

Unit 42 Cloud Security Assessment

Turn Cloud Complexity into Actionable Security Insights

Cloud Security Challenges

Securing cloud environments presents unique challenges for organizations today. Adversaries are now highly skilled in cloud-specific attacks, while the rapid pace of cloud change creates visibility gaps and misconfiguration risks. This dynamic environment, coupled with inherent complexity and excessive trust, makes cloud assets prime targets.

Threat Actors Are Faster and More Capable

Today's adversaries demonstrate a profound understanding of cloud environments. They leverage cloud-specific tools and APIs with precision and speed, executing targeted and scalable attacks. This expertise allows them to quickly exploit vulnerabilities and navigate cloud infrastructures effectively.

Cloud Environments Change Fast. Your Defenses Need to Keep Up

Cloud environments are inherently dynamic, with 45% of resources and configurations changing monthly.¹ This rapid pace of change, combined with the increasing complexity of cloud architectures, creates significant visibility gaps and opportunities for misconfigurations, leading to potential security weaknesses.

Complexity, Blind Spots, and Excessive Trust Make the Cloud a Prime Target

As cloud environments grow in scale and sophistication, limited visibility into assets and overly permissive access controls create the perfect storm for attackers. These gaps allow threats to linger undetected, with 80% of security exposures now originating in the cloud.² Reducing complexity, tightening access, and improving visibility are critical to stopping breaches before they start.

Misunderstanding the Shared Responsibility Model Leaves Critical Gaps

A common misconception persists regarding cloud security responsibilities. Organizations often underestimate their own obligations within the shared responsibility model, leading to critical blind spots and a failure to adequately protect their cloud environment. Ultimately, securing your data and cloud assets is your responsibility.

Unit 42 Cloud Security Assessment Benefits



Turn Cloud Threats into Actionable Intelligence

Translate the noise of evolving cloud risks into clear, prioritized guidance to inform strategic security decisions.



Secure Your Cloud Environment

Bolster your security posture, from Code to Cloud™, and enhance visibility, monitoring, and detection capabilities in your cloud ecosystem.



Accelerate Your Cloud Security Resilience

Drive down risks and build advanced cloud security capabilities with a threat-informed roadmap tailored to your business, technology, and team.

A Better Approach: Unit 42 Cloud Security Assessment

The Unit 42 Cloud Security Assessment proactively hunts the cloud threats and critical issues that matter most, delivering actionable intelligence and a clear path to remediation.

Our experts bring years of frontline experience, having witnessed firsthand the techniques used in successful cloud breaches. This unique perspective enables us to identify and prioritize the cloud threats and misconfigurations that pose the most significant risk to your organization. You get much more than a report of findings. We provide a strategic blueprint for building a robust and resilient cloud security program, aligning your defenses with the speed and scale of your cloud environment, from the earliest development stages to full deployment.

A Strong Foundation to Secure Cloud Data and Assets

Build Secure Cloud Apps	Adopt a "shift-left" approach, integrating security early and continuously throughout the application development process. Empower developers with the knowledge and tools to build secure code from the start.
Monitor and Harden Cloud Security	Implement processes for ongoing discovery and inventory of cloud assets and data. Continuously assess and rapidly remediate security misconfigurations and vulnerabilities to reduce the overall cloud attack surface.
Stop Cloud Attacks in Real Time	Protect the organization by stopping cloud application runtime attacks. Implement security controls that actively identify and prevent malicious activity targeting your cloud workloads, networks, and applications. Continuously fine-tune rules and context to support incident response.
Strengthen Cloud Detection and Response	Equip your security teams with the necessary tools, data, and skills to effectively detect, investigate, and respond to cloud-specific threats. Focus on building proactive threat hunting capabilities and continuously improving incident response processes.

About Unit 42

Unit 42® brings together our world-renowned threat researchers and hunters with an elite team of security consultants to create an intelligence-driven, response-ready organization. The Unit 42 Threat Intelligence team provides threat research that enables security teams to understand adversary intent and attribution while enhancing protections offered by our products and services to stop advanced attacks. As threats escalate, Unit 42 is available to advise customers on the latest risks, assess their readiness, and help them recover when the worst occurs. For the latest threat intel and research, please visit <https://unit42.paloaltonetworks.com>.

1. [Unit 42 Attack Surface Threat Report](#), September 14, 2023

2. Ibid



3000 Tannery Way
Santa Clara, CA 95054
Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087
www.paloaltonetworks.com

© 2025 Palo Alto Networks, Inc. A list of our trademarks in the United States and other jurisdictions can be found at <https://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies.
unit42_ds_unit-42-Cloud-Security-assessment_052325