algosec

WHITE PAPER

Optimizing security and efficiency in the cloud

How AlgoSec Cloud Enterprise (ACE) delivers measurable ROI

ACE | Cloud connectivity without compromise

CONTENTS

algosec

Executive summary

The problem

Cloud network security managers face a tough job. You're dealing with multiple cloud setups, trying to keep security consistent, struggling to see the big picture, and spending way too much time on manual security tasks. It's like trying to keep all the plates spinning at once!

Here's the breakdown:

Lack of centralized view

You're using different tools, so you can't really see how everything connects. It's like having puzzle pieces that don't fit.

Messy change management

Manual processes slow down updates and deployments. This makes you less responsive and hurts the business.

Higher security risk

Manual work leads to mistakes and inconsistent security, making you more vulnerable to attacks.

Inefficient operations

You're wasting time and resources on manual policy management. Your team is overworked.

Cloud migration headaches

Moving to the cloud is hard enough, but keeping security consistent across different environments adds another layer of difficulty.

algosec

The solution

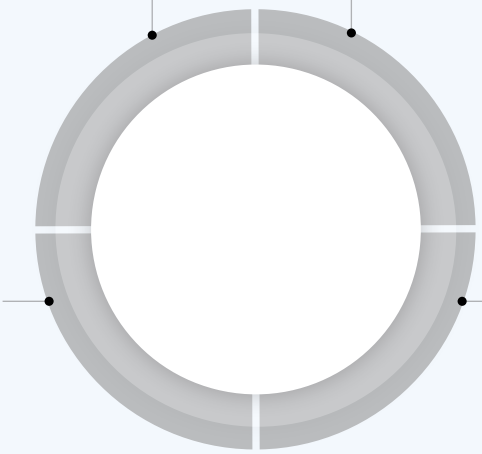
To get a handle on cloud security, you need a smart solution that gives you:

One clear view

A single place to see all your application connections, dependencies, and security policies across your hybrid setup.

Smooth processes

Easy policy changes that fit into your DevOps workflows, cutting down on manual approvals and speeding up releases.



Smart risk analysis

Tools that help you spot potential problems and stay compliant.

Self-service options

Let application owners and developers make their own secure policy changes, so your security team can focus on bigger things.

The benefits

This kind of solution will help you:

Improve security

Proactively reduce risk and enforce policies.

Boost efficiency

Streamline your security workflows.

Get real ROI

Save money on cloud security operations and reduce the risk of costly breaches.

algosec

The cloud security manager's challenge

Being a cloud network security manager is tough. You're always dealing with new threats and complex environments. Since most companies (over 79%) use more than one cloud service, managing security across these complex setups is leading to more mistakes.

The growing complexity

Hybrid and multi-cloud setups have increased the number of ways you can be attacked. It's like defending a castle with more and more entrances. With most companies using multiple cloud providers, misconfigurations are a big problem. You have to manage security across AWS, Azure, GCP, and different firewalls, all with their own quirks.

Cloud environments change constantly, making it hard to keep policies consistent. On top of that, you have to meet strict compliance rules (like PCI DSS and HIPAA). And to make matters worse, cloud security breaches are on the rise. You need a system that gives you a unified view and control, so you can enforce consistent policies and automatically see how applications connect.

The operational pressure

Manual security processes just don't work in the cloud. It's like trying to build a skyscraper with hand tools. Bottlenecks in change management, slow approvals, and the risk of mistakes hold you back. Making things worse, cloud security problems are happening more often. Almost half (45%) of companies reported a security issue in the cloud last year, according to IBM. Security changes can cause downtime, which costs money.

You need to respond quickly to incidents, but manual processes slow you down. And data breaches are getting more expensive. When a data breach happens in the cloud, it hits companies hard, costing them nearly $5 million on average (IBM).

You need a solution that automates security policy changes and monitors compliance across your hybrid environment. It should also help you check for risks and customize security to fit your needs. By focusing on application security, you can move away from old-fashioned perimeter security, which doesn't work well in the cloud.

Key challenges

Lack of a central view

Messy change management

Increased security risk

Inefficient operations

Cloud migration complexity

You need a solution to automate and orchestrate cloud network security, giving you the control and visibility you need.

algosec

AlgoSec Cloud Enterprise (ACE):
Empowering cloud network security managers

What ACE does

AlgoSec's application-centric solution changes how you manage security policies by:

Giving you a clear view

See your application connectivity, dependencies, and security policies across your hybrid environment.

Analyzing risk

Proactively identify potential problems and ensure compliance with advanced application modeling (AppViz).

Making things run smoothly

Integrate policy changes into your DevOps workflows, reducing manual approvals and speeding up releases.releases.

Providing self-service options

Let application owners and developers make secure policy changes, freeing up your security team.

Key features

Unified cloud security policy management

Control security groups, network ACLs, and virtual firewalls across AWS, Azure, and GCP.

Streamlined cloud change management workflows

Make security changes easily, reducing manual work and errors.

Proactive cloud risk assessment and compliance reporting

Find security risks and generate compliance reports.

Real-time cloud application connectivity management

See and manage application connectivity, ensuring secure and reliable application delivery.

Consistent security across hybrid and multi-cloud

Enforce consistent security policies across all your environments.

How ACE works

ACE integrates with cloud providers to give you a central platform for managing cloud network security.

Cloud-native integration

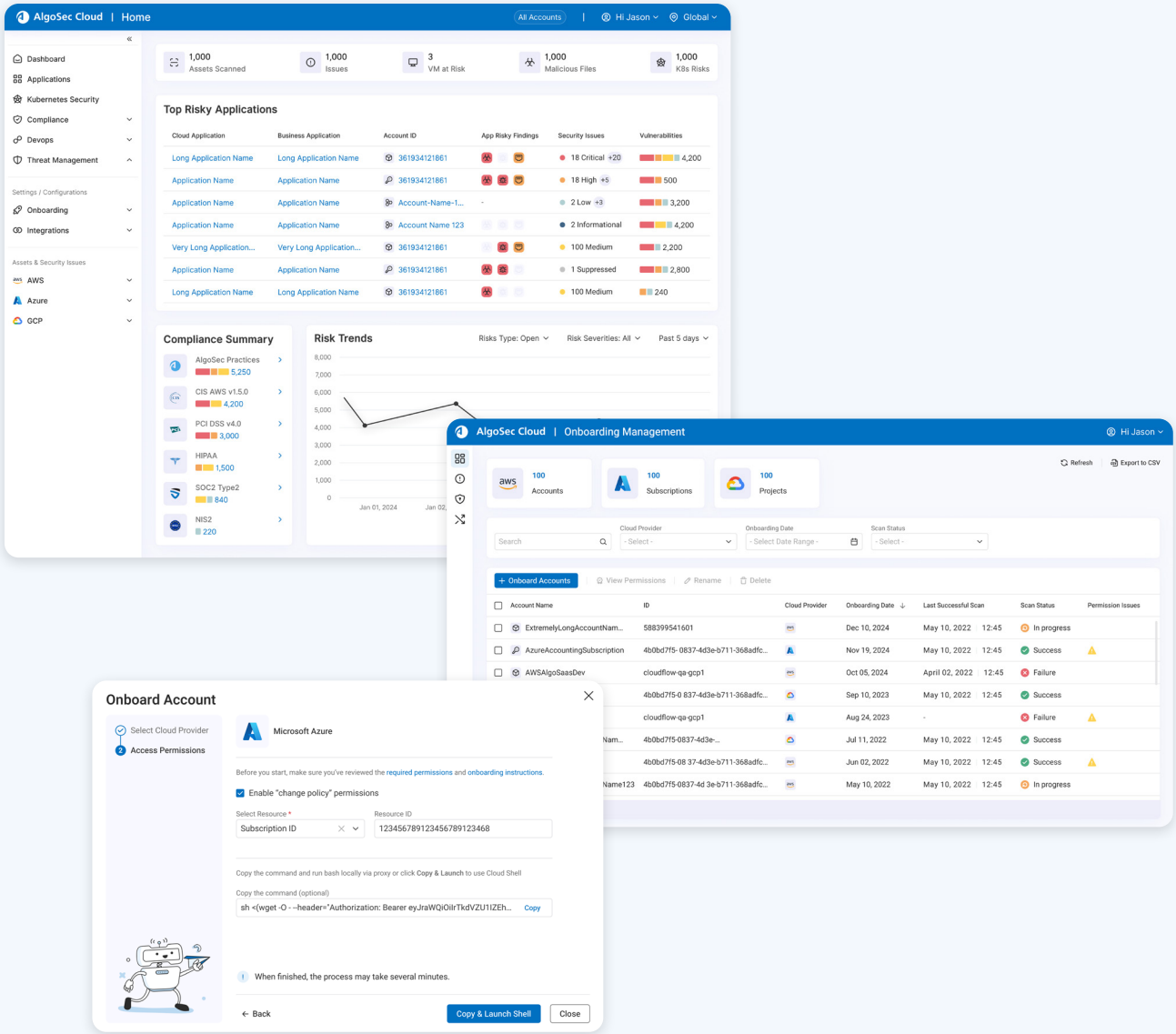
Uses cloud services to streamline security changes.

Visualized cloud security

See your cloud security policies and application connectivity clearly.

Continuous cloud risk analysis

Regularly check for vulnerabilities and compliance gaps.



Boosting your cloud security

ACE helps you improve your cloud security by reducing risks and ensuring compliance.

Proactive risk reduction

Find and fix vulnerabilities

Detect problems in cloud security configurations, like overly open security groups.

Enforce consistent policies

Make sure security policies are applied consistently across your cloud environments.

Reduce your attack surface

Use segmentation and access controls to limit the impact of breaches

Integrate threat intelligence

ACE includes information about new threats, helping you stay ahead of the game.

Simplified compliance

Automated reporting and auditing

Generate compliance reports automatically.

Use best practices

Utilize pre-built compliance templates for cloud security best practices and industry regulations.

Maintain an audit trail

Keep records of cloud security changes to prove compliance..

Case Study: Finance Industry

Company: Global financial services company

Challenge: Migrated banking apps to AWS and Azure. Manual firewall management was slow and risky. They struggled to comply with PCI DSS.

Solution: ACE automated security policy management. ACE provided visibility into application connectivity, streamlined change workflows, and ensured PCI DSS compliance.

Results:

- 80% faster security policy changes
- 65% fewer security misconfigurations
- 50% faster PCI DSS audit preparation
- 40% faster application deployment

Case Study: Retail Industry

Company: Retailer

Challenge: This retailer processes a high volume of transactions and needs to strictly adhere to PCI DSS (Payment Card Industry Data Security Standard) requirements in their AWS environment. Their manual firewall rules were becoming complex and difficult to manage, increasing the risk of misconfigurations that could lead to a data breach and significant fines. Auditing their security controls for PCI DSS compliance was also a time-consuming and error-prone process.

Solution: They implemented ACE to automate and centralize the management of their network security policies in AWS. ACE provided a clear view of their application connectivity and helped them define and enforce granular security rules specifically aligned with PCI DSS requirements, such as restricting traffic to cardholder data environments. Automated change management workflows ensured that all security updates were implemented accurately and quickly. ACE also streamlined PCI DSS audit preparation by automatically generating compliance reports and demonstrating adherence to relevant controls.

Results:

- 85% reduction in time spent managing PCI DSS related firewall rules.
- 98% reduction in potential PCI DSS violations related to network segmentation and access control.
- 70% faster preparation time for PCI DSS audits.
- 40% improvement in the speed of deploying new e-commerce features securely.

Making your team more efficient

ACE streamlines cloud security operations, making your team more efficient.

Cloud security change management

Streamlined change workflows

Simplify the entire security change process.

Reduced manual effort

Eliminate manual tasks, freeing up your team.

Faster deployments

Deploy applications faster by automating security changes.

Workflow examples

Security group review workflow

- Regularly review security group rules to remove unnecessary ones.
- Automatically generate reports on potential risks.
- Send notifications to security teams for immediate action.

Automated compliance report generation

- Automatically collect compliance data.
- Generate reports for standards like PCI DSS and HIPAA.
- Schedule automated delivery of reports.

Optimized cloud network operations

Deep visibility and control

See cloud security policies and application connectivity.

Minimized downtime

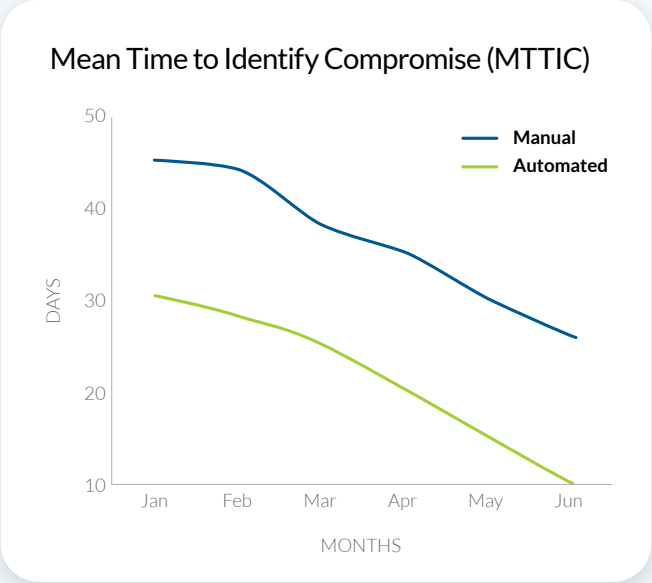
Prevent downtime with accurate security changes.

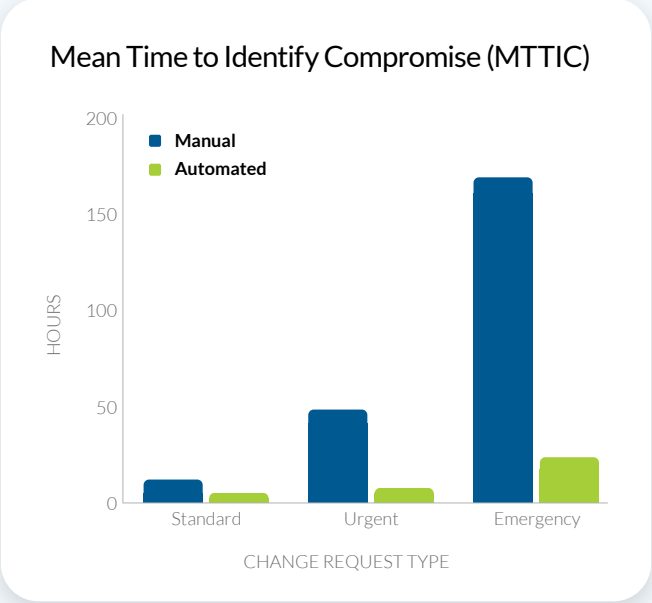
Cloud troubleshooting

Quickly identify and fix security issues.

Metrics and KPIs

To measure efficiency, track these:





Mean time to implement security changes (MTTIC)

How long it takes to make changes.

Number of manual security change requests

How much manual work is still needed.

Rate of successfully implemented security changes

How often changes are made without errors.

Mean time to remediate cloud security incidents (MTTR)

How long it takes to fix incidents.

Number of cloud security-related downtime incident

How often security issues cause downtime.

Compliance audit preparation time

How long it takes to prepare for audits.

Percentage of security policy exceptions

How often policies are bypassed.

Number of cloud security policy misconfigurations detected

How many errors are found.

Best practices

- Create clear workflows that align with your security policies.
- Implement policy management gradually.
- Regularly review and update policies.
- Train your team on ACE.
- Analyze metrics to find ways to improve.

Getting real ROI

AlgoSec ACE helps you turn cloud security into a strategic asset by saving you money and increasing productivity.

Cost savings

Reduce cloud operational expenses

Automate tasks to free up your team and reduce reliance on consultants.

Areas of saving: Overtime costs, consultant fees, training costs.

Minimize risk of costly cloud breaches

Prevent financial losses, fines, and reputational damage.

Areas of risk reduction: Regulatory fines, data loss costs, brand damage.

Optimize cloud resource utilization

Use resources efficiently by optimizing policies.

Areas of optimization: Unnecessary cloud resource consumption, security group rules, tool usage.

Increased Productivity

Faster cloud security response times

Respond to threats quickly with automated incident response.

Response time improvements: Mean Time to Resolution (MTTR), faster alerts, better containment.

Improve cloud application availability

Deploy security changes without disrupting applications.

Cloud application improvements: Reduced downtime, better service level agreements (SLAs).

Reduce time spent on manual cloud tasks

Free up your team from manual tasks to focus on strategic work.

Time teduction savings: Compliance reporting, security policy updates, vulnerability assessments.

Calculating ROI

Framework: Use the AlgoSec Cloud Enterprise (ACE) ROI calculator.

Metrics: Focus on time saved per change, compliance audit time reduction, cloud breach cost avoidance, and reduction in security incidents.

Example: Mean Time to Implement Security Changes (MTTIC)

- Formula: MTTIC = (Total time spent on security changes) / (Number of security changes implemented)
- Benchmarks:
  - Industry average (manual): Several days to weeks per change.
  - Target (streamlining): Hours or minutes per change.
- Example: Reduce MTTIC from 72 hours to 4 hours.

Conclusion

Cloud security is complex, and traditional approaches don't cut it. You need an application-centric, cloud-native solution.

A platform like ACE, which automates security policy changes, risk assessments, and compliance reporting, is essential. ACE helps you reduce risks, improve efficiency, and get real ROI.

To manage cloud security effectively, you need a solution that provides streamlining, visibility, and intelligence. By moving to a proactive security approach, you can protect your assets and ensure smooth business operations.

Future trends

The cloud security landscape is always changing, with trends like serverless computing, containerization, and AI-driven threats. ACE is designed to adapt, offering continuous monitoring, streamlined policy updates, and advanced threat detection. By staying ahead of these trends, you can keep your cloud environment secure.

Next steps

Request a personalized demo
See the benefits of ACE firsthand.

Calculate Your ACE ROI

Discover significant cost savings in your hybrid and multi-cloud environments. This calculator provides a personalized ROI estimate for AlgoSec Cloud Enterprise (ACE). Input your details to see how ACE can optimize your security and improve your bottom line.

ACCESS THE ACE ROI CALCULATOR

Appendix A
Glossary of cloud security terms

To ensure a clear understanding of the concepts discussed in this white paper, we've included a comprehensive glossary of cloud security terms in this appendix. This section defines key terminology related to cloud computing, security practices, provider-specific services, emerging threats, and compliance. By providing these definitions, we aim to equip readers with the necessary knowledge to fully grasp the complexities of cloud network security and the solutions offered within this document.

Core cloud computing concepts

Cloud infrastructure as a service (IaaS)
A cloud computing model where virtualized computing resources (e.g., servers, storage, networks) are provided over the internet.

Cloud platform as a service (PaaS)
A cloud computing model where a platform and environment are provided to developers, allowing them to build and deploy applications without managing the underlying infrastructure.

Hybrid Cloud
A cloud computing environment that combines on-premises infrastructure with public cloud services.

Multi-Cloud
The use of multiple cloud computing services from different providers.

Virtual private cloud (VPC)
A logically isolated section of a public cloud where you can launch cloud resources in a virtual network that you define.

Serverless computing
A cloud computing execution model in which the cloud provider dynamically manages the allocation of machine resources.

Containerization
A virtualization method that allows applications and their dependencies to be packaged into containers, which can run consistently across different environments.

Container orchestration (e.g., Kubernetes)
The security of container operations, including deployment, scaling, and management.

Auto-scaling
The ability of a cloud environment to automatically adjust its resources (e.g., compute, storage) based on demand. This ensures optimal performance and cost efficiency.

Cloud security fundamentals

Cloud network security
The process of protecting cloud-based networks, data, and applications from unauthorized access, cyber threats, and security vulnerabilities.

Cloud security posture
The overall security status of a cloud environment, including its vulnerabilities, compliance, and risk level.

Cloud security group
A virtual firewall that controls inbound and outbound traffic to cloud resources, such as virtual machines and databases.

Network access control list (Network ACL)
A security feature in cloud environments that acts as a stateless firewall, controlling network traffic at the subnet level.

Network segmentation
The practice of dividing a network into smaller, isolated segments to improve security and performance.

Microsegmentation
The practice of dividing a network into smaller, isolated segments to limit the impact of security breaches.

Zero trust xecurity
A security model that assumes no implicit trust within a network, requiring all users and devices to be authenticated and authorized.

Identity and access management (IAM)
A framework for managing digital identities and controlling access to resources.

Access control list (ACL)
A list of permissions associated with a system resource (e.g., a file or process). It specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects.

Encryption
The process of converting data into an unreadable format, protecting it from unauthorized access.

Firewall
A network security device that monitors and controls incoming and outgoing network traffic based on predefined security rules.

Cloud native security
Security practices that are designed to protect cloud-native applications and infrastructure.

Security as code
The practice of managing security configurations and policies using code.

Immutable infrastructure
Infrastructure that is never modified after it's deployed; it's replaced with a new instance if changes are needed.

Cloud provider specific services

AWS security hub
A security service that provides a comprehensive view of your security posture in AWS.

Azure security center
A security management system for Azure, providing threat protection and security recommendations.

Google cloud security command center
A security and risk management platform for Google Cloud.

CloudTrail (AWS)
A service that records AWS API calls for your account and delivers log files to you.

Azure monitor
A service that collects and analyzes telemetry data from Azure and on-premises environments.

Cloud logging (Google Cloud)
A service that allows you to store, search, analyze, monitor, and alert on logging data and events from Google Cloud Platform and Amazon Web Services.

Security tools and practices:

Security information and event management (SIEM)
A security solution that collects and analyzes security logs and events from various sources to detect and respond to threats.

DevSecOps
The practice of integrating security into the DevOps lifecycle, ensuring that security is considered throughout the development and deployment process.

Infrastructure as code (IaC)
The practice of managing and provisioning infrastructure using code, enabling consistency.

Application programming Interface (API)
A set of defined rules that enable different software applications to communicate with each other. In cloud security, APIs are often used to automate tasks and integrate security tools with cloud platforms.

Threat intelligence
Information about existing or emerging threats that can be used to inform security decisions.

Threats and attacks

Distributed Denial-of-Service (DDoS) Attack
A type of cyberattack that floods a target server or network with traffic, making it unavailable to legitimate users.

Zero-Day Exploit
A cyberattack that exploits a software vulnerability that is unknown to the software vendor.

Ransomware
A type of malware that encrypts files and demands a ransom for their release.

Phishing
A cyberattack that uses deceptive emails or websites to trick individuals into revealing sensitive information.

Compliance

Cloud compliance
Adherence to regulatory requirements and industry standards that apply to cloud computing environments. Examples include PCI DSS, HIPAA, etc.