알고섹을 이용한 클라우드 보안 정책관리

ALGOSEC SECURITY MANAGEMENT FOR HYBRID CLOUD

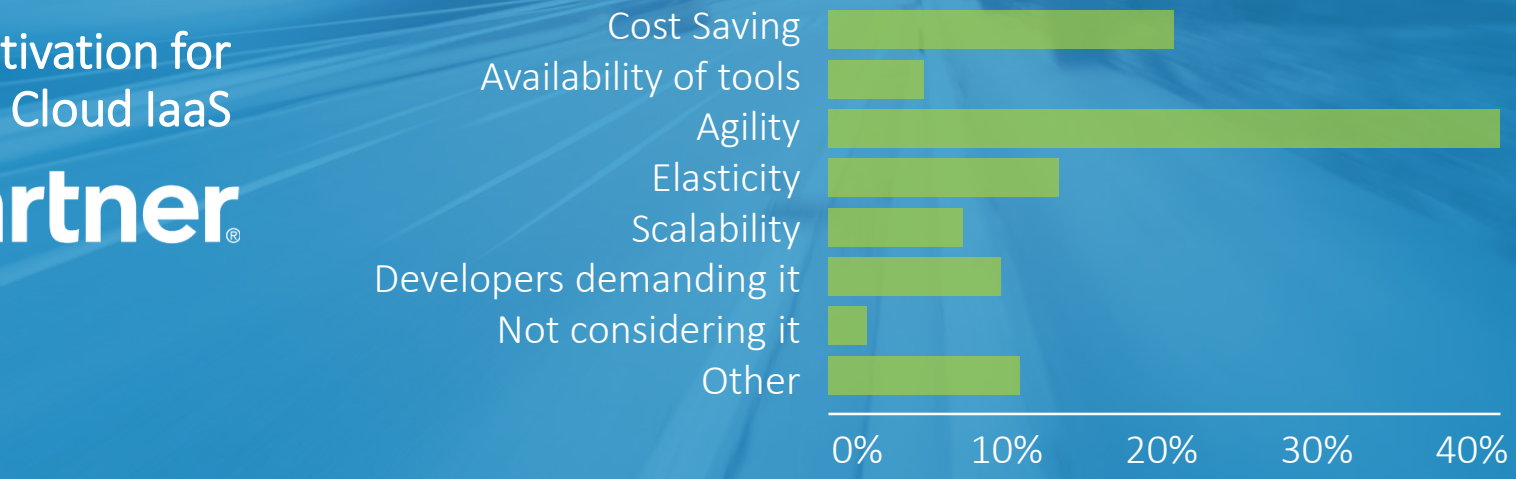
MANAGE SECURITY
AT THE SPEED OF BUSINESS

algosec

In the cloud, agility and automation are more important than ever

What is your PRIMARY motivation for deploying Public Cloud IaaS

Gartner®



algosec

Security Controls are Different

Security fundamentals remain the same

"Through 2019, 80% of cloud breaches will be due to customer misconfiguration, mismanaged credentials or insider theft, not cloud provider vulnerabilities."

Gartner

algosec

NOT EVERYBODY MIGRATES TO THE CLOUD

- We know our customer's **vision** – *migration*
- It involves our cutting edge features
  - Application (Auto) Discovery
  - Seamless submission of FireFlow change requests
  - End to end automation including ActiveChange
  - Accurate analysis of tens of Security Groups, NACLs
  - Etc.
- A **BIG project** that requires **heavy resources** and **careful planning**

But wait, there is another use case…

algosec

THE OVERWHELMED SECURITY TEAMS

- Professionals at managing on premise devices
- Fluent in their firewalls' policies
- Understand their security posture and policy

And one day their manager tells them about the cloud…

- How to make *first contact* with these unmanaged cloud servers?
- This is what they need *NOW*

algosec

CLOUD SECURITY – THE PRAGMATIC START

- Change monitoring – very valuable!
  - Alerting
  - Reviewing

- Visibility into running servers
- Detailed change reporting
- Policy visibility
- Risk and compliance reports
- Troubleshooting (Traffic Simulation Queries)

algosec

ALGOSEC SUPPORT FOR THE SIMPLE STORY

Amazon Web Services (AWS) and VMWare NSX

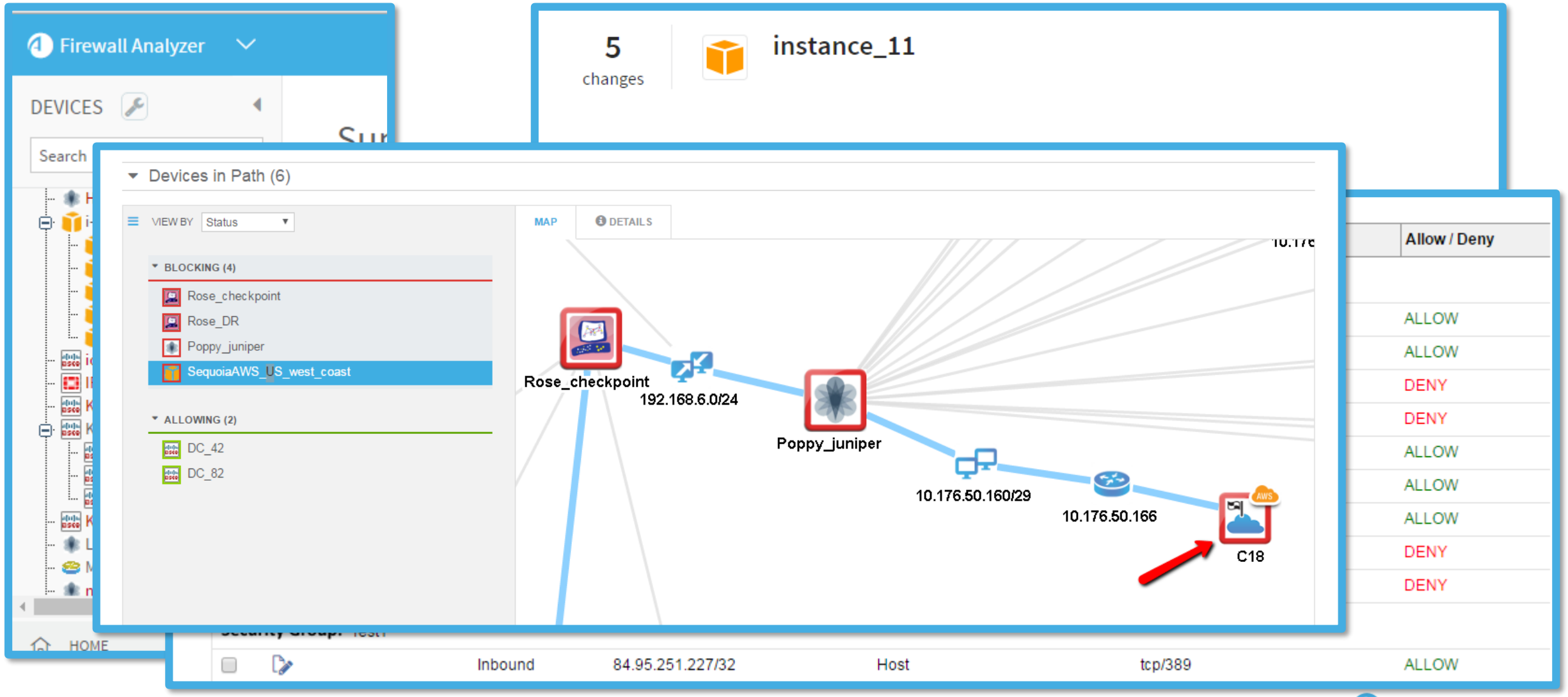
- Visibility into running servers
- Full policy visibility
  - 6.9 – Security Groups and Distributed Firewalls
  - 6.10 – Network ACLs (NACLs)
- Detailed change monitoring
- Troubleshooting capabilities
- Change management support

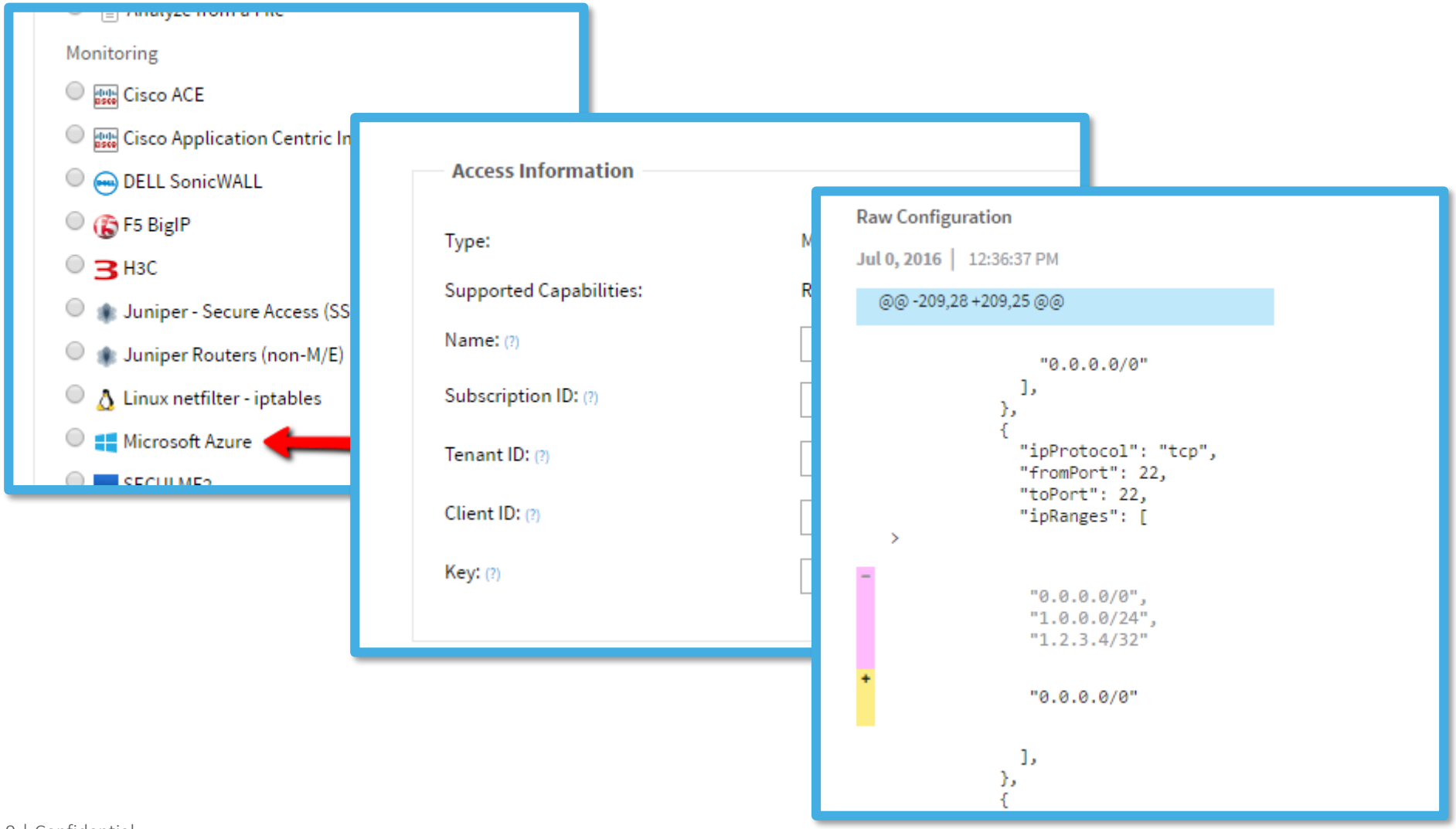
Microsoft Azure (6.10)

- Change monitoring

algosec

AWS SUPPORT


Firewall Analyzer
DEVICES
Search
5
changes
instance_11
Devices in Path (6)
VIEW BY Status
MAP
DETAILS
BLOCKING (4)
Rose_checkpoint
Rose_DR
Poppy_juniper
SequoiaAWS_US_west_coast
ALLOWING (2)
DC_42
DC_82
Rose_checkpoint
192.168.6.0/24
Poppy_juniper
10.176.50.160/29
10.176.50.166
C18
Allow / Deny
ALLOW
ALLOW
DENY
DENY
ALLOW
ALLOW
ALLOW
DENY
DENY
HOME
Inbound
84.95.251.227/32
Host
tcp/389
ALLOW


Monitoring
Cisco ACE
Cisco Application Centric In
DELL SonicWALL
F5 BigIP
H3C
Juniper - Secure Access (SS
Juniper Routers (non-M/E)
Linux netfilter - iptables
Microsoft Azure
Access Information
Type:
Supported Capabilities:
Name: (?)
Subscription ID: (?)
Tenant ID: (?)
Client ID: (?)
Key: (?)
Raw Configuration
Jul 0, 2016 | 12:36:37 PM
@@ -209,28 +209,25 @@
"0.0.0.0/0"
],
},
{
"ipProtocol": "tcp",
"fromPort": 22,
"toPort": 22,
"ipRanges": [
"0.0.0.0/0",
"1.0.0.0/24",
"1.2.3.4/32"
"0.0.0.0/0"
],
},
{

BUSINESS-DRIVEN SECURITY POLICY MANAGEMENT FOR HYBRID CLOUD ENVIRONMENTS

Application Migration to the Cloud

- Application auto-discovery and connectivity requirements mapping
- Automatic translation from firewall rules to cloud security controls
- End to end automation of new security policy creation

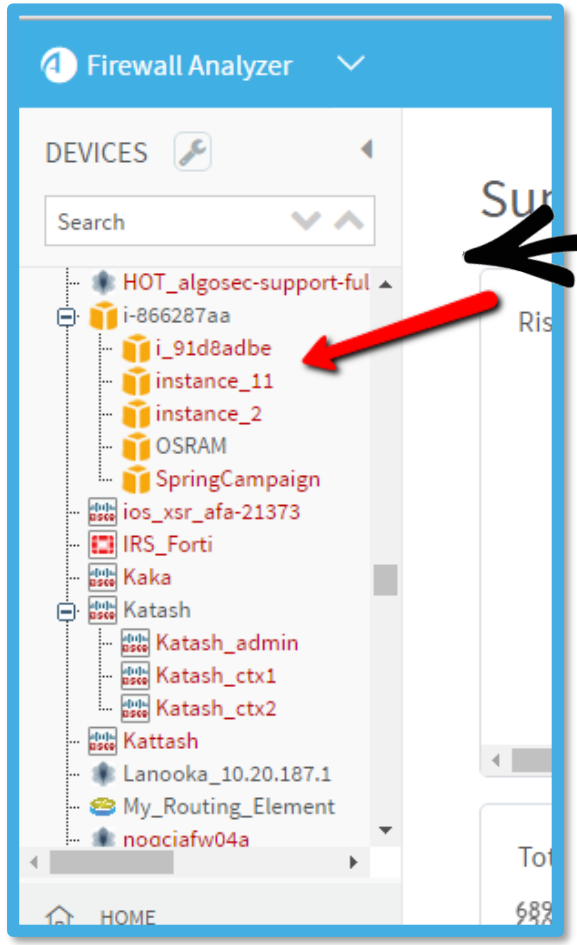
Unified Security Policy Management across the Hybrid Environment

- Single pane of glass for firewall rules and cloud security controls
- Security policy visibility, monitoring and alerting
- Risk and compliance reports
- Troubleshooting and traffic simulation

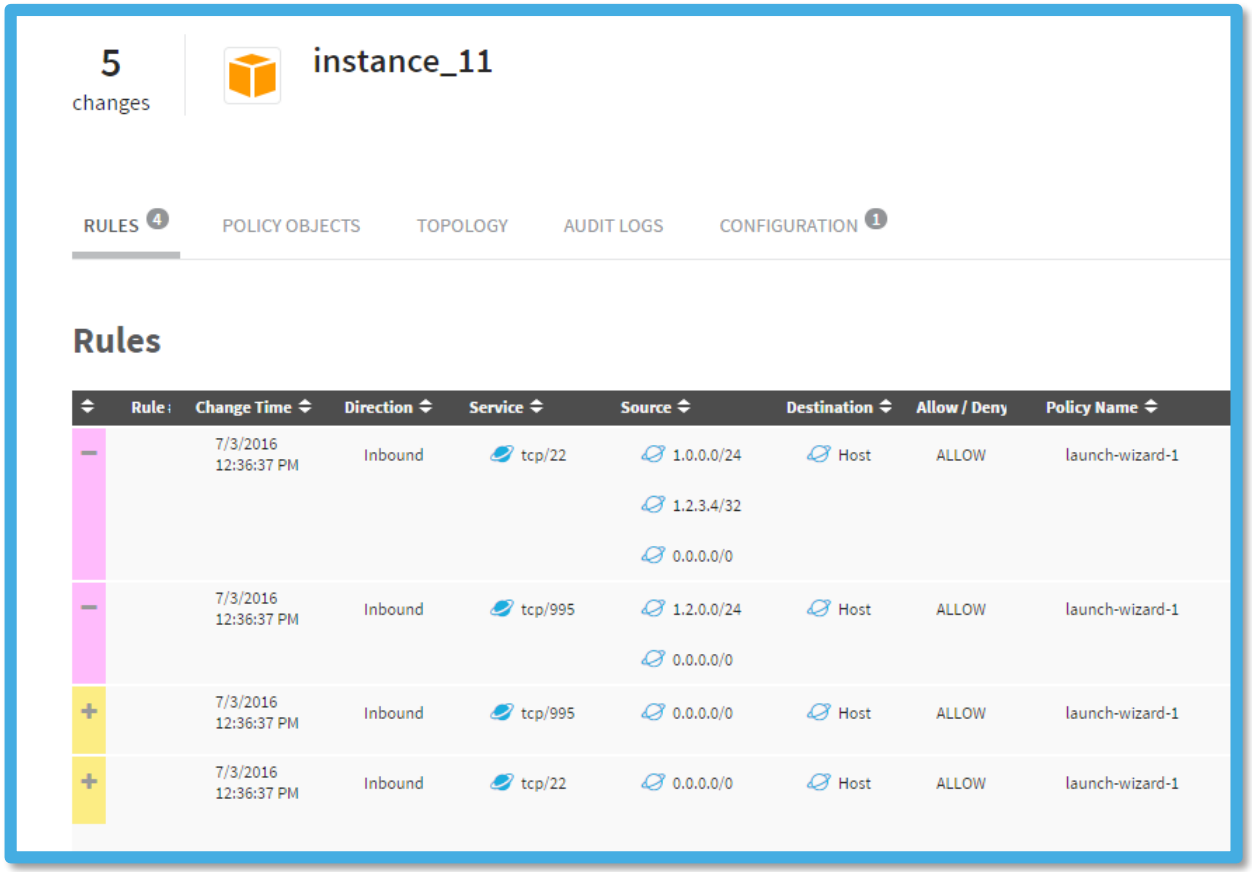
Supported platforms: amazon web services, vmware NSX, Microsoft Azure

algosec

HYBRID CLOUD SECURITY POLICY MANAGEMENT



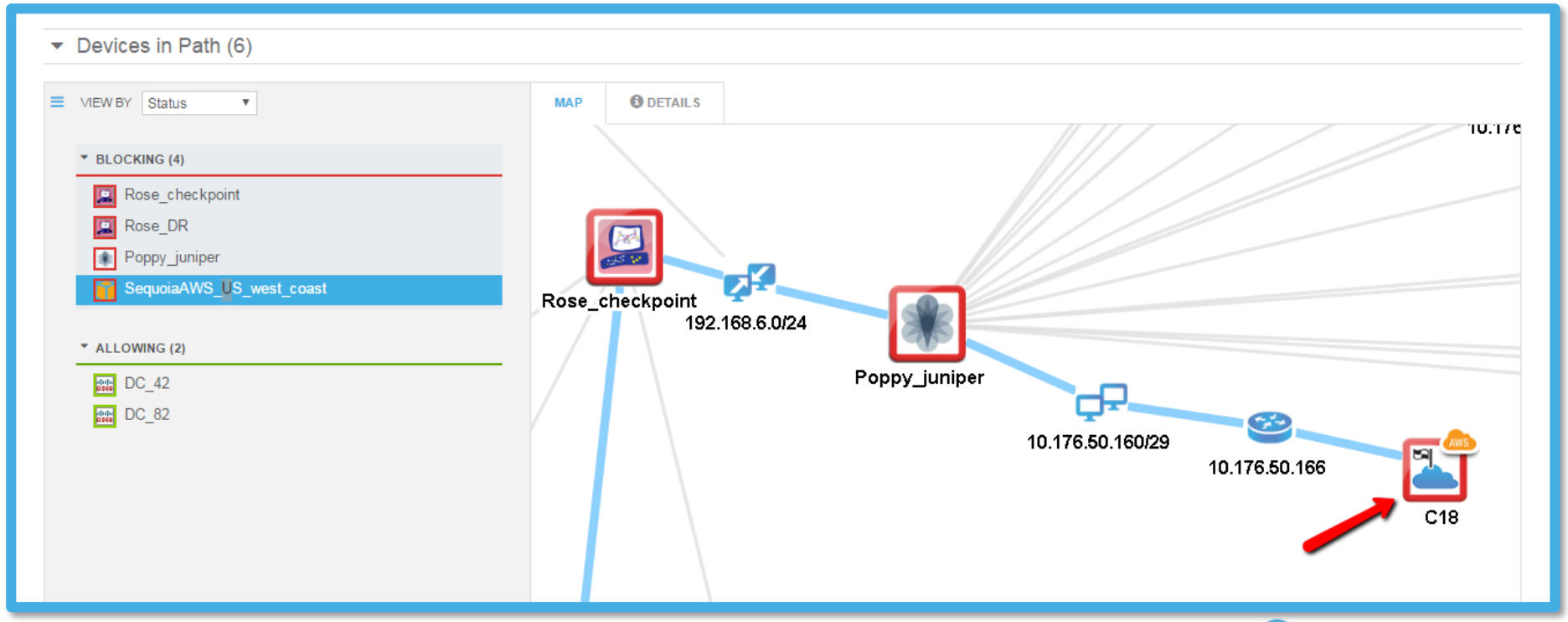
Visibility into running instances and their security controls



algosec

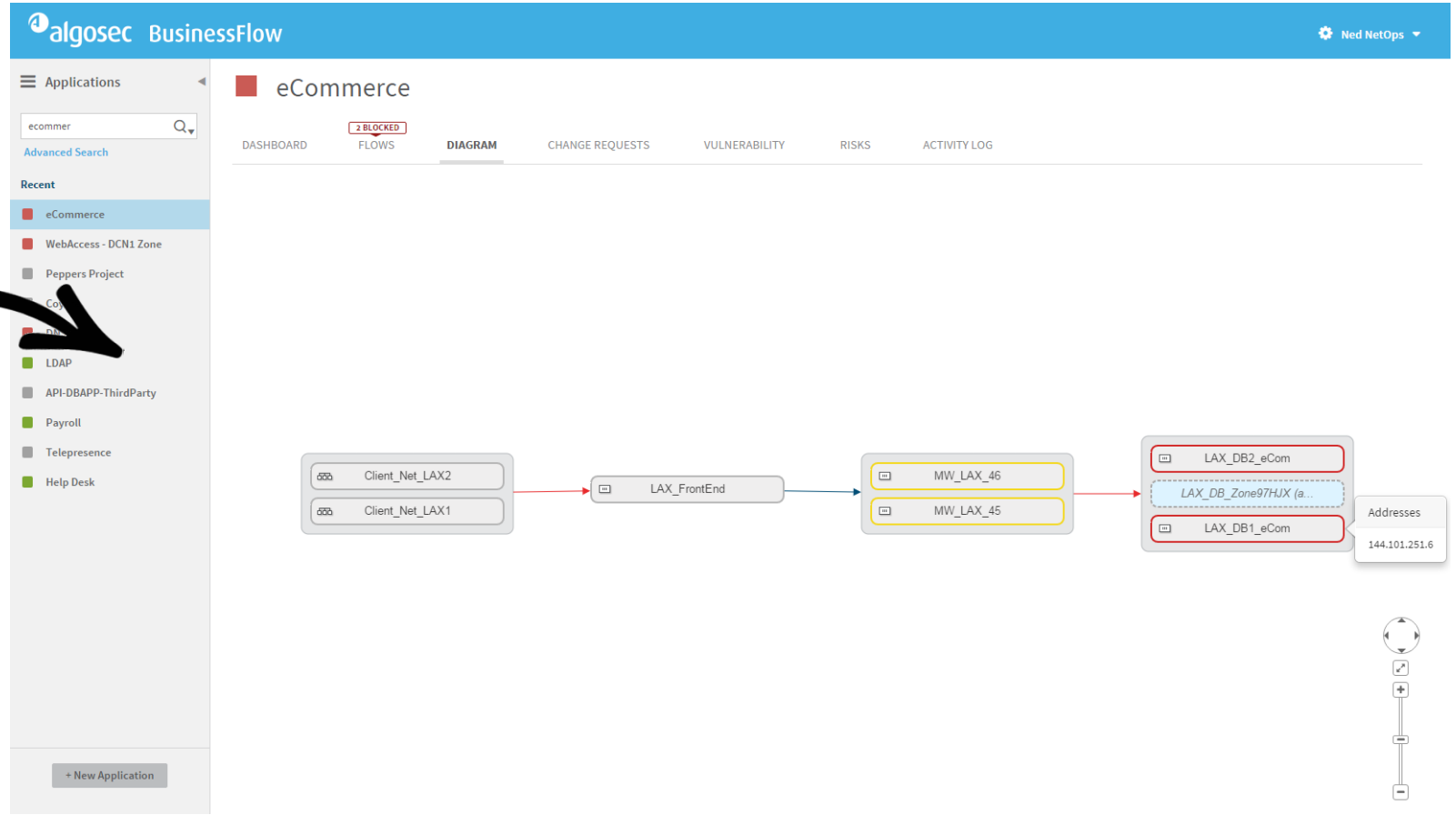
HYBRID CLOUD SECURITY POLICY MANAGEMENT

Traffic simulation queries across the hybrid environment



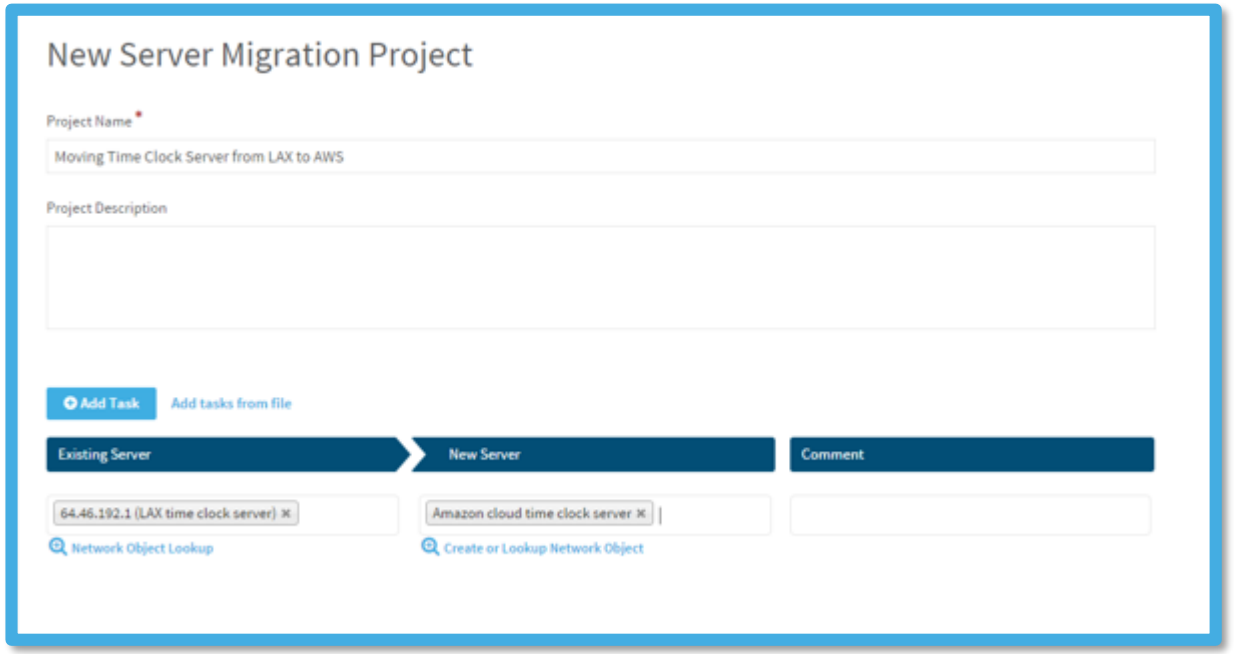
APPLICATION MIGRATION

Auto-discover applications and their connectivity requirements with zero prior knowledge



APPLICATION MIGRATION

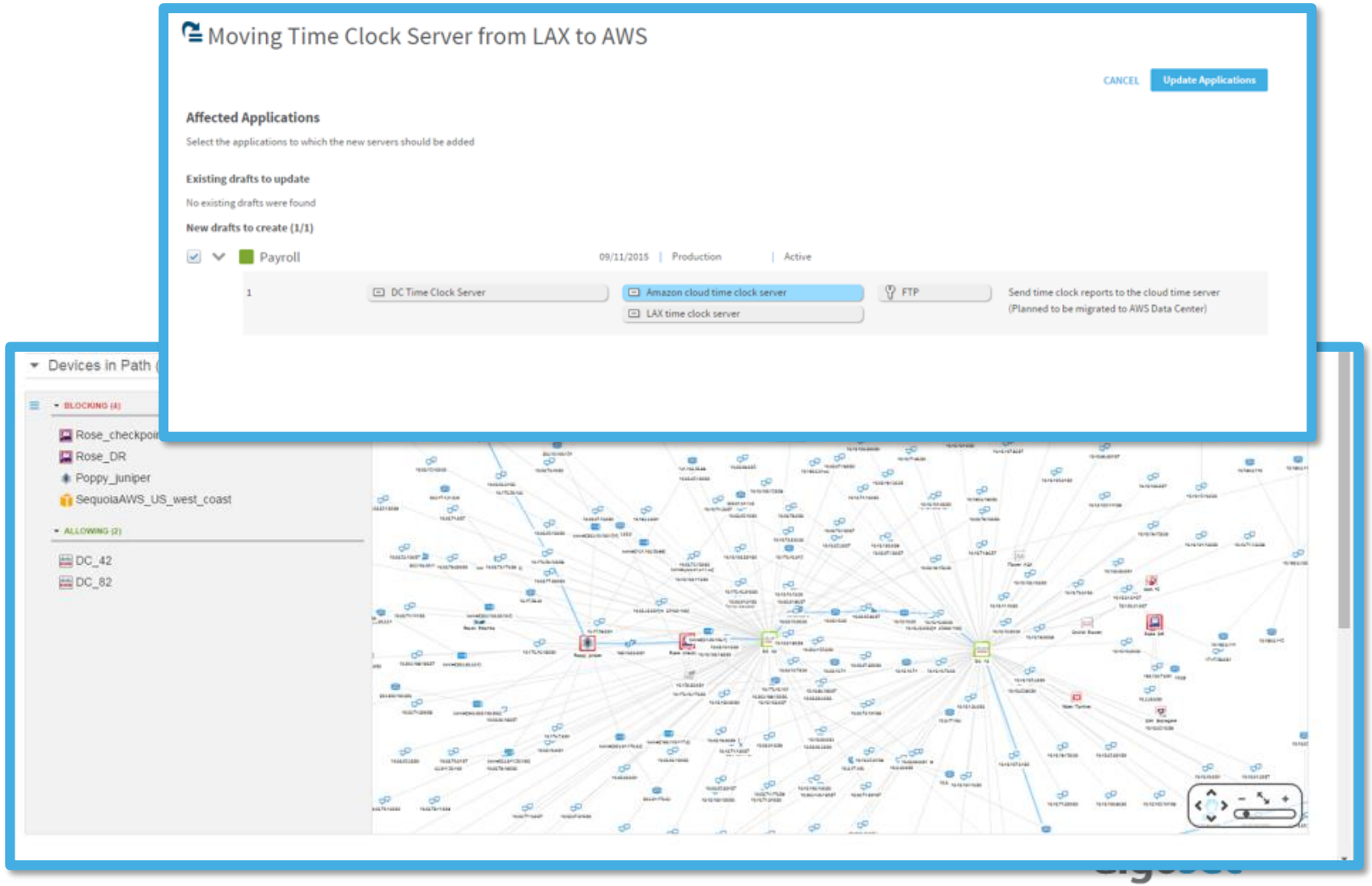
Create projects to migrate specific server(s) or entire applications



algosec

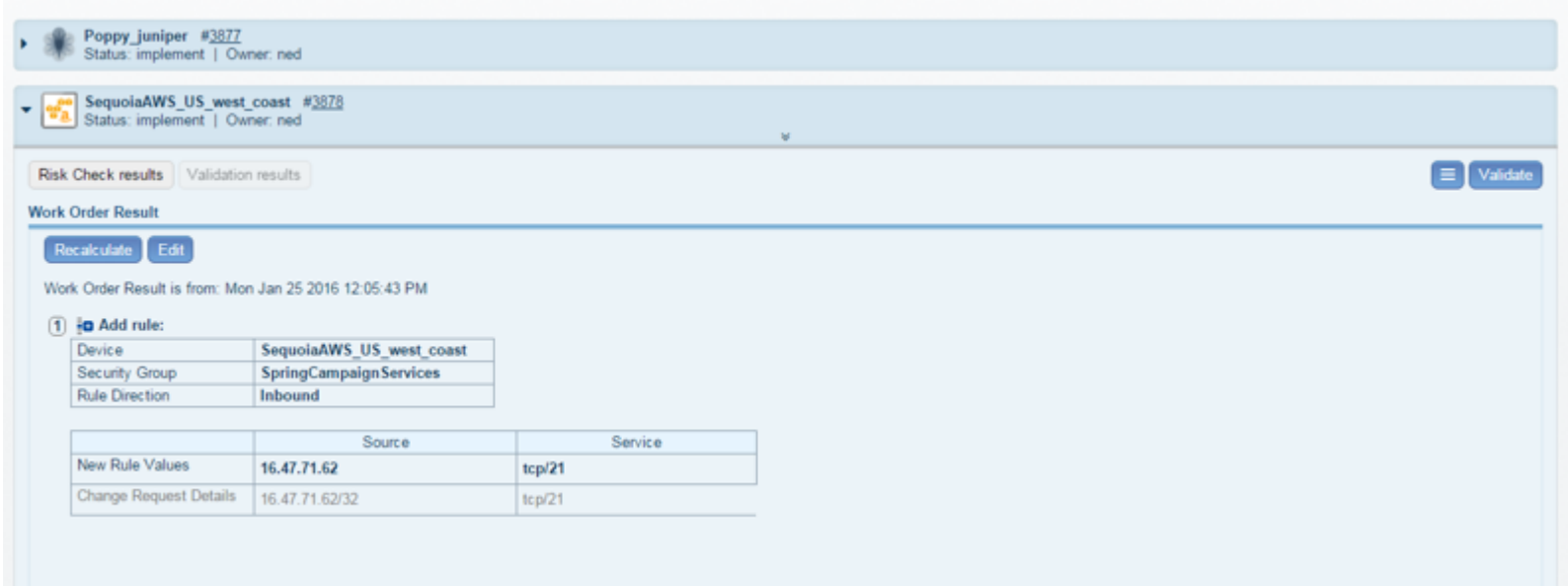
APPLICATION MIGRATION

AlgoSec discovers affected applications and computes required changes to firewall rules and cloud security groups



APPLICATION MIGRATION

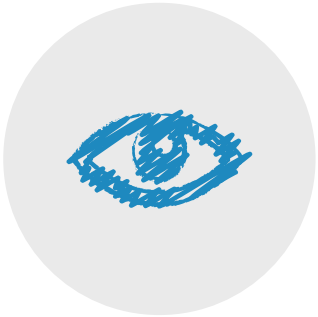
AlgoSec designs and provisions new cloud security controls, including risk assessment, validation and documentation



Save months of manual labor!

algosec

ALGOSEC'S HYBRID APPROACH

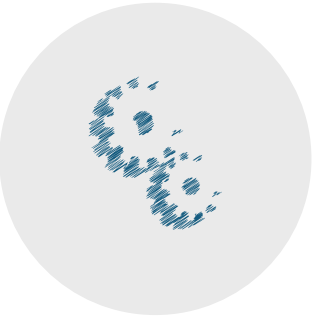


Visibility

A single pain of glass across the organization's entire estate

Compliance

Risk assessment and compliance reporting across the hybrid environment.



Orchestration & automation

Automated & orchestrated across any heterogeneous environment

algosec

아마존 클라우드 보안관리

algosec

THANK YOU

www.algosec.com