HCLTech | Google Cloud

HCLTech Google Cloud Platform Security

Building dynamic and resilient cloud enterprise ecosystems on the Google Cloud Platform

Overview

Google Cloud Platform (GCP) is used by organizations across the globe as they step into a cloud-first paradigm with a remote workforce and digital workloads. But as adoption rates rise, so do the threats from cyberattacks. Recent trends have shown that the threat to this growth is continually rising, with 98% of organizations having experienced at least one cloud breach over 2021-22.

Securing an enterprise's Google Cloud Platform can help unleash its full capabilities and help businesses achieve an agile, responsive, and intelligent enterprise cloud ecosystem designed to solve the modern business challenges.

Mitigating these threats requires a new and sophisticated approach such as HCLTech's Cloud-Security-as-a-Service (CSaaS) with its Borderless Security Framework. Now, enterprises can leverage HCLTech' CSaaS with their Google Cloud Platform to experience an effcient, quick, and agile method to securing their cloud ecosystem.

As cloud becomes a business imperative, enterprises are rapidly realizing the various gaps and obstacles that hinder their security posture. This includes:

Lacking comprehension of key security use cases

Most companies misalign their security use cases with their specific business risk requirements leading to a misunderstanding consumption and outcomes.

Security attacks and breaches due to misconfigured controls

Targeted security attacks result in data loss and theft due to weakly configured cloud security controls which exploit errors and vulnerabilities in the cloud deployment.

Lack of security and transformation expertise

The ever-changing nature of the cloud needs skilful architects that can design security architecture for rising workloads demand and understand emerging security innovations.

Budget constraints

Most IT organizations are still adapting to a post-pandemic paradigm and re-evaluating their strategic IT spend leading to myopic errors in areas like cloud security investments.

Lacking security of modernized applications

The shift to dynamic development, with continuous integration & deployment, Functions-as-a-Service, and distributed serverless architectures, requires embedded security in the SDLC.

Ineffective user access monitoring and controls

Cloud platforms are increasingly more complex as users and endpoints exponentially rise. This leads to critical user access control issues and greatest major security vulnerabilities.

Our solution

HCLTech Cloud Security-as-a-Service and Borderless Security Framework, can assess and cater to the specific needs of global enterprises. It provides a comprehensive, 360o services approach of Strategy, Consulting & Architecture, Transformation & Integration, and Managed Security Services. The Google Cloud Platform Security offerings include:

1. GCP Landing Zone Security

- Unified/simplified tenancy structure for least privilege, governance policies, and Segregation of Duties
- Unified identity across environments
- Shared VPC for connectivity and segregated network control
- Interface to on-prem with Direct Interconnect
- Protection against DDoS and external threats
- Automated centralized logging across projects for monitoring and threat analysis
- Data segregation and security to ensure compliance with data protection standards
- Environment designed based on Zero Trust principles

2. Risk and Compliance as Code (RCaC)

- Reduces organizational risk by modernizing governance and compliance functions
- Integrated offering with secure foundation building pre-deployment and "Detect, Prevent, & Remediate" capabilities post-deployment
- Leverages various GCP products such as Assured Workload, Security Command Center+, and Risk Protection Program
- Onboards HCLTech Platforms & Service Enablers such as Cloud Native SIEM/SOAR, Cloud Fusion Portal, and IaC Security Platform
- Establishes foundational blueprints of Secure Foundation, Secure Data Warehouse, GKE blueprints, and FedRAMP
- Enables continuous improvements with Google enabled workshops and best practices for security organization transformation and DevSecOps transformation

3. Infrastructure as Code (IaC)

- Engages technologies and processes to help manage and provision infrastructure using sophisticated software solutions
- Enables continuous compliance, continuous risk assessment, data encryption, and automates monitoring & alerts
- Secures all the stages of continuous integration and continuous development pipeline, from source to build to test to deploy
- Provides access to essential code tools such as Ansible, Terraform, CloudFormation from AWS, and Pulumi

4. GCP Assessment and Advisory

- Covers various security standards and frameworks, while also documenting existing controls which helps establish greater visibility of gaps and strengths in the system
- Provides customized recommendations and best practices to align with the specific capabilities and controls weakening the cloud ecosystem
- Benchmarks current controls and practices against best-in-class standards to assess the security posture of the organization
- Assesses effectiveness of current cloud security policies and their alignment with organizational business goals

Value Delivered

Compliance with data protection standards

Reduced organizational risk by modernizing governance and compliance functions

Continuous improvements with Google enabled workshops

Continuous configuration assurance

Alignment of security strategy with the business goals and risks

Roadmap to improve security posture

To know more about the offering, write to us at: **Cybersecurity-grc@hcl.com**

HCLTech | Supercharging Progress™

BE-112206AII8220282-EN00GL

hcltech.com