

# Google Cloud Identity

## G-Cloud 15 – Service Definition

---

Google Cloud Identity – A unified identity, access, app, and endpoint management (IAM/EMM) platform that helps IT and security teams maximise end-user efficiency, protect company data, and transition to a digital workspace. Google grade security enables users one click access and protects user and company data.

|                                            |   |
|--------------------------------------------|---|
| Google Grade Security                      | 2 |
| User and IT Simplicity                     | 2 |
| Meeting you where you are                  | 2 |
| Single Sign On                             | 2 |
| Multi Factor Authentication                | 2 |
| Endpoint Management                        | 2 |
| Features                                   | 3 |
| Account Security                           | 3 |
| Device Security                            | 3 |
| Digital Workspace                          | 3 |
| Unified Management Console                 | 3 |
| Automated user provisioning                | 3 |
| Hybrid Identity Management                 | 4 |
| Context Aware Access                       | 4 |
| Account takeover protection                | 4 |
| Technical Support                          | 4 |
| Password-vaulted apps                      | 4 |
| Advanced Protection Program                | 4 |
| Integration with Applications              | 4 |
| Service Definition Details                 | 5 |
| Business continuity and disaster recovery  | 5 |
| Onboarding and offboarding support         | 5 |
| Implementation plans                       | 5 |
| Pricing                                    | 6 |
| Service constraints                        | 6 |
| Compensation if service levels are not met | 6 |
| The ordering and invoicing process         | 6 |
| Terminating a contract                     | 7 |
| After sales support                        | 7 |
| Technical requirements                     | 7 |
| Contact Information                        | 7 |

# Google Grade Security

Defend your organisation with the BeyondCorp security model and Google's threat intelligence signals. Control access to SaaS apps, enforce strong multi-factor authentication (MFA) to protect user accounts, manage endpoints, and investigate threats with Security Center.

## User and IT Simplicity

Maximise efficiency by enabling intuitive user experiences on endpoint devices, and unify user, access, app, and endpoint management with a single console. Enable users to access thousands of apps with single sign-on (SSO) and manage their company accounts using the same process as their personal Google accounts.

## Meeting you where you are

Transition to digital by integrating your existing systems on a reliable, trusted platform. Extend your on-premises directory to the cloud with Directory Sync, enable access to traditional apps and infrastructure with secure LDAP, and automatically synchronise user information with HR systems of record.

## Single Sign On

Give users one-click access to apps

Enable employees to work from virtually anywhere, on any device, with single sign-on to thousands of SaaS apps, including Salesforce, SAP SuccessFactors, Google Workspace, and more. [Learn more](#)

## Multi Factor Authentication

Protect user and company data

Keep user accounts safer with push notifications, one-time passwords, and enforcing the use of phishing-resistant security keys for high-value users and applications.- [Learn more](#)

## Endpoint Management

Enforce policies for personal and corporate devices

Set up devices in minutes and keep your company data more secure with endpoint management for Android, iOS, and Windows 10 devices. – [Learn More](#)

## Features

### Account Security

Help to protect users from phishing attacks with Google's intelligence and threat signals and multi-factor authentication (MFA), including push notifications, Google Authenticator, phishing-resistant Titan Security Keys, and using your Android or iOS device as a security key.

### Device Security

Improve your company's device security posture on Android, iOS, and Windows devices using a unified console. Enforce security policies, wipe company data, deploy apps, view reports, and export details.

### Digital Workspace

Enable employees to get up and running quickly with a digital workspace – login once and access 5000+ apps, including pre-integrated SAML 2.0 and OpenID Connect (OIDC) apps, custom apps, and on-premises apps.

### Unified Management Console

Use a single admin console to manage user, access, app, and device policies, monitor your security and compliance posture with reporting and auditing capabilities, and investigate threats with Security Center.

### Automated user provisioning

Reduce administrative overhead involved in managing your users in individual third-party cloud apps by automating user provisioning to create, update, or delete user profile information in one place and have it reflected in your cloud apps.

## Hybrid Identity Management

Increase the ROI of your existing investments by extending your Microsoft Active Directory (AD) users to the cloud with Directory Sync and enabling simpler user access to traditional apps and infrastructure with secure LDAP.

## Context Aware Access

A core component of Google's BeyondCorp security model, context-aware access enables you to enforce granular and dynamic access controls based on a user's identity and the context of the access request, without the need for a traditional VPN.

## Account takeover protection

Strengthen user security with Google's automatic multi-layered hijacking protection. Detect anomalous login behaviour and present users with additional challenges to prevent account takeovers.

## Technical Support

Get help when issues arise with 24/7 support from a real person. Phone, email, and chat support is available in 14 languages, included with your Cloud Identity subscription.

## Password-vaulted apps

With single-sign on for apps that require a username and password to authenticate and for apps that use modern identity standards like SAML or OIDC, Cloud Identity delivers one of the largest app catalogues in the industry.

## Advanced Protection Program

A constantly evolving and easy-to-use bundle of Google's strongest account security settings, ensuring that your most at-risk users always have the strongest possible protection.

## Integration with Applications

- GMail
- Calendar
- Chat

- Workday
- Asana
- Docusign
- Box
- SAP
- Marketo
- Slack
- Trello
- ServiceNow
- Dropbox
- Zendesk
- Salesforce

## Service Definition Details

### Business continuity and disaster recovery

The Google Chrome Enterprise services offer synchronous replication of customer data and hence user activities within the various components of the suite are simultaneously preserved in multiple secure data centres and on multiple servers within each data centre. If one data centre is unable to serve a customer request, the system is designed to instantly fall back to another data centre that can serve the customer account with no interruption to the service. Backup, restore and disaster recovery of customer data are therefore inherent features of the proprietary architecture underpinning Google's services. There is no planned downtime of the service/s.

### Onboarding and offboarding support

On boarding services are covered by the relevant Netpremacy Cloud Service offerings and are priced according to the published SFIA Rate Tables according to customer requirements (see separate service listings for details of services offered). Customer data extraction and off boarding assistance and advice where required is provided free of charge and is typically available in an open industry standard format but custom data extraction services via product APIs and additional data transformation may be subject to scope and requirements definition.

### Implementation plans

Implementation plans are covered by the relevant Netpremacy Cloud Service offerings and are priced according to the published SFIA Rate Tables according to

specific customer requirements (see separate service listings for details of services offered).

## Pricing

A pricing overview, including volume discounts or data extraction costs –  
See pricing document attached to the service

## Service constraints

Service constraints like maintenance windows or the level of customisation allowed. No planned downtime or maintenance windows are applicable to the Google Cloud services. Configuration and customisation is typically achieved by product settings offered through an admin console or interface, any bespoke customisations are available via rich API set and specific development services subject to scope and requirements. Deprecation of features and functions if applicable are published by the author typically 6 months in advance.

Service levels like performance, availability and support hours All Google products are provided with a 99.9% uptime guarantee, see individual terms of service for specific details. Netpremacy offers an optional Premium Technical Support Service during the hours of 8:30am to 5:30pm – for enhanced support services and the related pricing, please see separate options listed under Cloud Services. Cloud Software products include 24 x 7 vendor support in the licence price by email, chat and phone.

## Compensation if service levels are not met

The financial recompense model for our Google Workspace services is provided by way of service credits and is determined by Google. Please see the relevant Netpremacy Google Workspace Terms and Conditions provided as part of the individual service listing response.

## The ordering and invoicing process

Please contact Netpremacy for individual service order enquiries and for an initial quotation. Each Cloud Software product offered by Netpremacy has specific Terms of Service which are provided in the Service Listing and are referenced in the service Order Form which also gives the service term commitment and total order cost. Invoicing for Cloud Software is raised on order and payable in advance by 30 day terms. Cloud Hosting is invoiced at the end of each month in arrears and is payable within 30 days of invoice. Netpremacy Professional Services engagements are subject to customer requirements and will require direct engagement with our services team for an initial assessment and

recommendations. Each individual project is documented in a Statement of Work and includes a detailed breakdown of the tasks involved and commercials are calculated in accordance with the SFIA Rate Table provided in our service listings. The final SOW is signed by both parties and includes an estimated or confirmed fixed price cost for the project. Services are invoiced either monthly in arrears for Time and Materials billing or based on agreed milestone payments for fixed price billing.

## Terminating a contract

See Terms & Conditions.

The individual termination provisions and notice periods required for each Netpremacy Cloud product and/or service are subject to the individual Terms of Service provided as part of the individual service listing response.

## After sales support

The after sales support for each product is detailed in the individual product listing. Optional Premium Reseller Support is available from Netpremacy (see service listing) but is not mandatory.

## Technical requirements

All Netpremacy Cloud services are accessed via a standard (supported version) internet browser, e.g. Google Chrome.

# Contact Information

Netpremacy Public Sector Team

[publicsector@netpremacy.com](mailto:publicsector@netpremacy.com)

Call: +44 1420 481450