CLOUDVISORY

Complete Cloud Security Governance

Identify Risk, Guarantee Compliance, and enforce
Cloud-Native Micro-segmentation in a single platform

Gartner 2018
Cool Vendor

> “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

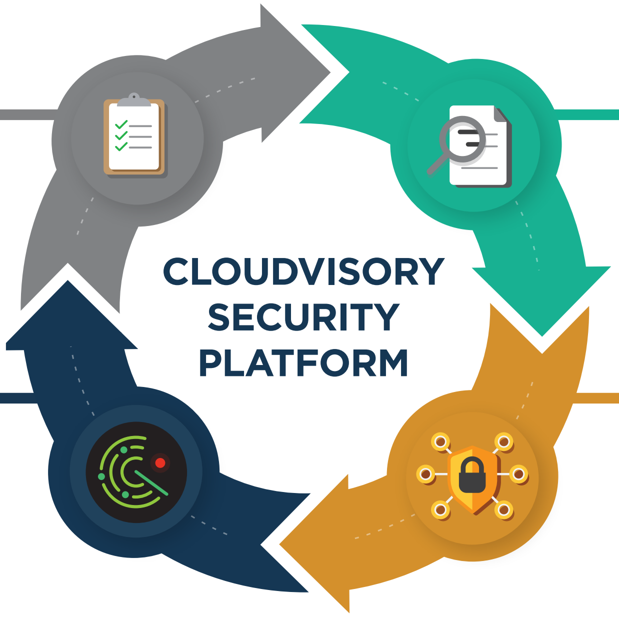
Cloud-native security controls are more secure than traditional data center approaches but are not being properly leveraged. This leaves enterprises with massive security holes that can be exploited by hackers and greatly impacts application uptime and business agility. Problem summary:

1. Real-time **visibility** into cloud infrastructure security is non-existent, delaying detection of critical threats.
2. Cloud security controls are not being used to “**least privilege**” allowing risky access and increasing threat of breach.
3. DevOps teams lack a method for organizing, testing, auditing, monitoring and enforcing provisioned controls, leading to misconfiguration of **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, leaves enterprises exposed to great risk.
6. Enterprises are not using a workload Micro-Segmentation strategy, a mandate in cloud for thwarting the East/West threat.

> **“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.

CLOUDVISORY | CLOUD SECURITY PLATFORM

The Cloudvisory Security Platform (CSP), is the only complete Cloud Security Governance Platform. CSP solves the security issues outlined above and is designed to support cloud, hybrid cloud and multi-cloud environments. CSP is a complete platform for Audit, Compliance, Micro-Segmentation and Enforcement, allowing for a phased implementation approach as outlined below:



PHASE 1

ACTIONABLE AUDIT

Discover, visualize & audit the infrastructure to uncover existing network risks and threats in minutes

PHASE 2

COMPLIANCE ASSURANCE

Cloud-native policy guardrails identify, alert on risk in hybrid, multi-cloud deployments

PHASE 3

INTELLIGENT MICRO-SEGMENTATION

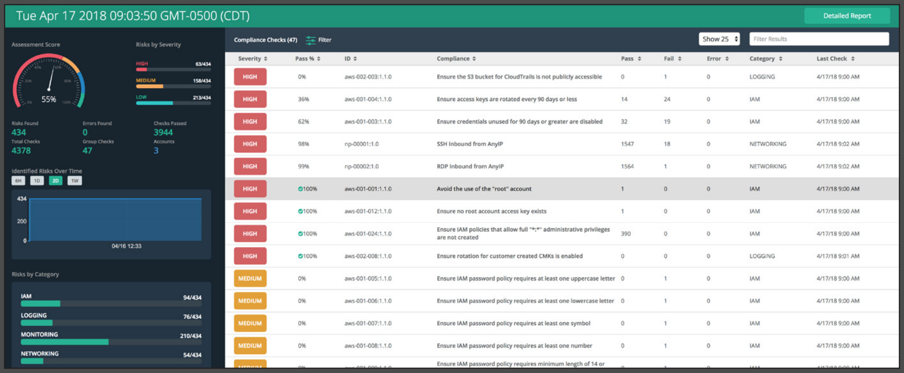
Automated cloud-native micro-segmentation, policy orchestration to guarantee immutable security

PHASE 4

AUTOMATED ENFORCEMENT

Identify and remediate risks, compliance breaks, policy violations and even quarantine compromised workloads

CSP works across public/private clouds, VMWare and even traditional virtualized and bare metal environments, reducing the need to learn multiple tools, while supporting business agility and fighting today's most dangerous hackers.



Tue Apr 17 2018 09:03:50 GMT-0500 (CDT)

Assessment Score: 55%

Risks by Severity

HIGH	63/434
MEDIUM	158/434
LOW	213/434

Risks Found 434
Total Checks 4378
Errors Found 0
Group Checks 47
Checks Passed 3944
Accounts 3

Identified Risks Over Time

Risks by Category

IAM	94/434
LOGGING	76/434
MONITORING	210/434
NETWORKING	54/434

Compliance Checks (47)

Severity	Pass %	ID	Compliance	Pass	Fail	Error	Category	Last Check
HIGH	0%	aws-002-003:1.1.0	Ensure the S3 bucket for CloudTrails is not publicly accessible	0	1	0	LOGGING	4/17/18 9:00 AM
HIGH	36%	aws-001-004:1.1.0	Ensure access keys are rotated every 90 days or less	14	24	0	IAM	4/17/18 9:00 AM
HIGH	62%	aws-001-003:1.1.0	Ensure credentials unused for 90 days or greater are disabled	32	19	0	IAM	4/17/18 9:00 AM
HIGH	98%	np-00001:1.0	SSH Inbound from AnyIP	1547	18	0	NETWORKING	4/17/18 9:02 AM
HIGH	99%	np-00002:1.0	RDP Inbound from AnyIP	1564	1	0	NETWORKING	4/17/18 9:02 AM
HIGH	✓100%	aws-001-001:1.1.0	Avoid the use of the "root" account	1	0	0	IAM	4/17/18 9:00 AM
HIGH	✓100%	aws-001-012:1.1.0	Ensure no root account access key exists	1	0	0	IAM	4/17/18 9:00 AM
HIGH	✓100%	aws-001-024:1.1.0	Ensure IAM policies that allow full "*:*" administrative privileges are not created	390	0	0	IAM	4/17/18 9:00 AM
HIGH	✓100%	aws-002-008:1.1.0	Ensure rotation for customer created CMKs is enabled	0	0	0	LOGGING	4/17/18 9:01 AM
MEDIUM	0%	aws-001-005:1.1.0	Ensure IAM password policy requires at least one uppercase letter	0	1	0	IAM	4/17/18 9:00 AM
MEDIUM	0%	aws-001-006:1.1.0	Ensure IAM password policy requires at least one lowercase letter	0	1	0	IAM	4/17/18 9:00 AM
MEDIUM	0%	aws-001-007:1.1.0	Ensure IAM password policy requires at least one symbol	0	1	0	IAM	4/17/18 9:00 AM
MEDIUM	0%	aws-001-008:1.1.0	Ensure IAM password policy requires at least one number	0	1	0	IAM	4/17/18 9:00 AM
			Ensure IAM password policy requires minimum length of 14 or					

Continuous compliance detects and alerts on policy breaks

ACTIONABLE AUDIT

Cloudvisory continuously discovers and builds visual maps of the native infrastructure, security policies and dynamic changes happening in the environment. For example, in AWS, Accounts, Regions, VPCs, Workloads, native security controls and even the 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 risky workload firewall settings that put the entire deployment at risk. This capability has proven to be invaluable to enterprises – every entity we have worked with, quickly identified major security risks that had been deployed by existing Dev/Ops processes.

COMPLIANCE ASSURANCE

CSP audit filters can be turned into continuous Compliance Assurance guardrails. For example, it may be important to check if policies have been created that allow "any IP ingress on Port 22." Additional checks for IAM, CIS benchmarks (e.g. is Cloudtrail turned on for all VPC's) along with other network settings can be configured for Compliance Assurance. These guardrails continuously run and identify policy violations, giving enterprises the ability to quickly identify risks that may have been overlooked within Dev/Ops processes.

INTELLIGENT MICRO-SEGMENTATION

Gartner stresses: micro-segmentation of workloads, micro-services, and containers "must be the default." CSP, is the only cloud-native micro-segmentation solution available today. CSP automatically organizes groups of workloads based on environment settings and meta data allowing for immediate provisioning of precise micro-segmentation 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, exact policies are provisioned. This greatly hardens security, halts East/West attacks, and makes security management less costly and more accurate.

AUTOMATED ENFORCEMENT

CSP is continuously monitoring all compliance and micro-segmentation policies. Any violations are immediately detected and alerted on. CSP can also be configured for automated enforcement of policies. If a policy break is identified by CSP, CSP can immediately correct the issue, such as removing a security group violation or turning on CloudTrail for all VPCs. Additionally, if a micro-segmentation rule is accidently or maliciously changed, CSP immediately rollbacks the environment to its compliant state. If rogue network data flows are detected, indicating a malware threat, workloads are quarantined to protect the underlying deployment from breach.

SUMMARY

CSP has been designed to deliver immediate cloud governance value with non-intrusive Audit and Compliance. Extended value is achieved when the audit and compliance information is used to define an intelligent micro-segmentation 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 cloud security policies; this results in dramatic reduction in development time and costs, greatly increases accuracy of controls, and speeds up cloud DevOps, while providing superior security.

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

aws
kubernetes
Azure
vmware
openstack
DATA CENTER

ABOUT US

Used by Security, Dev/Ops and Business teams, the Cloudvisory Security Platform was developed for cloud, hybrid cloud and multi-cloud environments. It was built to deliver the most powerful, complete cloud security governance, micro-segmentation and security orchestration solution available. The only Micro-Segmentation 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.