Unit 42 Cloud Threat Report, Volume 7.

Navigating the expanding attack surface

While cloud technology is not new, and many organizations have been on the cloud journey for years, cloud service providers continue evolving with new features and services.

The fast change and growth make it difficult for organizations to catch up, and, as a result, many inadvertently introduce security weaknesses into their environments.

In its annual Cloud Threat Report, Unit 42™ analyzed workloads in 210,000 cloud accounts across 1,300 different organizations and found:

- Threat actors are getting smarter and more powerful every day. They're learning from new security strategies and finding creative ways to work around them, exploiting hidden weak spots and using vulnerabilities to their advantage.
- MFA is not enforced for cloud users. 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 and the complexity of software dependency make securing the software supply chain difficult.
- Unpatched vulnerabilities continue to be low-hanging fruit for attacks. 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.

What we learned throughout our research is that threat actors have become masters at exploiting common oversights in cloud security.

Get the report to learn about the greatest risks to your cloud environment and how to manage them effectively. You'll also:

- Learn lessons from real cloud breach incidents.
- Get tips to stay ahead of cloud threat actors.
- Address the most common cloud security issues.
- Discover the impacts and risks of open-source software in the cloud.

Short on time? Read the Executive Summary.