CloudFlow

Cloud security policy and configuration management made simple

As organizations adopt cloud strategies and migrate applications to take advantage of cloud economies of scale, they face new levels of complexity and risk to their security posture. Security controls and network architectures from leading cloud vendors are distinct from each other and fundamentally different from those found in on-premise data centers – and not as stringent. Customers of these cloud services often do not know how to use them securely.

AlgoSec CloudFlow enables effective management of the security control layers across the hybrid and multi-cloud estate.

Cloud security main challenges

IT and Security staff find it difficult to create and maintain security in the cloud due to:

- **Complexity** of multiple layers of security controls including
  - Cloud providers' built-in configurations that impact security posture, such as IAM permissions, encryption state, security groups, public/private permissions, asset types like databases, storage and accounts, as well as configuration types like deployment location, networks ACLs, and more. Misconfigurations can result in security risks across various assets, including IaaS, PaaS and accounts.
  - Security products by cloud providers with many different mechanisms and operational rules and techniques (e.g., Azure Firewall).
  - Security products by independent security vendors (e.g., Next Generation Firewalls by Check Point and Palo Alto Networks).
- **Multiple public clouds** from AWS and Azure, along with private clouds and on-premise networks. Security professionals are challenged by the need to understand the differences in the technologies while managing them separately using multiple consoles and diverse tools.
- **Multiple stakeholders** managing the deployment in the cloud. Unlike on-prem networks where policies are typically managed by security teams, in the cloud, other stakeholders (application developers, DevOps, cloud teams) manage changes to cloud configurations and security rules, challenging consistency and control, and increasing the risk of misconfigurations.

All cloud security under one unified umbrella

AlgoSec *CloudFlow* enables effective security management of the various security control layers across the multi-cloud estate. CloudFlow's central management provides instant visibility, risk assessment and compliance analysis, enabling enforcement of company and regulatory policies, and proactive detection of misconfigurations.

Key Business Benefits

- Enhanced visibility across the entire hybrid and multi-cloud estate
- Improved cloud-security posture to avoid breaches
- Automatic compliance assurance with constant audit-readiness
- Secure change management at the speed of cloud deployment
- Reduced manual labor, errors and associated risks and costs

CloudFlow Advantages

- Unified view of the entire network, hybrid and multi-cloud estates from a single console
- Management of the complexity of the multiple layers of cloud security controls
- Automatic detection of risks and recommended best practices
- Avoidance of false alarms – risk analysis takes into consideration all security constructs
- Business-driven security

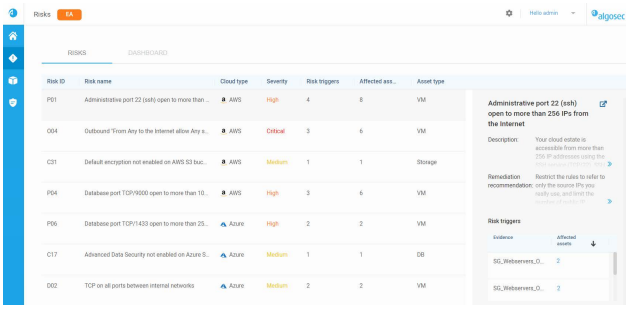
Manage the entire hybrid and multi-cloud security environment

When used in conjunction with AlgoSec's Firewall Analyzer and FireFlow, customers benefit from a hybrid approach, **spanning** on-premise**,** SDN and legacy network security.

Continuous Visibility. Always know about all the assets that need protection and the multiple security constructs and configurations protecting them. Monitor changes to the cloud configuration and the potential risk of each change.

Risk management and compliance. Enforce company and regulatory policies while verifying adherence to best practices. Proactively detect misconfigurations in access, permissions and other configurations to protect cloud assets, including cloud instances, storage, databases and more.

Automated central management of security policies. Manage network security controls (security groups, access lists, etc.) in one system across multiple clouds, accounts, regions and VPC/VNETs. Leverage a uniform network model and change-management framework that covers the hybrid and multi-cloud environment.

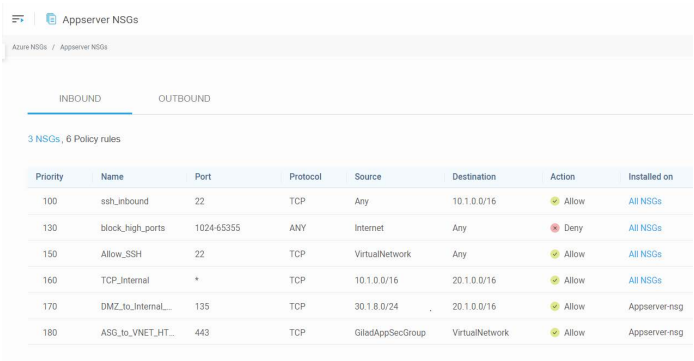


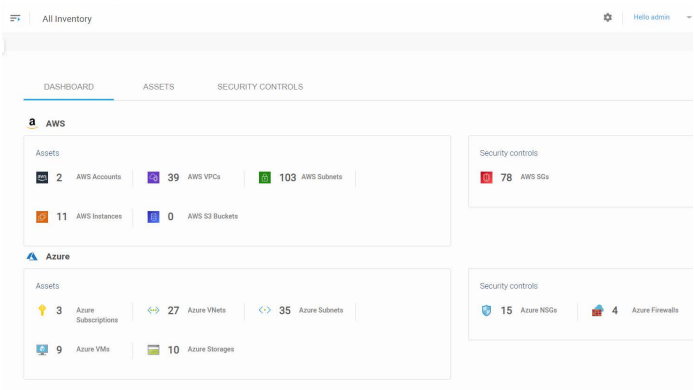
Ensure consistent security posture across the multi-cloud estate

CloudFlow provides an at-a-glance view of the multi-cloud security posture. The *dashboard* and *actionable risk list* feature clear and easy navigation, and can be filtered any way you like.

Quick deployment

CloudFlow is an agentless SaaS solution and is easy to deploy in minutes. It offers immediate ROI and significant improvements.





Comprehensive and Unified Security for Heterogeneous Environments

AlgoSec seamlessly integrates with all leading brands of traditional and next-generation firewalls and cloud security controls as well as routers, load balancers, web proxies and SIEM solutions, to deliver unified security policy management across any hybrid-cloud, multi-cloud, SDN and on-premise network. Additional devices can be added via the AlgoSec Extension Framework.

algosec CLOUD

AlgoSec.com