CLOUDVISORY

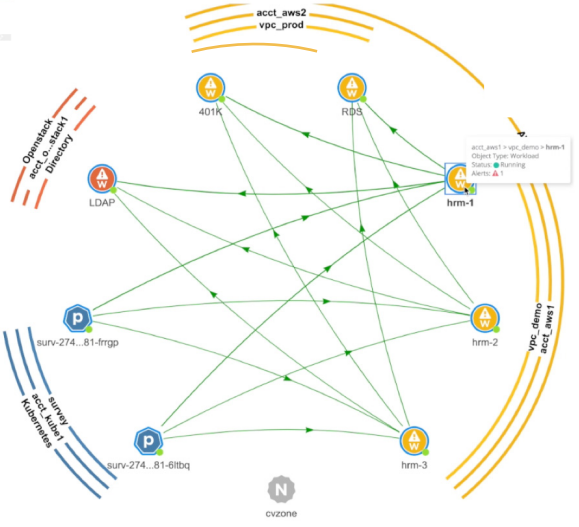
Security Orchestration and Micro-Segmentation for Public and Private Cloud

> *"Through 2020, 80% of cloud breaches will be due to misconfiguration and mismanagement of controls, not cloud provider vulnerabilities."*
>
> **Source: Gartner, 2017**

Cloud Security: The Problem

Cloud-native security controls are more secure than traditional data center approaches but are not being properly leveraged. This leaves enterprises with massive security holes that can be exploited by hackers and greatly impacts application uptime and business agility. Problem summary:

1. Cloud security controls are not being used to least privilege allowing excess access, increasing risk.
2. DevOps teams are coding security into orchestration tools without a method for organizing, auditing, monitoring, or enforcing provisioned controls, rising costs and reducing security, while also increasing risk
3. Misconfiguration of cloud security controls is the leading cause of risk and breach. Coding offers no method to visually test and validate security controls, further exposing enterprises to threats and risk of non-functioning applications
4. Enterprises are not using a workload Micro-Segmentation strategy, a mandate in cloud for thwarting the East/West threat
5. Real-time visibility into cloud infrastructure security is non-existent, delaying detection of critical threats.



Cloudvisory: Cloud Security Platform

Used by Security, DevOps and Business teams, the Cloudvisory Security Platform (CSP), responds to all these cloud security issues. Developed for cloud, hybrid cloud and multi-cloud environments, CSP is a central management, orchestration, and enforcement solution for cloud security. Leveraging the cloud-native controls of various providers, CSP is a scalable, portable, enterprise-class solution providing:

- Continuous Discovery and Visualization of Infrastructure and Security Policies
- Policy Organization, Orchestration and Automated Provisioning
- Intelligent, granular, cloud-native Micro-segmentation
- Continuous Monitoring, Enforcement and auto-remediation of Security policies

"Cloudvisory's Security Platform immediately detected a policy breech when a workload attempted communication with a non-compliant public internet server. Cloudvisory's Micro-Segmentation blocked violations, quarantined the malicious code, avoiding critical data loss and preventing the threat from infiltrating our environment."

Fortune 50 Healthcare Co.

CSP works across AWS, Azure, Kubernetes, OpenStack, VMWare and even traditional virtualized and bare metal environments, reducing the need to learn multiple tools. CSP greatly support business agility and fights today's most dangerous hackers.

Cloud Visibility

A 2017 "C" level survey indicates that Visibility into Cloud Infrastructure security is one of the gravest concerns. Cloudvisory addresses this by continuously discovering and building a visual map of the native infrastructure (virtual instances), security policies and dynamic changes happening across the environment. For example, in AWS, Accounts, Regions, VPCs, Workloads, native security controls and even the network data flows are visually mapped. This "visualization" provides a comprehensive view into exactly how cloud security is structured and operating. As the environment changes, Cloudvisory will, in near real time, capture these changes and update the visual maps.

Hybrid, Multi-Cloud Security Policy Orchestration

Cloudvisory's Security Orchestration Plane provides a powerful platform to create, manage, and organize security policies for cloud, complex hybrid and/or multi-cloud deployments. With a simple point and click, natural language policies are created (or auto-discovered) inside of Cloudvisory. These policies are associated to cloud workloads (virtual instances) based on their "Context." A workload's Context is determined based on variables such as account or location, and/or meta data such as application, application tier, governance requirements and more. Cloudvisory translates these definitions into the cloud-native security controls for each provider environment.

Cloudvisory, thus, removes the complexity associated with learning, organizing, coding, updating, migrating and managing security policies. This capability dramatically reduces development time and costs, and greatly increases accuracy of the controls, speeding up cloud DevOps while providing superior security.

Micro-Segment by Default

In order to move to a "network of secure workloads," as Gartner recommends, micro-segmentation of workloads, micro-services, and containers must be the default.

CSP, is the only cloud-native micro-segmentation solution available today. By automatically provisioning micro- segmentation policies, CSP protects logical groups of workloads. This dynamic, granular policy segmentation allows only necessary network connections in or out of a workload or application, enforcing "least privilege," and blocking everything else. This greatly hardens security, halts East/West attacks, and makes security management more accurate and efficient.

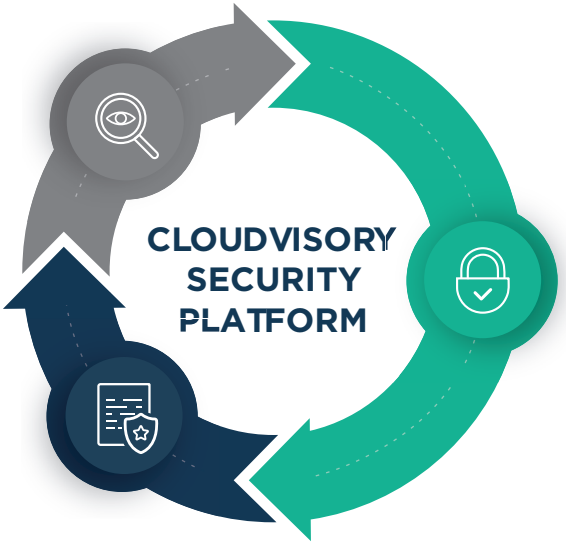
Monitoring, Enforcement and Compliance

Once policies are provisioned they must be monitored to ensure the environment is never compromised. CSP continuously monitors hybrid-cloud environments to enforce policy compliance and detect abnormal behavior in any workload. If detected, CSP automatically remediates and neutralizes the threat to keep the environment compliant and secure.

Automated Security-Policy Change Management

Today, Dev/Ops teams are often incorrectly coding security group rules, resulting in broken applications and/or increased risk because of too much allowed access. Furthermore, when policy changes/updates are required, complex calculations are often coded incorrectly, resulting in additional risk. These problems are only magnified in hybrid or multi cloud environments.

With CSP these misconfiguration issues disappear, as policies are precisely organized and managed. As the environment spins up additional workloads, or reduces the number of workloads, CSP immediately calculates and provisions/de-provisions the required micro-segmentation policies based on workload Context. The result is highly consistent and immutable security across complex hybrid or multi-cloud environments.



Strong security in the cloud requires the right automation. The right platform must have these pillars to deliver bulletproof security.

VISUALIZATION
AGILE OPERATIONS

Perpetual cloud/container discovery for real-time visualization of infrastructure, network flows, policies and security alerts.

CONTROL
IMMUTABLE SECURITY

Centralized security orchestration and intelligent micro-segmentation to simplify policy creation, automate provisioning, and harden security.

ENFORCEMENT
DEFEAT ATTACKERS

Continuous, real-time monitoring and enforcement of network flows and security policies in order to detect, block and remediate malicious threats.

CLOUD SECURITY MANAGEMENT PLATFORM

SIMPLIFIES
Singular interface for cloud-native automation across providers

DISCOVERS AND VISUALIZES
Multi-cloud infrastructures, context, data flows and critical security violations

AUTOMATES
Provisioning and rapid change management of policy and micro-segmentation of workloads

COMPLIANCE
Real-time monitoring and enforcement of cloud data flows and policies ensures continuous compliance

CROSS-DISCIPLINE
Manages multi-tenant environments; role-based solution for use by Dev/Ops, Security, and Business

"Misconfiguration and mistakes are the leading causes of operations incidents and successful security attacks"

GARTNER

amazon web services · openstack. · DATA CENTER · vmware · kubernetes · Microsoft Azure

About Us

Used by Security, Dev/Ops and Business teams, the Cloudvisory Security Platform (CSP), was developed for cloud, hybrid cloud and multi-cloud environments. It was built to deliver the most powerful, centralized cloud security management, micro-segmentation and security orchestration solution available. The only Security Orchestration solution that leverages the cloud-native controls of the various providers, CSP works across AWS, Azure, Kubernetes, OpenStack, VMWare and even traditional virtualized and bare metal environments, helping enterprises to speed up business, reduce risk and thwart today's most dangerous hacker.