PRESCIENT SECURITY | CACILIAN

Benefits of Cloud Penetration Testing

What is Cloud Penetration Testing?

Cloud Penetration Testing is a security assessment that simulates cyber attacks on an organization's cloud infrastructure and applications, and focuses on the customer's responsibilities within the shared responsibility model of cloud security, testing elements like misconfigured services, weak access controls, insecure data storage, and vulnerable API endpoints. Cloud Penetration Testing enables organizations in the cloud to identify vulnerabilities before threat actors can exploit them. Read the key benefits of Cloud Penetration Testing below.

1 Compliance and Data Protection

- Cloud security checks demonstrate compliance and help organizations meet regulatory requirements such as GDPR, HIPAA, and SOC 2 by identifying and addressing security risks.
- Protects sensitive data and secures confidential customer and business data stored in the cloud by finding and eliminating weak points and leaks.
- As a customer of the cloud, though Cloud Service Providers (CSPs) are responsible for the security of the cloud (physical infrastructure, hardware, and software), customers are still responsible for security "in" the cloud (their data, applications, user access, and certain network configurations). The exact division of responsibility varies depending on the cloud service model (SaaS, PaaS, or IaaS). Cloud Penetration Testing enables organizations to ensure their portion of the Shared Responsibility Model is met and that their instances are secure.

2 Enhanced Security and Risk Mitigation

Misconfigured cloud settings and other potential vulnerabilities are **flagged** and **fixed early** before they're exploited by bad actors.

By simulating real-world attacks, cloud penetration testing reveals **actionable insights** based on **plausible threats**.

Consistent cloud penetration testing enables organizations to **stay up to date** with **cloud changes** and ensure their security is in line with their cloud infrastructure.

For example public, private, hybrid, or multi-cloud deployment models or Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or Software as a Service (SaaS) service models.

Validates security controls and provides independent validation that security controls are working as intended, giving **confidence** in the **effectiveness of security measures**.

3 Operational & Business Advantages

Reveals **how attackers infiltrate systems**, strengthening incident response and making it easier for organizations to prepare for and handle real-world incidents.

Increases **customer confidence**, **cost savings** through **breach prevention**, and **improves visibility of potential risk**, allowing organization to better prioritize security investments.

Ready to get started?
amer-nnl@prescientsecurity.com

Learn More

Cacilian is powered by Prescient Security,
a CREST Certified Penetration Testing Company