Enterprise Strategy Group by TechTarget

SECURITY THAT SCALES WITH CLOUD-NATIVE DEVELOPMENT

THE NEED FOR A PLATFORM APPROACH

As organizations increasingly leverage cloud platforms and cloud-native development, security teams need an effective way to manage security risk while keeping up with faster development cycles.

Adapting Security to Cloud-native Development

Cloud-native application development allows developers to quickly assemble applications from third-party code and templates. While this saves them time, it increases the chances of introducing mistakes and vulnerabilities that may be exploited.

» **Usage of open source software (OSS)**

8 in 10 organizations use open source software in **programming cloud-native applications.**

» **Percentage of code composition that is OSS**

< 25%	25% to 50%	51% to 75%	> 75%
3%	42%	49%	6%

Organizations are concerned about hackers increasingly targeting OSS due to its wide usage. They need effective tools to better understand OSS usage risks so they can quickly respond when vulnerabilities are found.

» **Open source software challenges and concerns**

- Having a high percentage of application code that is open source: 54%
- Being victims of hackers targeting popular/commonly used open source software: 41%
- Trusting the source of the code: 40%
- Identifying vulnerabilities in the code: 39%
- Understanding code composition and producing a software bill of materials: 39%
- Applying an issued patch quickly once released: 39%
- Quickly remediating a vulnerability: 38%

» **Infrastructure-as-code (IaC) Adoption**

While utilizing IaC templates empowers developers to provision their own infrastructure instead of waiting for IT or operations teams to set it up for them, it also increases security risk.

96% of organizations are using or plan to use IaC.

83% of respondents say they are experiencing an increase in IaC template misconfigurations.

» **Top three impacts of misconfigured IaC**

46% Unauthorized access to applications and data

43% Introduction of crypto-jacking malware to mine cryptocurrency

41% Remediation steps impacted service level agreements (SLAs)

» **Organizations have also faced a variety of security incidents** and related consequences with their internally developed cloud-native applications in the last year, with only 3% not experiencing incidents.

Incident	%
Attacks that resulted in the loss of data due to the insecure use of APIs	38%
Exploit(s) that took advantage of known vulnerabilities in internally developed code	37%
Compromised services account credentials	35%
Exploit(s) that took advantage of known vulnerabilities in open source software	34%
Exploit of a misconfigured cloud service	33%
Secrets stolen from a source code repository	31%
"Zero day" exploit(s) that took advantage of new and previously unknown vulnerabilities in open source software	28%
"Zero day" exploit(s) that took advantage of new and previously unknown vulnerabilities in internally developed code	27%
Compromised privileged user credentials	26%
We haven't experienced one of these incidents in the last 12 months	3%

Incorporating Security into Development

Organizations are prioritizing developer-focused security strategies, including shifting some security responsibilities to developers because it's the only way for security teams to scale to support the increased speed and volume of releases.

» **Priority level for adopting a developer-focused security strategy**

68% **It's a high priority** (i.e., it will have a significant impact on our security program)

31% **It's important, but not a high priority** (i.e., we have higher security and/or AppDev priorities)

» **Security teams' comfort level adopting a developer-focused security strategy**

15% Slightly comfortable

49% Mostly comfortable

36% Completely comfortable

» **Organizations are also investing in solutions that integrate security processes into developer workflows to more efficiently mitigate risk and reduce security incidents.**

69% We expect to make significant investments

31% We expect to make moderate investments

0% — 100%

» **Top 10 priorities for securing cloud-native software development process**

1. Improving application security testing
2. Detecting secrets that have been committed and stored in source code repositories
3. Applying runtime API security controls
4. Identifying software vulnerabilities before deployment to production
5. Discovering and inspecting APIs in source code
6. Remediating malware before deployment to production
7. Scanning open source code components and third-party libraries
8. Remediating software vulnerabilities before deployment to production
9. Scanning production environments for misconfigurations
10. Identifying malware before deployment to production

Scaling with a Platform Approach

Organizations are increasingly looking for consolidated approaches, or cloud-native application protection platforms (CNAPPs), to efficiently mitigate security risk as development scales. These platforms tie security in development processes to improving security posture, helping security teams effectively manage risk for cloud-native applications.

» **Top 5 business drivers for cloud security posture management**

1. Addressing the sheer number of assets that are cloud-resident
2. Preparing for security incidents our organization may experience in the future
3. Meeting prescribed best practices for the configuration of cloud-resident workloads and the use of cloud APIs
4. Meeting demands from the organization's customers/partners/supply chain
5. Automating security controls via integration with existing DevOps tools

» **Most organizations believe that a platform approach will drive efficiency to enable security to scale with cloud-native development.**

85% of organizations said a CNAPP will give them a consolidated approach for more efficient cloud security risk mitigation.

87% of organizations said a CNAPP helps drive efficiency in connecting application security processes to security posture management.

Conclusion

As organizations increasingly adopt cloud-native development for faster release cycles, security teams need an advanced security platform that will enable them to scale to support the rapid growth enabled by cloud-native development. The right solution must drive efficiency by incorporating security into development processes while enabling security teams to effectively manage risk.

About Cisco

As a global industry leader in security, Cisco provides solutions that enable companies to safely move forward with cloud adoption, while protecting company and customer data from cybersecurity threats. Cisco Cloud Application Security helps companies secure and speed up cloud innovation. It delivers visibility and protection across the cloud application lifecycle so customers can reduce risks and increase team productivity. It also enables DevSecOps best practices. Developers can fix vulnerabilities faster while security teams can measure compliance and prioritize security findings from one tool with unmatched value.

To see how Cisco can address your cloud application security needs from development to runtime, please click the link below.

CISCO

LEARN MORE

Source: Enterprise Strategy Group Research Report, *Walking the Line: GitOps and Shift Left Security*, November 2022.
Source: Enterprise Strategy Group Research, *Cloud Entitlements and Posture Management Trends*.