PICUS
THE COMPLETE
SECURITY VALIDATION
PLATFORM

DATASHEET

CLOUD SECURITY VALIDATION

Optimize your cloud security with automated cloud assessment and attack attack simulation

Migration of workloads to the cloud continues to increase the challenge of defending against the latest cyber threats.

Picus Cloud Security Validation (CSV) helps security teams keep pace with cloud security posture management by identifying common misconfigurations and overly permissive IAM policies - the two primary causes of cloud data breaches.

ADDRESS CLOUD SECURITY ISSUES BEFORE THEY LEAD TO INCIDENTS

Due to the rapid pace of digital transformation, the increasing complexity of cloud environments, and human error, critical security gaps that could enable attackers to compromise your cloud services can arise daily.

Picus Cloud Security Validation helps you to proactively identify and address exposures by:

• Audit essential cloud services

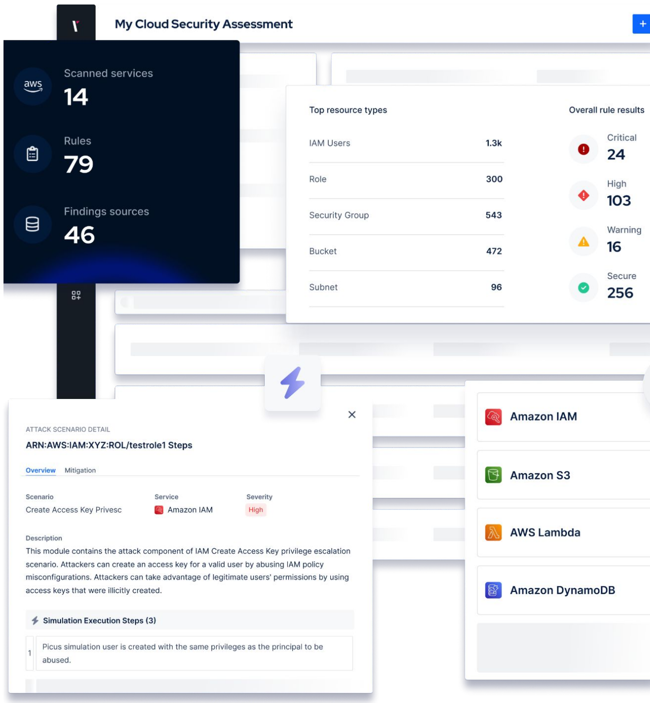
Identify critical misconfigurations that attackers could exploit, such as excessive privileges, unused resources, and cryptographic failures.

• Simulate privilege escalation scenarios

Use real-world cloud-specific attacks to uncover excessive user permissions that could enable attackers to compromise critical services.

aws Azure

Through 2025, at least 99% of cloud security failures will be the customer's fault, mainly in the form of cloud resource misconfiguration.
-Gartner


My Cloud Security Assessment

Scanned services 14
Rules 79
Findings sources 46

Top resource types	
IAM Users	1.3k
Role	300
Security Group	543
Bucket	472
Subnet	96

Overall rule results	
Critical	24
High	103
Warning	16
Secure	256

ATTACK SCENARIO DETAIL
ARN:AWS:IAM:XYZ:ROL/testrole1 Steps

Overview Mitigation

Scenario	Service	Severity
Create Access Key Privesc	Amazon IAM	High

Description
This module contains the attack component of IAM Create Access Key privilege escalation scenario. Attackers can create an access key for a valid user by abusing IAM policy misconfigurations. Attackers can take advantage of legitimate users' permissions by using access keys that were illicitly created.

Simulation Execution Steps (3)

1 Picus simulation user is created with the same privileges as the principal to be abused.

Amazon IAM
Amazon S3
AWS Lambda
Amazon DynamoDB

MITIGATE GAPS WITH ACTIONABLE INSIGHTS

Picus Cloud Security Validation doesn't just identify issues. It also provides the insights and recommendations you need to understand their severity and respond to risks quickly.

Built-in dashboards enable you to track improvements to your cloud security posture and prove your maturity.

Extend security validation to the cloud with The Picus Platform

REQUEST A DEMO

www.picussecurity.com