White Paper, sponsored by VMware
MARCH 2023

REGION FOCUS: WORLDWIDE

Modern Unified Cloud Workload Security: What You Need to Know

Philip Bues
Research Manager
Cloud Security, IDC

Table of Contents

CLICK BELOW TO NAVIGATE TO EACH SECTION IN THIS DOCUMENT.

Executive Summary

This paper explores cloud workload security and configuration solutions, discusses challenges, and provides essential guidance. Although worldwide gross domestic product (GDP) dropped at the beginning of the COVID-19 pandemic and many countries continue to see declines, information technology (IT) spend as a whole has not declined. Digital transformation (DX), which was accelerated by the pandemic along with multicloud, will continue to mature. The tailwinds driving this growth include businesses that see cloud as a key component of business recovery and resiliency. Cloud service providers (cloud SPs) continue to invest in and address demand for cloud and digital services. The cloud service provider sector remains stable compared with other sectors, such as communications or outsourcing. And, mainly due to the continued rise in ransomware attacks that involve lateral movement, cloud services have seen an increased focus on security.

IDC's comprehensive *Worldwide Security Products Taxonomy* is a foundational guide to illustrate how organizations can best provide confidentiality, integrity, and reliability to their IT assets and functions, a commonly used resource by both small and medium-sized businesses (SMBs) and large enterprises.

Customers now search for independent software vendor products and services that easily integrate with public cloud platforms, to the delight of many security practitioners. This new software delivery model, the implementation of which sometimes lies with the independent security providers found in the cloud marketplaces, enables the best of both worlds: best-in-breed solutions that are easy to find, test, buy, and deploy.

This paper discusses VMware and the cloud service providers, includes solutions delivered through the marketplaces, and makes a special note of CloudOps and DevOps, which are largely siloed. The industry, however, recognizes that to keep pace with cybercriminals, a unified "security first" approach is needed.

A worldwide survey conducted in September 2022 by IDC titled *Cloud Workload Protection Survey* ("survey" for the purposes of this paper) is referenced throughout the paper. Key themes in the paper include visibility, governance, automation, and shift left, with responses from 600 individuals across major industry verticals including finance, healthcare, retail, and life sciences framing our findings.

Situation Overview

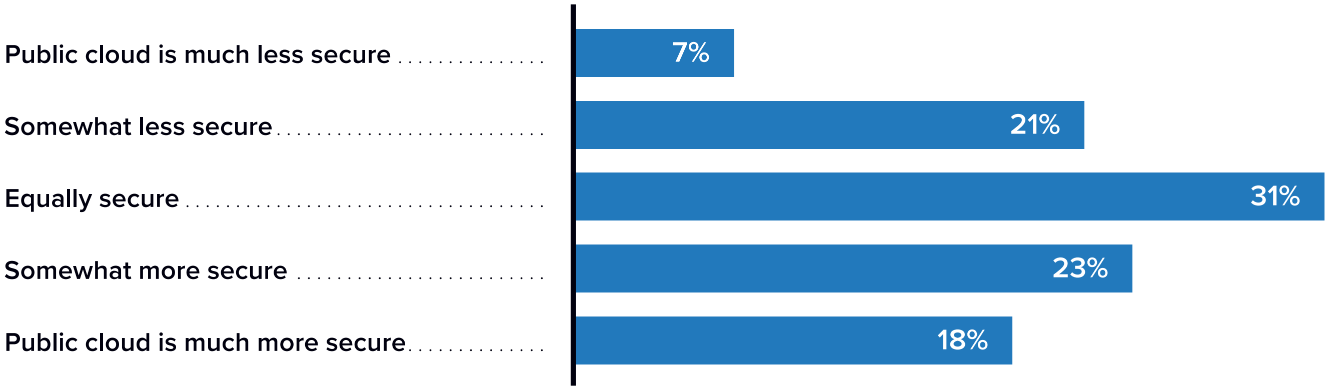
Organizations travailed through Digital Transformation 1.0 beginning in 2018, which was the experimentation phase. Next, Digital Transformation 2.0 kicked off in 2020 and was accelerated due to the pandemic. In 2022, organizations entered the nascent stages of "digital first" and looked at how to increase revenue from digital channels. Security investments have been steady — however, we still need to rethink the security threat landscape, as threat actors are making it past endpoint and perimeter defenses and using legitimate ports and protocols to start and progress their attacks.

The first step: trust. Lest we forget, some organizations are still feeling the burn from the initial lift-and-shift approach to the cloud. Otherwise, performance and security gaps may haunt you. It's important to plan your migration to realize the benefits. Since then, organizations have begun to see the return on investment from their cloud migration, and trust again is developed. As shown in **Figure 1**, 41% of respondents in IDC's *Cloud Workload Protection Survey* indicated that they believe public cloud is more secure when compared with security for on-premises environments.

FIGURE 1

41% of Organizations Assert That Public Cloud Is More Secure

Which one of the following best describes your organization's stance on security in the public cloud as compared with security that can be delivered with on-premises environments?



n = 620; Source: IDC's *Cloud Workload Protection Survey,* September 2022

To say that security is the only metric is a misnomer. Today, organizations view security risk as business risk. As part of this equation, organizations look to change a “want” to an “outcome.” Many benefits drive the movement to cloud, such as:

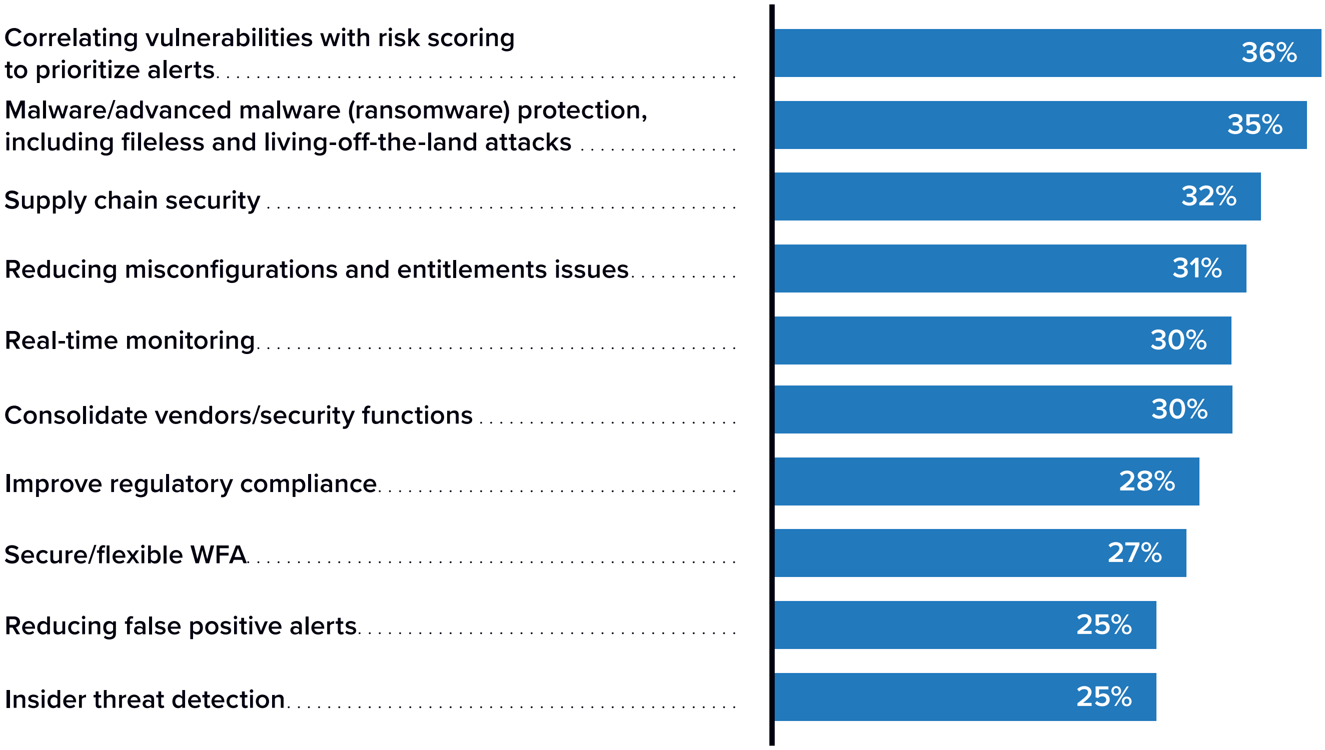
- Deploying resources quickly in response to changing business conditions
- Improved access to security offerings through the cloud marketplaces
- Multicloud visibility and governance to streamline internal processes
- Developing customer loyalty after organizations migrate to the cloud (A common refrain is better customer experience and loyalty due in part to the 24 x 7 cybersecurity talent and support offered by the cloud providers and third-party security vendors.)

Next, as organizations leverage cloud to take advantage of its scalability, reliability, and flexibility, they must take time up front to establish the security baseline for the confidentiality, integrity, and availability of systems. Also inherent is the shared responsibility model (SRM) with the public cloud provider. In general, the SRM means that a cloud service provider is responsible for the security of the cloud, and the users (customers) are responsible for securing the data they put in the cloud. Therefore, understanding security priorities and associated risks is the bedrock of cloud workload security. In fact, as shown in **Figure 2** (next page) from the survey, to meet customer requirements over the next 6–12 months, employing a holistic cloud security approach across the entire software development life cycle is necessary to keep up with the highest security priorities. Organizations know they need to be proactive and want advanced workload and lateral security controls along with the correlation of vulnerabilities with risk scoring to prioritize alerts and protection from malware and ransomware, including fileless and living-off-the-land attacks.

FIGURE 2

Top Security Priorities for a Holistic Security Approach

Overall Rank - Which of the following will be the highest security priorities for your organization in the next 6–12 months?



n = 620; Source: IDC's *Cloud Workload Protection Survey*, September 2022

Cloud security is complex. In the opinion of IDC, this complexity grows exponentially as additional clouds or software-as-a-service (SaaS) applications are added. Protecting applications in one cloud environment is not that daunting a task. Implementing proper configurations, access permissions, and policies is challenging but doable with a little elbow grease and stubborn resolve. Having two environments does not double the complexity of the task but rather quadruples it. An organization with three infrastructure-as-a-service (IaaS) environments and one on-premises virtualized environment faces 16 times the complexity. Multicloud and hybrid cloud are the reality for most organizations. Therefore, as cloud increases in complexity, the attack surface expands and the threat of breaches increases.

Shifting to multicloud and cloud-native applications has its own challenges. Organizations are concerned not only with data breach or loss due to ransomware but also with visibility across multicloud environments, automation of policy management, and managing multiple identity and access domains. This can most aptly be seen in operational efficiency. The time between a vulnerability being discovered and exploited is growing shorter. When organizations were asked on average how long it took for their security operations center (SOC) or cloud security analyst teams to perform basic research once a unique alert has been received, 30% of organizations answered one day or more. Organizations need to act quickly, having on-demand prioritization of alerts. Alert fatigue can be mitigated with access to additional resources, including targeted deep telemetry, by not only seeing the connections being made but also understanding the conversations happening on those connections. Prioritization of misconfigurations and vulnerabilities, artificial intelligence/machine learning–driven analytics, and network detection and response are just some of the services that need to be on tap to secure modern environments.

This level of foundational cloud security can be difficult. In security, when there is time, the SOC or tier 1 analyst will always opt to perform a root cause analysis, which is a best practice. However, there are several factors preventing that from happening:

- Inability to route alerts to developer teams fast enough
- Lack of infrastructure context
- Current security tools that are hard to use and not fully integrated
- No central dashboard from which to manage, monitor, alert, and remediate

Equally as important is the talent gap. When organizations were asked what is preventing them from investigating all suspicious alerts each week, most responded that existing IT/security professionals have insufficient skills. This is largely due to little time for retraining or certifications, all while the backlog begins to tower. Organizations know that increasing security compliance and risk requirements necessitates dedicated resources and the right tools.

Essential Guidance

Top priorities for enterprises should be to centralize observability, visibility, and control across clouds to get accurate threat detection, systematically address alerts (with the right security tools from a single, easy-to-use console), and automate policy recommendations as workloads get provisioned or migrated to a different environment to maintain a consistent security posture and avoid unforeseen regulatory costs. After all, security risk is business risk. Cloud security solutions are focused on protecting cloud resources, regardless of whether the solution resides on premises or in the cloud. As companies seek to understand their security health and hygiene, IDC has identified best practices when making cloud security decisions that are discussed in the sections that follow.

Cloud security solutions are focused on protecting cloud resources, regardless of whether the solution resides on premises or in the cloud.

Best Practices for Securing Public Cloud Environments

The cloud is open to the internet by default, making it completely dynamic, so security must be provisioned differently. Applications have moved from monolithic to microservices-based, linking hundreds or even thousands of loosely coupled services that are dynamic, ephemeral, and highly distributed. The transformation has expanded the attack surface, with the introduction of more intrusion points and lateral movement using allowed ports and protocols that require threat actors to be found and evicted. Asking the right questions and understanding the differentiation between cloud security vendors and their solutions are now imperative. IDC recommends a holistic approach to security with a special focus on visibility with cloud security posture management (CSPM) and cloud workload protection platforms (CWPPs), cloud governance, automation, and shift-left methodologies and tools.

Visibility

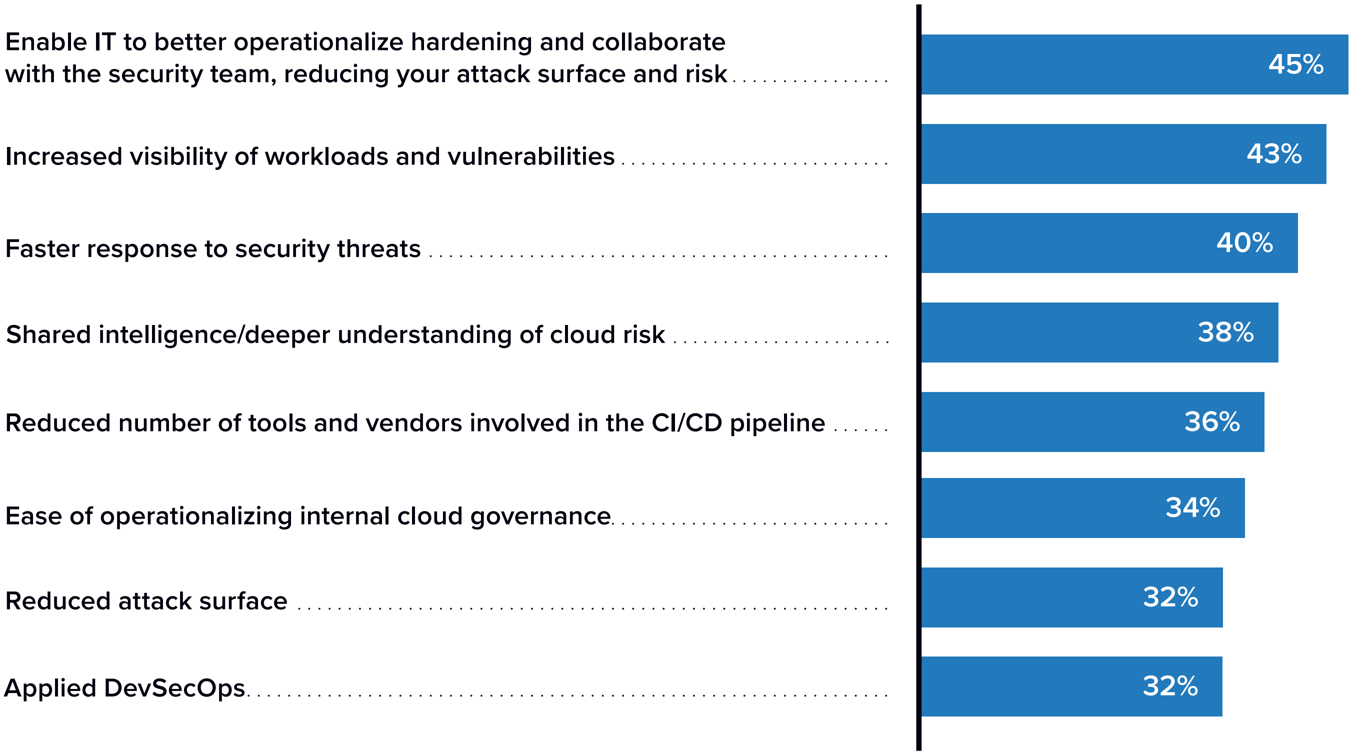
Depending on the maturity of an organization's security program, a typical cloud journey will include defining a cloud environment, determining a deployment model, partnering with the right cloud providers, and engaging with a third-party security vendor directly, either through a marketplace (e.g., AWS Marketplace) or with a managed security service provider to prepare a security audit road map. The end result and new reality for most organizations is multicloud, wherein visibility of environments takes the seat at the head of the table. The data collected should be high-fidelity data, including the traffic between virtual machines (VMs) on a single host, not just sample data from a network tap, as well as the inner workings of enterprise and modern apps including the data being accessed. This enables the ability to accurately make the critical distinction between normal behavior and anomalies.

One of the most important benefits that organizations expect from a cloud workload protection platform is increased visibility of workloads and vulnerabilities, as shown in **Figure 3** (next page). As workloads (virtual machines, containers, serverless) pass through different environments including on premises and private and public clouds (IaaS), the responsibility model changes. Add compliance for regulated industries, government certifications (e.g., FedRAMP), and ephemeral workloads that appear and disappear quickly, and as digital sovereignty mandates take shape, applying DevSecOps and disrupting attacks should be part of a managed end-to-end solution where visibility is the prime directive. You must see more to stop more attacks. Organizations need context-rich insights providing deeper visibility into multicloud assets and activities.

FIGURE 3

Top CWPP Benefits — Hardening an Increased Visibility

What are the most important benefits you would expect to receive from an advanced cloud workload protection solution provider?



n = 620; Source: IDC's *Cloud Workload Protection Survey*, September 2022

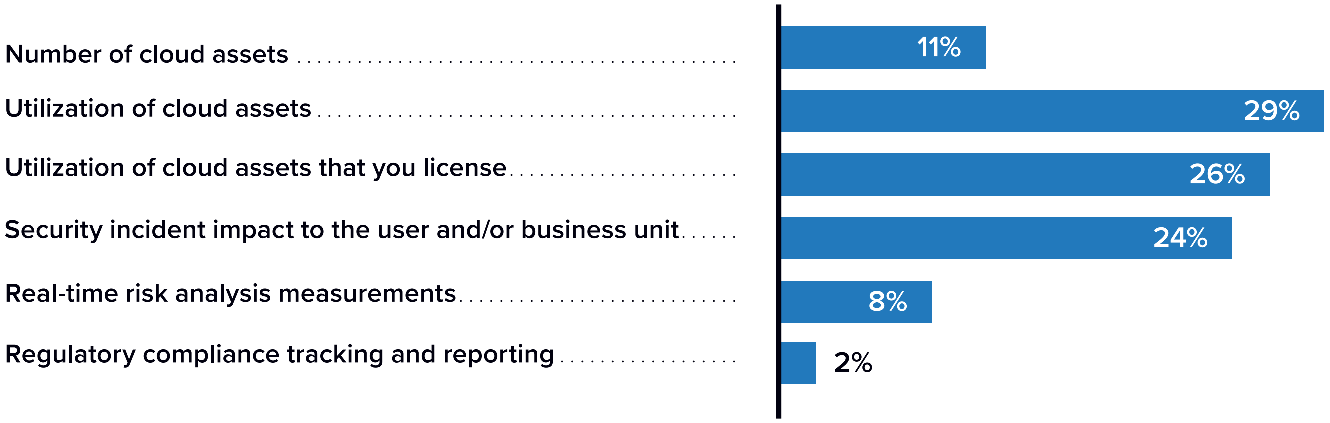
Governance

As with visibility, you can't protect what you can't see or what you don't know about. In fact, as shown in **Figure 4** (next page), increasingly, organizations are taking stock of their cloud assets and utilization. As part of the cloud governance process, having visibility/control of the utilization for licensed cloud assets is critical. Unused assets may create security gaps and affect the bottom line. Redirecting those resources to other security activities will have a positive impact on both staff and budget. Therefore, the visibility between securing multicloud environments and understanding cloud asset relationships is inherently linked.

FIGURE 4

Visibility/Controls into Utilization of Licensed Cloud Assets Highly Ranked

What visibility/controls are most important to you to understand your cloud asset relationships?



n = 620; Source: IDC's *Cloud Workload Protection Survey,* September 2022

Automation

Vital to a defense-in-depth strategy and an organization's security posture readiness is automation. Automation comes in many different forms.

The proliferation of data along with the growing sophistication of cybercriminals and directive to minimize costly breaches and fines requires:

- Automatic discovery of a workload with the flows to enable policy recommendations
- Capabilities that enable new workloads to inherit policies automatically, retire policies when a workload retires, and move policies with the workload without dropping connects
- Continuous monitoring and prioritization of vulnerabilities
- Cloud security posture management and Kubernetes security posture management (KSPM)
- Asset relationship mapping
- Machine learning to model for risk reduction

As oganizations shift left, solutions such as infrastructure as code/scanning should also be considered. This automated, immutable infrastructure approach eliminates configuration drift, scans for vulnerabilities/compliance issues, and ensures consistency across environments.

Moving to the cloud provides access to trained and specially certified third-party consulting partners and systems integrators with expertise including integrating cloud-native security solutions, especially around building automation in the workflow. Some security vendors have integrated solutions that dynamically detect findings from the cloud service provider tools such as AWS GuardDuty, which can provide additional visibility and insights into alerts about that environment.

Shift Left (and Identity)

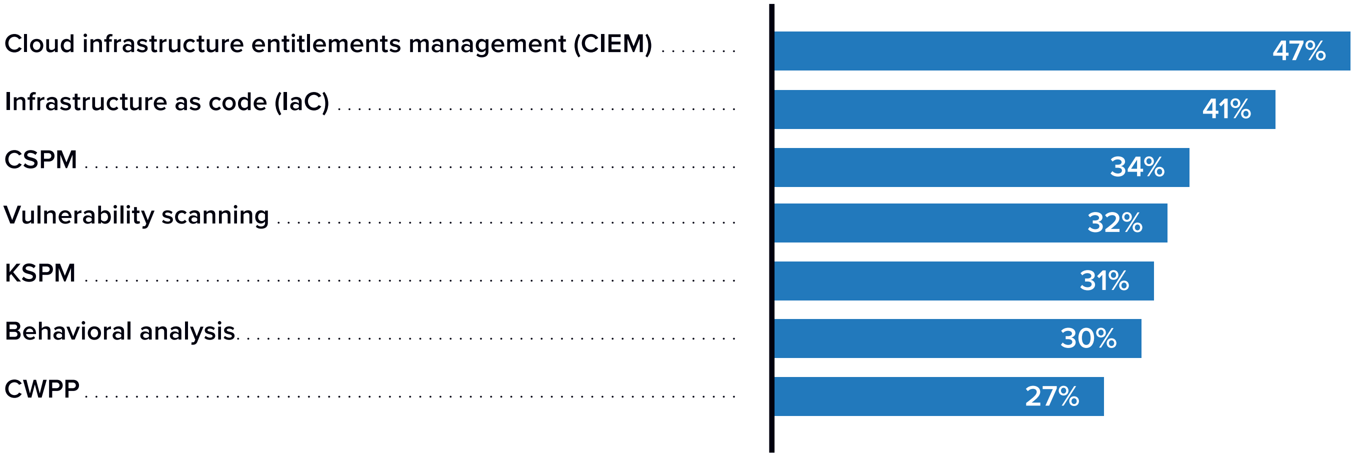
Shift-left security means to break down the silos of development teams, platform teams, and security teams and bring security early into the software development life cycle with methodologies such as DevOps and DevSecOps. The greatest challenge is a cultural one: Historically, developers have been skeptical of security getting in the way, holding up development and increasing time to market. Security practitioners are solely focused on securing the environment, from code to runtime, sometimes indifferent to tight deadlines. In these cases, it is recommended to partner with security vendors that have experience in not only reducing organizational friction but also gaining C-suite buy-in. However, it is important to note that the buyer personas for security solutions are evolving as the voice of the developer and practitioner grows. Not paying attention to these audiences during the vendor selection process is a lost opportunity for insights.

Shifting identity left should also be part of the security conversation. Identity has been referred to as the “new perimeter”, as compromised credentials are responsible for a majority of breaches. When organizations were asked, “Which of the following capabilities is your organization currently using or in the process of evaluating in order to support cloud security?” cloud infrastructure entitlements management (CIEM) was cited most often, by 47% of respondents (see **Figure 5,** next page).

FIGURE 5

Shift-Left and Identity as The New Perimeter Tell the Story

Overall Rank - Which of the following will be the highest security priorities for your organization in the next Which of the following capabilities is your organization currently using or in the process of evaluating in order to support cloud security?



n = 620; Source: IDC's *Cloud Workload Protection Survey*, September 2022

Solution

To maintain pace with today's complex and fast-evolving threat landscape, enterprises need to feel safe in the hands of a proven cybersecurity platform. A distributed, scale-out software security architecture can truly help "realize the cloud operating model," with automation and dynamic services that elevate the security baseline and posture. Enter VMware and preferred partner AWS. These solutions identify, assess, and mitigate cloud risks.

Organizations look to security vendors to help minimize the complexity created by the multicloud architectures that they implement. VMware Carbon Black Workload protection on AWS and VMware NSX reduce the attack surface, increase visibility and observability, and simplify operations with consistent configuration and policy management across clouds.

VMware deepens its visibility into private, public, and hybrid cloud workloads, providing valuable system context with leading prevention, detection, and response capabilities. This is accomplished with real-time system audits, by hardening workloads and making it easy for DevOps and CloudOps to operationalize defense in depth. For organizations to secure modern workloads against ransomware, malware/nonmalware attacks including insider threats, and known and unknown attacks made up of fileless and living-off-the-land attacks, broad cloud workload protection is necessary. To minimize vulnerability fatigue, prioritization of alerts and automated remediation features are built in.

As IDC has reported, organizations are looking for cloud security consolidation of functionality and tools in a single vendor. VMware Aria Automation for Secure Clouds answers the call, with an integrated security configuration solution including cloud security posture management, Kubernetes security posture management, cloud infrastructure entitlements management, user and entity behavior analysis, and threat correlation. While SaaS availability, multicloud hybrid functionality, ease of use, and regulatory compliance are among the biggest considerations for organizations when making cloud security decisions, VMware Aria Universal Suite gives you complete cloud management flexibility by combining on-premises and SaaS capabilities in a single license, helping enable a self-paced move to the cloud.

In the United States, organizations are keenly aware of the executive orders (EOs) signed by President Biden, including EO 14028, “Improving the Nation’s Cybersecurity.” These mandates must be met for organizations to contract with the U.S. federal government. VMware Carbon Black Workload carries framework certifications such as FedRAMP. And, as the future of digital sovereignty is written, the European Union and most organizations must comply with the General Data Protection Regulation and new regulations for each country. VMware-trained cybersecurity professionals also carry their own security tool certifications.

VMware has made an investment in the AWS partnership with recognition as a preferred partner, with VMware Cloud, VMware Carbon Black Workload, and VMware Aria Suite on the AWS Marketplace. As a result, organizations gain in-depth, cloud-native visibility and control into AWS application deployments and workloads.

Mitigate Multicloud Complexity

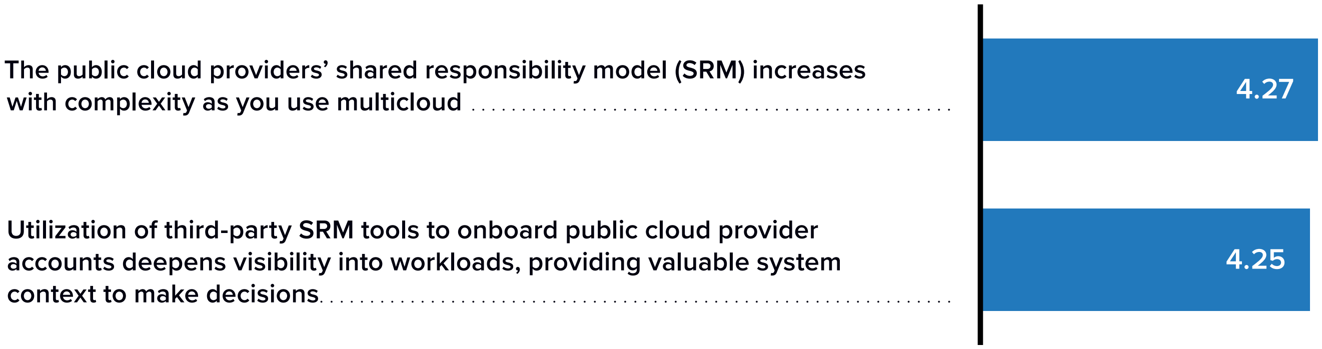
It's a cloud journey, so organizations need to be thinking long term. With each passing day, there is yet another new security company that may or may not add value to an organization's security architecture. Frankly, the multitude of vendors creates a lot of noise, and the noise can be deafening. Perceiving differentiation among vendors is key. IDC recommends focusing on the benefits offered to an organization's individual use case.

In addition, VMware and any other security vendor can only mitigate so much complexity for an organization, as organizations create their own complexity. Security hygiene must be exercised at every level, from the C-suite to the individual practitioner. Organizations will need to be proactive and continually educate their ranks on the importance of designing, building, embedding, and implementing cloud security. Keep in mind that multicloud visibility comes with latent complexity and that using third-party shared responsibility model tools to onboard public cloud provider accounts mitigates that complexity (see **Figure 6**).

FIGURE 6

SRM* Multicloud Complexity is Mitigated with Third-Party Tools

Indicate your level of agreement with the following statements.



n = 620; Source: IDC's *Cloud Workload Protection Survey*, September 2022

Conclusion

Benefits measured in terms of impact on the developer and security personnel are recommended, as cybersecurity professionals are an organization's most precious asset. VMware meets customers where they are in their cloud journey, delivering integrated solutions. Organizations seeking a holistic cloud security solution should:

- Understand their security health and hygiene
- Know the steps to securing modern cloud workload solutions, from build time to runtime, including visibility, governance, automation, and shift left
- Begin breaking down silos between the developers and security practitioners and implement shift-left security with the right cloud workload and automation tools
- Engage a third-party security vendor to minimize the complexity of multicloud environments and reduce organizational friction

Modern unified cloud workload security — it's what you need to know

About the IDC Analyst

Philip Bues
Research Manager, Cloud Security, IDC

Phil Bues is the research manager for IDC Cloud Security. In this role, Phil drives research, provides thought leadership, and advises clients on complex issues including cybersecurity of the cloud and in the cloud. His commentary addresses the benefits and challenges of what's been called the "shared responsibility model" and how that line may change going forward.

More about Philip Bues

IDC Custom Solutions

This publication was produced by IDC Custom Solutions. As a premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets, IDC's Custom Solutions group helps clients plan, market, sell, and succeed in the global marketplace. We create actionable market intelligence and influential content marketing programs that yield measurable results.

IDC

IDC Research, Inc.
140 Kendrick Street, Building B, Needham, MA 02494, USA
T +1 508 872 8200

@idc @idc idc.com

Privacy Policy | CCPA