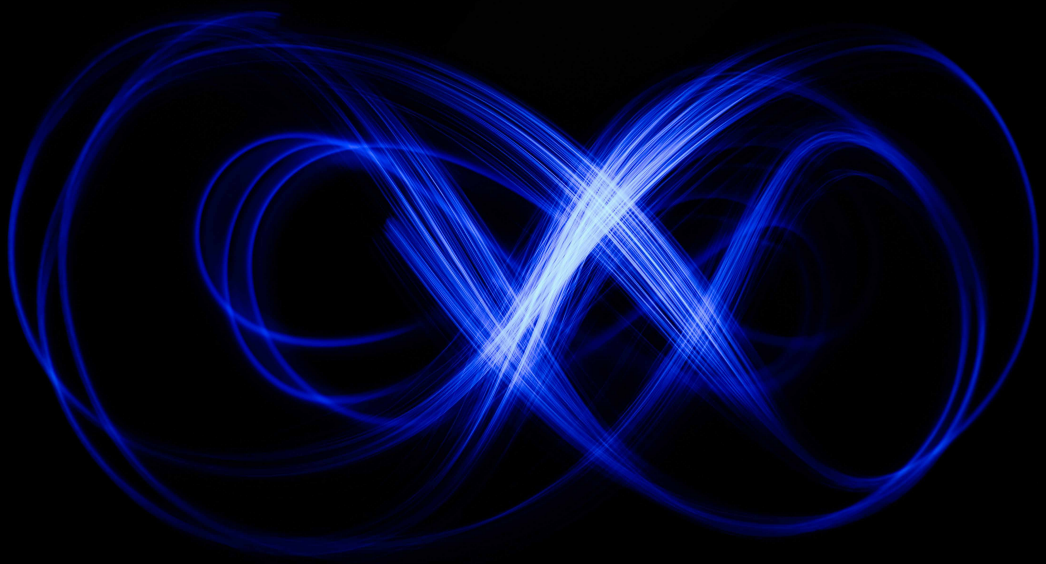
Synack



WHITE PAPER

Reducing Cloud Migration Risk

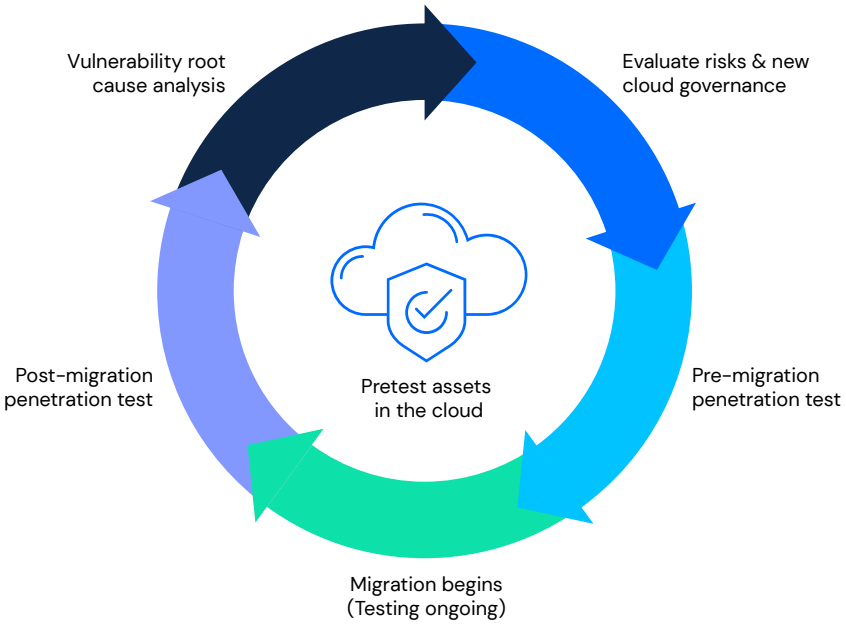
The value of penetration testing in the cloud

Table of Contents

OVERVIEW

Digital Transformation and Routine Pentesting for Cloud Assets

Cloud migration can feel like a delicate chemistry experiment where one misconfiguration leads to a blast – or in cloud security's case, a breach. With organizations facing increased risk due to ever-expanding attack surfaces, the remediation of vulnerabilities in hosts and applications prior/during/post migration has become a critical step to reducing exposures. In this paper, we'll address the state of application deployment in the cloud, the shared responsibility between providers and stakeholders in the cloud, and lay out a call for penetration testing apps and hosts in the cloud. For no matter where you are in your digital transformation journey, your security testing methodology for assets moved to the cloud should generally align with the diagram below.



Cutting through the fog around cloud security

In order for organizations to safely reap the benefits of shifting to cloud-native environments for hosting applications and infrastructure, they need to proactively test their cloud environments for potential security gaps. Practitioners are still struggling to wrap their heads around the shift to the cloud: O'Reilly's most recent Tech Trends report showed a 45% year-over-year increase in interest in the "cloud migration" topic even as more than 9 in 10 enterprises deploy cloud technologies.

For organizations further along in their cloud migration, cloud security is already synonymous with infrastructure security, app sec or even AI cybersecurity. Given the advantages in scalability and accessibility, it's not surprising that many of today's cutting-edge startups began in the cloud and keep their data and operations 100% in the cloud. Even air-gapped systems, required to be isolated from public networks and access, are embracing cloud technology for data transfer, secure updates, collaboration and processing of compute-intensive workloads.

Unfortunately, cloud computing has introduced a slew of cyber challenges that often take highly specialized skill sets or multiple security tools to address.

"The complexity of ingesting and managing data across these various security vendor solutions and the increasingly multi-cloud-based environments used to store and manage data and applications is outstripping the capabilities of even well-resourced sophisticated enterprises and governments," a White House advisory board noted in a recent report. The U.S. National Security Telecommunications Advisory Committee called the lack of trained personnel and technology needed to address these challenges "a serious barrier to effectively securing our nation's security future."

Meanwhile, attackers are leveling up their game with the onslaught of AI-enabled hacking tools.

With so many mission-critical assets and workloads making their way to the cloud as part of this digital transformation, there's never been a stronger case for regular cloud security testing to reduce the chance for exposure. Here's what you need to know about these seismic shifts and how to stay on top of them.

> *"The complexity of ingesting and managing data across these various security vendor solutions and the increasingly multi-cloud-based environments used to store and manage data and applications is outstripping the capabilities of even well-resourced sophisticated enterprises and governments."*
>
> WHITE HOUSE ADVISORY BOARD[1]

1. Draft NSTAC Report to the President.

Cloud Security 101

A shared responsibility

Let's start off with the basics. The cloud is any collection of servers that you access over the internet to process, manage and store data, rather than performing those functions locally. It could be a private cloud, a public cloud or a hybrid configuration with private and public components. You can also increase resiliency through multi-cloud deployment, using a strategy of combining multiple public cloud services from different providers.

In the cloud, you are trusting an external party to provide some level of compute resources. It's also important to consider who is expected to maintain each aspect of security around the cloud service model (or models) you choose. To help set proper expectations, the cloud shared responsibility model describes who is responsible for what, depending on the cloud provider and the type of service contracted (Infrastructure as a Service, Platform as a Service, Software as a Service).

Cloud service models

Infrastructure as a Service (IaaS)	*In IaaS, the cloud service provider (CSP) provides fundamental resources like processing, storage and networks, on top of which applications are built. The CSP is only responsible for the host infrastructure, physical security and a share of network flow. The organization is responsible for everything else, including the application and data, operating system and application configuration.*
Platform as a Service (PaaS)	*In PaaS the CSP also has responsibility for the network flow and for the operating system. Data storage and access controls can be shared. So the organization is only responsible for the application and application configuration.*
Software as a Service (SaaS)	*In SaaS the CSP provides, and is responsible for, everything you need to run the service. The organization is only responsible for app configuration.*

The liability of cloud configuration and APIs

Regardless of type of service, the organization will always be responsible for securely configuring the services being used and deciding which data to store in those services.

In addition to shared responsibility, cloud computing makes use of shared resources, so it presents a few security considerations in addition to those that already should be in place in a private system. Some of the most prominent risks are misconfigurations, insecure APIs and an increased attack surface.

While configuration management is essential for internal systems, it is even more critical in the cloud due to the increased risk of accidental misconfigurations. Configuration management establishes and maintains efficiency between hardware and software, specifying network configurations and user access and security controls. A misconfigured cloud system can lead to exposure of sensitive data, unauthorized access, and other vulnerabilities that can be exploited. The Open Web Application Security Project (OWASP) reported that 90% of applications it researched reported some misconfiguration. So it's essential for organizations to have personnel skilled in cloud configuration.

APIs enable components of a system to communicate with each other. Cloud security engineers are often tasked with understanding the dependencies among application components, including external services and third parties. Poorly secured APIs can be exploited, compromising the integrity and confidentiality of data. Conducting regular security testing and remediation is a vital step to knowing that such controls are being leveraged effectively.

Cloud security control types

Deterrent Controls *are deployed to keep malicious actors out of the system. They are like a warning system to would-be attackers.*

Preventative Controls *strengthen security posture by reducing or eliminating vulnerabilities that can be exploited.*

Detective Controls *are deployed to detect and respond to security threats and cyberattacks.*

Corrective Controls *are designed to limit the damage caused by a cyberattack.*

The State of Cloud App Development

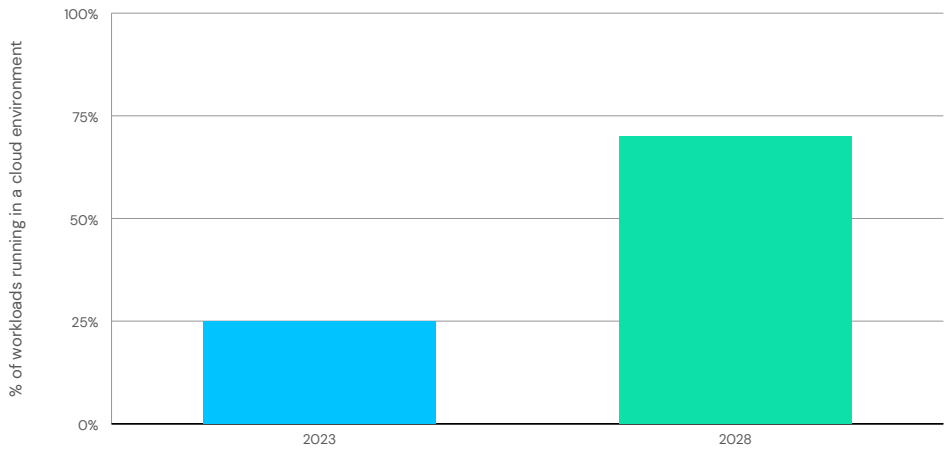
Accelerating the rate of change

Cloud app development is essential for organizations hoping to make the most of their cloud migration. It facilitates the creation of productivity-based applications and can allow for quick, cost-effective, low-code app development.

Here are some of the benefits of cloud-native app development.

- **Scalability:** Encapsulating applications using Kubernetes and containers helps maximize use of resources in response to fluctuating demand.
- **Speed and Agility:** Moving computations to the server side enhances speed and performance.
- **Cost Effectiveness:** Cloud app development can be less expensive since there is reduced need for onsite resources and capital expenditures.
- **Resilience:** Use of microservices helps minimize the potential impact of failures.
- **Continuous Improvement:** Using Continuous Integration/Continuous Delivery (CI/CD) techniques facilitates frequent and reliable incremental code changes.

More organizations, not just tech companies, have realized the benefits of cloud app development. According to a Gartner® Press Release, "By 2028, modernization efforts will culminate in 70% of workloads running in a cloud environment, up from 25% in 2023[1]."



Significant growth in cloud migrations is expected between 2023 and 2028.

Charts/graphics created by Synack based on a Gartner Press Release. Source: Gartner Press Release, Gartner IT Infrastructure, Operations & Cloud Strategies Conference 2023 London: Day 1 Highlights, November 20, 2023, https://www.gartner.com/en/newsroom/press-releases/2023-11-20-gartner-it-infrastructure-operations-and-cloud-strategies-conference-2023-london-day-1-highlights.

1. Gartner Press Release, Gartner IT Infrastructure, Operations & Cloud Strategies Conference 2023 London: Day 1 Highlights, November 20, 2023. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

Risks of migrating applications to the cloud

Migrating apps and workloads to the cloud presents some cloud-centric challenges. For example, legacy applications may not be compatible with cloud environments, resulting in the need to re-architect or redesign apps. Ensuring data integrity and consistency while moving large amounts of data to a cloud environment can be a complex process, requiring careful planning. Also of concern is the potential for vulnerability exposure during migration due to configuration differences between on-premises and cloud or from one cloud service provider to another. Successfully moving applications to the cloud can necessitate a change in business process and cultural mindset that often provokes resistance from on-prem teams. And moving apps to the cloud can require new skills, requiring the organization to invest in training or hiring of personnel to ensure that teams have the necessary expertise.

Risks associated with cloud app development are similar to those in traditional development, although the consequences can be greater. Using external resources and third parties greatly expands the organization's attack surface. Insecure APIs are a leading cause of data breaches, and inadequate encryption in transmission and in storage exposes data for potential exfiltration or corruption. Weak or insufficient Identity and Access Management (IAM) opens the door to unauthorized access. And failing to monitor and keep components up to date can leave known vulnerabilities open for exploitation.

The table below lays out a checklist for reducing these risks:

COMPLETE?	CLOUD MIGRATION RISK REDUCTION STEPS
✓	Map your attack surface – start with an inventory of your assets in the cloud
✓	Set up strong encryption for data at rest and in transmission
✓	Set security policies that employees understand and follow
✓	Regularly test the security of your apps, hosts & web APIs in the cloud
✓	Check to ensure that vulnerability patches have worked

Unpacking the Types of Cloud Security Testing

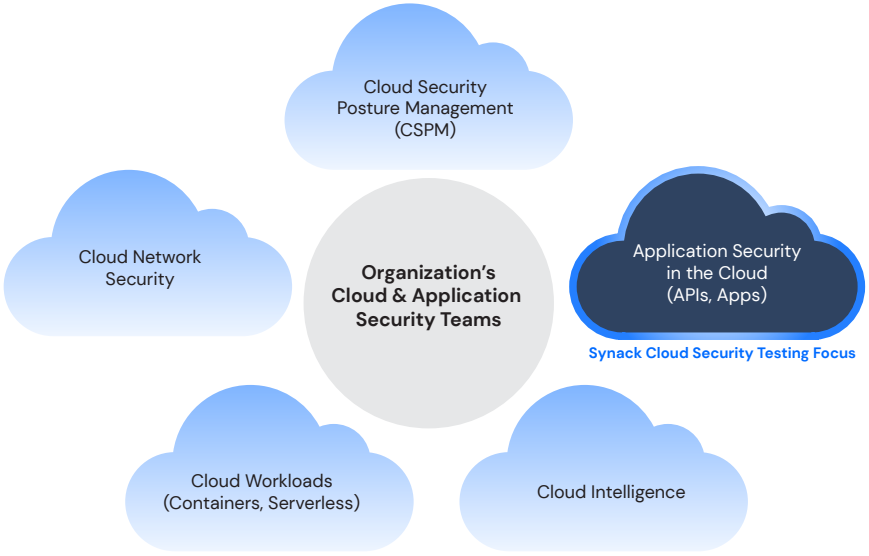
Organizations have a variety of options and needs when it comes to security testing in the cloud. These include testing to reach compliance requirements, testing configurations after migrating to GCP, AWS or Azure, and ensuring the integrity and security of applications moved to or built in a cloud-native paradigm.

CLOUD SECURITY TESTING TYPE	FOCUS AREA
Cloud Provider Infrastructure Testing	Providers test the security of their own underlying infrastructure.
Cloud Security Configuration Auditing	Security teams (or an external party or tool) test an organization to see if they have configured their cloud instances in accordance with ACLs, S3 Bucket and related best practices.
Identity and Access Management	Security teams validate policies controlling which users have access to specific resources, such as AWS IAM or Azure Active Directory.
Applications & Hosts in the Cloud	Cloud or Application security teams perform penetration testing or other methods to determine security of applications that are hosted in the cloud, as well as the security of Infrastructure in a Service (IaaS) paradigm.
Code Level Testing	Software deployed in the cloud may have accelerated release cycles. With code level testing, engineers examine source code for vulnerabilities that have been introduced.
Software as a Service (SaaS)	Organizations trust that SaaS providers are patching critical vulnerabilities and keeping their offerings secure (e.g. Zoom, Salesforce).

The Better Way to Pentest Your Assets in the Cloud

From issues with authorization permissions to web API glitches, there is ample potential for exploitable vulnerabilities to emerge – regardless of where organizations opt to host their infrastructure or build their applications. To ensure that apps and hosts held in the cloud have minimal chance for exposure, regular penetration testing and red teaming activities is a must.

The diagram below helps to visualize the cloud security environment as it relates to testing.



The Synack Platform's pivotal Cloud Security Testing Suite enables pentesting of apps, hosts and web APIs in the cloud. Members of the global Synack Red Team, a community of elite security researchers with deep experience uncovering cloud vulnerabilities, carry out the testing on in-scope external assets. To learn more about the Synack Cloud Security Test offering for customers migrating hosts, apps and APIs to the cloud, head to our solution brief.

Wherever your organization is on its digital transformation journey, it's likelier than not that cloud migration will be a major part of that journey. With the potential for misconfigured applications and poorly secured APIs in the cloud, a blend of continuous and on-demand testing strategies is key.

The Synack Platform enables hundreds of organizations across sectors with better security testing for speed, control and capacity, with comprehensive reporting that can integrate with your SIEM or SOAR for increased operational alignment. Reach out to Synack to learn more about how we can augment your cloud and application security teams' efforts.

Cheers to you and your team's continued cloud security education, and to your easier and less risky experience operating in the cloud.

© 2024 Synack Inc. All rights reserved. 2024-976