Enterprise Strategy Group | Getting to the bigger truth.™

ESG WHITE PAPER

What to Look for in Third-party Solutions to Augment and Strengthen AWS Security

Take AWS Security to the Next Level to Reduce Risk and Maximize Protection

By Doug Cahill, VP, Analyst Services and Senior Analyst

July 2022

This ESG White Paper was commissioned by Fortinet
and is distributed under license from TechTarget, Inc.

Contents

Executive Summary

Nearly all organizations are using the public cloud for a wide range of applications, from newer cloud-native workloads to the migration of legacy apps. As business leaders experience the benefits of the cloud in accelerating digital transformation initiatives, the pressure to move even more workloads to the cloud increases. ESG research shows that 95% of organizations are already using public cloud services, and the majority of applications and workloads that currently run in on-premises data centers are marked as candidates to move to public cloud services over the next five years.[1]

One of the traditional gating factors to moving more applications to the cloud has been concerns about cybersecurity. When looking back at virtually any market survey over the past decade, concerns about cybersecurity were usually one of the top impediments to more widespread cloud adoption. Security is still a key issue in 2022: An ESG research survey identified cybersecurity and public cloud applications as the two most commonly cited spending priorities for IT decision makers, with 69% of respondents reporting that they expect their organization to increase its cybersecurity spending in 2022, and 65% of respondents reporting that they expect their organization to increase its public cloud application spending in 2022.[2]

The new reality for IT leaders and chief information security officers (CISOs) is the necessity to make sure security is accounted for at every step of the cloud journey. For workloads in the public cloud, this means clearly understanding the shared responsibility model of the cloud security provider (CSP) and leveraging the CSP's security services to maximize protection, minimize risk, support compliance, and make the strongest contribution to the organization's bottom line.

When it comes to security, organizations moving workloads and applications to the AWS environment have some clear advantages:

1. AWS offers customers a wide range of easy-to-use integrated security tools that enable extended visibility, monitoring, prevention, and proactive controls.

2. Within the AWS partner ecosystem, customers have access to third-party tools that augment AWS services to ensure that workloads can be protected through the easy use of industry-leading solutions powered by automation, analytics, artificial intelligence, comprehensive threat intelligence, and more.

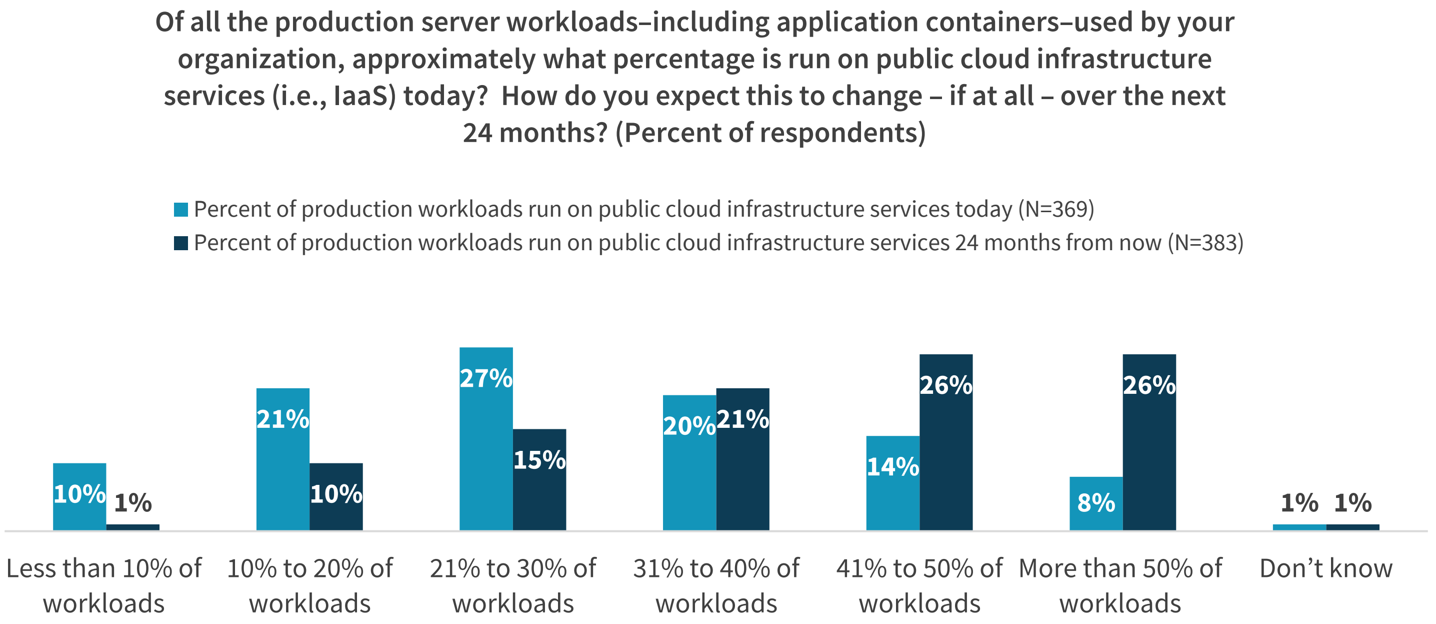
This white paper examines the trends driving the growing emphasis on public cloud usage and the impact on cybersecurity. We explore the business value of strengthening security, mitigating risk, supporting compliance, and optimizing ROI in AWS environments. Finally, we look at how organizations can enhance and augment their security posture with best-in-class cloud-native security solutions that are tightly integrated with AWS to provide broad protection across all cloud workloads and apps.

Market Overview

Business and IT leaders are increasingly recognizing the value and importance of public cloud as an enabler of digital transformation and business innovation. Per research from Enterprise Strategy Group, 26% of organizations expect to have more than 50% of their production workloads in the public cloud by 2023, versus only 8% in 2021. An additional 26% expect 41% to 50% of production workloads in the public cloud in the same time period (see Figure 1).[3]

[1] Source: ESG Research Report, *2022 Technology Spending Intentions Survey*, November 2021.
[2] Ibid.
[3] Source: ESG Research Report, *The Maturation of Cloud-native Security*, May 2021.

Figure 1. Companies Are Moving More Workloads to the Public Cloud



Source: ESG, a division of TechTarget, Inc.

The shift to public cloud is reflective of the significant business benefits public cloud delivers, particularly in today's environment where flexibility, speed, scalability, customer experience, and employee experience are top of mind for most business leaders. The reality, however, is that the ability to reap those benefits is directly correlated with the organization's ability to manage cybersecurity risk and protect workloads in the public cloud.

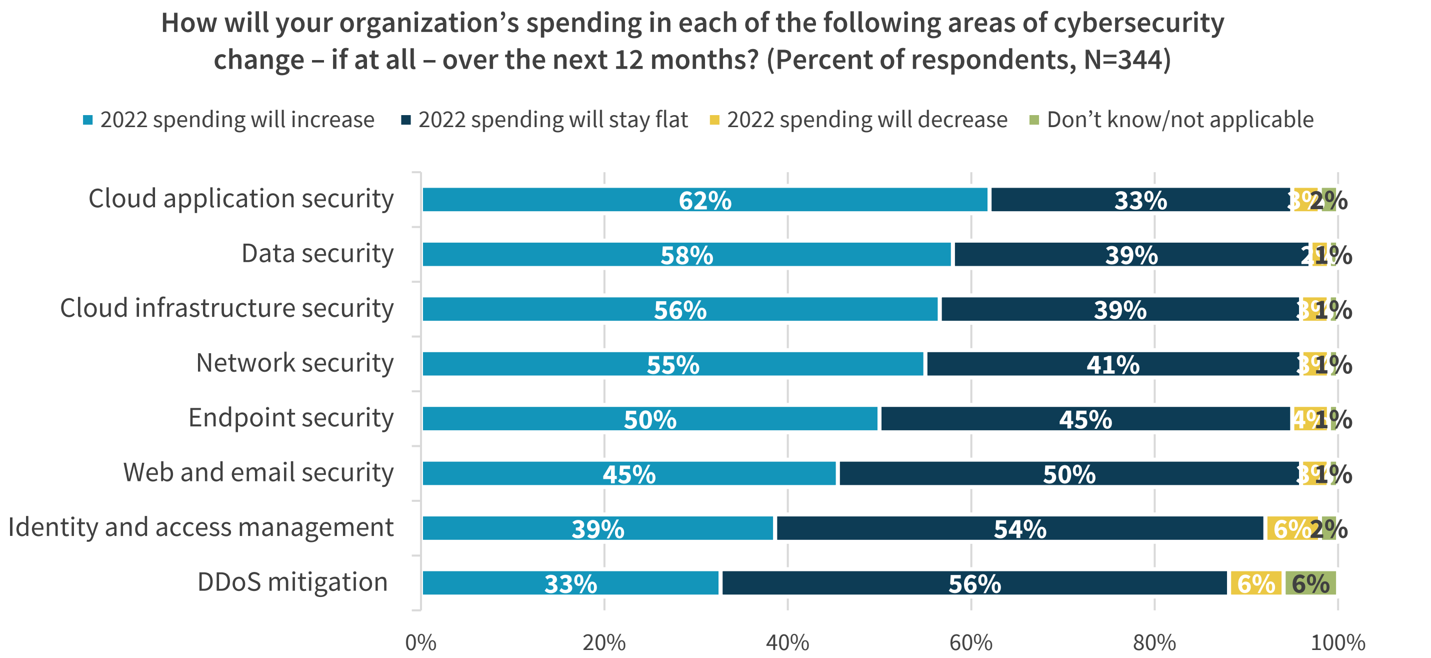
It has been said that cloud changes everything. Perhaps not everything, but it certainly changes how organizations need to address cybersecurity. According to ESG research, 88% of respondents said that their organization's cybersecurity program needs to evolve to secure their cloud-native applications and use of public cloud infrastructure.[4]

In addition, while ESG research shows that cybersecurity and public cloud applications are the two most commonly cited areas in which organizations expect to increase spending in general, cloud application security and data security are the most commonly cited cybersecurity spending priorities for 2022 (see Figure 2).[5]

[4] Ibid.

[5] Source: ESG Research Report, *2022 Technology Spending Intentions Survey*, November 2021.

Figure 2. Cloud and Data Are Top 2022 Cybersecurity Spending Priorities



Source: ESG, a division of TechTarget, Inc.

With 88% of decision makers believing that their cybersecurity program needs to evolve to secure their cloud-native applications and use of public infrastructure,[6] it is important for IT and cybersecurity leaders to understand their own organization's risk profile and where there may be gaps. Among the most common problems organizations experience as they migrate more applications to the cloud are:[7]

- Too many disparate tools.
- Lack of integration between traditional security tools and cloud-native security services.
- Alert fatigue caused by lack of context.
- A much broader, distributed, and diverse attack surface.
- Lack of vision across the entire environment.
- Lack of centralized control for prevention, response, and remediation.
- A need to take a more holistic cybersecurity approach, incorporating features such as comprehensive threat intelligence to augment the capabilities and tools offered by their cloud security provider.

If an organization can overcome these challenges, it can maximize the benefits of the cloud with more confidence, which means it has a much greater ability to accelerate digital transformation; support hybrid work initiatives; deliver exceptional, data-driven experiences for employees and customers; and strengthen its digital supply chains. Organizations can scale

[6] Source: ESG Research Report, *The Maturation of Cloud-native Security*, May 2021.
[7] For a more detailed look at public cloud security challenges, please see the related eBook: *A Guide to Managing Security Risks and Protecting Workloads in AWS*.

their businesses with greater ease knowing their security can scale with its workloads and applications. An organization will not only be able to respond to security risks with more speed and better precision, but it can also be far more proactive in identifying risks, if given broader context about the overall impact, as well as what actions should be taken to mitigate the risk. Implementing third-party solutions that can complement AWS security services can improve their return on investment and create a culture that is more agile and innovative. This is all within an organization's grasp, now and in the future.

Leveraging AWS Security Services

Cloud service providers offer a range of security services to help customers overcome the challenges (and fears) about moving applications to the public cloud. In fact, the CSPs have long been ahead of the curve and are considered innovators in upgrading security to give customers unprecedented trust and confidence. Their business models depend on security to succeed.

Among the leading CSPs, AWS has been at the forefront in driving continuous cybersecurity improvements. Its shared responsibility model and technology innovations are widely regarded as best practices in cloud security across the industry, ranging from code testing in development, to monitoring workloads in production, to helping with incident response.

For example, AWS provides:

- 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 add-on services that are easy to deploy, making it simple for security operations center (SOC) teams to incorporate security testing and monitoring for the applications in their cloud environments.

Augmenting AWS Security Services

While the AWS portfolio of security services is extensive, it is not designed to address every potential security gap. That's why AWS has its shared responsibility model and why it relies on an ecosystem of third-party partners to supplement and augment its services.

For many deployments, organizations should use these third-party solutions to rationalize the volume of data produced by the cloud-native tools to effectively address their cloud risk. The combination of AWS services with third-party cloud-native tools can create a comprehensive security solution for managing cloud risk, improve security coverage and deliver a holistic approach to cybersecurity that enables business innovation and faster time to value to the bottom line.

In evaluating solutions to augment AWS, there are certain features and characteristics to look for in a potential partner. These include:

- Deep integrations with AWS security services to help simplify security management and provide broad protection across your applications and workloads with zero-permission security coverage.

- Full visibility across AWS environments, with a solution that natively integrates into AWS to provide single-pane-of-glass management and cloud-native visibility.

- An integrated model that incorporates security findings across the cloud-native services to prioritize the highest risks for security teams to focus on.

- Context-rich, actionable insights about resources that present the highest risk to help security teams proactively manage cloud risk.

- Within the broad AWS partner ecosystem, the portfolio of products and services from Fortinet stands out in the area of cybersecurity, offering solutions to enable organizations to gain added confidence and protection. To effectively secure cloud workloads, FortiCNP, Fortinet's cloud-native protection solution, manages cloud risks by correlating alerts and findings from multiple security sources, to prioritize the highest impact risks with actionable insights. FortiCNP integrates with AWS's security services to gain broader context across a customer's AWS cloud footprint to enhance the actionable insights for managing risk.

- FortiCNP's Resource Risk Insights technology helps organizations prioritize the actions they need to take in order to reduce risk by correlating and normalizing security alerts and findings generated by Fortinet Cloud Security solutions along with security data from AWS security services such as Security Hub, Amazon Inspector, and Amazon Guard Duty to prioritize cloud resources using a risk-based approach 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, as its security outputs become useful in the context of a broader security solution

- The business benefits of FortiCNP can be realized across an organization. The productivity of security teams will increase by taking the volume of alerts into actionable insights. Collaboration between security teams and other operations, such as DevOps and line-of-business managers, will improve to accelerate speed to market. Developers will be able to adopt a "shift-left" model, enabling security to be built-in at every stage of the development cycle. Risk managers will be able to improve governance and compliance, possibly even reducing premiums for cyber insurance. CISOs will be able to realize the value of their products and track risk reduction over time.

The Bigger Truth

Organizations are moving more workloads to cloud services such as AWS to modernize their operations, enable rapid innovation, keep pace with the speed of cloud adoption, and best serve the needs of customers and employees. In order to truly reap the business value of AWS, however, organizations need an effective security strategy that enables them to scale and protect the rapidly growing number of workloads in the cloud.

It is critical to leverage the security services of a CSP like AWS because their solutions are extensive, comprehensive, and easy to implement. For more complex deployments, however, it is often necessary to add third-party solutions that integrate natively with AWS.

FortiCNP helps turn the volume of security alerts generated by CSP security services and Fortinet Security solutions into actionable insight for faster remediation. This helps security keep pace with the rapid adoption of the cloud, helping security teams use their time more efficiently and remediating high priority security issues while protecting the organization’s cloud applications and resources.

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