The Top 5 Cloud Security Risks: How Hacker-Powered Security Can Help

Jenny Kanevsky

Application Security

September 21st, 2021

Widespread digital transformation means increased cloud security risk. Learn how human intelligence—hacker-powered security—can help your organization defend against new attack vectors, mitigate risk, and improve cloud security.

Software Supply Chain Attacks Are On the Rise

Because open source component use is widespread in cloud-native application development, software supply chain attacks present a significant cloud risk. A 2020 Sonatype State of the Software Supply Chain Report showed a 430% increase in third-party software attacks, which will continue to grow. As cybercriminals adapt to changing attack surfaces, they find new software supply chain weaknesses to exploit.

Proving Compliance

Compliance is about more than passing audits and checking a box. While cloud providers maintain basic compliance standards and provide security capabilities and tools, your cloud network's security is also your organization's responsibility. According to a 2021 SANS Cloud Security Survey, many organizations want to include penetration testing in their cloud security strategies, supplementing current compliance practices.

Unsecured APIs

APIs streamline cloud computing processes by opening internal applications and data to third parties. They are fundamental to digital transformation initiatives and powering a new generation of cloud applications. However, unsecured APIs leave organizations open to attack. A Radware 2020-2021 State of Web Application Security Report found that 84% of organizations saw API manipulation attacks against web servers or applications.

Rapid Digital Transformation Application Risk

Over 31% of global security leaders surveyed in our 4th Annual Hacker-Powered Security Report report implementing digital transformation ahead of plan due to COVID-19. Digital transformation is now a common business strategy with significant benefits, including improved productivity, efficiency, cost savings, and more. But it also brings more substantial risk and new attack surfaces. According to a Verizon 2020 DBIR, 43% of all breaches last year involved web applications. IDC estimates that by 2023, over 500 million digital apps and services will be developed and deployed using cloud-native approaches.

Cloud Misconfiguration

A Check Point 2020 Cloud Security Report found that 68% of enterprises reported cloud misconfiguration as their biggest cloud security threat. Misconfiguration creates critical gaps in cloud security, leaving you vulnerable to destructive, costly attacks. In 2020, the HackerOne global hacker community reported an increase of 12,286% in misconfiguration vulnerabilities. Gartner predicts that through 2025, 99% of these security failures will be the customer's fault.

Mitigate Risk with Hacker-Powered Security

These risks are significant. But you can protect your organization, mitigate risk, and safeguard new attack surfaces with hacker-powered security. Fortify security teams, complement automation tools, and keep pace with today's rapid release cycles and attack threats. Hacker-powered security and human intelligence deliver continuous, comprehensive testing and vulnerability discovery throughout the cloud computing ecosystem.

Download The Top 5 Cloud Security Risks and How Hacker-Powered Security Can Help infographic here.