Identity & Access

**Access Approval**: Access Approval allows customers to approve eligible manual, targeted accesses by Google administrators to their data or workloads before those accesses happen.

**Access Context Manager**: Access Context Manager allows Google Cloud organization administrators to define fine-grained, attribute based access control for projects, apps and resources.

**BeyondCorp Enterprise**: BeyondCorp Enterprise is a solution designed to enable zero-trust application access to enterprise users and protect enterprises from data leakage, malware and phishing attacks. BeyondCorp Enterprise is an integrated platform incorporating cloud-based services and software components, including:

* **On-premises Connector**, which forwards Identity-Aware Proxy traffic from Google Cloud Platform to applications and VMs deployed in non-Google Cloud Platform environments.
* **BCE app connector**, which provides secure access to private applications in non-Google cloud environments using a remote agent installed on a customer-owned virtual machine.
* **BCE client connector**, which provides end users secure access to private non-web applications using a remote endpoint agent installed on customer endpoint devices.
* **Endpoint Verification**, which allows administrators to build an inventory of devices and set the security posture of the devices.
* **Threat and Data Protection Services**, which are a set of security services that work by aggregating threat intelligence and are designed to protect enterprise users from malware transfers, phishing, malicious site visits, and sensitive data leakage.
* **BeyondCorp Enterprise Integration with Chrome Browser Cloud Management**, which enables malware, phishing, and data leakage protection for managed Chrome browsers.
* Other features listed at <https://cloud.google.com/beyondcorp-enterprise/pricing> or a successor URL.

**Cloud Identity Services**: Cloud Identity Services are the services and editions as described at: [https://cloud.google.com/terms/identity/user-features.html](https://cloud.google.com/terms/identity/user-features) or such other URL as Google may provide.

**\*Firebase Authentication**: Firebase Authentication provides a service as part of the Firebase platform to authenticate and manage users in your applications. It supports authentication using email & password, phone number and popular federated identity providers like Google and Facebook.

**Google Cloud Identity-Aware Proxy**: Google Cloud Identity-Aware Proxy is a tool that helps control access, based on a user's identity and group membership, to applications running on Google Cloud Platform.

**Identity & Access Management (IAM)**: IAM provides administrators the ability to manage cloud resources centrally by controlling who can take what action on specific resources.

**Identity Platform**: Identity Platform provides you with functionality and tools to manage your users' identities and access to your applications. Identity Platform supports authentication and management of users with a variety of methods, including email & password, phone number, and popular federated identity providers like Google and Facebook.

**Managed Service for Microsoft Active Directory (AD)**: Managed Service for Microsoft Active Directory is a Google Cloud service running Microsoft AD that enables you to deploy, configure and manage cloud-based AD-dependent workloads and applications. It is a fully-managed service that is highly available, applies network firewall rules, and keeps AD servers updated with Operating System patches.

**Resource Manager API**: Resource Manager API allows you to programmatically manage Google Cloud Platform container resources (such as Organizations and Projects), that allow you to group and hierarchically organize other Google Cloud Platform resources. This hierarchical organization lets you easily manage common aspects of your resources such as access control and configuration settings.