PRISMA CLOUD | UNIT 42

CLOUD THREAT REPORT

Volume 7: Navigating the Expanding Attack Surface

Executive Summary

Public clouds offer the speed, scalability, and security that on-premises data centers cannot match. In particular, their modern security features can help more effectively secure cloud workloads if implemented correctly. However, the fast evolution of cloud technology and growth of cloud workloads—as well as the complexity of managing hybrid and multicloud environments—cause many organizations to fall behind and inadvertently introduce security weaknesses into their environments. These gaps give adversaries significant opportunities to gain a foothold in the cloud.

Unit 42's *Cloud Threat Report* takes a comprehensive look at the current cloud security landscape using the large-scale data collected in 2022. We examine real breaches that impacted medium and large-size companies, detail the issues observed in thousands of multicloud environments, and analyze the impact of open-source software (OSS) vulnerabilities on the cloud.

Study Revelations

Cloud users repeatedly make the same mistakes. In most organizations' cloud environments, **5%** of the security rules trigger **80%** of the alerts. Prioritizing the remediation of these issues can maximize the return on security investments.

Security alerts commonly take days to resolve. On average, security teams take **145 hours** (approximately 6 days) to resolve a security alert. Well over half **(60%)** of organizations take longer than **four** days to resolve security issues.

Sensitive data in the cloud poses hidden risks. Sensitive data, such as personally identifiable information (PII), financial records, or intellectual property, are found in **66%** of storage buckets and **63%** of publicly exposed storage buckets. This sensitive data is at risk for both insider and external threats.

Leaked credentials in source code are pervasive across all organizations. The vast majority **(83%)** of organizations have hard-coded credentials in their source control management systems, and **85%** have hard-coded credentials in virtual machines' user data. Credential access continues to be a common tactic across all cloud threat actors, and is the approach attackers take to move laterally or vertically in every major cloud breach.

Multifactor authentication (MFA) is not enforced for cloud users. At least three-quarters **(76%)** of organizations don't enforce MFA for console users, and **58%** of organizations don't enforce MFA for root/admin users.

Attacks on software supply chains are on the rise. The prevalence of open-source usage makes securing the software supply chain difficult. More than 7,300 malicious OSS packages were discovered in 2022 across all major package manager registries according to the GitHub Advisory Database. The impact of these types of attacks is far-reaching.

Managing code dependencies is challenging. Just over half **(51%)** of codebases depend on more than **100** open-source packages. However, only **23%** of the packages are directly imported by the developers. More than three-quarters **(77%)** of the required packages and vulnerabilities are introduced by non-root packages, defined as the dependencies of the directly imported packages. For instance, a developer may import package A to a project, but package A depends on package B and package C. Packages B and C are considered non-root dependencies.

Unpatched vulnerabilities continue to be low-hanging fruit for attacks. Nearly two-thirds **(63%)** of the codebases in production have unpatched vulnerabilities rated High or Critical (CVSS >= 7.0), and **11%** of the hosts exposed in public clouds have High or Critical vulnerabilities.

Download the full report

