Enterprise Strategy Group™ by TechTarget

WHITE PAPER

Securing Hybrid Cloud Environments

Enabling Security at Scale to Drive Innovation and Business Growth

By Melinda Marks, Practice Director, Cybersecurity
Enterprise Strategy Group

July 2024

Contents

Executive Overview

While organizations are adopting digital transformation initiatives, including cloud-first policies to speed up software development, security teams have faced challenges in supporting faster development cycles and dynamic workloads in cloud environments. At the same time, our research shows that hybrid clouds are the norm, with enterprises leveraging on-premises and colocation facilities using modernized, open application stacks. The disparate environments that comprise hybrid clouds have increased complexity for security, with many organizations finding it challenging to unify best practices across teams, technology stacks, and environments, negatively impacting operational, security, and compliance objectives and requirements.

Organizations need effective strategies to gain consistency across their heterogeneous hybrid cloud environments, from the data center, to public clouds, to the edge. This requires coordination across teams, including development, IT, and operations, from building and deploying applications to managing workloads across the hybrid cloud. This will be especially important with the expected growth and scale that will accompany increasing adoption of AI across workloads. This paper explores the composition of hybrid clouds and the challenges associated with securing these dynamic and complex environments, then outlines the best practices for a full-stack, modern security approach to support digital transformation that fuels business growth.

Modern Data Center Composition

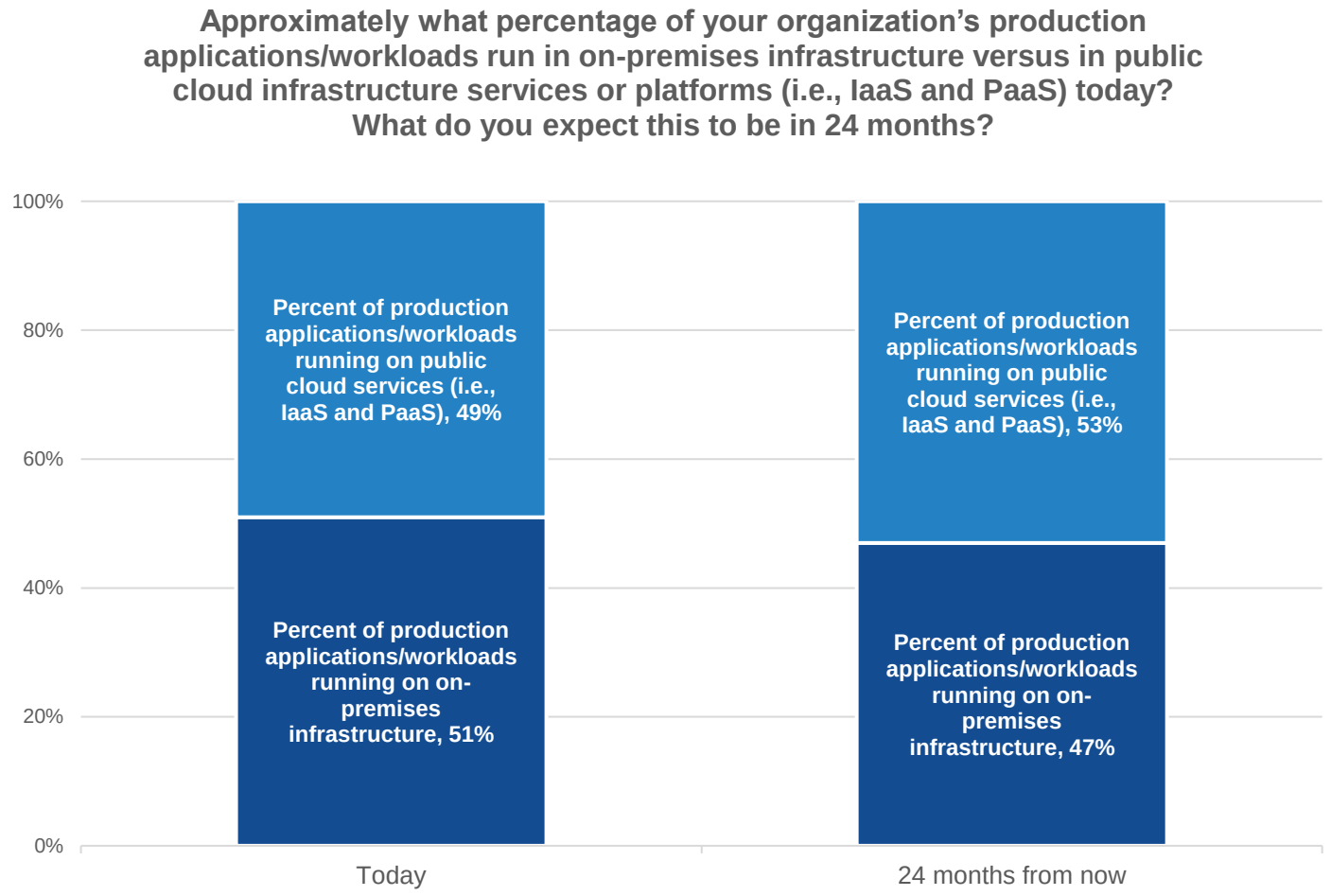
Organizations are under pressure to increase productivity and drive innovation to best serve their customers. To meet this demand, organizations are increasingly migrating their production workloads to the cloud, enabling them to leverage cloud services providers (CSPs) for state-of-the-art technology and services, without having to worry about the underlying infrastructure or maintenance.

Hybrid Data Center Composition

Research from TechTarget's Enterprise Strategy Group showed 49% of production applications/workloads are run on public cloud services today. In 24 months, this is expected to increase to 53%, but hybrid clouds will remain the norm, as 47% of the production workloads are predicted to be run on on-premises infrastructure two years from now (see Figure 1).[1]

[1] Source: Enterprise Strategy Group Research Report, *Distributed Cloud Series: The State of Infrastructure Modernization Across the Distributed Cloud*, November 2023.

Figure 1. Hybrid Cloud Is the Norm



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

Modernization efforts include the adoption of cloud-native applications with microservices architectures utilizing open source tooling, deployed on elastic infrastructure, and delivered and managed via the automated continuous integration/continuous delivery (CI/CD) orchestration processes of a DevOps methodology. Cloud technologies, such as Linux-based containers, Kubernetes for workload orchestration, and public cloud services, play leading roles in cloud-native environments, with serverless functions adding to the heterogeneity of modern applications.

However, this technology stack is not exclusive to public clouds; Enterprise Strategy Group research showed organizations are using microservices or functions for on-premises applications to achieve benefits including improved productivity, resilience, compliance, and scalability (see Figure 2).[2]

[2] Ibid.

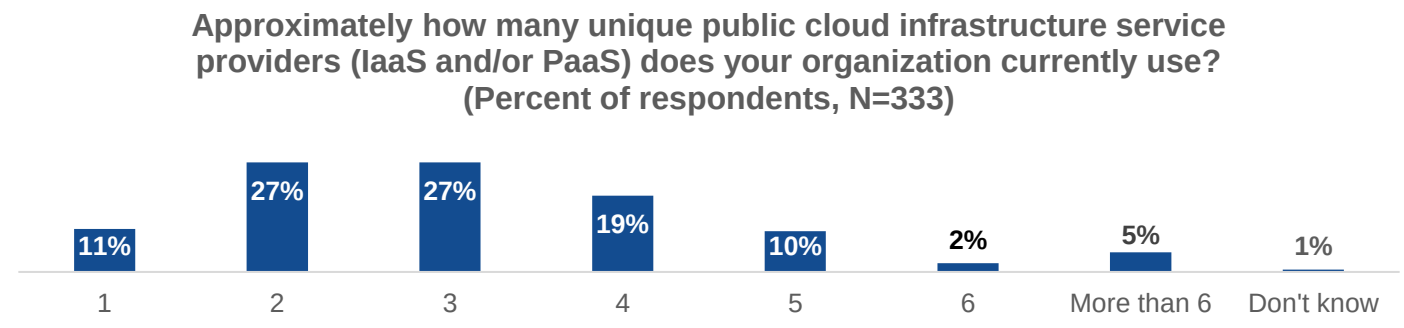
Figure 2. Microservices Adoption Drivers for On-premises Applications

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

Enterprise Strategy Group research also showed that the vast majority of organizations (89%) leverage cloud infrastructure services from multiple cloud service providers, with 62% leveraging three or more (see Figure 3). The study also indicated that 88% of organizations are moving data between data centers and public cloud services, with 30% reporting that they move data between environments "frequently," and 20% claiming they move data between environments "all the time."[3]

The transportability of workloads benefits organizations in many ways. For example, they can avoid lock-in and leverage innovations from multiple cloud providers, or they can move workloads to their data centers.

Figure 3. Number of Public Cloud Infrastructure Service Providers



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

[3] Ibid.

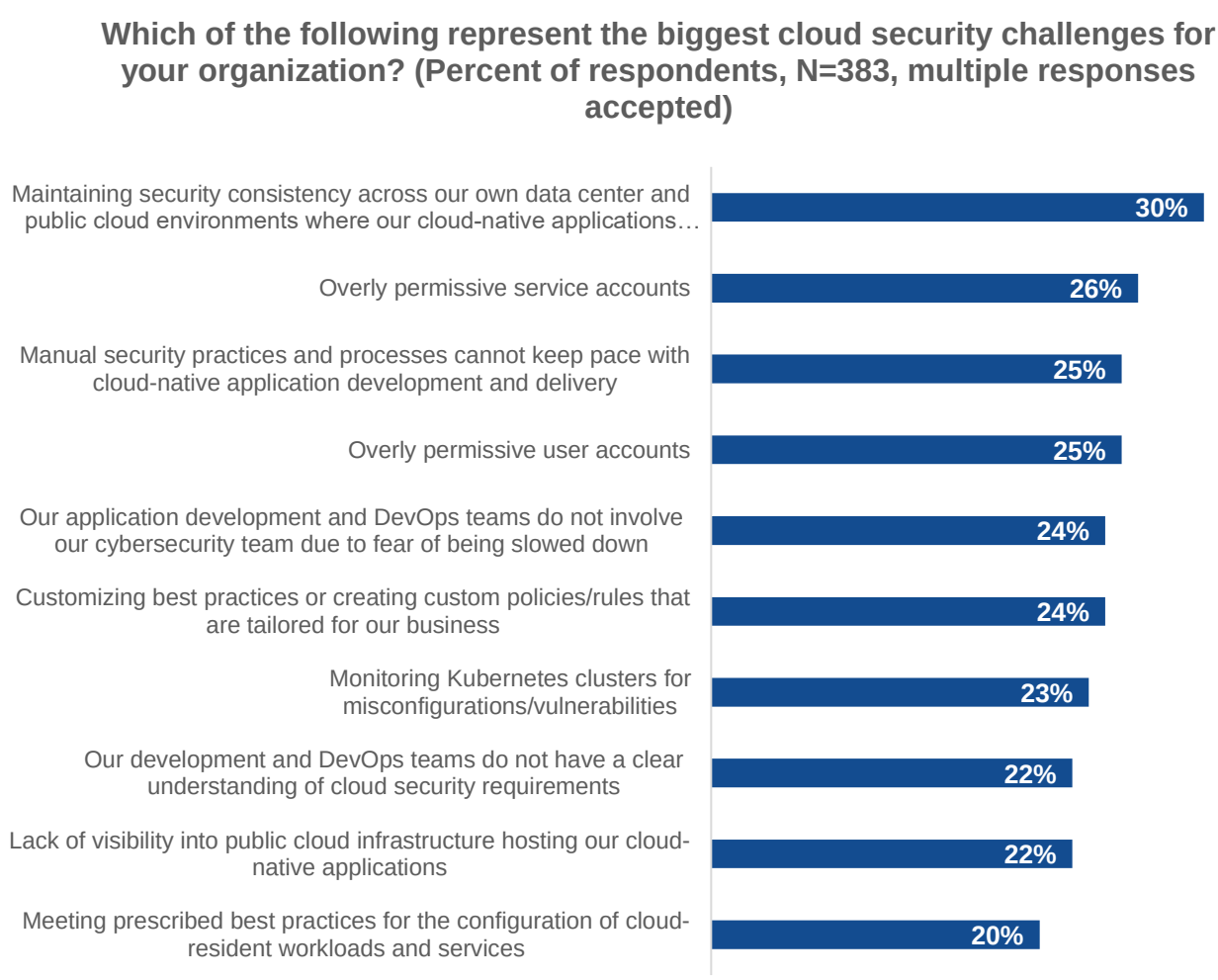
Hybrid Cloud Security Challenges

However, these modernization efforts across multi-cloud and hybrid cloud environments create complexity for security teams, as they need to manage multiple sets of controls to configure and secure workloads across their hybrid cloud environments. Research on cloud security posture management trends showed 70% of organizations find that the differences between cloud-native applications and the rest of their applications and infrastructure require a different set of security policies and technologies, and 73% believe the use of multiple clouds makes it challenging to maintain consistent security posture across environments.[4]

Increased Attack Surface

The study also showed the top 10 challenges reflecting the cloud-readiness gap that organizations face when trying to keep up with the higher scale and productivity from these modernization efforts, which expand the attack surface and increase exposure to attacks (see Figure 4).

Figure 4. Top 10 Cloud Security Challenges



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

[4] Source: Enterprise Strategy Group Research Report, *Cloud Entitlements and Posture Management Trends*, April 2023.

These challenges reflect the increased pressure on security teams as development teams deploy applications to production more quickly. However, as development teams scale with modernized processes, there is a higher chance for mistakes and misconfigurations across the technology stack. These security issues are not exclusive to public cloud environments; unpatched or otherwise misconfigured customer-managed assets can be successfully exploited by adversaries. The misconfigurations, whether in an enterprise's cloud estate or on-premises infrastructure, create attack paths for adversaries.

Compliance Challenges

Hybrid cloud heterogeneity and the shift of data assets to public clouds also complicates the need to meet and maintain compliance with industry regulations. For example, 73% of research respondents cited overly permissive service accounts as introducing significant security and compliance risk.[5] The speed of development and increased opportunity for misconfigurations also creates real business impact: 35% of organizations with misconfigured cloud services reported that they faced fines due to noncompliance with industry regulations in the past year.[6]

Gearing Up for AI Usage

Another important consideration for hybrid cloud security is the expected adoption of AI, especially generative AI (GenAI). Our research showed organizations are using or planning to use GenAI's assistive capabilities to further increase productivity and gain a competitive advantage: The vast majority of organizations (85%) are already utilizing or developing large language models (LLMs) for proprietary use, whether as part of a production GenAI environment or an ongoing development project, while another 13% reported that they are in the process of developing an LLM.[7]

Beyond LLMs, organizations are well underway in applying GenAI in areas like IT operations, software development, sales, and research. Organizations need to proactively address security risk, including understanding and protecting sensitive data, APIs, and permissions and access, which are already scaling rapidly with modern development processes that are difficult to secure across hybrid environments.

In fact, our research showed that 86% of organizations are taking early measures to block access to GenAI sites due to security concerns, impeding their organizations from adopting the innovative technology.[8]

Improving Security and Compliance Across Hybrid Clouds

Having explored the composition of hybrid clouds, as well as some of the associated security and compliance challenges, it's time to discuss best practices for effective security and risk management for workloads across hybrid cloud environments.

Cross-team Collaboration to Drive Efficiency

Securing the modern IT landscape requires collaborative organizational dynamics across people, processes, and technologies. This includes goal alignment across groups, including cloud/platform engineering, IT, operations, and development, with KPIs that measure application uptime, compliance with industry regulations, the meeting of service-level agreements (SLAs), data protection, and business growth.

It is important for teams to collaborate to select technology products and platforms that drive efficiency across the entire organization while ensuring security and compliance. Security should be incorporated as a design principle early in development, and this requires cooperation and coordination across stakeholders.

---

[5] Ibid.
[6] Ibid.
[7] Source: Enterprise Strategy Group Research Report, *Generative AI for Cybersecurity: An Optimistic but Uncertain Future*, April 2024.
[8] Ibid.

Successful modernization efforts need to focus on optimizing efficiency and productivity, with security controls scaling to support growth. When cross-functional teams collaborate, it better enables them to ensure security is built into their programs with shared tools and processes that optimize efficiency across teams.

Secure the Full Stack

The heterogeneous mix of today's hybrid clouds requires a full-stack approach inclusive of the host and network layers as well as management consoles. Here are key security considerations to secure the full stack:

Host-level Security Leveraging Built-in Linux Security Technologies

Linux is the open source operating system that provides the flexibility and portability to run critical infrastructure in any cloud environment or data center. Enterprise-class Linux distributions, including Red Hat Enterprise Linux, employ security principles, including least privilege and mandatory access control. These are critical in offering important security capabilities, including encryption, host-based firewalls, identity and access controls, and more.

Controls for Workload Types

It's important to apply layered, host-based controls across all server workload types deployed in hybrid clouds, including bare metal servers, virtual machines, application containers, and public cloud instances. These should include vulnerability management, virtual patching (i.e. detecting and preventing runtime behavior before the exploitation of a vulnerability), as well as controls such as file integrity monitoring (FIM), firewalls, and any auditing that might be required to satisfy regulatory requirements.

Automated Controls and Policies

While different environments might have different automation platforms to provision and configure applications, consistency can be achieved by employing common practices across systems as they are deployed within hybrid clouds. By establishing change control policies and automating key processes, security teams can achieve greater consistency to help developers improve the quality and security of their applications.

Examples include:

- Automating configuration management for repeatability, auditability, and reduction of human errors.
- Automating compliance to industry standards, such as benchmarks published by the Center for Internet Security (CIS).
- Automated discovery of assets for increased visibility.
- Patch management policies based on risk severity, SLAs, and the criticality of the affected system.
- Streamlined workflows via automation of processes with integrations to ticketing and messaging platforms.
- Monitoring, auditing, and reporting for investigations and compliance.

Addressing the Increasing Importance of Software Supply Chain Security

As developers increasingly use open source software (OSS) components as well as container images sourced from public registries to more quickly build their applications, it is important to understand the code composition and provenance to ensure that it is free from vulnerabilities and that access is secure to prevent unwanted tampering. Utilizing enterprise-class OSS that is actively managed by a commercial entity, such as Red Hat, can help with software supply chain security.

Organizations should also incorporate software composition analysis and software bills of materials into their application security programs, including the extension of static application security testing (SAST) and dynamic

application security testing (DAST) to identify and remediate vulnerabilities in third-party components beyond their internally developed code.

Network Security

For applicability and consistency across disparate environments, policies and controls that secure network connectivity via the use of segmentation and security groups should be based on tags and server workload roles as an abstraction from the underlying infrastructure. For cloud-native environments, this will entail the use of Container Network Interface and/or service mesh for securing east-west traffic between containers.

For response purposes, network detection and response controls that support both virtual private clouds and on-premises networks will provide SOC teams visibility across hybrid clouds. Where possible, organizations should take a zero-trust security approach by employing the principle of least privilege.

Data Security

Digital transformation, with the increased adoption of AI, especially GenAI, also includes rapidly scaling large amounts of data, which can be more difficult to manage and secure as data moves across cloud environments. After all, the ability to rapidly release applications to the cloud and make them available for global audiences presents opportunities for attackers to steal valuable data.

Organizations need to understand the data they have—particularly sensitive data, including personally identifiable information—and where it resides to ensure they take the proper measures to protect it. This includes managing access, retention, and recoverability of data to ensure both security and data resiliency.

DevSecOps Adoption to Automate Security Into DevOps Processes

Enterprise Strategy Group research showed that a majority of organizations (79%) have adopted DevOps processes that streamline and automate IT and operations to enable developers to provision and deploy software applications with CI/CD processes. According to the survey, 34% of organizations use DevOps processes and methodologies extensively, and an additional 9% plan to integrate them in the next 12-24 months.[9]

DevSecOps, or Secure DevOps, is a collaborative software engineering, operations, and cybersecurity approach incorporating cybersecurity measures and controls at each phase of the application lifecycle, including development, integration, delivery, and runtime.

As mentioned earlier, incorporating security into cross-team processes following aligned goals is crucial for hybrid cloud security success. As a result, our research shows the increasing adoption of DevSecOps, or Secure DevOps, which is a collaborative software engineering, operations, and cybersecurity approach incorporating cybersecurity measures and controls at each phase of the application lifecycle, including development, integration, delivery, and runtime.

Unfortunately, its adoption lags DevOps adoption, with only 26% securing more than half of their cloud-native applications via DevSecOps. However, it is promising to see that organizations are planning to increase the percentage in the next 24 months, with 43% of organizations planning to have more than 50% of their cloud-native applications secured via DevSecOps.[10]

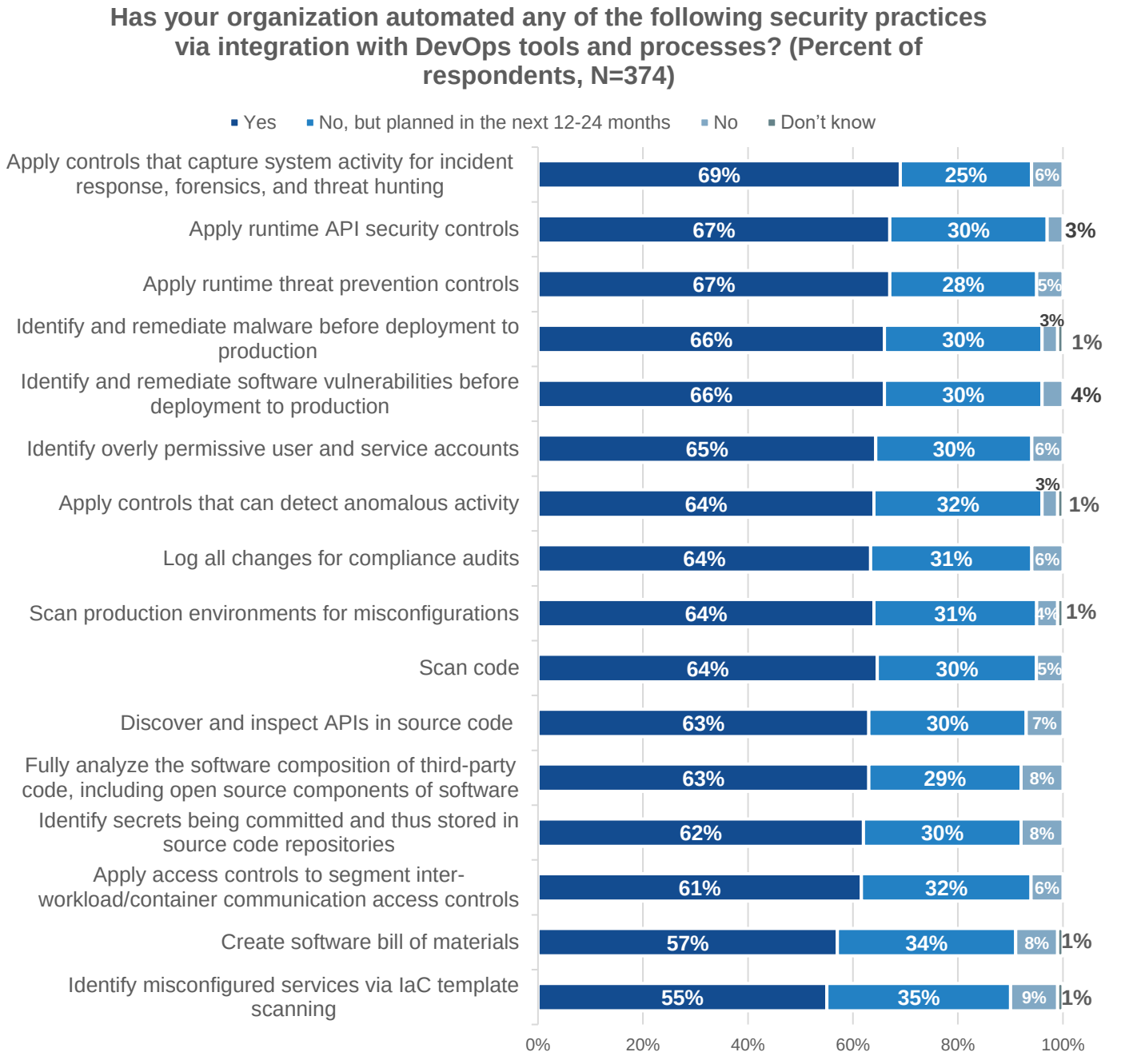
Enterprise Strategy Group research also explored how organizations are incorporating security throughout the software development lifecycle to optimize risk mitigation and rapid remediation of issues.

[9] Source: Enterprise Strategy Group Complete Survey Results, *2024 Cloud Security Platforms and DevSecOps*, June 2024.
[10] Ibid.

As shown in Figure 5,[11] these measures include:

- Predeployment security practices, starting as early as possible in development, including code scanning and policies as guardrails.
- Runtime security practices, including monitoring of workloads and related resources, detection of configuration drift, and threat detection and response.

Figure 5. Current and Planned Security Practices Integrated With DevOps Tools



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

[11] Ibid.

Red Hat Enterprise Linux, OpenShift, and Ansible Automation Platform for Security at Scale Across Hybrid Environments

As organizations leverage Linux-based containers as the foundation of their cloud-native and AI stack, Red Hat Enterprise Linux (RHEL), OpenShift, and Ansible Automation Platform provide an effective way to incorporate security and automation into building, deploying, and managing cloud-native and AI applications across hybrid cloud environments.

RHEL delivers the operating system platform as a container image, providing a single workflow to better incorporate security through container-based tooling and workflows, including CI/CD processes to manage security at scale. OpenShift, the hybrid cloud application platform powered by Kubernetes, drives a consistent experience, incorporating security into workloads across multiple clusters on premises, in the hybrid cloud, and at the edge. Red Hat Ansible Automation Platform helps automate all aspects of the hybrid cloud environment, from cloud resources and services to operating systems, applications, and security.

These tools also provide the following:

- Consistency, simplification, and portability of workloads across environments spanning the hybrid cloud, including mixed environments and use cases.
- An easier way to integrate security into DevOps processes, enabling security teams to apply container security tools for scanning, validation, and attestation and laying the groundwork for better DevSecOps processes across CI/CD and GitOps workflows.
- Faster ways to develop and distribute secure applications with easier ways to build, test, and distribute RHEL-based applications, including AI workloads.
- Support for AI usage with RHEL as an operating system that supports the needed scale and speed of AI, along with OpenShift and Ansible to help organizations create and deliver AI-enabled applications at scale, in an automated way, across hybrid clouds.

Thus, the combination of RHEL, OpenShift, and Ansible enables organizations to meet the needs of increased development speed and efficiency, along with the emerging need for AI applications that spur innovation while integrating security through the cloud-native and AI stack.

Conclusion

Digital transformation leveraging modern development processes with cloud-native technologies and cloud services have helped organizations increase productivity. While this has resulted in cloud-first policies, which require new IT projects be delivered via cloud services when possible, as well as increased migration of existing workloads to public cloud platforms, Enterprise Strategy Group research showed that customer-managed environments will continue to be an important part of the equation as enterprises continue to rely on existing workloads and infrastructure.

This creates challenges for cybersecurity and compliance programs that need to set up consistent controls and policies to mitigate security risk across disparate environments. Security effectiveness for hybrid clouds requires consistency and centralized efforts to secure applications and infrastructure based on unified policies, a collaborative culture, and a common vernacular.

Enterprise Strategy Group recognizes the importance of utilizing containers based on a common OS such as RHEL to help unify policies and automate needed hardening processes on top of a strong foundation to enable developers to secure their applications, starting at the infrastructure level, across any environment: on premises, in the cloud, and at the edge. Red Hat OpenShift also optimizes development processes at scale and incorporates security into the building, testing, and distribution of containerized applications across multiple clusters in hybrid environments. Additionally, Red Hat Ansible Automation Platform can help automate all aspects of the hybrid cloud environment at scale. This is increasingly important as organizations adopt AI to further speed up development processes, requiring enhanced security controls.

About Enterprise Strategy Group
TechTarget's Enterprise Strategy Group provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

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