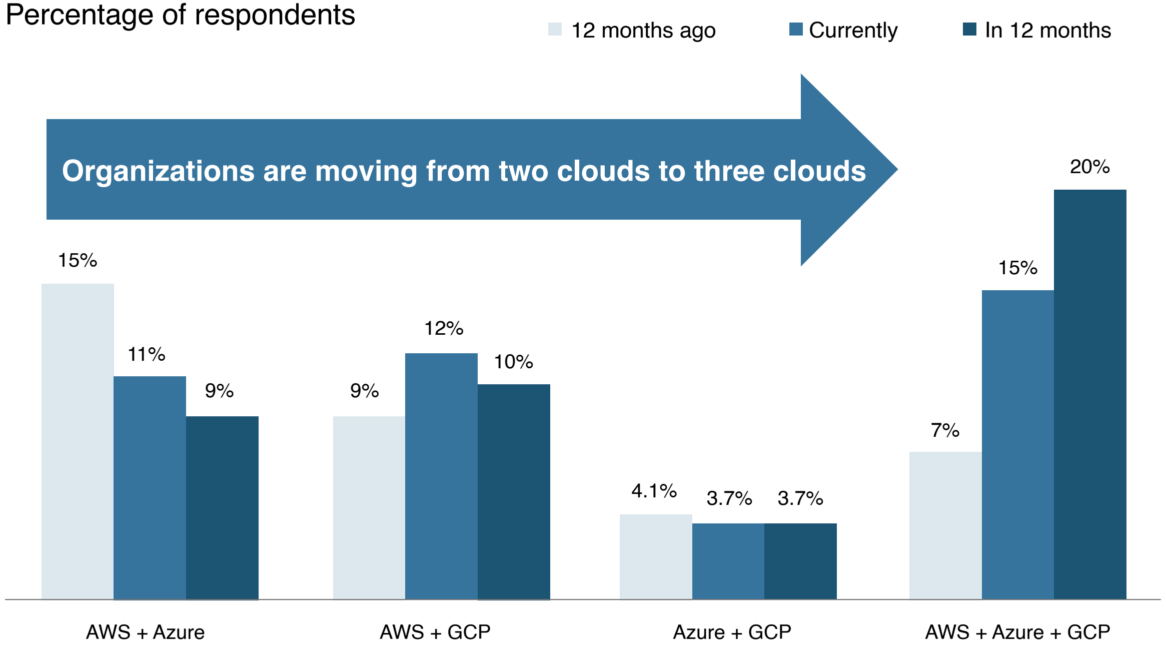
About Radware

Changing Combinations of Multi-Cloud

Organizations using two public clouds are juggling which cloud to use in combination with AWS, with an anticipated shift of the second cloud from Azure to Google Cloud platform. However, the more significant trend line is the transition of organizations towards using three public clouds in parallel, with the growth in this approach expected to triple over a two-year period from 7% to 20%. See Figure 2.

Figure 2: Changing Mix of Public Cloud Providers

Percentage of respondents



Source: Osterman Research (2022)

< Prev Next >

Respondents indicated that the adoption of multiple cloud services at their organization was most frequently driven by forces outside the IT department. More specifically, two primary drivers: individual business units adopting new applications and/or services and the adoption of shadow IT services.

As organizations juggle where they host applications across a changing mix and count of public cloud platforms, there will be a growing requirement for cloud platform agnostic security capabilities that work irrespective of the cloud platforms embraced by an organization, without forcing the security team to start over, or be left floundering as business groups respond to changing competitive market dynamics.

On-Premise Data Centers and Private Clouds are Still With Us

Using multiple public cloud platforms is only one component of the overall infrastructure reality at organizations, with most of them hosting applications across on-premises infrastructure and private cloud services. Although the use of on-premise infrastructure is expected to decline over time, and the use of private cloud services is expected to increase over time, there is a significant proportion of users expected to use these environments for the foreseeable future. See Figure 3 on the following page.

A small set of organizations use public cloud services exclusively. Only 5% of respondents indicated that their organization used public cloud platforms without also using on-premise infrastructure or private cloud services. While cloud-native and cloud-only approaches are heralded by firms in Silicon Valley as the way of the future, it remains a niche approach which is not widely adopted elsewhere.

3x

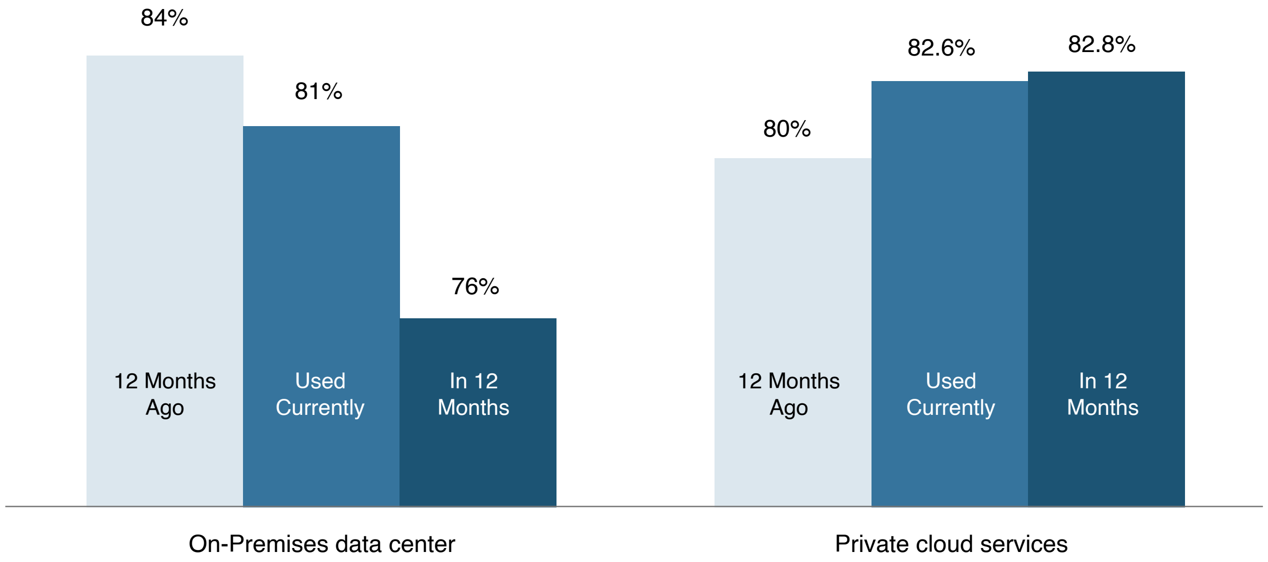
growth rate among organizations using three public clouds for hosting applications.

95%

of organizations are not cloud-native or only using public cloud platforms.

< Prev Next >

Figure 3: Other Environments for Hosting Applications
Percentage of respondents



Source: Osterman Research (2022)

Public cloud environments are the most widely used platform for hosting production applications. However, on-premise data centers and private cloud environments continue to host a significant proportion of applications. See figure 4 on the following page.

< Prev   Next >

Executive Summary

Growth Dynamics with Multi-Cloud

Attacks and Incidents in Multi-Cloud

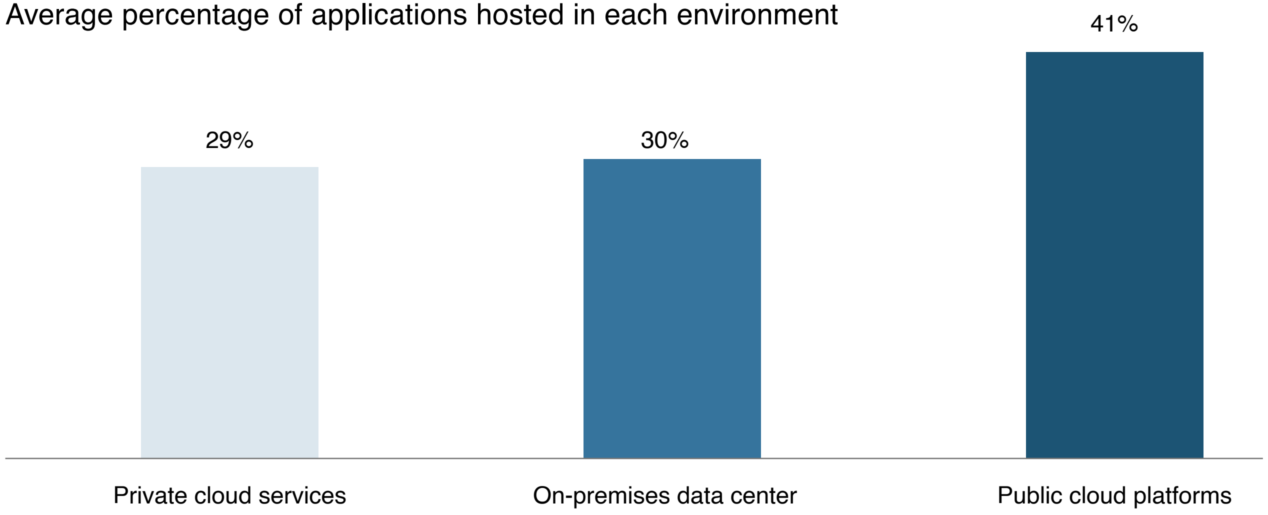
Conclusion

Methodology

About Radware

Figure 4: Hosting Approaches for Production Applications

Average percentage of applications hosted in each environment



Source: Osterman Research (2022)

< Prev Next >

The Multi-Cloud, Hybrid, and Cross-Cloud Infrastructure

Organizations are hosting applications across a changing mix of multi-cloud, hybrid, and cross-cloud infrastructure. The research found that:

- **Triple infrastructure design**
  45% of organizations currently use the following combination: private cloud services, on-premise infrastructure, and two or more public cloud services.
- **Hybrid infrastructures almost universally adopted**
  92% of organizations were using any combination of at least two of these types of infrastructure 12 months ago, and this has increased to 98% over the past year. Hybrid infrastructure is a deeply ingrained approach nearing market saturation.
- **Add CDNs to the mix**
  43% of organizations are currently using two CDNs across cloud-native and pure-play offerings. Over time, more organizations expect to use five or more.

45% of organizations use three types of infrastructure.

98% of organizations currently rely on hybrid infrastructure.

< Prev Next >

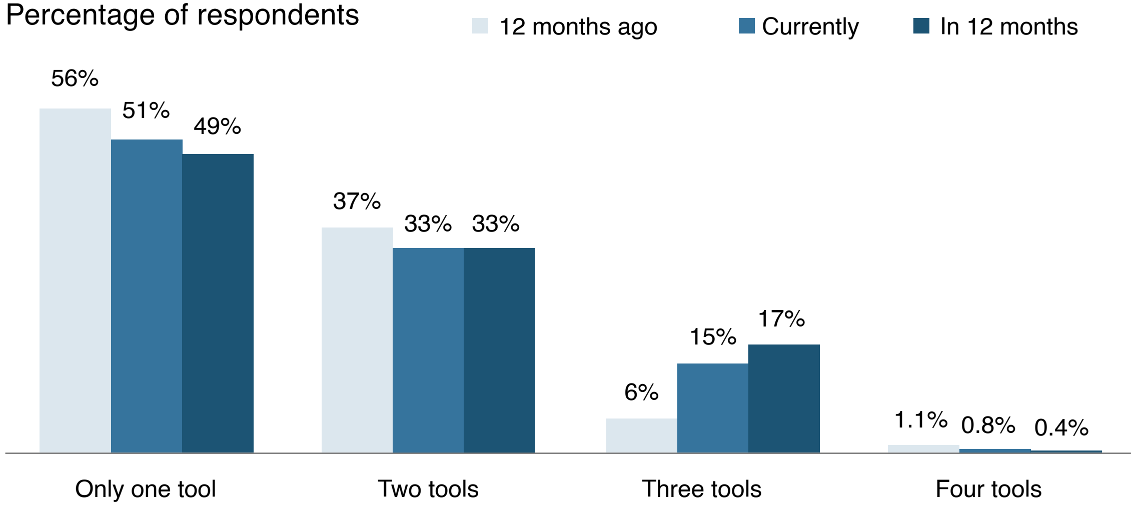
The Number of Security Tools is Increasing Too

An increasing percentage of organizations are using two or more cloud security tools—such as native public cloud WAFs (for example, AWS WAF) and CDN-based WAFs (for example, Akamai, Cloudflare). Currently, 49% of organizations use two or more cloud security tools, and 51% will use two or more in 12 months. The research found that the highest growth rate is amongst the organizations that use three cloud security tools—with a threefold increase expected from 6% of organizations 12 months ago, to 17% in 12 months. See Figure 5.

3x
growth rate of organizations using three cloud security tools.

Figure 5: Adoption of Cloud Security Tools

Percentage of respondents



Source: Osterman Research (2022)

Three out of four respondents are using a native public cloud WAF, and one out of two are using a CDN-based WAF.

< Prev Next >

Attacks and Incidents in Multi-Cloud

This section provides information about security threats and incidents that organizations face while embracing multi-cloud approaches, and how the organizations assess the efficacy of their security tools.

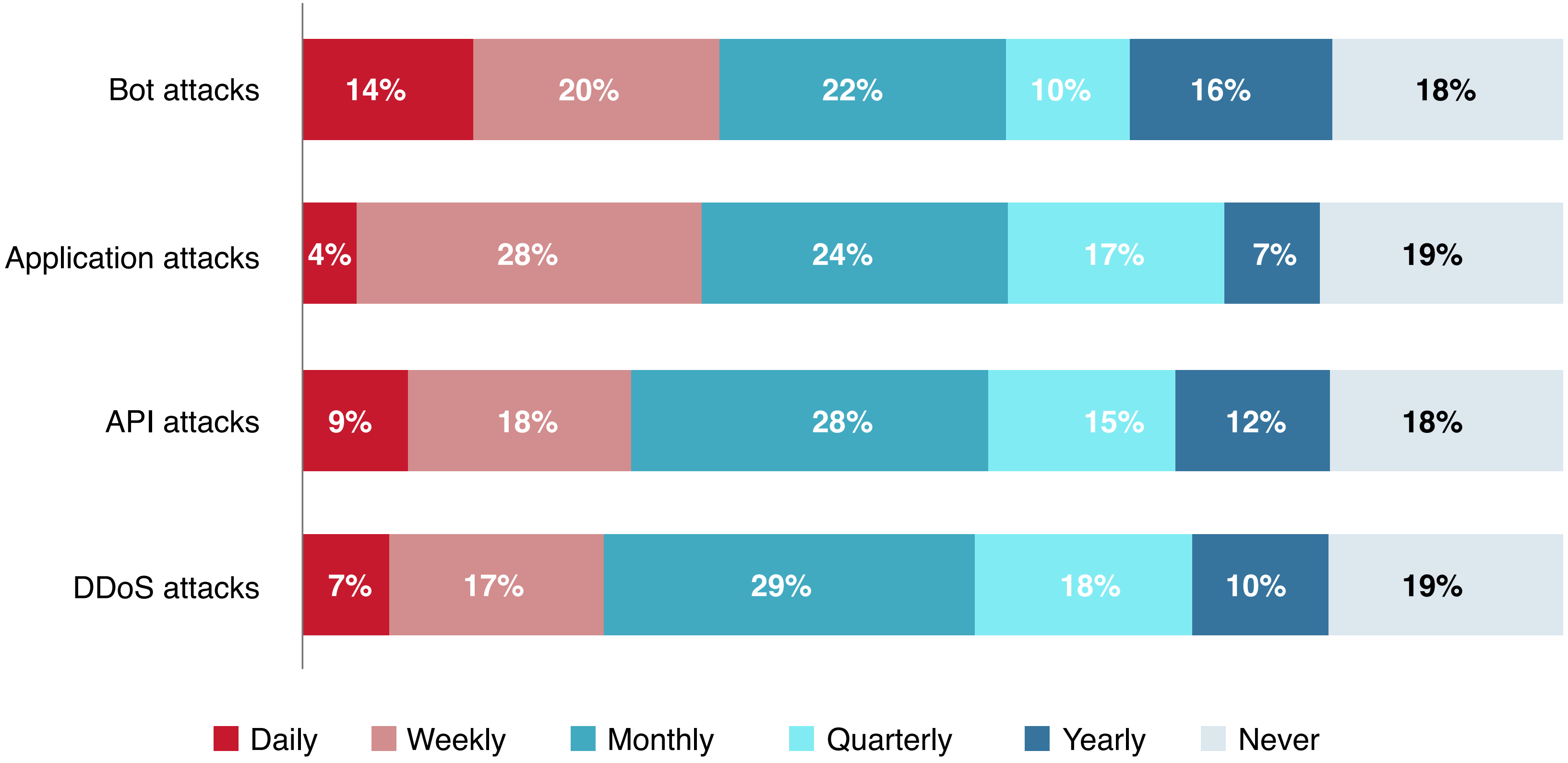
Attacks are Frequent

More than half of the respondents see four types of attacks against the applications used by their organization on a daily, weekly, or monthly basis. Bot attacks occur most frequently, with 14% of respondents reporting daily attacks and a further 20% indicating a weekly cadence. Application attacks are the second most frequently occurring type of attack, with 4% of the respondents seeing daily attacks and 28% weekly. See figure 6 on the following page.

< Prev Next >

Figure 6: Frequency of Attacks against Applications

Percentage of respondents



Source: Osterman Research (2022)

Executive Summary

Growth Dynamics with Multi-Cloud

Attacks and Incidents in Multi-Cloud

Conclusion

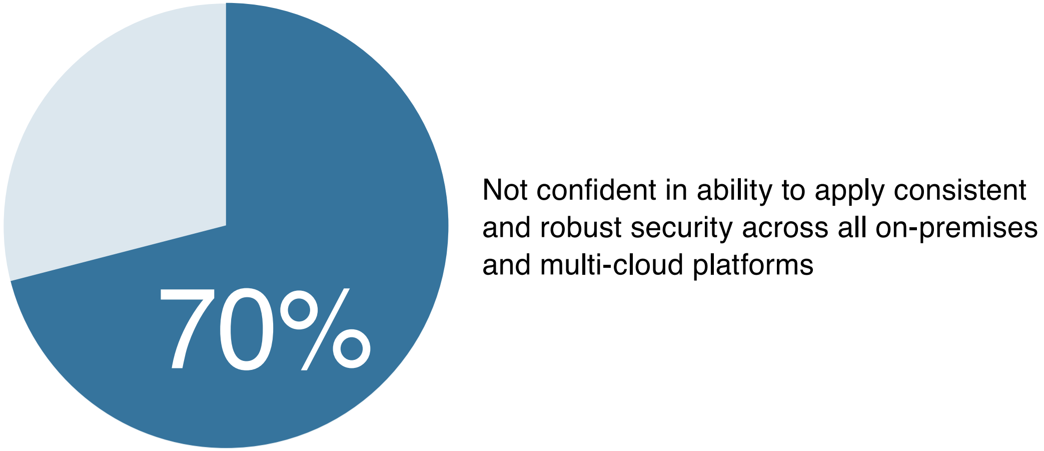
Methodology

About Radware

Confidence In Protection is Lacking

Almost 70% of the respondents are not confident in their ability to apply consistent and robust security across all on-premises and multi-cloud platforms in use. Lack of consistency in security policy configurations results in variations that can be weaponized in cyberattacks. See Figure 7.

Figure 7: Lack of Confidence in Applying Consistent and Robust Security in Multi-Cloud
Percentage of respondents



Source: Osterman Research (2022)

> *70%*
> *of organizations are not confident in their ability to apply consistent and robust security for applications hosted across all on-premises and multi-cloud platforms.*

Executive Summary

Growth Dynamics with Multi-Cloud

Attacks and Incidents in Multi-Cloud

Conclusion

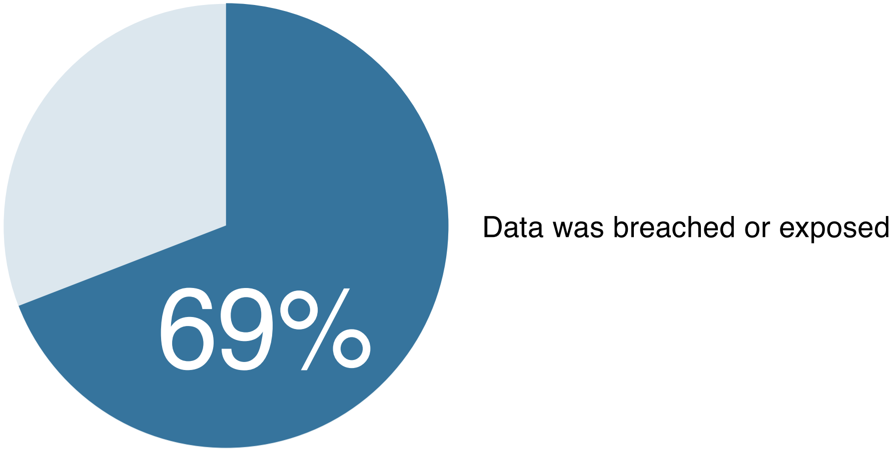
Methodology

About Radware

Breaches are Common

Around 69% of respondents acknowledged that they knew about data breaches or exposures, due to variations in how application security was configured across the different public cloud platforms that their organization uses to host applications. See Figure 8.

Figure 8: Data Breaches or Exposures from Variations in Application Security
Percentage of respondents



Source: Osterman Research (2022)

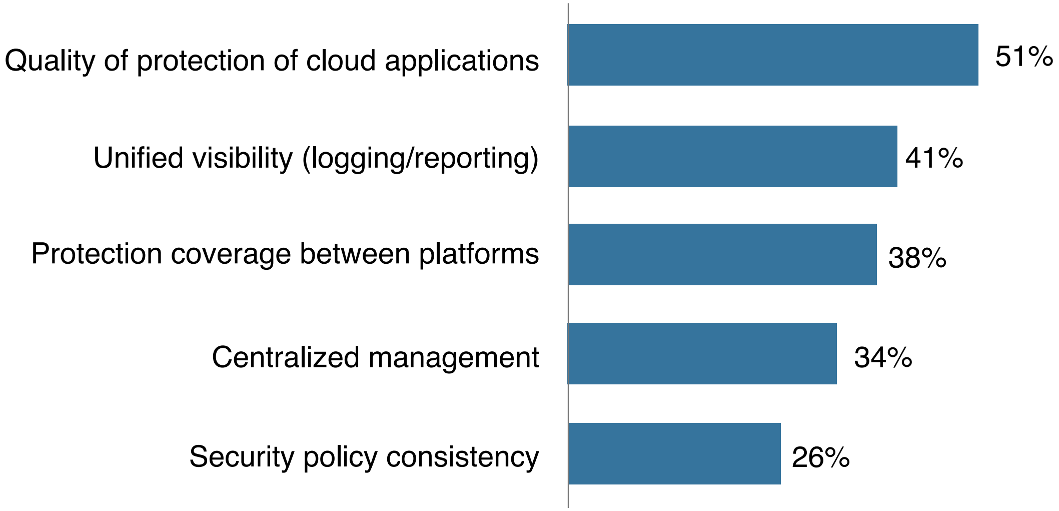
69%
of organizations have experienced data breaches or exposures due to inconsistent configurations in application security across public cloud platforms.

< Prev Next >

Biggest Problems are Quality of Security and Visibility

The lack of quality protection for cloud applications is a significant problem for half of the respondents, meaning that their current security solutions which are in use are unable to detect, block, prevent, or otherwise mitigate a cyberattack. Lack of unified visibility for logging and reporting is the second highest rated problem—an issue which will only intensify as organizations adopt more cloud platforms. Organizations are experiencing a barrage of attacks, 69% acknowledge a data breach or exposure from variations in application security across public cloud platforms, and hence it is highly concerning that security tools prove insufficient across a range of dimensions. See Figure 9.

Figure 9: Assessing Problems with Threats against Applications on Public Cloud Platforms
Percentage of respondents indicating "problem" or "extreme problem"

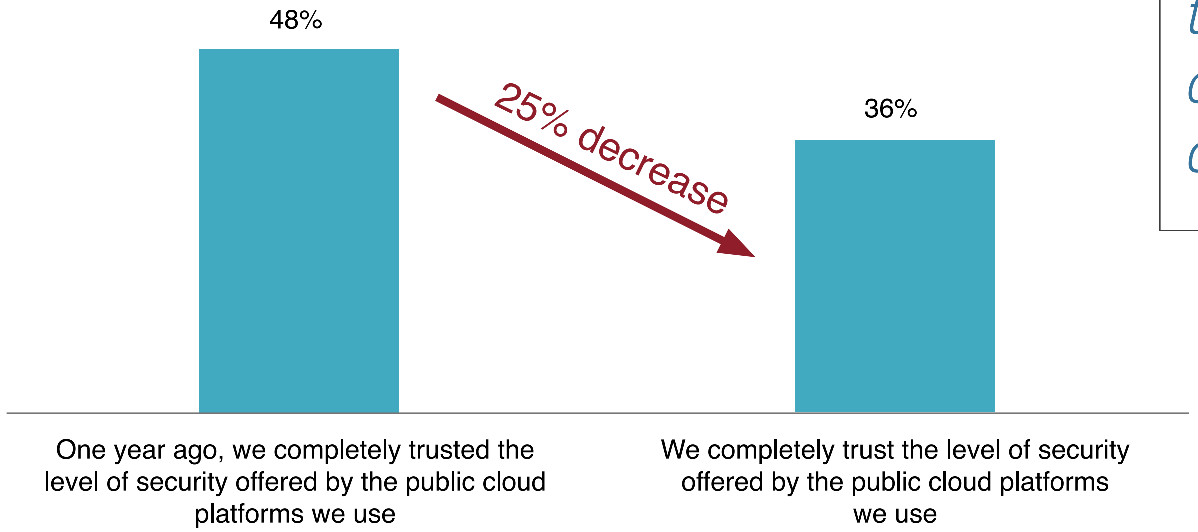


Source: Osterman Research (2022)

Trust In Cloud Security Tools is Declining

The trust in the efficacy of security protections offered by the public cloud platforms used by respondents is declining, with a 25% drop over the past 12 months. Only one-third of respondents currently indicate that they trust the level of security offered, down from half of respondents a year ago. See Figure 10.

Figure 10: Declining Trust in Security of Public Cloud Platforms
Percentage of respondents indicating "agree" or "strongly agree"



Source: Osterman Research (2022)

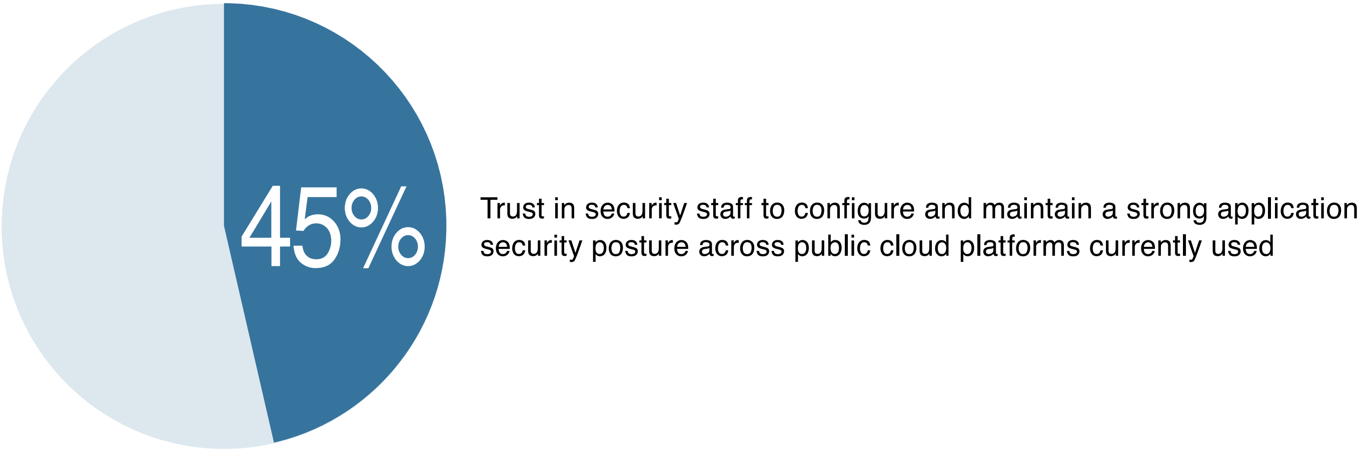
25% decrease over the past 12 months of organizations that trust the security offered by public cloud platforms.

< Prev Next >

Staff Shortages are Taking a Toll On Protection Quality

Less than half of the organizations indicate that they completely trust their security staff to configure and maintain a strong application security posture across the public cloud platforms that they currently use for hosting applications. When combined with the decreasing trust in the efficacy of security tools offered by public cloud platforms, organizations face decreasing capability to protect against a threat environment increasing in frequency, intensity, and business consequence. See Figure 11.

Figure 11: Trust in Security Staff 12 Months Ago
Percentage of respondents



Source: Osterman Research (2022)

Conclusion

As organizations increasingly deploy application in multi-cloud and hybrid cloud environments, they will face more and more challenges with cross-cloud application security management: maintaining quality of protection, consistency across platforms, centralized visibility and centrality in security management.

The conflation of these trends with data breaches caused by inconsistent security configurations and low trust in security staff at many organizations means that urgent action is required to reevaluate how to assure security irrespective of where applications are hosted.

< Prev Next >

Executive Summary

Growth Dynamics with Multi-Cloud

Attacks and Incidents in Multi-Cloud

Conclusion

Methodology

About Radware

Methodology

This report was commissioned by Radware and conducted by Osterman Research. 269 respondents in security roles were surveyed during May-June 2022. 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, China fielded in French, German, and Chinese respectively. The survey was cross-industry, and no industries were excluded or restricted from the survey.

JOB ROLE

Senior network security admin	30%
Senior DevOps and/or DevSecOps admin	28%
VP or senior manager of research and development	24%
Application security architect	13%
Cloud security architect	4%
API architect or senior developer	1%

< Prev Next >

Geography

North America (41%)	
Canada	26%
United States	15%
EMEA (31%)	
United Kingdom	12%
France	10%
Germany	9%
APAC/LATAM (28%)	
Australia or New Zealand	6%
Brazil	6%
China	6%
India	6%
Mexico	6%

Industry

Manufacturing	12%
Logistics/Transportation	9%
Professional Services (e.g., Legal, Marketing, Real Estate)	9%
Retail/Distribution	9%
Healthcare	8%
Technology	7%
Consumer Products	6%
Education	6%
Life sciences (Pharmaceuticals, Medical, Biotech)	6%
Financial Services/Banking	5%
Insurance	5%
Energy/Utilities/Oil/Gas/Minerals/Mining	4%
Construction/Architecture/Engineering	4%
Aerospace/Defense	3%
Chemicals	3%
Food/Beverage	3%
Government	2%
Media/Entertainment	0.4%

< Prev Next >

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.

< Prev