rabco
payroll · time · hr · benefits

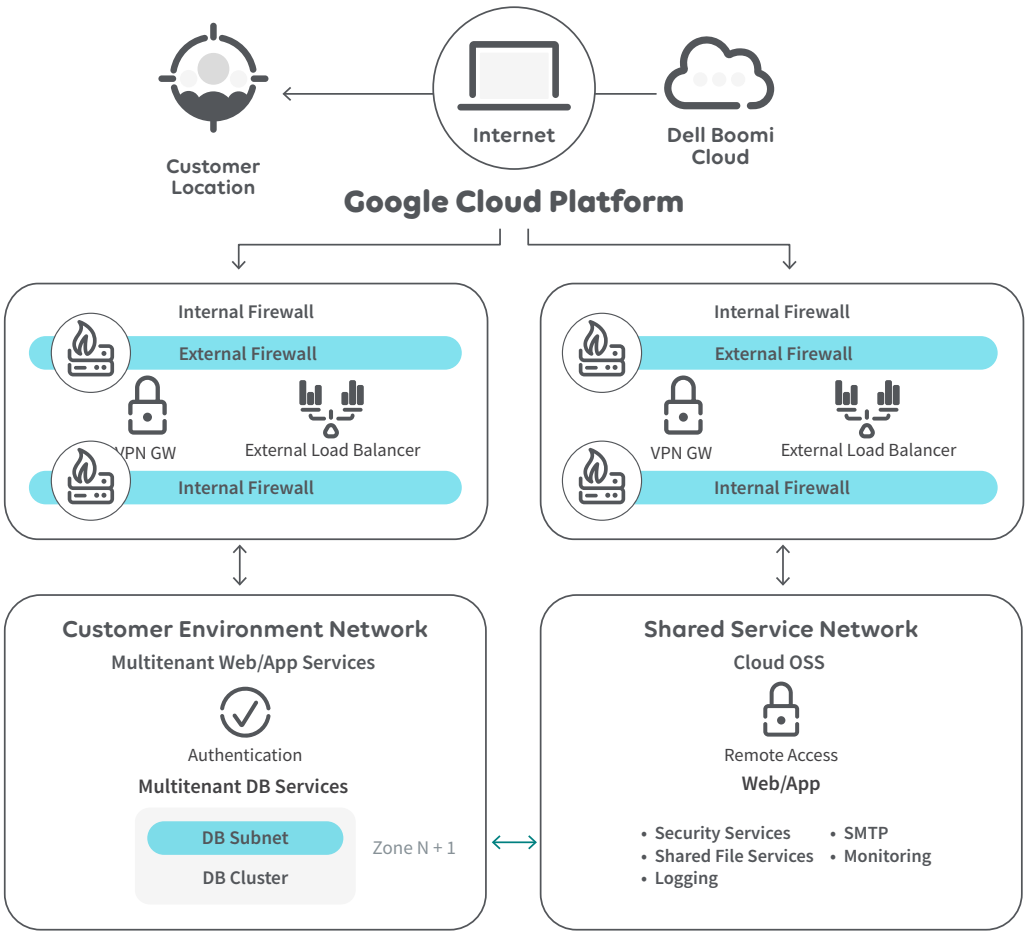
World-Class Infrastructure, Security, and Support

Introduction

Our HCM platform is a full-suite human capital management (HCM) cloud solution that helps you manage your entire workforce from prehire to retire. Its comprehensive tool set integrates HR, payroll, recruiting, benefits administration, workforce management, and more so that you can manage and nurture your organization's most valuable asset, while giving managers single-source access to real-time employee data for engaging employees, attracting top talent, and making more informed business decisions. Offered exclusively as software as a service (SaaS), any module in our HCM platform can be used individually, as part of a complete, integrated solution, or in conjunction with other third-party applications, content, and/or services. We deliver our HCM platform through a single HCM application that is available to you at any time, from anywhere.

The cloud-based HCM solution is the ideal choice for organizations looking to achieve their HCM goals without exceeding their capital equipment budget or placing additional demands on their busy in-house IT staff. Because the platform is hosted in the Google Cloud, you get 24/7 access to your solution without having to purchase additional hardware, operating systems, or database licenses. You gain peace of mind knowing that our experienced technical consultants are managing the solution infrastructure, as well as your applications and employee data, to help ensure high availability, reliable performance, and multilayer security. In addition, because upgrades and add-ons take place in the cloud, you enjoy instant access to the latest software enhancements to help you manage your workforce for optimal results.

Ecosystem



Architecture/System Design

We understand that SaaS offerings must be backed by a world-class technology infrastructure that customers can count on day in and day out. That's why our cloud infrastructure environment features a true multitenant architecture that provides the highest levels of data security, system uptime, and built-in redundancy.

Security and auditing

Our HCM environment has achieved the American Institute of Certified Public Accountants (AICPA) SOC 1 Type II and AT101 SOC 2 Type II criteria for security, availability, and confidentiality. The cloud environment undergoes an annual audit by an independent Tier 1 auditing firm that publishes the SOC Type II reports attesting to the suitability and operating effectiveness of the controls in place. We have certified its compliance with the EU/US Privacy Shield Framework.

System uptime

Our HCM platform works closely with Google to help ensure both the physical security and consistent availability of your data and applications. As a result of these efforts, our uptime has historically measured 99.79% or greater monthly for unscheduled outages.

Uptime architecture and disaster recovery

Our HCM solution's database availability strategy relies on synchronization to maintain copies of its production database on four different servers. This strategy helps ensure that your data, application customizations, and stored code continue to be available even if a database server or Google Cloud site experiences failure. The primary database syncs to a secondary database in real time, and the secondary database syncs to two other databases to provide instant redundancy in the event one server fails.

Full database backup is performed weekly — with incremental backups running daily — to further minimize risk.

- Recovery Point Objective (RPO): 6 hours
- Recovery Time Objective (RTO): 72 hours

Security Policies and Processes

Data security is a top priority, and our team implements policies and procedures designed to protect and safeguard customers' workforce data.

Data collection and encryption options

Your organization's users access the HCM cloud environment from a web browser or mobile device via encrypted Transport Layer Security (TLS) sessions using port 443. Our timeclock terminal connections are Ethernet-based, using port 80 or 443. They can utilize TLS to encrypt data transmission when you provide a digital ID certificate from a third-party vendor. Data at rest is encrypted across the our HCM solution environment by utilizing Transparent Data Encryption.

Secure system login

Users authenticate using a unique password. We use industry-standard, modern hashing algorithms to secure these passwords, and they are never stored in clear text.

You may gain access to our HCM platform via Single Sign-On (SSO). To implement Security Assertion Markup Language (SAML) 2.0, the system requires an X.509 certificate, which may be self-signed. You will also need to provide the entity ID of your Identity Provider, such as ADFS 2.0, and a login redirect URL. Once a user is logged in via SSO, a multifaceted security profile controls the role-based functional and data access rights of supervisors and employees.

Browser support

You may access our HCM applications via a web browser or mobile app provided the following requirements are met:

- Internet Explorer®: Versions 10 or 11
- Edge
- Chrome™/Firefox®/Safari®: Current versions
- Mobile: We have limited support for mobile platforms using the browsers listed above

Mobile app support

Our Mobile app — HCMToGo — runs on the following Apple or Android mobile devices with a data plan or Wi-Fi:

- Apple® iOS: Latest versions
- Android™ OS: 5.0 and higher

Physical and Logical Security Features

Our HCM solution hosts and manages our HCM platform on the ISO 27001 and SSAE 18 Type II compliant Google Cloud Platform with multilevel physical and logical security features, including:

Intrusion Prevention System (IPS)/Intrusion Detection System (IDS): We deploy next-generation firewalls, which restrict network traffic to authorized traffic.

Secure Transmission Sessions: Secure protocol versions TLS 1.2 and above are supported.

Virtual Code Authentication: Our HCM Solution requires virtual code authentication — user name, password, and a system-generated code. Passwords are required to be complex, with a minimum number of characters and expiration at a predefined interval.

Best-Practice Coding: We employ secure coding practices and control processes across application development and software maintenance. Code reviews are conducted regularly to identify potential security flaws.

Penetration Testing: We use a qualified third-party vendor to perform penetration testing annually.

Vulnerability Scanning: We conduct vulnerability scanning using a third-party tool, evaluates identified risks, and develops remediation and/or mitigation plans to address the vulnerability.

Antivirus Software: We deploy a third-party, commercially available antivirus solution on servers to prevent viruses and malware from being deployed in the cloud environment.

Patch Management: We patch our HCM solution environment regularly as a routine part of maintaining a secure cloud infrastructure. Patches are reviewed by our engineers as they are released from the vendors. Approved patches are tested and then deployed to the environment in accordance with our change management policies.

Risk Assessment: We conduct an annual risk assessment of our HCM cloud environment to determine whether the control framework achieves the data privacy and data security objectives.

Security Incident Management: We maintain an escalation procedure to notify appropriate our management staff and customer contacts in the event of a security incident. The event is worked to resolution and a root-cause analysis is performed.

Cloud Services

Support

Our support services provide access to valuable tools and information to help you diagnose and resolve issues quickly and efficiently in order to optimize productivity and realize continuous value from your investment. When our self-help tools aren't enough, our skilled, knowledgeable support professionals — with nearly 10 years of domain experience, on average — are ready to put their expertise to work for you.