Enterprise Strategy Group | Getting to the bigger truth.™

ESG SHOWCASE

Scaling Enterprise Security With Cloud-native Protection on AWS

Date: July 2022 **Author:** Doug Cahill, VP, Analyst Services and Senior Analyst

ABSTRACT: Organizations are moving more workloads to the public cloud to increase agility, reduce costs, and simplify management and scalability to empower digital transformation and other vital business initiatives. In moving workloads to the cloud, however, every organization is responsible for managing and minimizing security risk. Leveraging the security capabilities of a CSP is the first step. AWS, in particular, is a pioneer and leader in public cloud security. But even with AWS' extensive capabilities, customers often choose to augment security with a third-party AWS partner to strengthen protection, simplify scalability, reduce risk, enhance compliance, and optimize ROI.

Market Overview

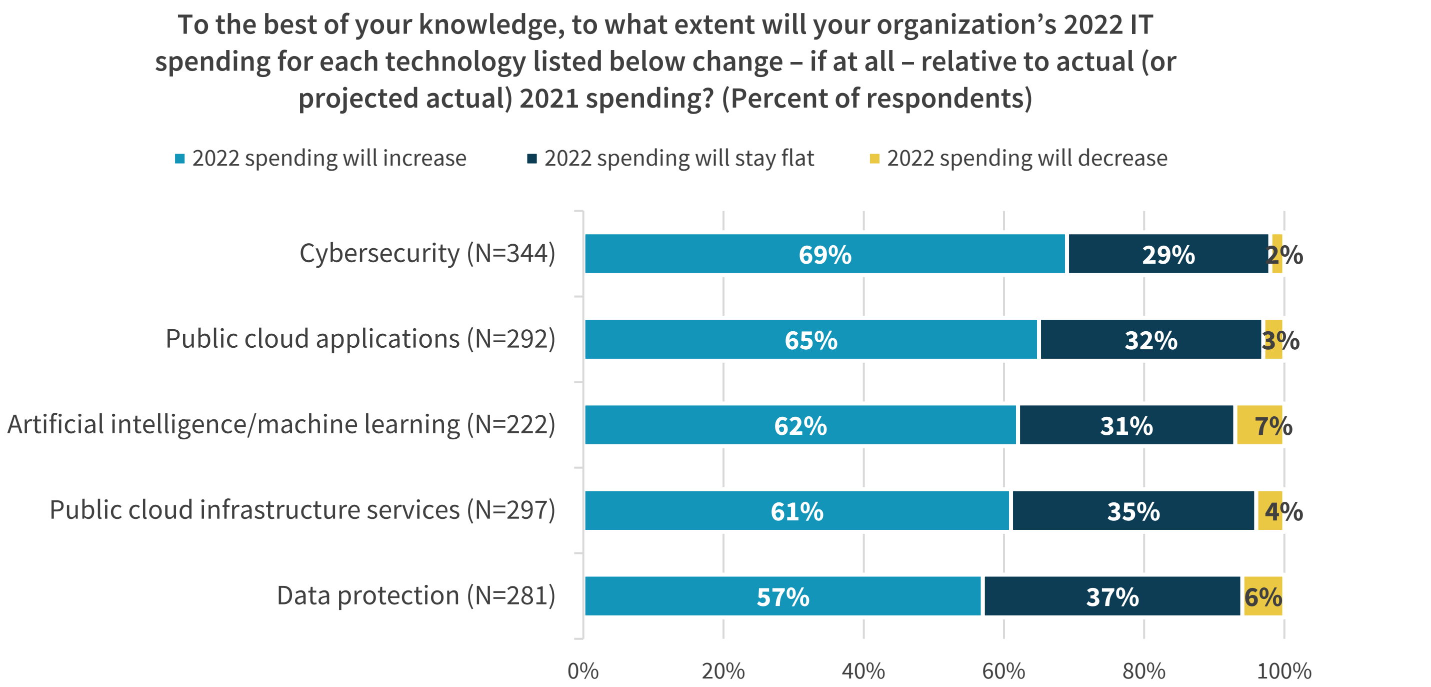
Moving workloads to the public cloud and cybersecurity are inextricably linked. You can't have one without the other. With many organizations striving to move as many workloads as feasible to the public cloud, the importance of effectively managing cybersecurity risk is taking center stage in executive suites and boardrooms all around the world.

Reducing risk and maximizing protection are key priorities. But, with decision makers focused on managing costs, coupled with an industry-wide shortage of cybersecurity talent, generating return on investment (ROI) is vital to establishing the organization's risk management profile and deciding how much money to budget for cybersecurity. Any solution that can mitigate risk *and* optimize ROI puts an organization ahead of the game and ahead of potential cyber-attackers.

Research from Enterprise Strategy Group (ESG) shows organizations investing in cybersecurity along with increasing spending on cloud services and other key technologies for moving workloads to the public cloud, with 69% of respondents reporting that their organization will increase its cybersecurity spending this year and 65% of respondents reporting that their organization will increase its public cloud application spending (see Figure 1).[1]

[1] Source: ESG Research Report, *2022 Technology Spending Intentions Survey*, November 2021. All ESG research references and charts in this showcase have been taken from this research report, unless otherwise noted.

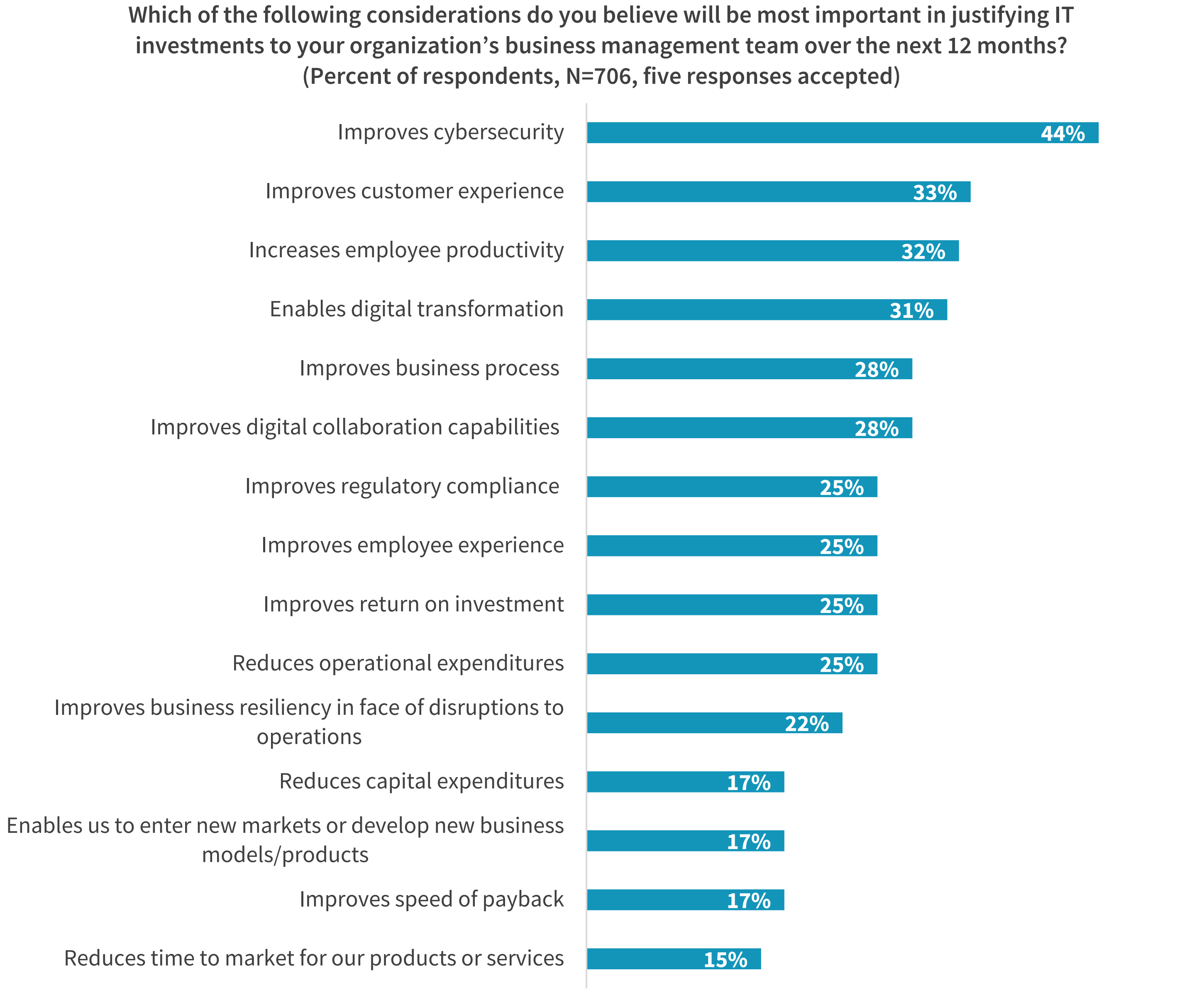
Figure 1. Top Five IT Spending Initiatives for 2022



Source: ESG, a division of TechTarget, Inc.

ESG research also shows that cybersecurity is by far the most important consideration respondents cited for justifying IT investments to their organization's management team. Other key priorities justifying investments include increasing employee productivity; enabling digital transformation; improving business processes and employee experiences; improving regulatory compliance, and ROI; reducing operational expenditures; and improving business resiliency in the face of disruptions to operations (see Figure 2).

Figure 2. Cybersecurity Is Key to Justifying Investments

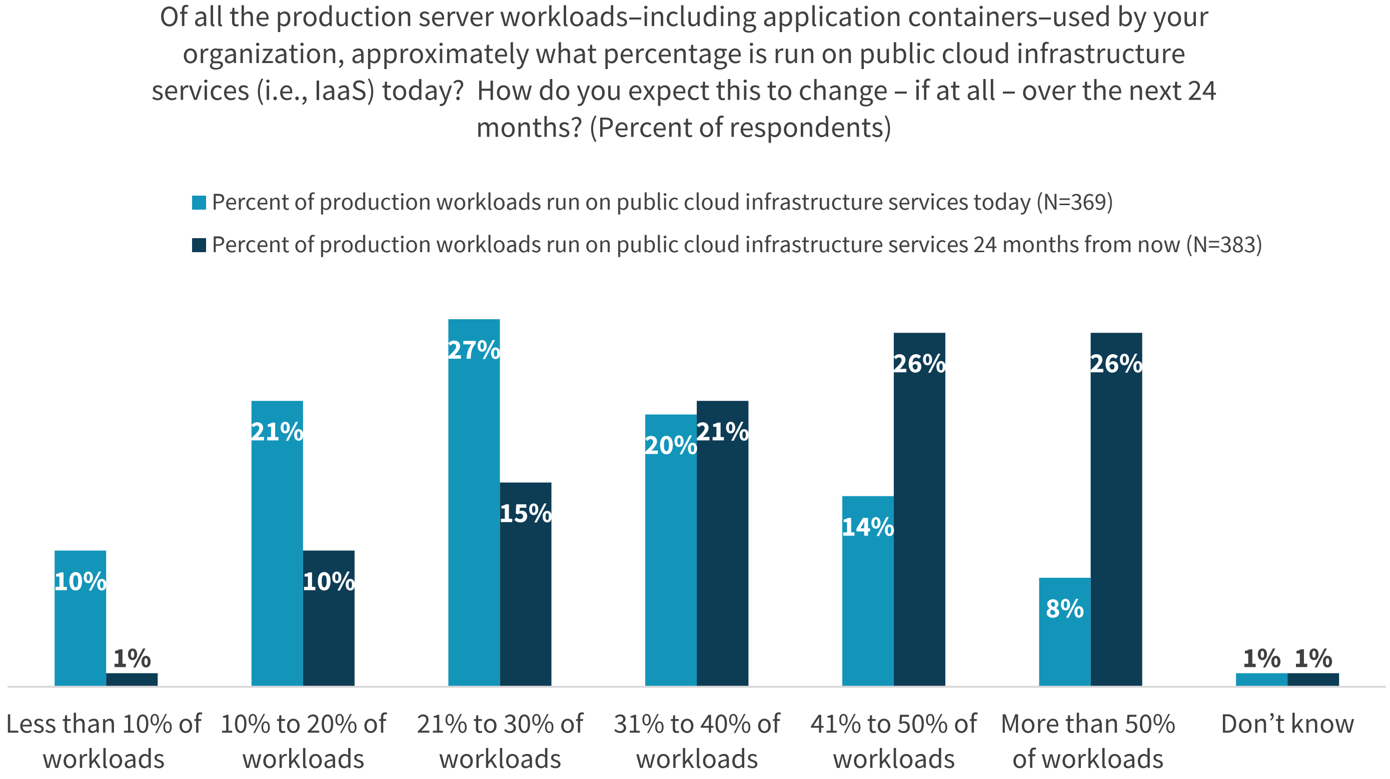


Source: ESG, a division of TechTarget, Inc.

Effectictively Managing Cybersecurity Risks in Scaling Public Cloud Usage

By moving workloads too quickly to the public cloud, organizations can increase cybersecurity risk if they don't take the proper precautions and leverage modern cloud-native technology solutions. This can blow up even the best of intentions and wreak havoc on the organization's desired risk management profile. This is a particular challenge as organizations accelerate the movement of public workloads to the public cloud (see Figure 3).

Figure 3. The Path to Public Cloud Continues for Production Applications



Source: ESG, a division of TechTarget, Inc.

Organizations need to take a measured and strategic approach to cybersecurity in the public cloud to effectively manage risk, simplify scalability, and ensure compliance. This starts with an understanding of the shared responsibility model and cybersecurity capabilities of the organization's communications service provider (CSP). AWS offers a wide range of built-in security features, as well as add-on capabilities to help developers secure their workloads in the cloud.

Organizations using AWS security services can augment them with a cloud-native solution that delivers a wide range of value-added features—including real-time visibility into threats, centralized management, integration with existing tools, and the ability to rationalize the alerts generated by AWS' security solutions into actionable insights for proactive risk management.

Using this "AWS-plus" model can enable strong visibility, particularly if the "plus" is an industry-leading solution that is designed specifically to strengthen security and reduce risk in AWS environments by giving organizations a full technology stack. Here are just some of the ways in which this approach can improve security coverage, strengthen visibility, reduce risk, and support overburdened cybersecurity teams:

- Reduce costs, risks, and complexity of having too many security tools. One of the ways organizations deal with the increased attack surface in the cloud is to add more tools to avoid insufficient coverage. This creates a fragmented security architecture that is inefficient, generating an overwhelming amount of alerts that lack context for cyber teams to prioritize. It not only increases risks, but is also expensive, forcing teams to manage different consoles, train personnel, and pay for upgrades. In the cloud era, this model no longer works. With a centralized, cloud-native model, you can reduce costs and risks by simplifying security management, ensuring visibility across all environments and providing broad protection across your applications and workloads.

- Reduce the risk of successful cyber-attacks and compliance violations. According to ESG research, 48% of respondents reported that their organization was a victim of a successful ransomware attack at least once, and 64% of those respondents said their organization paid a ransom.[2] And, with vulnerabilities being the most common entry point for attacks, nearly half of organizations (42%) still have gaps in their vulnerability management programs, according to research from ESG.[3] Having an AWS-plus model can provide a full stack with broad visibility to proactively manage and mitigate cloud risk.

- Reduce stress, burnout, and potential turnover of cybersecurity teams. Alert fatigue is a real issue among cybersecurity personnel. So are burnout, low morale, and job dissatisfaction. At a time when there is a shortage of cybersecurity personnel, using highly automated solutions with artificial intelligence and machine learning can help you retain, motivate, and inspire workers. Any time you have to replace and train a new cybersecurity professional, you are spending money and losing valuable time.

- Accelerate speed to market with “shift-left” built-in security protections. Integrating security best practices into applications and infrastructure enables developers to build security into development cycles via DevSecOps processes. This makes security more strategic and scalable, enabling organizations to deploy application workloads and develop new products and services with cybersecurity embedded in the solution.

- Drive innovation with a secure, scalable path to bring more workloads to AWS. The ability to securely scale applications and workloads in the cloud means you can use AWS as a path to grow your business, taking advantage of the benefits of both AWS and your third-party cloud-native security partner. This empowers business leaders to be more innovative and confident in developing products and services to create new revenue streams, thrill customers, and meet today’s demands for a hybrid workforce.

AWS and Fortinet: A Better-together Combination

When it comes to effectively managing security risk to optimize ROI, the combination of AWS with Fortinet offers advantages that other solutions are hard pressed to match.

For example, AWS offers:

- Amazon Inspector – scans workloads for vulnerabilities and open network exposure to help operationalize security throughout the resource lifecycle.

- AWS Security Hub – collects security data from across AWS accounts, services, and supported third-party partner products to identify security issues.

- Amazon GuardDuty – identifies suspicious traffic and API activity in AWS environments.

These are simple add-on services available through Amazon, making it easy for developers to add security to their processes. While AWS security services are extensive, for more complex deployments, organizations should augment them with third-party solutions that address more advanced security needs.

That’s where Fortinet comes in. With tools designed to mitigate security risk, improve protection, and reduce complexity, Fortinet Security Fabric solutions leverage capabilities such as threat intelligence, data correlation, automation, AI, and

[2] Source: ESG Research Report, *2022 Technology Spending Intentions Survey*, November 2021.
[3] Source: ESG Research Report, *The Long Road Ahead to Ransomware Preparedness,* June 2022.

machine learning, which are all designed to interoperate and respond to threats as a single, coordinated system. The key product Fortinet offers in combination with AWS services includes:

- FortiCNP, Fortinet's cloud-native protection solution, integrates with AWS's cloud-native security services, as well as Fortinet's Security Fabric products and FortiGuard Labs, to deliver friction-free cloud security by correlating and contextualizing the volume of security alerts and findings into actionable insights.
- FortiCNP's patented Resource Risk Insights (RRI) technology incorporates the security findings from AWS Security Hub, Amazon Inspector, and Amazon Guard Duty, as well as Fortinet cloud security solutions and FortiGuardLabs, to produce an aggregated risk score with prioritized, context-rich, and actionable insights about resources that present the highest risk to address, helping customers get the most out of these security tools to manage and mitigate cloud risk.
- Integrations with digital workflow solutions such as Jira and ServiceNow help streamline and manage the remediation process.
- For fixes that will be implemented in the CI/CD pipeline, stop-gap remediations can be triggered with Fortinet cloud security solutions to protect against threats before the permanent fixes are implemented.

The Bigger Truth

Organizations need a way to operationalize security, maximizing the value of the security services and products they have—not just to improve protection and reduce risk, but to also fully leverage the value of public cloud to gain broader context across cloud workloads to drive faster transformation and mitigate risk. In this environment, more than ever, cloud, cybersecurity, and digital business initiatives are inextricably entwined.

AWS includes extensive services to secure workloads in the cloud. But to minimize risk, maximize protection, simplify scalability, and optimize ROI, organizations should leverage third-party security solutions such as FortiCNP. FortiCNP utilizes results from AWS cloud-native security services to rationalize the outputs of these services and speed up remediation workflows. By prioritizing the high-risk items and enabling efficient remediation, FortiCNP improves cloud security and maximizes ROI by augmenting AWS security services to effectively manage risk as development grows.

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.

ESG a division of TechTarget

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

www.esg-global.com contact@esg-global.com 508.482.0188