SAVIYNT

DATA SHEET

GOOGLE CLOUD PLATFORM (GCP)

MANAGE IDENTITY. SECURE ACCESS. PROVE GOVERNANCE.

CLOUD SECURE: Own Your Responsibility

As enterprises adopt Cloud First or Cloud Only for flexibility and speed, they migrate workloads to IaaS providers like Google Cloud Platform (GCP). Under the Shared Responsibility Model, providers secure access to the cloud, while customers must secure authorized identity and access within the cloud. Migrating workloads to the cloud is new territory for many enterprises, and the security pitfalls are not as well-known as they were in the on-premises data center.

As the enterprise embraces cloud migration, it often incorporates more than one cloud service provider, each with its own management console and monitoring capabilities.

This leads to the organization managing cloud security from multiple dashboards. The speed of the IaaS environment, however, complicates risk reviews needed for identity governance and administration (IGA) as well as privileged access management (PAM).

To review risk, organizations need visibility into their ecosystem, yet IaaS environments inherently reduce insight. The volume and velocity of interconnected users, workloads, and processes in GCP lead to IGA risks arising from:

- **Complex Identities:** VPCs, subnets, databases, and data object.
- **Interconnected Relationships:** robotic processes and enterprise systems (HRMS, DLP) work together.
- **Escalated Just-in-Time Privileges:** DevOps Security.

VIEW

CONSOLIDATE

REMEDIATE

MITIGATE

Creating risk-based policies sounds simple, but a single project member account can compromise the entire infrastructure. Creating a single-point-in-time risk tolerance fails as the enterprise adds more accounts and users.

- **Joiner/Mover/Leaver:** Expired users create data breach risk
- **Application Access:** Segregation-of-Duties management
- **File Access:** Maintaining Least Privilege Necessary
- **Workloads:** Dynamic access requirements and sensitive data
- **Shadow IT:** Users granting access without administrator knowledge

SAVIYNT, INC. (Headquarters) 1301 E. El Segundo Bl, Suite D, El Segundo, CA 90245, United States **Tel. 310. 641. 1664** **www.saviynt.com** | info@saviynt.com

MATURE

Monitoring data access as a middle-man provides insight into paths and traffic. Securing access requires the enterprise to mature its IGA programs:

- **Assure:**
  Right access to the right environment
- **Rationalize:**
  Review access for ongoing need
- **Organize:**
  Prevent multiple identities and groups with the same access

AUTOMATE & ASSURE:
Stay Secure. Stay Compliant.

Identity governance and administration is no longer "set and forget." The cloud's dynamic nature means, companies need dynamic solutions that enable protection and documentation.

- **Stay Secure.**
  Continuously monitor to discover and remediate new risks
- **Stay Compliant.**
  Proving governance and compliance keeps your company safe from penalties and fines.

Saviynt enables real-time risk identification across the GCP implementation, access lifecycle management process automation and security policy enforcement. The comprehensive, cloud-native offering extends to and secures DevOps platforms such as Chef, Puppet, Ansible and Jenkins.

Risk Discovery

- Automate the identification of over 80 risks across GCP IAM and DevOps resources such as VM, Buckets, Firewall, VPC Network, Kubernetes Engine and Cloud SQL
- Integrated access analysis and remediation recommendations
- Support for multiple GCP Organizations

Security Intelligence

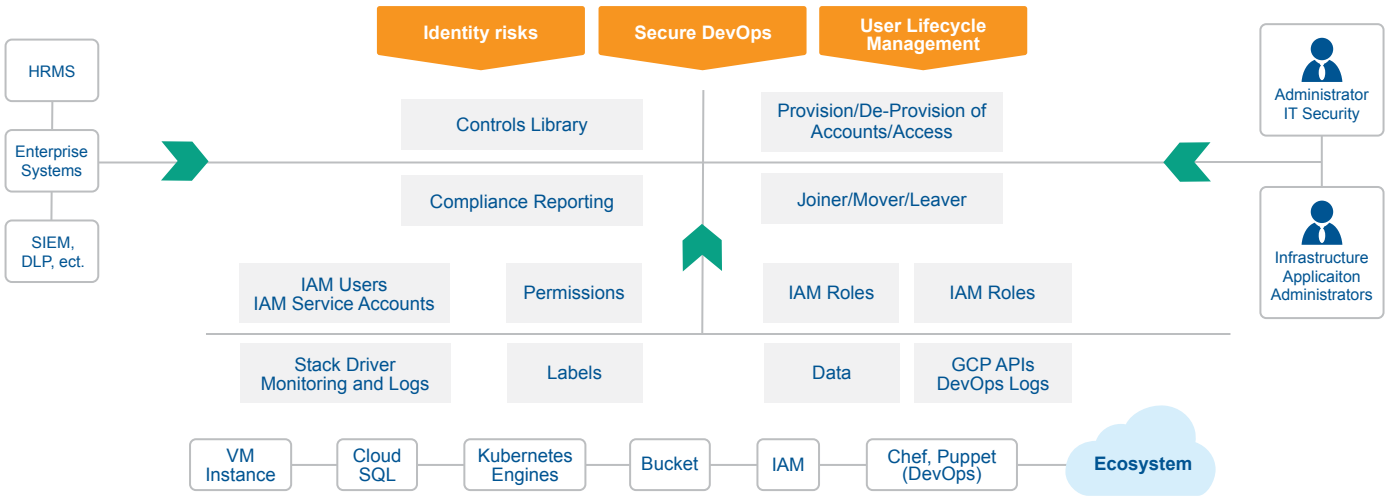
- Prioritized, risk dashboards for actionable investigations
- Behavioral pattern analysis and peer comparison to detect outliers and unknown/ insider threats

Access Management

- Provision and de-provision accounts and access. Automatic provisioning of access based on authoritative HRMS feeds
- Life Cycle Management of users - Joiners/ Movers/Leavers

Compliance Controls

- Out-of-box mapping of controls to compliance regulations such as CIS Foundation, PCI etc.
- Provide recommendations for remediation of risk



SAVIYNT, INC. (Headquarters) 1301 E. El Segundo Bl, Suite D, El Segundo, CA 90245, United States **Tel. 310. 641. 1664** **www.saviynt.com** | info@saviynt.com