Enterprise Strategy Group | Getting to the bigger truth.™

The Maturation of Cloud-native Security

Securing Modern Applications and Infrastructure

The composition of cloud-native applications is a mix of APIs, containers, VMs, and serverless functions. Securing these applications, the underlying infrastructure, and the automation platforms that orchestrate their deployment necessitates revisiting threat models, gaining organizational alignment, and leveraging purposeful controls. Additionally, cloud security controls are being consolidated, project teams are evolving their strategies for securing cloud-native applications and platforms, and vendors are consolidating multiple technologies into integrated cloud security suites.

The Importance of Containers

Containers play a leading role in a heterogenous stack deployed across distributed cloud environments.

CURRENT USAGE

77%
of organizations currently use containers for production applications.

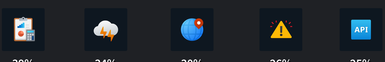
LENGTH OF TIME IN USE

The Perils of Program Maturity Gaps

Program maturity gaps result in inconsistency, misconfigurations, and visibility gaps.

73%
report that the lack of access to the physical network and the dynamic nature of cloud-native applications and elastic infrastructure **create visibility blind spots, making security monitoring challenging.**

FIVE MOST IMPORTANT APPROACHES TO IMPROVING SECURITY VISIBILITY



39%
Audit trail of privileged user/service account activity

34%
Identifying out of compliance workload configurations

30%
Location and disposition of secrets

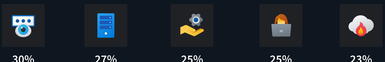
26%
Identifying software vulnerabilities

25%
APIs and serverless function activity

The Need for an Evolved Strategy

A diverse threat model is driving the need for an integrated defense-in-depth strategy.

FIVE MOST COMMON CLOUD MISCONFIGURATIONS IN THE PAST 12 MONTHS



30%
Default or no password for access to management consoles

27%
Externally facing server workloads

25%
Overly permissive service accounts

25%
Overly permissive user accounts

23%
No external firewall and/or load balancer

FIVE MOST COMMON CLOUD-NATIVE SECURITY INCIDENTS EXPERIENCED IN THE LAST 12 MONTHS

27%
Malware that has moved laterally to cloud workloads

25%
Targeted penetration attacks

25%
"Zero-day" exploit(s) that took advantage of vulnerabilities

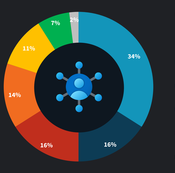
25%
Privileged account, secrets, or access keys via stolen credentials

23%
Attacks resulting in the loss of data due to the insecure APIs

IT Ops Is Front and Center

The shift from a bottom-up to a top-down approach is increasing the role of IT ops.

GROUP WITH PRIMARY RESPONSIBILITY OF SECURING CLOUD-NATIVE APPS AND INFRASTRUCTURE



PERSONNEL APPROACH TO SECURING CLOUD-NATIVE APPS AND INFRASTRUCTURE

We have different teams responsible for securing cloud-native applications, but we plan to merge these responsibilities.
55%

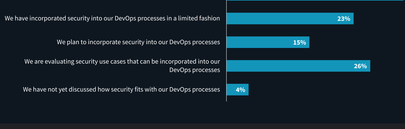
We have already centralized and unified security responsibility across all our applications and aspects of our environment.
20%

The Processes of Cloud-native Security

Automation via software development lifecycle integration spans the application lifecycle.

41%
say automating the introduction of controls and processes via integration with the software development lifecycle and CI/CD tools is a top priority.

INTEGRATION OF SECURITY PROCESSES AND CONTROLS VIA DEVOPS PROCESSES



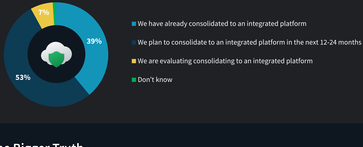
Enter Integrated Platform Modules

The requirement for breadth of coverage and depth of functionality is leading the consolidation of point tools into integrated platform modules.

PREFERRED SECURITY CONTROLS
FOR PROTECTING CLOUD-NATIVE APPLICATIONS AND INFRASTRUCTURE

> *"We prefer a consolidated set of controls based on an integrated platform with coverage across environments (i.e., public cloud vs. on-premises) and server workload types."*

PLANS FOR DEPLOYING AN INTEGRATED PLATFORM
TO PROTECT CLOUD-NATIVE APPLICATIONS AND INFRASTRUCTURE



The Bigger Truth

Cloud-native applications now serve critical front-, middle-, and back-office business operations. However, the rate at which cloud-native technologies methodologies have been adopted has outpaced organizational readiness to secure these environments.

For more data and analysis from this ESG research study, as well as specific recommendations for closing the cloud readiness gap, read the ESG Research Report, *The Maturation of Cloud-native Security: Securing Modern Applications and Infrastructure.*

LEARN MORE

Source: ESG Research Report, The Maturation of Cloud-native Security: Securing Modern Applications and Infrastructure, March 2021.
© 2021 TechTarget, Inc. All Rights Reserved.