cymulate

Why You Need Cloud Security Validation

4 Cloud Security Pitfalls and How to Solve Them

Cloud environments come with a unique set of challenges—they are complex, ephemeral and often multi-layered.

Because organizations often adopt multiple cloud infrastructure providers as they grow, cloud environments are a hotbed for cyber threat exposure, with a 75% increase in cloud intrusions reported over the past year.

Common cloud security technologies, like cloud security posture management (CSPM), are often not enough to prevent and detect cloud breaches on their own. Why? Cloud architectures are made up of multiple layers, each of which rely on different security controls for protection. For example, code, configuration, container deployment and runtime are all protected differently, even when secured by the same vendor. Separate controls require continuous validation to ensure they are operating as intended, and capable of detecting and preventing anomalous threat activity, gaps and exposures.

75%

increase in cloud intrusions reported over the past year

4 Reasons Why You Need Cloud Security Validation

Cloud technology is still evolving

The cloud market hasn't reached peak maturity, which means technologies like CSPM, Kubernetes security and cloud infrastructure entitlement management (CIEM) haven't been fully tested and operationalized. And best practices are still evolving as new features and services are added.

There is a cloud security skills gap

Factors such as rapid cloud adoption, the evolving threat landscape, automation and multi-cloud complexity have put a strain on security teams. There is a need for specially trained cloud security architects, and this demand is currently outpacing supply.

Everything in the cloud is configurable

Most cloud environments are provisioned and configured using infrastructure as code (IaC), meaning a single mistake in either a misconfigured container or workload, or faulty security control settings could weaken your cyber defenses and lead to risky gaps and exposures.

The scale of a cloud breach is huge

Auto-scaling in cloud environments increases the attack surface and the impact of a breach. Threat actors can use a single misconfiguration, gap or exposure to access and exploit your entire cloud environmen—and they can replicate novel attacks repeatedly in different cloud environments.

If you're not validating your cloud, you're not protecting.

Securing your cloud is not the same as securing your perimeter – the same methods, resources and technologies simply aren't enough to stop threat actors from accessing and exploiting your most valuable resources. You need a comprehensive exposure validation platform that includes advanced, automatic validation techniques that protect each layer of your cloud architecture.

Here's what you can achieve with cloud security validation:

1. **Confidence that sensitive data stored in the cloud is protected.**
   The cloud contains an organization's most critical – often sensitive or confidential – data. Regular validation tests the effectiveness of security controls and configurations to make sure that your data stays safe and out of reach from attackers.
2. **Prove that you can detect the latest cloud threat activity.**
   Threat actors can often go undetected in your cloud environment for weeks – or even months – at a time as they look for systems, applications, and high-value data and resources. Cloud security validation tests the detection and response capabilities of your security operations to ensure they quickly detect when a threat actor is operating in stealth mode across your cloud environment.
3. **Identify weaknesses and gaps in cloud security.**
   Continuous testing and validation against the latest tactics and techniques used by threat actors to exploit cloud platforms identifies the vulnerabilities, weaknesses and gaps in your cloud security controls.
4. **Optimize cloud security remediation.**
   Validation can help you identify and prioritize the most impactful vulnerabilities, weaknesses and gaps in your cloud so you can mitigate them quickly.
5. **Ensure operational resilience in your cloud.**
   Cloud platforms are used to host critical IT assets and run critical workloads for your business operations. Validating your cloud security controls on a frequent basis – ideally, every week – ensures that these critical systems and data are resilient to the latest cyber attacks.

About Cymulate

Cymulate, the leader in security and exposure validation, provides the single source of truth for threat exposure and the actions required to close security gaps before attackers can exploit them. More than 1,000 customers worldwide rely on the Cymulate platform to baseline their security posture and strengthen cyber resilience with continuous discovery, validation, prioritization, and guided remediation of security weaknesses. Cymulate automates advanced offensive security testing to validate controls, threats, and attack paths. As an open platform, Cymulate integrates with existing security and IT infrastructure and drives the workflows of the exposure management process. For more information, visit www.cymulate.com.

Get a Demo