Enterprise Strategy Group | Getting to the bigger truth.™

Elevate Your Hybrid Cloud Security

Organizations face challenges consistently applying security across their hybrid cloud environments. Using enterprise-class open source software (OSS) actively managed by a commercial entity is an effective way to mitigate risks.

The Need to Consistently Apply Security Controls and Processes

As a high percentage of organizations host their workloads across different cloud platforms, it is difficult for them to unify best practices across teams, technology stacks, and environments, impacting operational, security, and compliance objectives and requirements.

TOP 3 CLOUD-NATIVE APPLICATION SECURITY CHALLENGES

47%
Security consistency across our data center/public cloud environments where our cloud-native apps are deployed

40%
Use of multiple cybersecurity controls increases cost and complexity

32%
Meeting prescribed best practices for the configuration of cloud-resident workloads and services

Container portability and the desire by some to manage Kubernetes deployments both on-premises and in the cloud means that cloud-native applications span both public and private clouds—i.e., hybrid clouds.

Our container-based apps are/will be deployed in a combination of public cloud platforms and private data centers:

- **Today**
- **In 12-24 months**

Assessing Open Source Software (OSS) for Application Development Security

Developers often use OSS from shared communities on the internet. Security teams are leveraging security tools and processes to secure open source components.

ORGANIZATIONS ARE INVESTING IN SECURITY CONTROLS FOR THEIR USE OF OPEN SOURCE SOFTWARE (OSS)

48%
We have already invested in specific security controls to scan for open source vulnerabilities.

43%
We are planning to invest in specific security controls to scan for open source vulnerabilities in the next 12 months.

Objectives for Automation and Portability

The key to scaling security with the high velocity of modern software development is automation and the ability to consistently apply security processes across different cloud environments for portability of workloads.

TOP TWO PRIORITIES FOR CLOUD NATIVE SECURITY

41%
Automate the introduction of controls and processes via integration with our software development lifecycle and continuous integration/delivery tools.

32%
Build a cloud security strategy that can be used across heterogeneous public and private clouds.

ORGANIZATIONS ARE INTEGRATING APPSEC TOOLS INTO THEIR DEVOPS PROCESSES

55%
We have incorporated security into our DevOps processes

15%
We plan to incorporate security into our DevOps processes

26%
We are evaluating security use cases that can be incorporated into our DevOps processes

The Bigger Truth

As organizations focus on policies and control; automation of security processes; and the promotion of collaborative culture between security, operations, and developers, they benefit from using enterprise-class OSS managed by Red Hat, including trusted Linux distributions such as Red Hat Enterprise Linux. This helps to ensure that the components are built adhering to security standards, having undergone testing and verification. With shared code bases and integrations, it is also easier to incorporate security processes and controls via automation.

LEARN MORE

Red Hat

Sources:
ESG Survey Results, *The Maturation of Cloud-native Security: Securing Modern Apps and Infrastructure*, June 2021.
ESG Research Report, *Securing Modern Application Development Environments*, December 2020.
© 2021 TechTarget, Inc. All Rights Reserved.