



Enterprise Strategy Group | Getting to the bigger truth.™

# A Guide to Managing Security Risks and Protecting Workloads in AWS

Accelerate Digital Transformation with Confidence by Augmenting AWS Security Services with Best-in-class Third-party Solutions

By **Doug Cahill**, Vice President, Analyst Services and Senior Analyst

JULY 2022

# CONTENTS

CLICK TO FOLLOW



## 3 Executive Summary

---

Organizations are moving workloads and applications to public cloud platforms...



## 5 Market Overview

---

Public cloud represents a generational shift in computing. No organization can effectively compete in today's market...



## 7 Cybersecurity Challenges

---

While the shift to public cloud can be great for business agility and innovation...




## 13 The Bigger Truth

---

As organizations move their workloads to AWS to optimize business operations and enable rapid innovation to best serve their customers...

---



ESG research shows **that strengthening cybersecurity tools and processes is the top IT initiative in 2022.**”

---

## Executive Summary

Organizations are moving workloads and applications to public cloud platforms to facilitate faster product delivery, data-driven customer experiences, business innovation, and digital transformation, to name just a few of the cloud’s myriad benefits. Because of the cloud’s speed and flexibility in empowering richer experiences for customers and employees, organizations need a comprehensive, in-depth approach to cybersecurity that is agile enough to keep up with the versatility, speed, and scalability of the cloud.

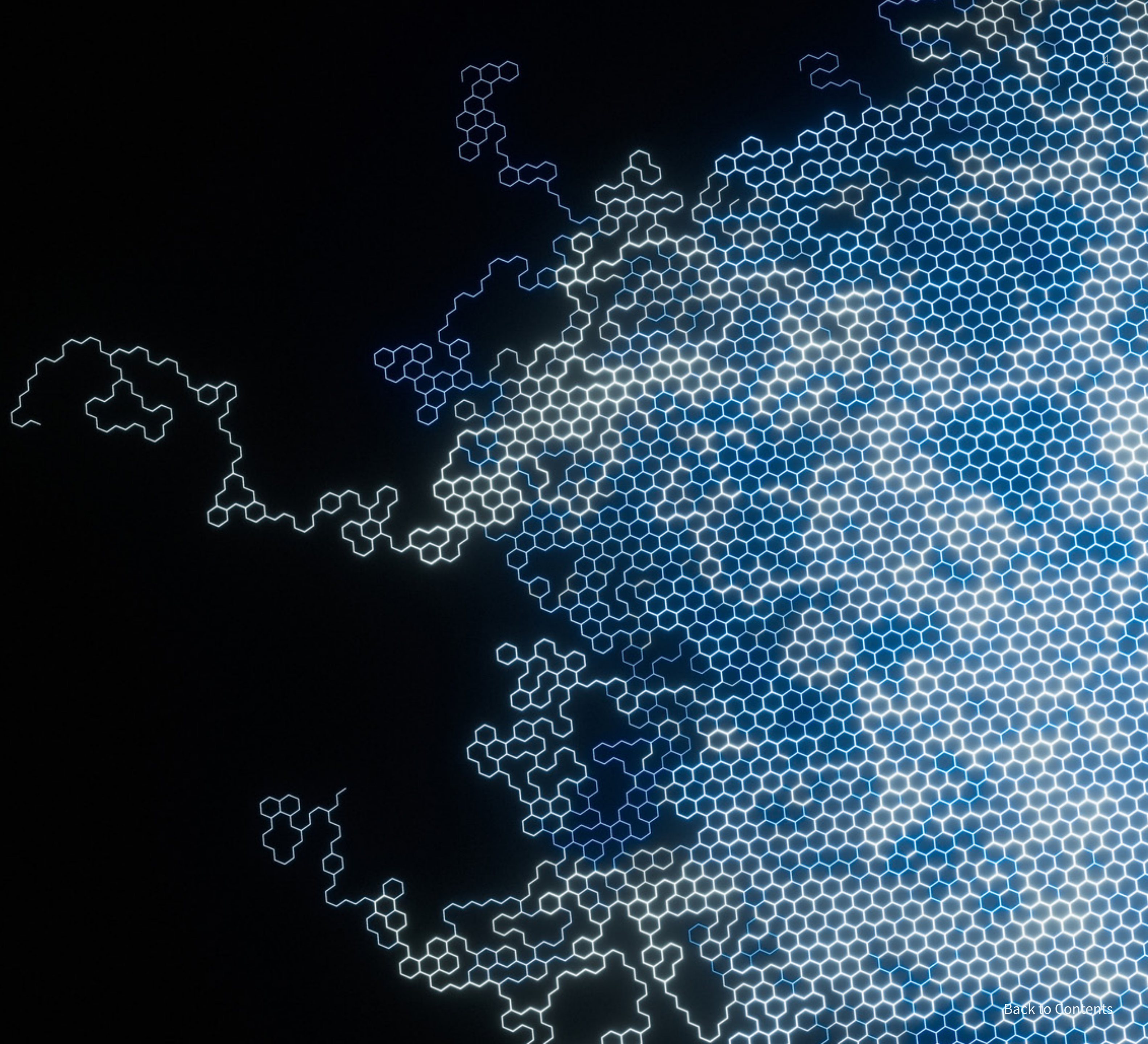
ESG research shows that strengthening cybersecurity tools and processes is the top IT initiative in 2022, followed by the use of public cloud for applications and infrastructure.<sup>1</sup> The reality that cybersecurity and public cloud are so tightly linked should come as no surprise to anyone, let alone business leaders, IT teams, and chief information security officers (CISOs). They are living on the front lines every day and are well aware of the risks a successful cybersecurity attack can pose to any organization in today’s environment.

Managing security risks and protecting workloads in the public cloud is far different than on-premises cybersecurity architectures. With their shared responsibility models, public cloud service providers (CSP) take care of many aspects that would traditionally be the responsibility of the customer, particularly infrastructure in the cloud. For the organization, they would be responsible for their data, customers, and compliance obligations. Organizations are also responsible for their overall security posture and they are best served when they regard the CSP as their partner, not their end-to-end complete solution.

When it comes to public cloud security, AWS offers resources and services to help its customers. AWS has been a leader since the early days of public cloud, and their shared responsibility model represents industry-accepted best practices. Within the AWS environment, there are tools and services AWS offers directly to manage security risks and protect workloads.

There are also third-party cloud-native solutions that augment AWS security services to provide added protection and reduced risk. The best of these third-party products are valuable for a wide range of use cases, adding capabilities such as centralized management, integrated threat intelligence, and extended visibility to address more advanced security needs. But more importantly, third-party solutions that can also simplify and rationalize security findings in a way that can enable security teams to focus and respond to the most critical security risks easily will undoubtedly set them apart from the many other third-party solutions in the market.

This eBook examines the business opportunities of moving more applications and workloads to the public cloud and the cybersecurity challenges that must be addressed, focusing on the AWS environment. We explore issues such as the use of too many tools, alert fatigue, lack of visibility, and more—all of which can slow down, hinder, or, worse, derail your cloud journey. Finally, we look at one of AWS's third-party cybersecurity partners, Fortinet, and AWS solutions, which are designed to work together to help organizations effectively manage security risks, meet compliance obligations, and protect workloads in AWS.



## Market Overview

Public cloud represents a generational shift in computing. No organization can effectively compete in today's market or hope to leverage the benefits of digital transformation without a commitment to and reliance on public cloud. ESG research shows that public cloud usage is already ubiquitous, with 95% of organizations currently using public cloud services and a desire to move many more applications and workloads to the public cloud in the future (see Figure 1).<sup>2</sup>

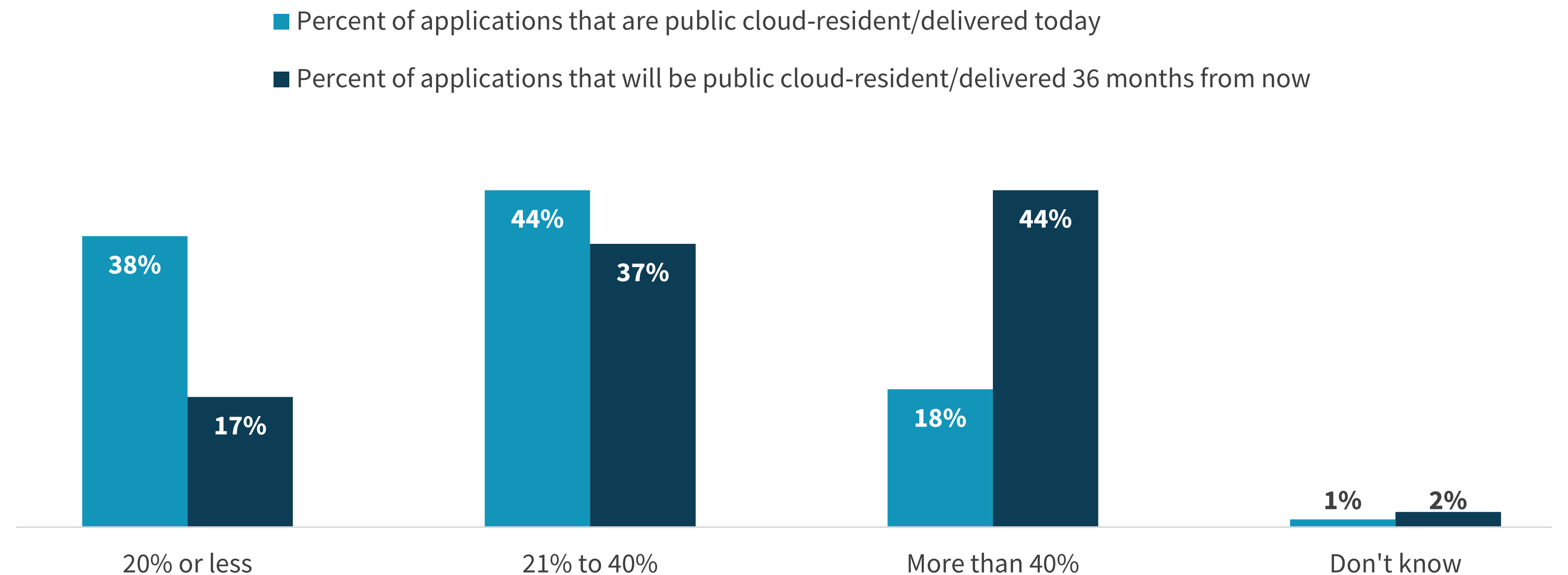


# 95%

of organizations currently use public cloud services

“ESG research shows that public cloud usage is already ubiquitous.”

Figure 1. Public Cloud Adoption Is Ubiquitous with Usage Deepening.



<sup>2</sup> Ibid.

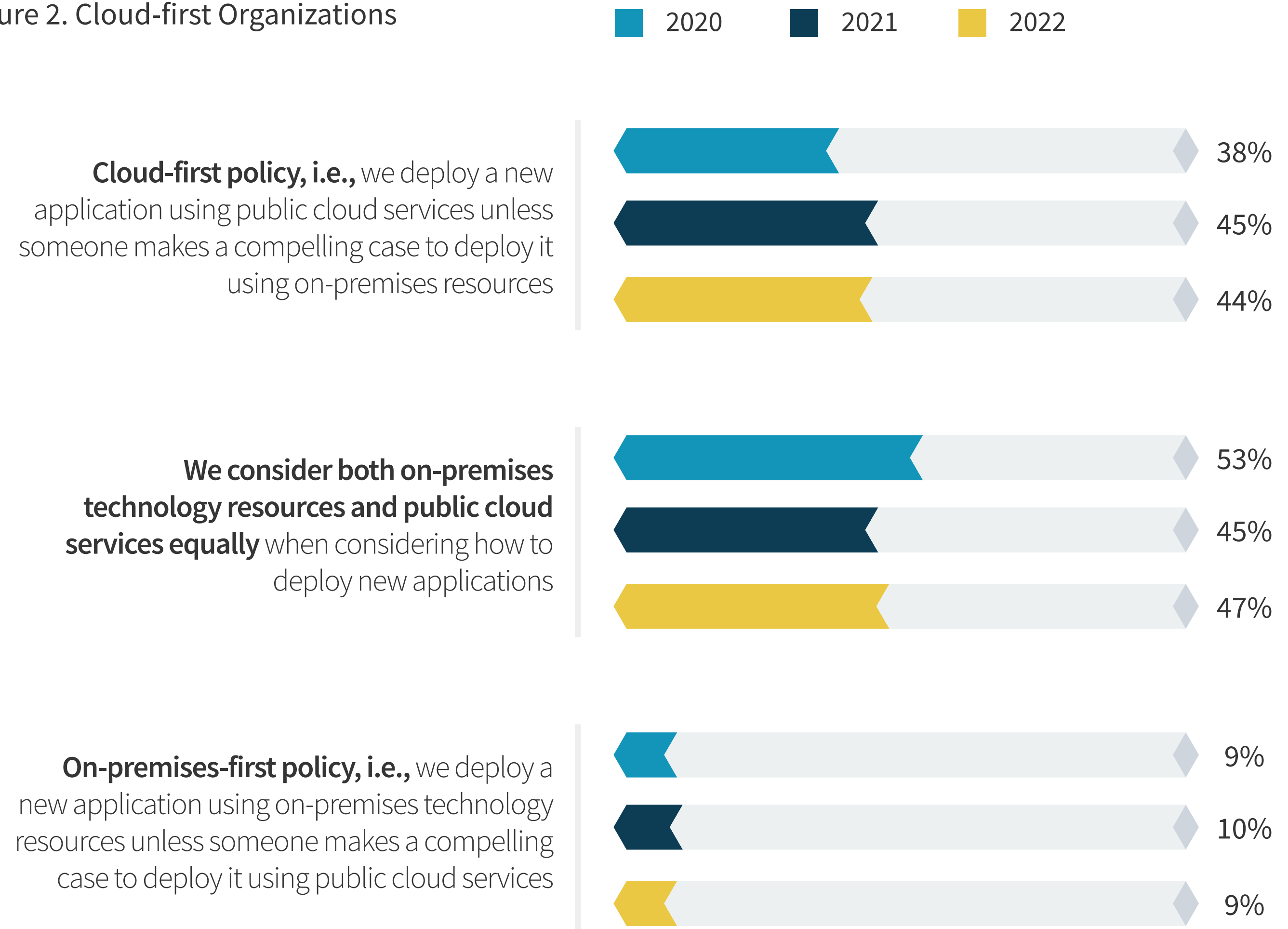
In fact, the shift to public cloud has become so predominant, especially among younger and digitally transformed companies, that more than four in 10 organizations in 2022 consider themselves to be “cloud-first.” Among companies that consider themselves to be at the mature stage of digital transformation, 54% of respondents described themselves as cloud-first, which means that most companies still have a huge opportunity to expand their use of public cloud to drive digital business opportunities and innovation (see Figure 2).



**4 in 10**

organizations in 2022 consider themselves to be **cloud-first**.<sup>3</sup>

Figure 2. Cloud-first Organizations



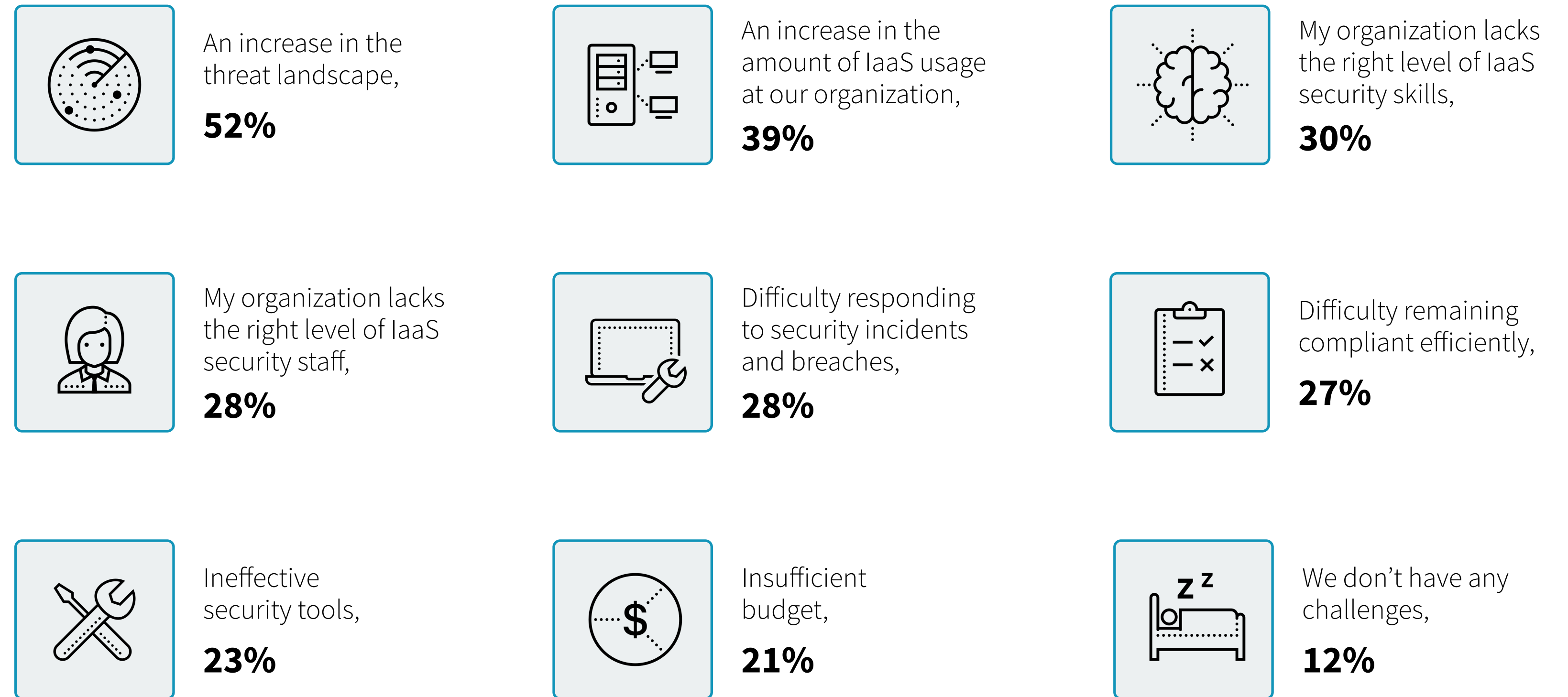
<sup>3</sup> Ibid.

## Cybersecurity Challenges

While the shift to public cloud can be great for business agility and innovation, organizations can only reap those benefits if they can effectively manage cybersecurity to mitigate risk, protect workloads, and assure compliance. The challenges are compounded by the reality that cybersecurity must be seamless and cannot get in the way of operational efficiency, which is an important consideration for businesses and IT teams. In fact, a majority of the respondents to the ESG 2022 Technology Spending Intentions Survey (52%) said that becoming more operationally efficient was a top objective for their organization’s digital transformation initiatives.

In looking at the specific challenges of public cloud infrastructure security, among the most often cited challenges are an increase in the threat landscape, increased usage of public cloud services, lack of skills, difficulty responding to security incidents and breaches, difficulty in compliance, and ineffective security tools (see Figure 3).<sup>4</sup>

Figure 3. Public Cloud Infrastructure Challenges



There are many ways these challenges manifest in ways that can create additional risks in security, data protection, and compliance, which, in the end, can stall or even stop the best-intentioned digital transformation initiatives. Among the most common challenges facing organizations and their cybersecurity teams are:

**Too many tools.** The rush to the cloud leads to customers adding more tools to avoid insufficient security coverage. According to ESG research, organizations typically use tools from more than five vendors,<sup>5</sup> and they are focusing their efforts on consolidating their tools. This is because the tools from different vendors may not be integrated, so the alerts tend to pile up. Plus, using too many tools can be costly and time consuming to manage, causing a negative impact on return on investment (ROI).<sup>6</sup>

**Lack of visibility due to a fragmented architecture:** Too many tools leads to a fragmented architecture, which leads to a lack of visibility and lack of integration across an organization's environment. How can an organization respond to threats if it can't see them? How can the organization rely on a coordinated response when its security tools are not coordinated? How can it introduce new capabilities, such as automation or comprehensive threat intelligence, when its tools are siloed and managed from separate panes of glass? The answer is that an organization can't do any of these things with confidence and trust that they will be truly effective.

**Alert fatigue caused by lack of context:** Organizations are dealing with a much larger attack surface than ever, and it continues to grow exponentially. The shift to cloud is a major contributor, but there are many additional factors, primarily the expansion of hybrid work and the growth of Internet of Things. When cybersecurity teams and security operations centers (SOC) don't have context to prioritize alerts, they can't be effective. Plus, alert fatigue leads to burnout, low morale, and job dissatisfaction. At a time when there is a severe shortage of qualified cybersecurity talent, this can have a corrosive effect on your entire organization.

**Increased risk due to a more sophisticated threat environment:** As noted in Figure 3, the increase in the threat landscape was cited most often by decision makers as a top challenge in public cloud infrastructure security. It's not just the alert fatigue as described above; it's the reality that threats are becoming more sophisticated all the time. Adversaries are using automation, machine learning, and artificial intelligence to be more targeted, and they are specifically identifying gaps in coverage, such as phishing and malware attacks aimed at hybrid and remote workers. Organizations need constant vigilance through advanced threat intelligence, and they need to fight fire with fire—i.e., if adversaries are leveraging automation, machine learning, and AI, organizations had better do the same.

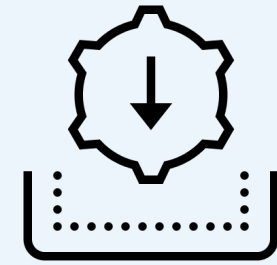
<sup>5</sup> Source: ESG Survey Results, *Modern Application Development Security*, November 2020.

<sup>6</sup> See related Showcase: [Scaling Enterprise Security with Cloud-native Protection on AWS](#), July 2022.



# THE BOTTOM LINE:

Virtually all of these challenges can be avoided with better processes and technologies in place—particularly in AWS environments where customers can take advantage of best-of-breed solutions from AWS as well as trusted cybersecurity brands such as Fortinet. Here’s what organizations need to look for.



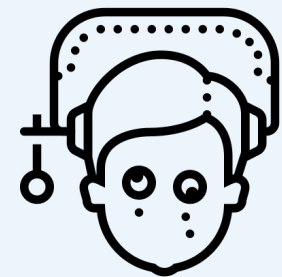
Too many tools require separate management consoles and updates.



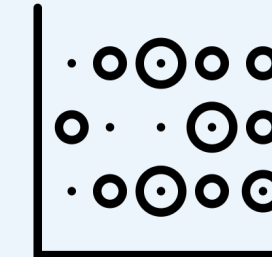
The number of tools used multiplies the number of alerts.



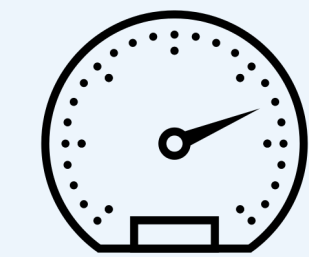
Alerts without context make it challenging to prioritize and respond.



Tools are siloed, not integrated, often with different interfaces, causing alert fatigue for SOC and cyber teams and friction with DevOps, etc.



The organization is faced with a fragmented view of risk that is challenging, if not impossible, to manage.



Security risks accumulate faster than they can be resolved.

## The AWS and Fortinet Value Proposition

**In managing risks and protecting workloads in AWS, what are some of the most important factors to consider?**

First, cloud security starts with AWS. Most customers turn to AWS for a number of reasons, including simplicity, scale, speed, flexibility, agility, consumption-based pricing, data sovereignty, compliance, trust, resilience, and business continuity. It's a long list. But right at the top of that list of reasons customers turn to AWS is cybersecurity. When a customer signs up with AWS, they know they are getting the most comprehensive cybersecurity coverage among any of the CSPs. They also know they can rely on AWS to uphold its end of the shared responsibility model with best-of-breed infrastructure cybersecurity.

Then, within AWS, it is a matter of choosing the right services to meet the needs of an organization for scale, compliance, resilience, speed—basically, any of AWS's offerings that you need. It is always a good idea to make an initial assessment of what you already have in place, what you need, and, perhaps most importantly, what is the agreed-upon risk management profile of your organization. This will help with budgeting, but it will also help the cybersecurity team to understand where it may need additional areas of coverage and additional areas of investment.

It would be unusual for an organization to go through these processes and not find any gaps at all. Assuming that AWS will not solve all of an organization's end-to-end security challenges, including visibility, centralized management, integrated threat intelligence, and more, then it is time to look at AWS' partner ecosystem for best-in-class security solutions.



## Organizations' top priorities are likely:



**To maximize the value and effectiveness of their existing AWS services** by implementing solutions that natively integrate with AWS security services, such as Amazon GuardDuty and Amazon Inspector with zero permission security coverage to reduce friction from deployment through to operations. This also helps accelerate ROI from the solutions deployed.



**Real-time visibility across AWS environments** with a solution that integrates into AWS to provide single-pane-of-glass management, full-time visibility, and broad protection in a single platform resulting in more predictable outcomes and more efficient cloud-security operations.



**Clear prioritized view of the critical risks** helps security teams focus on the risks that matter the most. Combined with actionable insights, a prioritized view also help teams minimize gaps in security coverage.



**Solutions that simplify security operations** should be easy to activate, enable collaboration across an organization for mitigating and remediating, and not require expertise in extensive security technologies in order to enable rapid responses to manage risk.



**Easy deployment via AWS Marketplace**, including full software lifecycle management to make it easy to access, deploy, and onboard a portfolio of integrated, value-added security services.



**Adaptive security solutions** that are available in multiple consumption models, including virtual machine, container, and software-as-a-service form factors that offer bring-your-own-license and pay-as-you-go billing options.



**Continuous updates to support safe cloud growth and scale** as part of an ongoing partnership with AWS to ensure that an organization is equipped with an industry-leading security posture at every stage of the cloud journey.

When it comes to best-of-breed solutions that augment AWS for effective coverage and reduced risk, Fortinet has significant advantages that apply to all potential customers—whether an organization is expanding its AWS footprint, securing cloud assets, or currently migrating to AWS. The Fortinet Cloud Security portfolio includes:

- **FortiCNP**, Fortinet’s cloud-native protection solution, which manages cloud risks by correlating alerts and findings from multiple sources to prioritize highest impact risks with actionable insights and extends the value of current security technologies to protect assets and monitor threats, helping organizations fully leverage the security services from AWS: AWS Security Hub, Amazon Inspector, and Amazon Guard Duty.
- **FortiCNPs Resource Risk Insights** technology helps organizations take the actions they need to reduce risk by taking in security alerts and findings generated by Fortinet security solutions along with data from AWS Security Hub, Amazon Inspector, and Amazon Guard Duty. It leverages the Fortinet security fabric products and services to create a risk-based prioritization with context-rich actionable insights so security teams can take the actions that are most impactful to reducing risk.
- **For high-priority risk insights**, FortiCNP helps streamline the mitigation and remediation process by integrating with digital workflow solutions, such as JIRA and ServiceNow, to get high-priority alerts to the right people efficiently.
- **For fixes that should be implemented in the CI/CD pipeline**, stop-gap remediation can be implemented to protect workloads from threats before the permanent fixes are implemented.
- **FortiCNP maximizes the value** of AWS’s cloud-native security services to help organizations prioritize risk management for AWS workloads.





## The Bigger Truth

As organizations move their workloads to AWS to optimize business operations and enable rapid innovation to best serve their customers, they need an effective security strategy that enables them to scale with the increased volume and speed of releases.

They should leverage security services from AWS to help developers incorporate security processes into their workflows, and organizations can augment the data from those services with third-party security solutions.

FortiCNP helps turn the data from the AWS security services into actionable insights, maximizing the value of the services you already have. This helps security scale for the rapid adoption of cloud services, enabling organizations to take the actions that are most impactful in reducing security risk and protecting workloads.

[LEARN MORE](#)

**FORTINET**®

All product names, logos, brands, and trademarks are the property of their respective owners. Information contained in this publication has been obtained by sources TechTarget, Inc. considers to be reliable but is not warranted by TechTarget, Inc. This publication may contain opinions of TechTarget, Inc., which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget, Inc.'s assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget, Inc. makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

This publication is copyrighted by TechTarget, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of TechTarget, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact Client Relations at [cr@esg-global.com](mailto:cr@esg-global.com).



**Enterprise Strategy Group** is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.

© 2022 TechTarget, Inc. All Rights Reserved.