Security and Identity

**Security**

**Access Transparency**: Access Transparency captures near real-time logs of manual, targeted accesses by Google administrators, and serves them to customers via their Cloud Logging account.

**Assured Workloads:** Assured Workloads provides functionality to create security controls that are enforced on your cloud environment. These security controls can assist with your compliance requirements (for example, FedRAMP Moderate).

**Binary Authorization**: Binary Authorization helps customers ensure that only signed and explicitly-authorized workload artifacts are deployed to their production environments. It offers tools for customers to formalize and codify secure supply chain policies for their organizations.

**Certificate Authority Service:** Certificate Authority Service is a cloud-hosted certificate issuance service that lets customers issue and manage certificates for their cloud or on-premises workloads. Certificate Authority Service can be used to create certificate authorities using Cloud KMS keys to issue, revoke, and renew subordinate and end-entity certificates.

**Certificate Manager**: Certificate Manager provides a central place for customers to control where certificates are used and how to obtain certificates, and to see the state of the certificates.

**Cloud Asset Inventory**: Cloud Asset Inventory is an inventory of cloud assets with history. It enables users to export cloud resource metadata at a given timestamp or cloud resource metadata history within a time window.

**Cloud Data Loss Prevention:** Cloud Data Loss Prevention is a fully-managed service designed to help you discover, classify, and protect your most sensitive data. You can inspect, mask, and de-identify sensitive data like personally identifiable information (PII).

**Cloud External Key Manager (Cloud EKM):** Cloud EKM lets you encrypt data in Google Cloud Platform with encryption keys that are stored and managed in a third-party key management system deployed outside Google's infrastructure.

**Cloud HSM:** Cloud HSM (Hardware Security Module) is a cloud-hosted key management service that lets you protect encryption keys and perform cryptographic operations within a managed HSM service. You can generate, use, rotate, and destroy various symmetric and asymmetric keys.

**Cloud Key Management Service:** Cloud Key Management Service is a cloud-hosted key management service that lets you manage cryptographic keys for your cloud services the same way you do on premises. You can generate, use, rotate, and destroy AES256, RSA 2048, RSA 3072, RSA 4096, EC P256, and EC P384 cryptographic keys.

**Event Threat Detection**: Event Threat Detection helps detect threats in log data. Threat findings are written to Security Command Center and optionally to Cloud Logging.

**Key Access Justifications (KAJ):** KAJ provides a justification for every request sent through Cloud EKM for an encryption key that permits data to change state from at-rest to in-use.

**Risk Manager**: Risk Manager allows customers to scan their cloud environments and generate reports around their compliance with industry-standard security best practices, including CIS benchmarks. Customers then have the ability to share these reports with insurance providers and brokers.

**Security Command Center:** Security Command Center is Google Cloud’s centralized vulnerability and threat reporting service. Security Command Center provides asset inventory and discovery and allows you to identify misconfigurations, vulnerabilities and threats, helping you to mitigate and remediate risks.

**VPC Service Controls:** VPC Service Controls provide administrators the ability to configure security perimeters around resources of API based cloud services (such as Cloud Storage, BigQuery, Bigtable) and limit access to authorized VPC networks, thereby mitigating data exfiltration risks.

**Secret Manager:** Secret Manager provides a secure and convenient method for storing API keys, passwords, certificates, and other sensitive data.

**Web Security Scanner**: Web Security Scanner is a web application security scanner that enables developers to easily check for a subset of common web application vulnerabilities in websites built on App Engine and Compute Engine.