algosec

Secure application connectivity.
Anywhere.

Business-driven
security management



An AlgoSec Horizon Platform eBook

6 Must-Dos to Secure Hybrid, Multicloud & AI-Ready Cloud Environments

01

Make identity the new security perimeter

02

Segment by workload, not by network location

03

Build one exposure map across hybrid and multicloud

04

Automate cloud posture and policy hygiene

05

Put security guardrails into every cloud change

06

Protect data, keys, AI workloads, and third-party access

Introduction

Hybrid cloud security is no longer just a firewall problem. Modern risk spans identities, workloads, APIs, SaaS apps, cloud configurations, data, AI services, and CI/CD pipelines. Use these six practices to reduce exposure before it becomes an incident.

82% of organizations maintain some form of hybrid infrastructure, 63% use more than one cloud provider, and 59% identify insecure identities and riskypermissions as the top cloud infrastructure risk. For AI workloads, 34% of organizations in the same CSA / survey reported an AI-related breach.

Here are six practics to adopt to help prevent this.



01
Make identity the new security perimeter

02
Segment by workload, not by network location

03
Build one exposure map across hybrid and multicloud

04
Automate cloud posture and policy hygiene

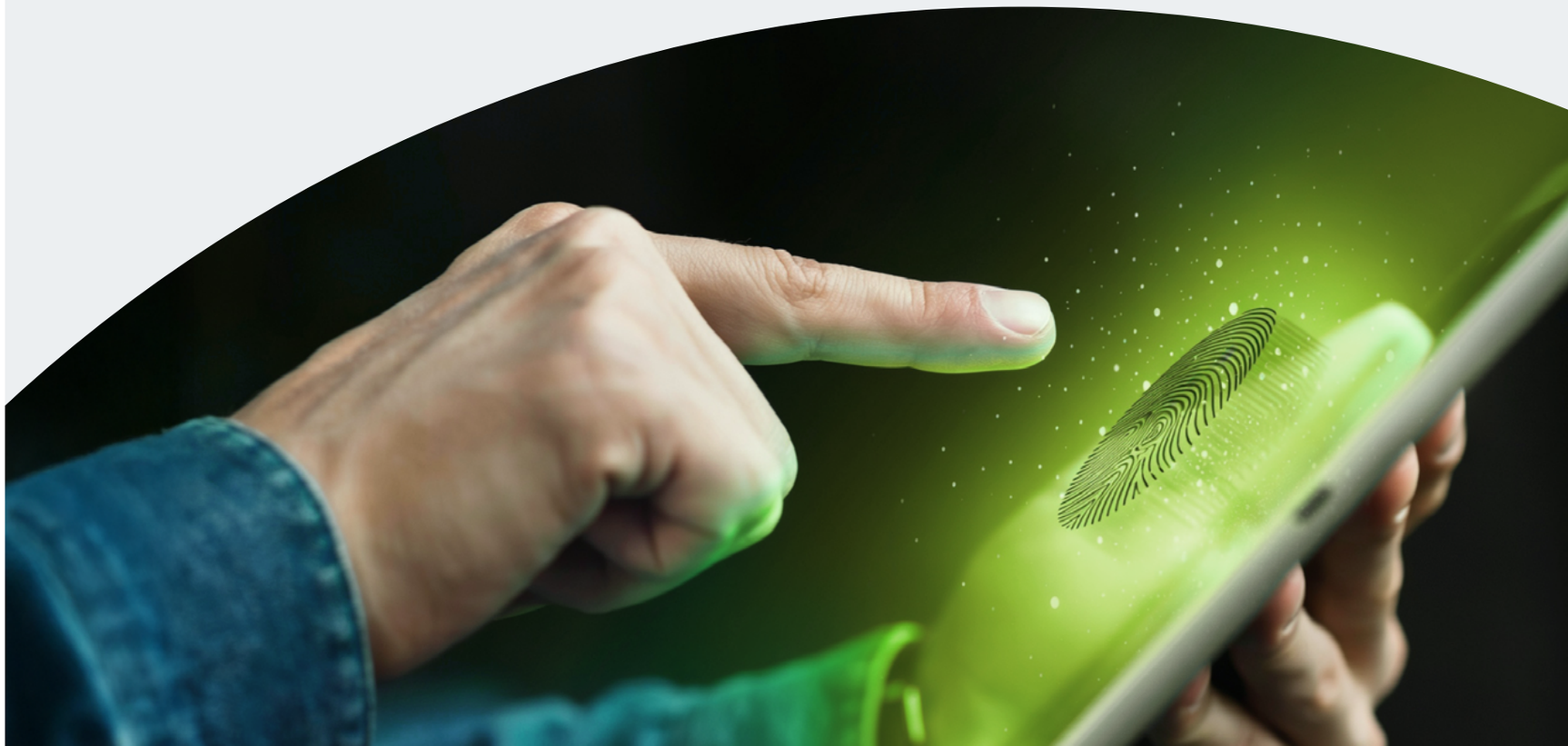
05
Put security guardrails into every cloud change

06
Protect data, keys, AI workloads, and third-party access

Make identity the new security perimeter

Inventory every human, service, workload, and third-party identity. Enforce phishing-resistant MFA for privileged users, least privilege, just-in-time access, short-lived credentials, and continuous permission review. Treat exposed keys, stale accounts, and over-permissioned identities as critical cloud risks.

CISA and NSA emphasize that IAM is central to cloud security and that cloud access controls are often misconfigured in ways that expose resources.



01

Make identity the new security perimeter

02

Segment by workload, not by network location

03

Build one exposure map across hybrid and multicloud

04

Automate cloud posture and policy hygiene

05

Put security guardrails into every cloud change

06

Protect data, keys, AI workloads, and third-party access

Segment by workload, not by network location

Move beyond perimeter-only protection. Use Zero Trust segmentation, identity-aware access, tags and labels, micro-segmentation, private connectivity, and encrypted traffic between users, apps, data, and cloud services. NGFWs still have a role, but they should be part of a broader Zero Trust control fabric rather than the headline control.

NSA and CISA recommend tying identity into network requests, implementing end-to-end encryption, and micro-segmenting cloud environments.



01

Make identity the new security perimeter

02

Segment by workload, not by network location

03

Build one exposure map across hybrid and multicloud

04

Automate cloud posture and policy hygiene

05

Put security guardrails into every cloud change

06

Protect data, keys, AI workloads, and third-party access

Build one exposure map across hybrid and multicloud

You cannot protect what you cannot see. Maintain a unified view of internet-facing assets, cloud accounts, Kubernetes clusters, SaaS integrations, data stores, APIs, vulnerabilities, firewall rules, cloud security groups, identities, and on-prem-to-cloud paths. Prioritize the attack paths that combine exposure, sensitive data, exploitable vulnerabilities, and excessive permissions.

CSA's current cloud threat list includes limited visibility/observability, misconfiguration, IAM, insecure APIs, and third-party resources among the top cloud risks.



01

Make identity the new security perimeter

02

Segment by workload, not by network location

03

Build one exposure map across hybrid and multicloud

04

Automate cloud posture and policy hygiene

05

Put security guardrails into every cloud change

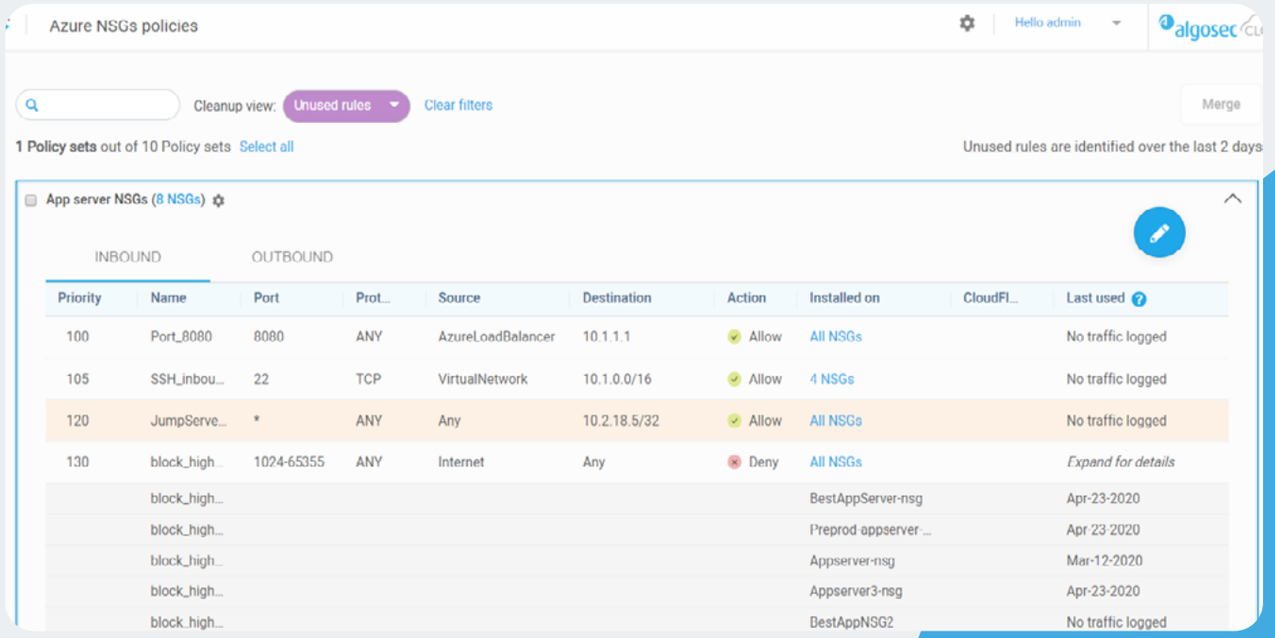
06

Protect data, keys, AI workloads, and third-party access

Automate cloud posture and policy hygiene

Security groups, firewall rules, IAM policies, routes, storage permissions, and exceptions change constantly. Continuously detect drift, stale rules, public exposure, open admin ports, unused permissions, risky shadow access, and policy conflicts. Tie every finding to an owner, business application, and approved remediation path.

CISA and NSA recommend policy-as-code, periodic policy review, least privilege, and frequent drift checks for cloud access policies.



01

Make identity the new security perimeter

02

Segment by workload, not by network location

03

Build one exposure map across hybrid and multicloud

04

Automate cloud posture and policy hygiene

05

Put security guardrails into every cloud change

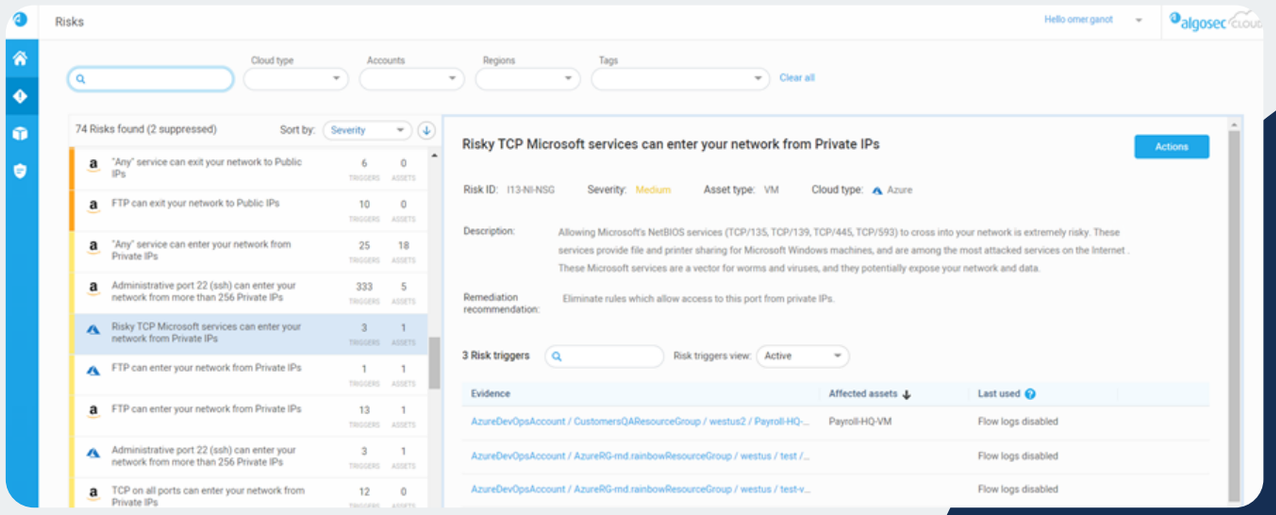
06

Protect data, keys, AI workloads, and third-party access

Put security guardrails into every cloud change

Shift from “review after deployment” to “prevent before merge.” Scan IaC, containers, code, dependencies, secrets, APIs, and cloud permissions before changes reach production. Use approved templates, pre-deployment risk checks, automated remediation guidance, and CI/CD gates that block high-risk changes.

NIST’s Secure Software Development Framework recommends integrating secure development practices into the SDLC to reduce vulnerabilities and address root causes.



01

Make identity the new security perimeter

02

Segment by workload, not by network location

03

Build one exposure map across hybrid and multicloud

04

Automate cloud posture and policy hygiene

05

Put security guardrails into every cloud change

06

Protect data, keys, AI workloads, and third-party access

Protect data, keys, AI workloads, and third-party access

Classify sensitive data, limit public exposure, encrypt data in transit and at rest, manage keys intentionally, maintain immutable backups, and monitor abnormal data movement. Extend the same governance to AI workloads, model access, prompts, training data, SaaS integrations, OAuth apps, MSPs, and third-party connections.

NSA's cloud mitigation guidance highlights key management, segmentation, encryption, data protection, and recovery planning; NIST's Generative AI Profile provides a framework for managing unique AI risks across design, use, and evaluation.



01

Make identity the new security perimeter

02

Segment by workload, not by network location

03

Build one exposure map across hybrid and multicloud

04

Automate cloud posture and policy hygiene

05

Put security guardrails into every cloud change

06

Protect data, keys, AI workloads, and third-party access

algosec

Ready to reduce hybrid cloud risk before the next change goes live?

Get a hybrid cloud exposure assessment ›

