

WHITE PAPER

# Developing the Right Security Strategy When Using Multiple Cloud Service Providers

Optimize Protection of Cloud Applications and Resources

By Melinda Marks, Senior Analyst

December 2022

This Enterprise Strategy Group White Paper was commissioned by Google and is distributed under license from TechTarget, Inc.

## Contents

Executive Summary .....	3
Digital Transformation with Multiple CSPs.....	3
Security and Compliance Challenges .....	4
The Multitude of Cloud Threats .....	5
Meeting the Biggest Security Challenges .....	6
Taking Full Advantage of Native CSP Security Capabilities.....	8
Achieving Consistency Across Cloud Environments.....	9
Utilizing Google Cloud Platform (GCP) .....	9
The Bigger Truth .....	10

## Executive Summary

Organizations are utilizing cloud platforms to power their applications, so they can focus their scarce IT resources on faster product delivery and innovation. While this enables them to better serve customers, partners, and employees with applications delivered from the cloud, it makes security imperative to keep the applications running and to protect customer and company data.

Developing an effective security strategy is particularly challenging as security teams typically need to support multiple public cloud environments. It is challenging because each cloud service provider (CSP) has a different platform architecture with different security features and capabilities. This makes it difficult to effectively manage risk and apply consistent security policies and processes across disparate environments.

Organizations should fully leverage threat detection, vulnerability management, and risk solutions available from their CSPs, while solutions supporting multiple environments can be useful for security operations to drive consistent policies, controls, and processes across cloud environments. While third-party solutions can be helpful, it's important to be cautious about using solutions that could add more complexity and attack surface area to manage, including adding agents or separate security solutions that rely upon information published via public APIs.

This paper examines how to build an effective strategy to efficiently manage security risk with applications running in different cloud environments. By fully leveraging security controls and risk management intelligence natively built into the CSP stack, organizations can optimize protection of their cloud applications and resources.

## Digital Transformation with Multiple CSPs

Organizations are undergoing digital transformations as they are pressured to increase productivity for better business results and to gain a competitive advantage. Using public cloud infrastructure enables organizations to move to more efficient cloud-native development processes while leveraging state-of-the-art technologies from CSPs so they don't have to worry about setting up or maintaining hardware or underlying infrastructure. It frees up their resources so they can focus teams on delivering products and serving customers.

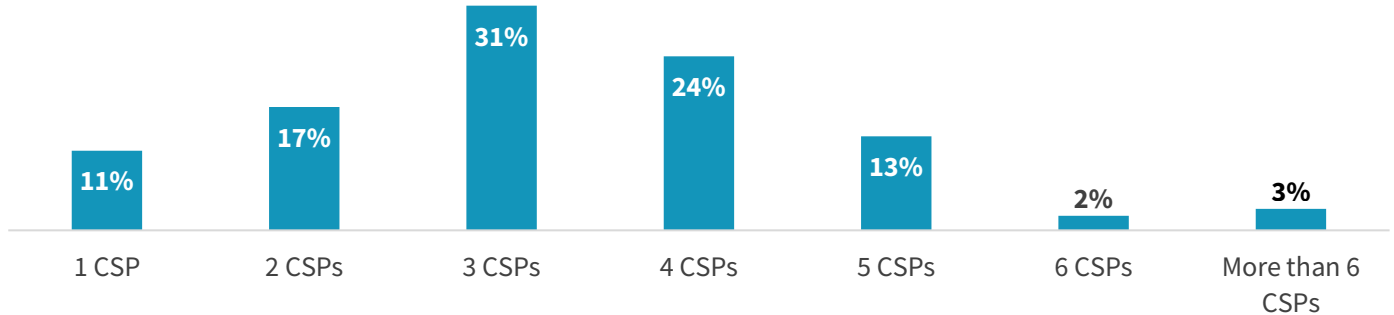
Often with multiple development teams with different preferences for where they want to deploy their applications, most organizations utilize multiple CSPs. Research from TechTarget's Enterprise Strategy Group (ESG) shows that 90% of organizations are leveraging multiple CSPs (see Figure 1), with 42% using at least four CSPs,<sup>1</sup> giving developers the flexibility to choose their CSP.

---

<sup>1</sup> Source: Enterprise Strategy Group Research Report, [Cloud-native Applications](#), May 2022.

**Figure 1. CSP Usage**

Approximately how many unique public cloud infrastructure service providers (IaaS and/or PaaS) does your organization currently use? (Percent of respondents, N=339)



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

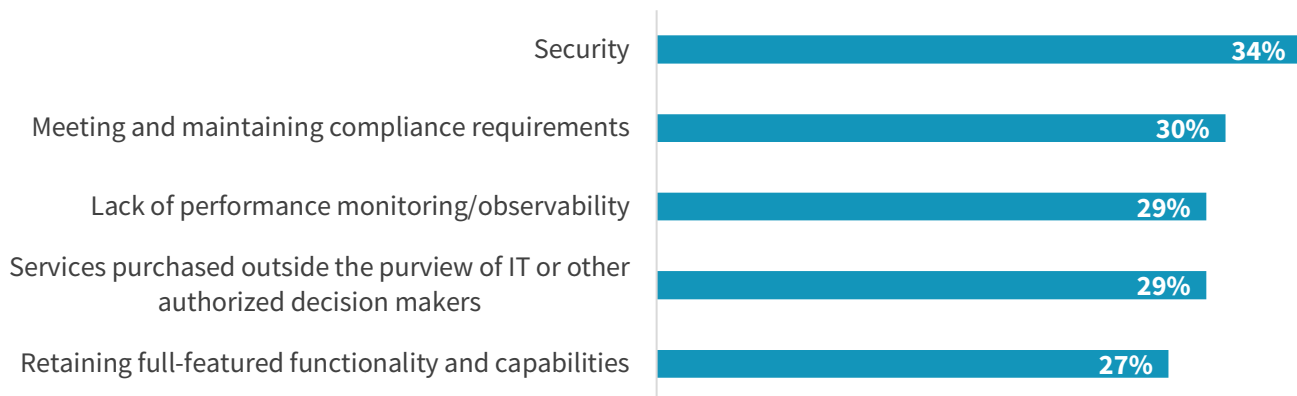
The CSPs are typically selected by their IT and development teams, based on their requirements, including alignment with SLAs, cost requirements, and data analytics needs. While ESG research shows that a majority of organizations (78%) would prefer to use a single cloud vendor for aspects such as data management and consistent analytics,<sup>2</sup> organizations are typically using multiple CSPs out of fear of vendor lock-in and loss of flexibility.

### Security and Compliance Challenges

While organizations are meeting their objectives of faster, more efficient development cycles with their move to the cloud, Enterprise Strategy Group (ESG) research shows security and compliance top the list of challenges they have faced, or expect to face, in the cloud (see Figure 2).<sup>3</sup>

**Figure 2. Top 5 Challenges Faced with Cloud-native Applications**

What are the biggest challenges your organization has faced, or expects to face, with its cloud-native applications? (Percent of respondents, N=387, multiple responses accepted)



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

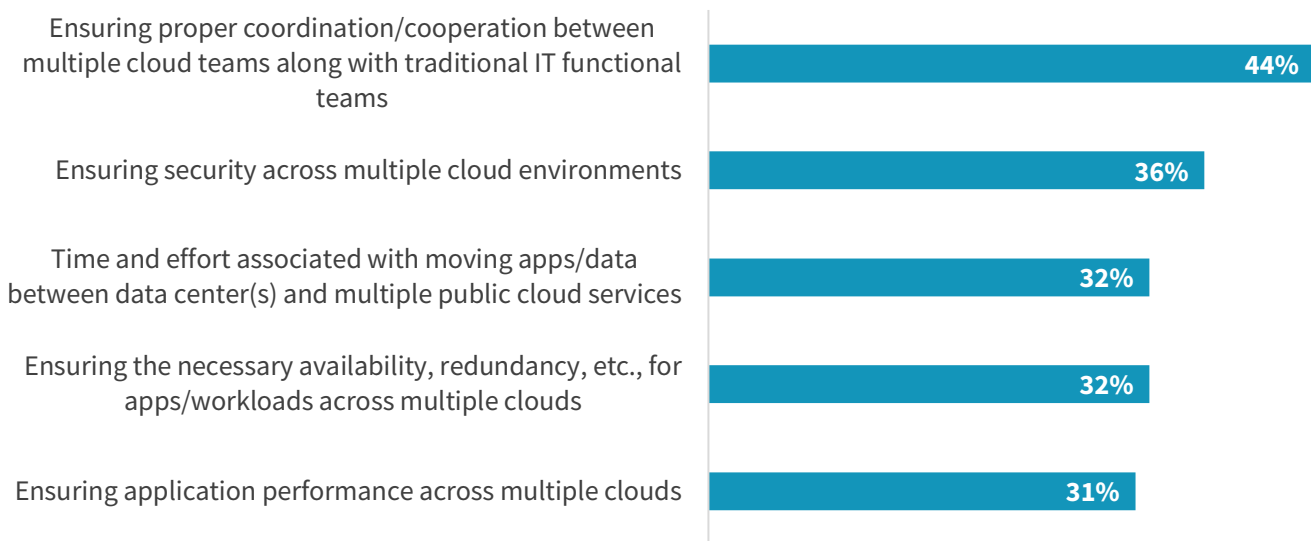
<sup>2</sup> Source: Enterprise Strategy Group Complete Survey Results, [Cloud Analytics Survey](#), March 2022.

<sup>3</sup> Source: Enterprise Strategy Group Research Report, [Cloud-native Applications](#), May 2022.

These challenges are exacerbated with the usage of multiple CSPs, compounded by the difficulty of coordinating and ensuring consistent processes across development groups deploying their applications in different cloud environments. According to ESG research, security is a top challenge of using multiple CSPs reported by organizations (36%, see Figure 3).<sup>4</sup>

**Figure 3. Top 5 Challenges of Using Multiple CSPs**

**What are the greatest challenges your organization faces as a result of using multiple CSPs? (Percent of respondents, N=279, multiple responses accepted)**



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Organizations are looking for a better approach to ensure security across multiple cloud environments while delivering their applications.

### The Multitude of Cloud Threats

Security teams need to ensure they can protect their company and customer data while supporting digital transformation and leveraging multiple cloud environments. This is challenging, as security teams need a strategy that does not interfere with operational efficiency; it needs to keep up with the faster speed of software releases, while addressing security threats in dynamic and complex cloud environments where computing resources are easily spun up and spun down.

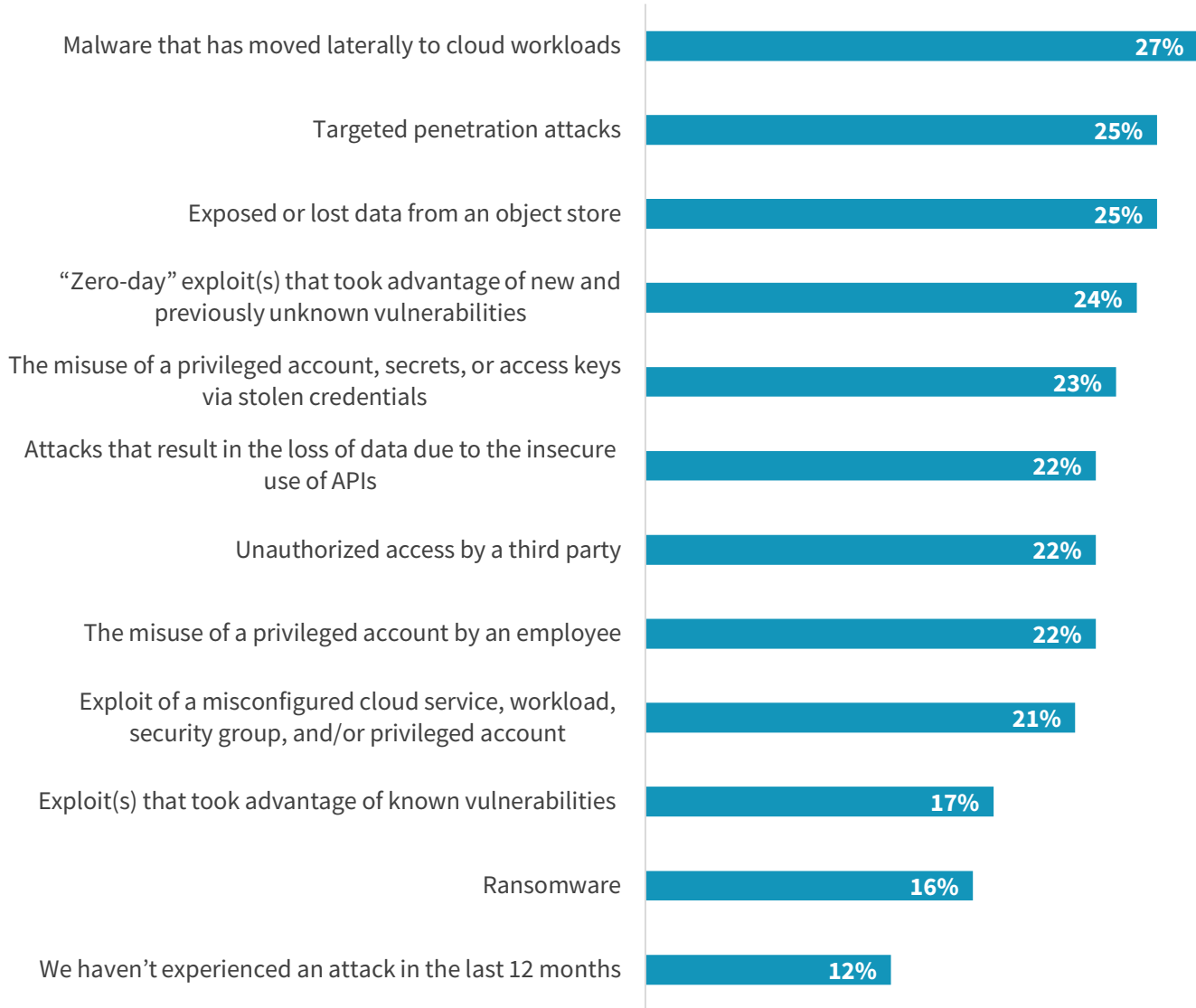
Enterprise Strategy Group (ESG) research shows that organizations have faced a wide range of attacks on their cloud-native applications, making it clear that they need to take steps to reduce their security risk. 88% of organizations reported having been attacked across a wide range of incidents, including malware moving laterally across workloads, targeted penetration attacks, and exposed or lost data from an object store (see Figure 4).<sup>5</sup>

<sup>4</sup> Source: Enterprise Strategy Group Complete Survey Results, [Application Infrastructure Modernization Trends](#), March 2022.

<sup>5</sup> Source: Enterprise Strategy Group Research Report, [The Maturation of Cloud-native Security](#), May 2021.

**Figure 4. Types of Cybersecurity Incidents Experiences**

Which of the following cybersecurity incidents, if any, has your organization experienced in the last 12 months related specifically to cloud-native applications and infrastructure?  
(Percent of respondents, N=383, multiple responses accepted)



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

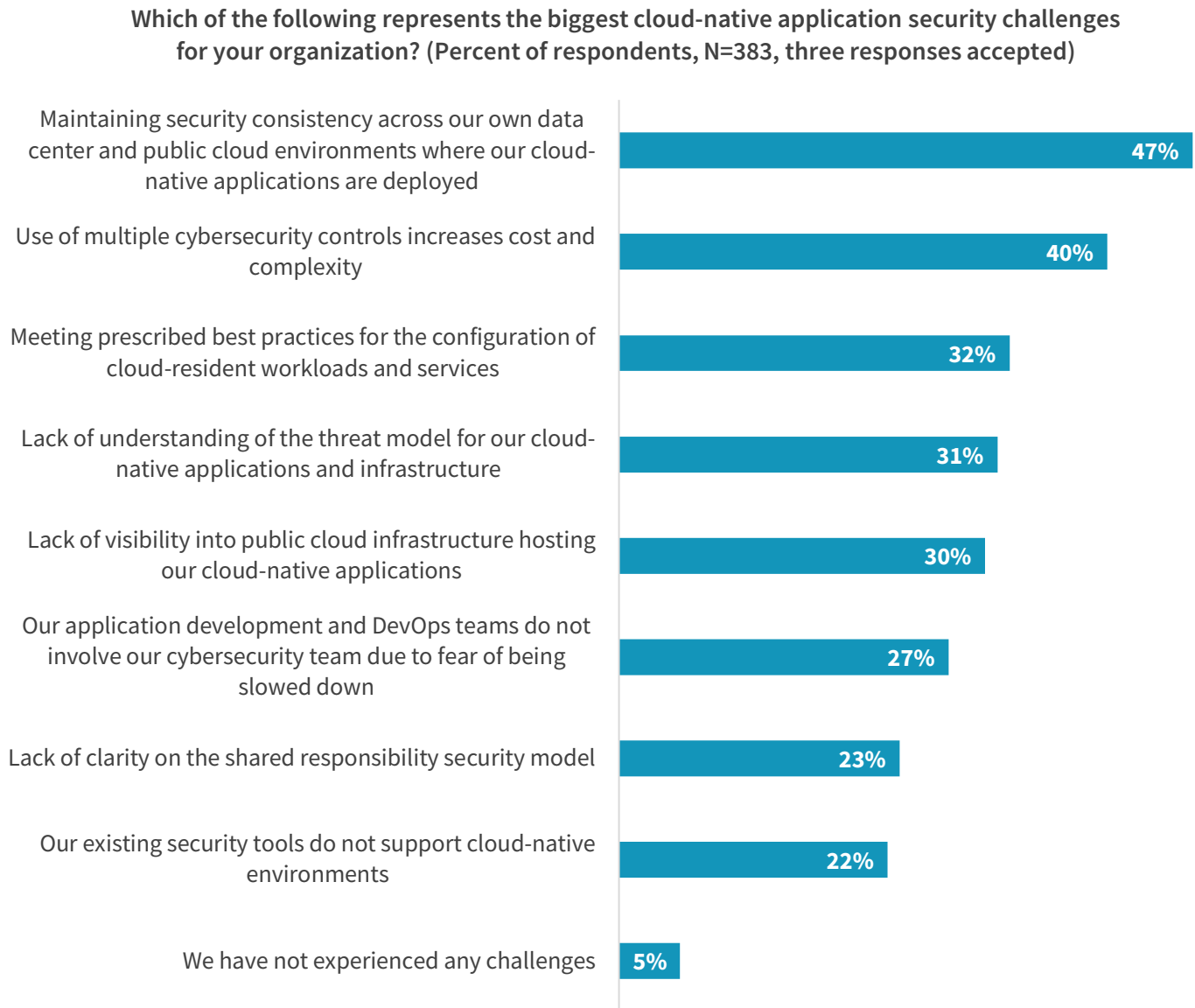
It’s important for organizations to find the right security strategy that can efficiently reduce their security risk and exposure to attack.

### Meeting the Biggest Security Challenges

Enterprise Strategy Group (ESG) research showed that 88% of organizations feel their cybersecurity programs need to evolve to secure their cloud-native applications and use of public cloud infrastructure. The research showed the biggest challenges around the lack of consistency across disparate cloud environments (see Figure 5).<sup>6</sup>

<sup>6</sup> Source: Enterprise Strategy Group Research Report, [The Maturation of Cloud-native Security](#), May 2021.

**Figure 5. Lack of Consistency Across Disparate Environments Highlights the Need to Evolve Cybersecurity Programs**



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

It is not surprising that the top challenge is around maintaining consistency across data center and cloud environments. Data centers and public clouds have fundamentally different constructs for how compute, storage, and networking are deployed, managed, and scaled—posing obstacles to the uniform application of security controls.

There are also significant differences among the different public cloud platforms in how individual services are architected and implemented, making it difficult to deliver consistency in critical areas, such as cloud configuration and detection.

Also, the traditional approach to protecting applications in data centers with well-defined perimeters doesn't easily translate to protecting public clouds. Organizations are using the cloud to ensure their applications are more available to employees, partners, and customers, making it impossible to protect them with a perimeter approach. Instead, they need to address public APIs, along with identity and access, to protect their applications.

To help address these challenges, organizations can take the following proactive measures:

- **Drive greater visibility and control with standardization in security operations.** Security leaders should look to standardize controls and processes judiciously to ensure they aren't adding complexity or costs. Information can be aggregated from multiple CSPs for centralized alerting, threat investigation, and incident response.
- **Adopt best practices for cloud-resident workloads by setting policies as guardrails.** This helps ensure that configuration settings are already in place, and anything out of policy is blocked from being deployed. It also reduces the number of repetitive security alerts and remediation due to common misconfigurations.
- **Understand the threat model across different cloud services.** Cloud providers implement services differently, creating unique attack surfaces and threat exposure. Not all threats can be detected via public APIs and logs, so it is important to understand if there is instrumentation via the CSP to provide real-time signaling of abnormal behaviors or access patterns for efficient incident detection and response.
- **Gain visibility of cloud assets.** It is important to have an understanding of cloud assets to enact proper configuration controls, including identity and access controls. When new cloud services are released, it's important to have full visibility, with no gap in coverage.

## **Taking Full Advantage of Native CSP Security Capabilities**

To manage multi-cloud security risk, organizations should leverage the native features of the CSPs because they have an inherently better understanding of service architecture and implementation to engineer security into deeper layers of the technology stack that add-on services don't have access to utilizing.

When selecting a solution, look for those that provide a clear path to:

- **Minimize attack surface area.** Security products should not increase exposure to attack with add-ons, such as extra service accounts or agents, which add more technical components and complexity that can increase exposure to risk.
- **Integrate threat detection with the cloud substrate** to discover a broader array of threats. One example is Google Cloud's VM introspection in its virtual machine threat detection (VMTD) service, which opens up new methods of detecting threats to production workloads, without introducing operational or performance overhead.
- **Ensure the security approaches work with the cloud-native tech stack**, such as making certain they can keep up with the speed and ephemeral nature of workloads for threat detection.
- **Minimize the exposure window.** As enterprises put new cloud services into production, security vendors can help provide assurance that they can deliver adequate coverage of these services, ideally aligned with development and release cycles.
- **Assist reducing risk by helping manage access and entitlements.** Managing access to services is typically overprovisioned for faster development and collaboration, and it is a complex, tedious process to ensure least-privilege access. Solutions should provide visibility and control to manage risk, while providing context to accurately determine risk of security threats.



- **Control costs** by optimizing operational efficiency. Native cloud solutions may offer an economic advantage, as cloud providers do not typically charge for API, compute, storage, and egress consumption when used for implementation of security controls.

## Achieving Consistency Across Cloud Environments

Standardization of security processes across cloud environments can drive operational efficiency. But it can be challenging to standardize security processes when each cloud service provider has a different architecture, features, capabilities, and add-on offerings. When considering multi-cloud solutions, organizations should keep in mind the following:

- Each cloud provider has different security tools and processes to help developers and DevOps teams provision and build their applications.
- Each cloud provider implements services differently, creating uniqueness in the attack surface and threat exposure.
- CSPs can provide more visibility based on their infrastructure for deeper detection than third-party vendors; not all threats can be detected via testing, scanning, or looking at public APIs and logs. There are suspicious behaviors that happen “below the surface.”
- When threats are detected, organizations need near-real-time signaling for timely incident response, so extra steps or tools can slow things down.
- If instrumentation or agents are added for monitoring or to detect threats, they should not increase the attack surface or create higher vulnerability to attack. For example, agents and more integrations with APIs increase access for more processes to occur and can create new vectors to attack.
- Identity information and controls can be difficult to extract and analyze via APIs, thus making it difficult to accurately assess risks to resources and the overall environment.

## Utilizing Google Cloud Platform (GCP)

Google is committed to supporting customers’ security and risk mitigation in Google Cloud, and across multiple cloud environments.

For Google Cloud deployments, security leaders should leverage:

- **Secure by Design Foundation**, which provides multiple layers of security built into Google Cloud’s infrastructure.
- **Security Command Center** security and risk management platform for managing cloud security posture, identifying vulnerabilities, detecting threats, and reporting on compliance.

For securing multiple cloud environments, organizations should consider Google solutions built for security operations centers (SOCs):

- **Chronicle Security Operations Suite**, which aggregates and analyzes security information across clouds, data centers, and users, for faster analysis and incident response.

## The Bigger Truth

As organizations move their applications to the cloud, they need to ensure security keeps up with cloud utilization to stay ahead of threats. For most organizations using multiple CSPs to host their applications, it can be difficult to manage the security risk to consistently put the right security policies and processes in place. This can be challenging, as each cloud platform is built differently and offers different security features and capabilities.

Organizations should fully leverage threat detection, vulnerability management, and risk solutions available from their CSPs, while security solutions supporting multiple cloud environments can be useful for security operations to drive consistent policies, controls, and processes across cloud environments. While third-party solutions can be helpful, it's important to be cautious about using solutions that could add more complexity and attack surface area to manage, or separate security solutions that rely on information published via public APIs.

GCP offers security support for customers developing strategies to secure their applications across multiple cloud environments. Organizations should fully use the security features of GCP as well as solutions that can aggregate security information streams into a single platform for broader visibility, faster analysis, and more effective response, without adding complexity, cost, or security exposure.

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 that provides market intelligence, actionable insight, and go-to-market content services to the global IT community.