TELUS Cloud Security Posture Management

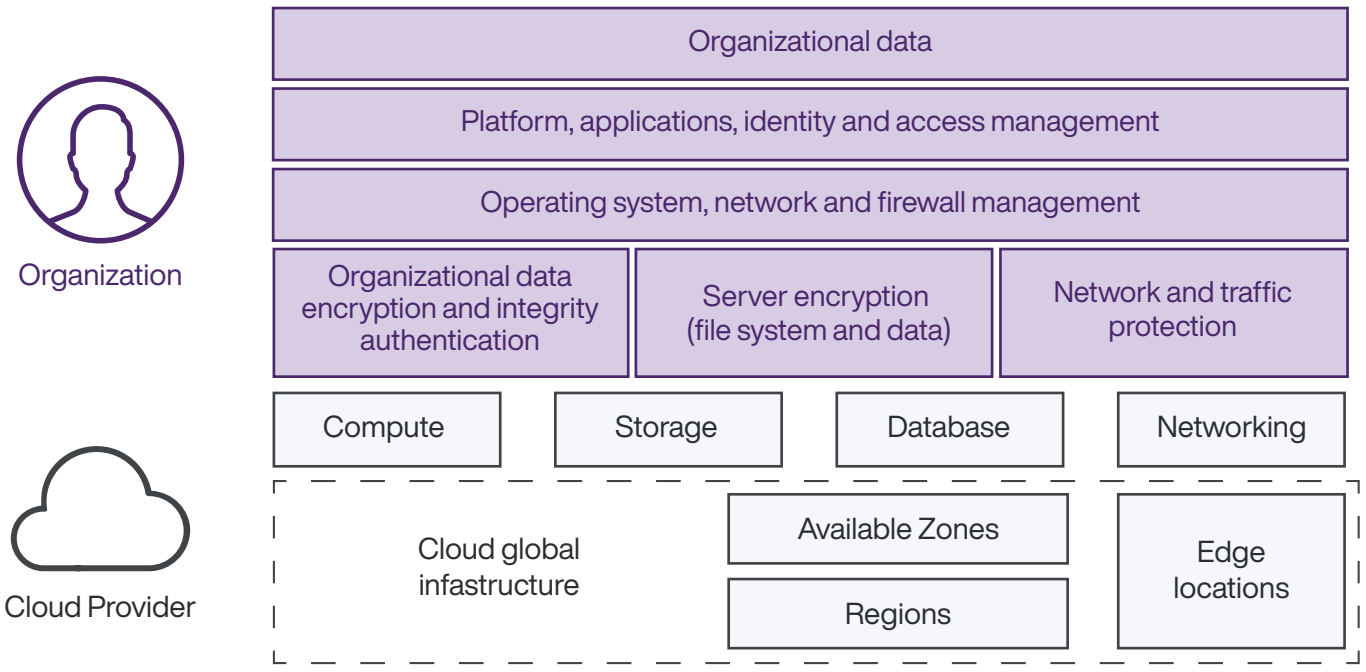
Ensure secure implementation, management and compliance of your cloud environments

Organizations are adopting cloud services at a rapid pace and security teams are struggling to keep up.

When moving to the cloud, organizations often assume their hosting provider is responsible for security. This mistaken belief can lead to data breaches and other security incidents due to lack of awareness and misconfigurations.

The reality is that both the organization and provider have a role to play. A cloud provider's role is to secure the infrastructure cloud stack – the security of the cloud. Meanwhile, organizations are responsible for security in the cloud, configuring the cloud and securing applications and data.

The Shared Responsibility Model



TELUS Business

Organizations face several key security challenges in the public cloud, including:

- Protecting an increased attack surface
- Lack of visibility and tracking
- Managing ever-changing workloads
- Managing access (granular privilege and key management)
- Managing multi-cloud environments
- Meeting compliance and regulatory deployments

Not to mention, it's expensive to train and maintain monitoring specialists in-house for your cloud deployments.

Gain visibility, mature your cloud security posture, and simplify the complexity of managing multi-cloud environments

With the number of cloud resources on the rise, many organizations don't know how many cloud resources are running and how they're all configured. This lack of visibility can allow misconfigurations to go undetected, increasing the risk of an incident.

The TELUS Cloud Security Posture Management (CSPM) service provides organizations with a complete view of their cybersecurity posture across their cloud environments. The service enables the smooth transition and intelligent provisioning of cloud applications, ensures consistent security configuration, continuously monitors to detect misconfigurations, and provides recommendations for remediation and configuration of new cloud features. The TELUS Cloud Security Posture Management (CSPM) service ensures that organizations have the information they need to mature their cloud security posture.

Realize return on your investment by:

- Gaining visibility across your multi-cloud environment and identifying blindspots or misconfigurations that could put your organization at risk
- Simplifying the complexity of managing security at cloud speed with one tool for multi-cloud management
- Achieving and maintaining compliance across all of your cloud environments and ever-changing cloud workloads
- Detecting and remediating problem areas with continuous configuration assessments, risk analysis, and automatic remediation of security policy violations and misconfigurations

The 5 pillars of the TELUS Cloud Security Posture Management service

Security Policies - Develop and implement consistent security policies across your cloud environments that align with compliance frameworks and best practices (i.e. SOX, PCI DSS, GDPR, and HIPAA, etc.)

Visibility - Provide a complete view of your cloud assets and how they are configured.

Monitoring and Detection - Continuous monitoring of configuration changes with impact analysis and immediate reporting of modifications that are outside of acceptable security parameters.

Enforcement - Automated remediation of security policy violations.

Compliance Reporting - Report and monitor compliance against security standards and best practices

For more information, contact your Account Manager or email cybersecuritymarketing@telus.com

TELUS Business