Cloud Control | CATALINK YOUR CHANGE CATALYST

PRODUCT BRIEF

EASE OF MANAGING SECURITY IN THE CLOUD

C3M's Cloud Control is a 100% API based agentless cloud security and compliance management platform that offers enterprises complete cloud control through actionable cloud security intelligence across AWS, GCP, and Azure. Cloud Control protects cloud environments from the risks of misconfigurations, policy violations, and IAM challenges.

Top challenges faced by organizations in cloud security management are:

- ☑ Lack of visibility.
- ☑ Lack of an effective monitoring and reporting mechanism.
- ☑ Security breaches from misconfigurations and human errors.
- ☑ Ever-evolving compliance framework.
- ☑ Identity and Access Management.

Cloud Control automates cloud security and compliance monitoring and management while helping organizations to enforce cloud security best practices and ensure compliance with applicable security standards and regulations. Enterprises can assess their security posture, detect misconfigurations and threats, and remediate violations.

TARGET AUDIENCE:

SOC Teams:

Real-time alerts along with continuous compliance assessments to help SOC teams respond to threats in near real-time and take quick and informed actions.

Compliance Teams and Auditors:

Automated compliance checks and audits can be run at pre-defined frequencies, ensuring continuous compliance to best practices along with audit capabilities. Auditors can view security and compliance posture in real-time and download assessment reports for authorized cloud accounts.

IAM Administrators:

Management of user permissions and privileges and monitoring of user and service account activities become easier. IAM reports can also be generated, thereby giving the IAM administrator complete control over user activities, identities, and their privileges.

CLOUD CONTROL FEATURES

☑ Security Governance for AWS, GCP, and Azure
☑ Cloud visibility and asset inventory
☑ Continuous cloud compliance and reporting -ISO 27001, PCI DSS, GDPR, NIST, CIS Benchmarks, GLBA, and HIPAA
☑ Automated Policy Remediation
☑ Network topography visualization
☑ Cloud Query Language
☑ Custom Policies and Packages
☑ Cloud Identity and Access Management
☑ Resource Grouping
☑ Integrations with Splunk, Slack, and Jira

SOLUTIONS

CLOUD SECURITY

Being in the public cloud means that the responsibility of security is shared between the cloud service provider and the enterprise. Cloud Control discovers assets and sensitive data across AWS, GCP, and Azure, and detects misconfigurations, data leakage, and vulnerabilities while also monitoring compliance with out-of-the-box policies. Cloud Control implements policy guardrails that will detect risks in real-time and remediate the risks keeping assets and data protected while catering to the needs of the dynamic public cloud environments.

COMPLIANCE

Cloud Control offers industry and geography-specific compliance, enabling enterprises to mitigate the risk of non-compliance by providing a compliance process that is dynamic and easy to implement. A compliance report is only a click away, and this makes reporting to the management and board easier. Cloud Control ensures compliance with regulatory standards and best practices such as:

ISO 27001

ISO 27001 is the international standard that defines requirements for an Information Security Management System. Being compliant with ISO 27001 is proof of the enterprise's adherence to industry best security practices. ISO 27001 is industry agnostic and applies to any enterprise where the protection of information is critical.

PCI-DSS

The Payment Card Industry Data Security Standards (PCI-DSS) sets the operational and technical requirements for any entity that stores, processes or transmits cardholder data. These standards also apply to software developers and manufacturers of applications and devices used in such transactions. In case of non-compliance fine can be up to 100,000 USD per month or 500,000 USD per incident.

HIPAA

Health Insurance Portability and Accountability Act ("HIPAA") mandates health care providers and their business associates to develop and follow procedures that ensure the confidentiality and security of protected health information (PHI) when it is transferred, received, handled, or shared irrespective of their form. Fine for non-compliance is up to 1.5 Million USD per violation per year.

NIST

National Institute of Standard and Technology's ("NIST") provides a cybersecurity framework to enable more significant development and application of practical, innovative security technologies and methodologies that enhance US's ability to address current and future computer and information security challenges.

GLBA

The Gramm-Leach-Bliley Act ("GLBA") mandates that financial institutions – companies that offer consumers financial products or services like loans, financial or investment advice, or insurance – should explain their information-sharing practices to their customers and safeguard sensitive data. Non-compliance can cost an enterprise fine of up to 100,000 USD for each violation; its officers and directors up to 10,000 USD for each violation and 5 years imprisonment.

CIS

The Center for Internet Security ("CIS") has defined a set of controls and benchmarks for cloud service providers to enable enterprises to safeguard systems against the ever-evolving threats.

GDPR

The General Data Protection Regulation (GDPR) is an EU regulation that sets out stringent standards on controlling and processing data, and a fine of 20 million Euros or 4 percent of annual global turnover, whichever of both is highest. It applies to all enterprises that deal with data of EU citizens.

Cloud Control offers customized security and regulatory compliance depending on the industry and business of an enterprise.

AUTOMATION

Enterprises spend a lot of time and effort in managing their security. Cloud Control enables enterprises to bring onboard better efficiency and productivity by automating security in the cloud. Cloud Control allows a business to be agile and secure by automatically assessing the security posture, identifying vulnerabilities and violations, and offering remediation by pre-configured and customizable security policies.

IDENTITY AND ACCESS MANAGEMENT

The biggest challenge faced by enterprises in the cloud is the lack of insights into:

☑ What identities have access to cloud resources?

☑ What are the privileges these identities have?

☑ Are any of these identities over-provisioned?

☑ Who are the privileged users, and do they use their privileges?

Cloud Control enables enterprises to gain granular control and manage identity privilege across the public cloud environment. Enterprises are empowered with the ability to enforce the principle of least privilege ensuring users and identities have the necessary privileges to perform their day to day operations but nothing more.

VISIBILITY

Cloud Control gives a single pane of glass view to oversee and gain insights into the security and compliance posture across the public cloud environment. Cloud Control does an asset inventory to give enterprises a bird's eye view into all the cloud assets thereby giving them complete visibility into cloud. Enterprises can also gain complete visibility over their network topology by way of a unique and easy to understand visualization. The visualization also enables enterprises to continuously monitor their topology, map out the traffic, and gain real-time insights to identify vulnerabilities, their source, and channel of entry.

INTEGRATIONS

Cloud Control integrates with popular productivity, ticketing and SIEM tools such as Slack, Splunk, Jira etc., to aggregate information that is essential to create valuable insights for the SOC team in detecting and responding to incidents.

AUDIT TRAIL

Cloud Control offers accurate, readily accessible, and a complete log of historical cloud compliance information, enabling enterprises to have proper internal business controls. The audit trail gives complete visibility into history of operation of the cloud including the "who, what, when and where." In the event of a violation or incident, audit trails can be used to identify who was responsible for the violation/vulnerability and the events that lead to it.

REPORTING

Cloud Control enables enterprises to perform cloud security and compliance posture assessment of their cloud infrastructure and generate audit reports of their current security and compliance. Reports can be generated one-time or can be produced at predefined intervals and customized according to the needs of an enterprise. The SOC teams at an enterprise can use these reports to take necessary actions to rectify any risks, and these reports may be submitted to their boards to showcase their security and compliance posture.

Contact Us : cloudsecurity@catalink.com.au | www.catalink.com.au