COMPLETE MULTI-CLOUD SECURITY GOVERNANCE, RISK MANAGEMENT & COMPLIANCE

Identify risk, guarantee compliance, and enforce security policies in a single platform

CLOUDVISORY

Gartner 2018 CoolVendor

CLOUD SECURITY » THE PROBLEM

Traditional security tools either don't work at all in cloud environments or have only limited functionality. Cloud providers such as AWS, Azure, GCP, Kubernetes and OpenStack have native security controls and logs that must be used to protect your cloud services and workloads. If these cloud-native security controls are not configured properly, enterprises will be left with massive security holes that can be exploited by hackers and greatly impact application uptime and business agility.

1. Real-time **visibility** into cloud infrastructure security is limited, delaying detection of critical threats.
2. Cloud security controls are not being used to "**least privilege**" allowing risky access and increasing the attack surface.
3. DevOps teams lack a method for organizing, testing, auditing, monitoring and enforcing provisioned controls, leading to misconfiguration of security **policies**.
4. Misconfiguration of cloud security controls is the leading cause of **risk** and **breach**.
5. Lack of continuous **compliance** validation and enforcement of policy controls exposes enterprises to great risk.
6. Enterprises are not using a workload microsegmentation strategy, a mandate in cloud for thwarting the East/West threat.

> Cloudvisory's Security Platform immediately detected a policy breach when a workload attempted communication with a non-compliant public internet server. Cloudvisory's microsegmentation blocked violations, quarantined the malicious code, avoiding critical data loss and preventing the threat from infiltrating our environment.
>
> **Fortune 50 Healthcare Co.**

CLOUDVISORY » CLOUD SECURITY PLATFORM

The Cloudvisory Security Platform (CSP) is the only complete Cloud Security Platform. CSP solves the security issues outlined above and is designed to protect large cloud environments, including hybrid- and multi-cloud environments. CSP is a complete multitenant platform for Audit, Compliance, Microsegmentation and Policy Enforcement — allowing for a phased implementation approach for a given Organization as outlined below:

PHASE 1
ACTIONABLE AUDIT
Discover, visualize and audit multi-cloud environments to gain visibility, uncover risks and improve security posture

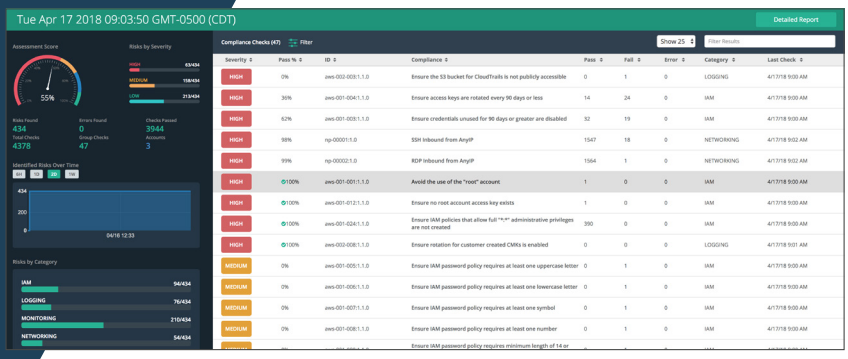
PHASE 2
COMPLIANCE ASSURANCE
Cloud-native policy guardrails identify, alert and report on risk in hybrid, multi-cloud deployments

PHASE 4
AUTOMATED ENFORCEMENT
Identify and remediate risks, compliance breaks, policy violations and even quarantine compromised workloads

PHASE 3
INTELLIGENT MICROSEGMENTATION
Automated policy recommendations for cloud-native microsegmentation and orchestration to protect applications and microservices

CLOUDVISORY

CSP centralizes the monitoring and management of cloud security, reducing the need to learn multiple tools. It works across public and private clouds as well as virtualized and baremetal environments.



Continuous compliance detects and alerts on policy failures, while automated remediation fixes them

aws openstack. Azure kubernetes Google Cloud vmware DATA CENTER

PHASE 1: ACTIONABLE AUDIT

Cloudvisory continuously discovers and builds visual maps of the native infrastructure, security policies and dynamic changes happening in the environment – while storing this information for security analytics. For example, in AWS, Accounts, Regions, VPCs, Workloads, tags, native security controls and network data flows are mapped. This "Visualization" provides a comprehensive view into exactly how cloud security is structured and operating. As the environment changes, CSP captures these changes and updates the visualization. CSP then provides the ability to query the underlying environment through point-and-click Audit screens. These Actionable Audits allow companies to quickly identify risk across their multi-cloud deployments. CSP empowers Enterprises to quickly identify and remediate security risks in massive cloud deployments – with every customer able to use CSP to clearly detect misconfigurations deployed and/or ignored by existing DevOps processes.

PHASE 2: COMPLIANCE ASSURANCE

Agility is paramount to cloud self-service users. Instead of "policy gates" that slow users down, "policy guardrails" should be created to manage risk according to best practices and business requirements. Taking this structured approach will minimize friction while increasing cloud protection. Compliance guardrails are automations that constantly watch your deployments, find deviations from desired baselines, and can even automatically remediate issues. These guardrails continuously run and identify policy violations, giving enterprises the ability to quickly identify risks that may have been overlooked within DevOps processes. For example, it may be important to check if policies have been created that allow "any IP ingress on Port 22" on cloud workloads, and automatically remove that rule to decrease the attack surface. Cloudvisory provides out-of-the-box sets of Compliance Checks for vulnerabilities in cloud environments, dynamically evaluating Compliance and Risk in accordance with templated, industry-standard best practices such as CIS benchmarks. Existing guardrails can be modified and custom guardrails can be created to support the business processes of any Enterprise.

PHASE 3: INTELLIGENT MICROSEGMENTATION

Gartner stresses: microsegmentation of workloads, micro-services, and containers "must be the default." CSP is the only microsegmentation solution available today that utilizes cloud-native security controls for enforcement. CSP automatically discovers and organizes groups of workloads based on environment settings and metadata, allowing for immediate provisioning of precise microsegmentation policies. This dynamic, granular policy segmentation allows only specific network connections in or out of a workload or application, enforcing the critical "least privilege" model, blocking everything else. As new workloads spin up, precise policies are automatically provisioned. This greatly hardens security, halts East/West attacks, and makes consistent security policy management a reality.

PHASE 4: AUTOMATED ENFORCEMENT

CSP is continuously monitoring all compliance guardrail and microsegmentation policies. Any violations are immediately detected and alerted upon. CSP can also be configured for automated enforcement of policies. If a policy failure is identified, CSP can immediately correct the issue – such as removing a security group violation or turning on CloudTrail for all VPCs. Additionally, if a microsegmentation rule is accidently or maliciously changed, CSP immediately rolls back the environment to its compliant state. CSP enables Enterprises to detect actual attacks such as malware trying to move laterally within a traditional "trust zone" such as a subnet, Project, VPC, etc. If a breach is detected, CSP can orchestrate the network quarantine of the affected Workload(s) according to a configurable quarantine policy.

SUMMARY

CSP has been designed to deliver immediate cloud security value with non-intrusive Audit, Compliance and Governance. Extended value is achieved via Machine Learning of actual network flows and corresponding recommendations for building an intelligent microsegmentation strategy. Enforcement controls make sure policies remain compliant at all times, delivering real-time remediation. CSP removes the complexity associated with learning, organizing, coding, updating, migrating and managing least-privilege security policies – which dramatically reduces development time and costs, greatly increases accuracy of controls, and synchronizes DevOps with superior security.

> **Misconfiguration and mistakes are the leading causes of operations incidents and successful security attacks.**
> **Gartner**

ABOUT US

Used by Security, Audit, Compliance, DevOps, Developers and Network teams – the Cloudvisory Security Platform (CSP) is engineered to protect hybrid- and multi-cloud environments. CSP was built to deliver the most powerful, complete solution available for cloud security governance, risk management and compliance. CSP is the only microsegmentation solution that leverages the cloud-native security controls of the various providers and works across AWS, Azure, Kubernetes, GCP, OpenStack, VMWare and even traditional virtualized and baremetal environments, helping enterprises to speed up business, reduce risk and thwart today's most dangerous hackers.