INTRODUCTION

Organizations continue to shift workloads to the cloud at a rapid pace to achieve faster time to market, increased responsiveness, and cost reductions. With the majority of organizations expected to have more than half their workloads in the cloud within the next 12-18 months, it is no surprise that cloud security continues to remain a top concern.

This 2022 Cloud Security Report, based on a comprehensive global survey of cybersecurity professionals, reveals these security challenges and offers fresh insights on the state of the cloud and cloud security today. The study reviews organizations’ choices and responses as they try to gain more confidence in securing their cloud environments.

The following survey results highlight the insights uncovered in this report:

• Most organizations continue to pursue a hybrid (39%, up from 36% last year) or multi-cloud strategy (33%) to integrate multiple services, for scalability, or for business continuity reasons. Seventy-six percent are utilizing two or more cloud providers.

• Organizations continue to shift workloads to the cloud at a rapid pace. Today, 39% of respondents have more than half of their workloads in the cloud, while 58% plan to get to this level in the next 12-18 months.

• Cloud users confirm that the cloud is delivering on the promise of flexible capacity and scalability (53%), increased agility (50%), and improved availability and business continuity (45%).

• Security professionals highlight lack of visibility (49%), high cost (43%), lack of control (42%), and lack of security (22%) as the biggest unforeseen factors to slow or stop cloud adoption.

• Cloud security continues to be a significant concern for cybersecurity professionals. With an increase of two percentage points from last year, 95% of organizations are moderately to extremely concerned about their security posture in a public cloud environment.

• Over three-quarters (78%) of respondents consider it very to extremely helpful to have a single cloud security platform with a single dashboard to protect data consistently and comprehensively across their cloud footprint.

We would like to thank Fortinet for supporting this important industry research project. We hope you’ll find this report informative and helpful as you continue your efforts in securing your organization’s cloud journey against evolving threats.

Thank you,

Holger Schulze
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current State of Cloud Adoption</td>
<td>4</td>
</tr>
<tr>
<td>Benefits of the Cloud: Best of Both Worlds</td>
<td>10</td>
</tr>
<tr>
<td>Barriers to Adoption</td>
<td>13</td>
</tr>
<tr>
<td>Security Concerns in the Cloud</td>
<td>16</td>
</tr>
<tr>
<td>Key Priorities for Cloud Security</td>
<td>19</td>
</tr>
<tr>
<td>Methodology &amp; Demographics</td>
<td>25</td>
</tr>
</tbody>
</table>
Current State of Cloud Adoption
Organizations continue to shift workloads to the cloud at a rapid pace. Today, 39% of respondents have more than half of their workloads in the cloud, while 58% plan to get to this level in the next 12-18 months.

What percentage of your workloads are in the cloud today?

39% are running more than 50% of workloads in the cloud

What percentage of your workloads will be in the cloud in the next 12-18 months?

58% will be running more than 50% of workloads in the cloud

Share of workloads in the cloud
We asked cybersecurity professionals what services and workloads their organizations are most frequently deploying in the cloud. Security services top the list (58%), followed by compute (56%), storage (55%), and virtualization (53%).

What services and workloads is your organization deploying in the cloud?

- **Security** (identity management, access control, data protection, etc.)
  - 58%

- **Compute** (servers, containers, etc.)
  - 56%

- **Storage** (object storage, archive, backup, etc.)
  - 55%

- **Virtualization**
  - 53%

- **Business applications** (CRM, marketing automation, ERP, BI, project management, etc.)
  - 52%

- **Database** (relational, NoSQL, caching, etc.)
  - 49%

- **Productivity applications** (email, collaboration, instant messaging, etc.)
  - 47%
Most organizations continue to pursue a hybrid (39%, up from 36% last year) or multi-cloud strategy (33%, down from 35% last year) for integration of multiple services, scalability, or business continuity reasons. Seventy-six percent are utilizing two or more cloud providers.

What is your primary cloud deployment strategy?

- **39%** Hybrid (e.g., integration between private and public clouds)
- **33%** Multi-cloud (e.g., multiple providers without integration)
- **27%** Single cloud

How many cloud providers does your organization currently use?

- **76%** use two or more cloud providers
- **20%** One
- **34%** Two
- **22%** Three
- **20%** More than 3
- **4%** None
The most popular cloud providers, Microsoft Azure and Amazon Web Services (AWS), are tied (73%), as AWS has gained three percentage points since last year’s survey. This is followed by Google Cloud Platform (38%). Year-over-year, Oracle Cloud use increased the most (from 15% to 21%).

What cloud IaaS provider(s) do you currently use?
DevSecOps helps ensure that security is addressed as part of DevOps practices by integrating security and compliance throughout the entire software development process. While only 19% of respondents already have comprehensive DevSecOps in place, 40% incorporate some aspects of DevSecOps within the organization.

What is your organization’s current position on DevSecOps?

- Comprehensive DevSecOps program in place: 19%
- DevSecOps in some parts of the organization: 40%
- We’re considering DevSecOps adoption: 25%
- DevSecOps is just a novel word, it’s nothing new: 11%
- We’re not interested in DevSecOps adoption: 10%
- I’m not familiar with DevSecOps: 10%
- Other: 3%
Benefits of the Cloud: Best of Both Worlds
CLOUD DELIVERS BUSINESS RESULTS

The survey confirms that organizations are receiving the promised business outcomes of cloud computing: faster time to market (51%), increased responsiveness (50%), and cost reductions (39%).

What business outcomes have you realized by moving to the cloud?

- **51%** Accelerated time to market
- **50%** Increased responsiveness to customer needs
- **39%** Reduced cost
- **37%** Reduced risk and improved security
- **21%** Expanded market reach to new markets
- **19%** Accelerated revenue growth in existing markets
- **19%** Gained parity with competitors

Other 7%
Does cloud computing deliver the expected benefits? Cloud users confirm that the cloud is delivering on the promise of flexible capacity and scalability (53%), increased agility (50%), and improved availability and business continuity (45%).

What overall benefits have you already realized from your cloud deployment?

- More flexible capacity/scalability: 53%
- Increased agility: 50%
- Improved availability and business continuity: 45%
- Improved security: 27%
- Increased geographic reach: 27%
- Increased employee productivity: 22%
- Improved regulatory compliance: 21%
- Reduced complexity: 19%
- Not sure/other: 12%
- Moved expenses from fixed CAPEX (purchase) to variable OPEX (rental/subscription): 40%
- Improved performance: 38%
- Reduced cost: 35%
- Accelerated time to market: 32%
Barriers to Adoption
BARRIERS TO CLOUD ADOPTION

Cloud-based solutions offer significant advantages, yet barriers to cloud adoption still exist. The survey reveals that the biggest challenges organizations are facing are not primarily about technology, but people and processes. Lack of qualified staff (40%, up from 37% last year) is the biggest impediment to faster adoption, followed by legal and regulatory compliance (33%), and data security issues (31%).

What are the biggest barriers holding back cloud adoption in your organization?

- Lack of staff resources or expertise: 40%
- Legal and regulatory compliance: 33%
- Data security, loss and leakage risks: 31%
- Integration with existing IT environment: 30%
- Fear of vendor lock-in: 26%
- General security risks: 24%
- Loss of control: 21%
When we asked what surprises security professionals uncovered that hinder cloud adoption, we discovered lack of visibility (49%), high cost (43%), lack of control (42%), and lack of security (22%) are the biggest unforeseen factors that slow or stop cloud adoption.

What surprises did you uncover that may slow/stop cloud adoption?

- 49% Lack of visibility
- 43% High cost
- 42% Not enough control
- 22% Not secure
- Other 13%
Security Concerns in the Cloud
PUBLIC CLOUD SECURITY CONCERNS

Cloud security continues to be a significant concern for cybersecurity professionals. With an increase of two percentage points from last year, 95% of organizations are moderately to extremely concerned about their security posture in a public cloud environment.

How concerned are you about the security of public clouds?

95% of organizations are moderately to extremely concerned about cloud security

- Extremely concerned: 32%
- Very concerned: 43%
- Moderately concerned: 20%
- Slightly concerned: 4%
- Not at all concerned: 1%
We asked cybersecurity professionals about the cloud security threats that most concern them. The misconfiguration of the cloud platform remains the biggest cloud security risk, according to 62% of cybersecurity professionals in our survey. This is followed by insecure interfaces/APIs (52%, up from 49% last year), exfiltration of sensitive data (51%), and unauthorized access (50%).

What do you see as the biggest security threats in public clouds?

- Misconfiguration of the cloud platform/wrong setup: 62%
- Insecure interfaces/APIs: 52%
- Exfiltration of sensitive data: 51%
- Unauthorized access: 50%
- Hijacking of accounts, services, or traffic: 44%
- Foreign state-sponsored cyber attacks: 37%
- Malware/ransomware: 36%
- Malicious insiders: 34%
- Denial of service attacks: 33%
- Cloud cryptojacking: 20%
- Theft of service: 18%
- Lost mobile devices: 10%
- Don't know/other: 8%
Key Priorities for Cloud Security
When asked about their security priorities for the current year, organizations highlighted preventing cloud misconfigurations (20%), reaching regulatory compliance (19%), securing cloud apps (16%), and defending against malware (15%).

What are your cloud security priorities for your company this year?

- Preventing cloud misconfigurations: 20%
- Reaching regulatory compliance: 19%
- Securing major cloud apps already in use: 16%
- Defending against malware: 15%

- Cloud security training: 11%
- Securing mobile devices: 8%
- Discovering unsanctioned cloud apps in use: 5%
- Securing BYOD (bring your own device): 5%
Security professionals are looking for ways to improve the security of public clouds. When asked which controls would increase their confidence in adopting cloud services, three controls top the list: encryption of data-at-rest (54%), automating compliance (46%), and setting and enforcing security policies (46%).

Which of the following security controls would most increase your confidence in adopting public clouds?

- Encryption of data-at-rest: 54%
- Automating compliance: 46%
- Setting and enforcing security policies across clouds: 46%
- APIs for reporting, auditing and alerting on security events: 42%
- Isolation/protection of virtual machines: 41%
- Creating data boundaries: 41%
- Leveraging data leakage prevention tools: 41%

Leveraging threat prevention tools 34% | Limiting unmanaged device access 32% | Protecting workloads 31% | Proxying traffic for real-time security at access 23% | Other 3%
MULTI-CLOUD SECURITY CHALLENGES

Multi-cloud environments continue to add complexity and security challenges. Lack of security skills becomes the top challenge (61%, up from 57% last year), followed by data protection (53%), understanding how different solutions fit together (51%), and loss of visibility and control (47%).

What are your biggest challenges securing multi-cloud environments?

- Having the right skills to deploy and manage a complete solution across all cloud environments: 61%
- Ensuring data protection and privacy for each environment: 53%
- Understanding how different solutions fit together: 51%
- Loss of visibility and control: 47%
- Understanding service integration options: 44%
- Keeping up with the rate of change: 37%
- Selecting the right set of services: 36%
- Managing the costs of different solutions: 36%
Organizations prioritize several critical drivers for considering cloud-based security solutions over legacy platforms. The biggest drivers are better scalability (55%) and faster time to deployment (50%), followed by cost savings (43%) and better visibility into user activity and system behavior (40%).

What are the main drivers for considering cloud-based security solutions?

- Better scalability: 55%
- Faster time to deployment: 50%
- Cost savings: 43%
- Better visibility into user activity and system behavior: 40%
- Reduced effort around patches and upgrades of software: 39%
- Meet cloud compliance expectations: 37%
- Easier policy management: 36%
- Need for secure app access from any location: 35%
- Better uptime: 34%
- Better performance: 32%
- Our data/workloads reside in the cloud (or are moving to the cloud): 31%
- Reduction of appliance footprint in branch offices: 29%
- Other: 3%
SINGLE CLOUD SECURITY PLATFORM

It’s no surprise that over three-quarters (78%) of respondents consider it very to extremely helpful to have a single cloud security platform to protect data consistently and comprehensively across their cloud footprint.

How helpful would it be to have a single cloud security platform with a single dashboard where you could configure all of the policies needed to protect data consistently and comprehensively across your cloud footprint?
The 2022 Cloud Security Report is based on a comprehensive global survey of 823 cybersecurity professionals conducted in March 2022 to uncover how cloud user organizations are responding to security threats in the cloud, and what training, certifications, and best practices IT cybersecurity leaders are prioritizing in their move to cloud. The respondents range from technical executives to IT security practitioners, representing a balanced cross-section of organizations of varying sizes across multiple industries.

**METHODOLOGY & DEMOGRAPHICS**

**CAREER LEVEL**

- Specialist: 24%
- Manager/Supervisor: 19%
- CTO, CIO, CISCO, CMO, CFO, COO: 16%
- Consultant: 12%
- Director: 10%
- Other: 19%

**DEPARTMENT**

- IT Security: 54%
- IT Operations: 16%
- Engineering: 7%
- Compliance: 5%
- SecOps: 3%
- Operations: 3%
- Other: 12%

**COMPANY SIZE**

- Fewer than 10: 4%
- 10-99: 14%
- 100-499: 14%
- 500-999: 9%
- 1,000-4,999: 16%
- 5,000-9,999: 11%
- Over 10,000: 32%

**INDUSTRY**

- Technology, Software & Internet: 24%
- Financial Services: 17%
- Government: 16%
- Professional Services: 7%
- Healthcare, Pharmaceuticals & Biotech: 7%
- Telecommunications: 4%
- Energy: 4%
- Manufacturing: 4%
- Education & Research: 3%
- Other: 14%

**SECURITY CERTIFICATIONS HELD**

- CISSP: 86%
- CISM: 24%
- CCSP: 19%
- CISA: 19%
- Security+: 16%
- CEH: 13%
- Network+: 10%
- CRISC: 9%
- Other: 41%
Fortinet (NASDAQ: FTNT) secures the largest enterprises, services providers, and government organizations around the world. Fortinet empowers our customers with complete visibility and control across the expanding attack surface and the power to take on ever-increasing performance requirements today and into the future. Only the Fortinet Security Fabric platform can address the most critical security challenges and protect data across the entire digital infrastructure, whether in networks, application, multi-cloud, or edge environments. Fortinet ranks #1 as the company with the most security appliances shipped worldwide and more than 500,000 customers trust Fortinet to protect their businesses.

www.fortinet.com
Cybersecurity Insiders is a 500,000+ member online community for information security professionals, bringing together the best minds dedicated to advancing cybersecurity and protecting organizations across all industries, company sizes, and security roles.

We provide cybersecurity marketers with unique marketing opportunities to reach this qualified audience and deliver fact-based, third-party validation thought leadership content, demand-generation programs, and brand visibility in the cybersecurity market.

For more information please visit www.cybersecurity-insiders.com