



Google Apps Data Security provides for a secure and reliable platform for your data, bringing in the latest technologies and best practices for datacenter management.

Google Apps Data Security

Overview

As part of our mission to organise the world's information, Google is responsible for the safekeeping of data for tens of millions of users. We take this responsibility very seriously, and we have gone to great lengths to live up to the trust of our users. We recognise that secure products are instrumental in maintaining the trust users place in us and strive to create innovative products that both serve their needs and operate in their best interest. Google Apps for Enterprise benefits from this extensive operational experience in producing secure and reliable products.

In particular, Google focuses on several aspects of security that are critical to our enterprise customers;

Protecting your data	Making sure that your data is stored in secure facilities and behind secure servers.
Evading threats	Protecting you and your corporation from malicious attacks.
Safe access	Ensuring that only authorised users can access the data, and that access channel is secure.
Protecting your privacy	Ensuring that your confidential information is kept confidential.
Giving you control	Letting you use your existing methods of protection around our system.
Guarding against disaster	Keeping your data safe in case of unforeseen system failures.
Living up to your trust	Externally audited controls, processes and policies.

This document details what Google Apps for Enterprise offers in each of these areas.

Protecting Your Data

Protection of your data is divided into two key components; physical protection of our datacenters and network security against vulnerabilities. Google operates one of the largest networks of distributed datacenters in the world and we go to great lengths to protect the data and intellectual property on these servers. The datacenters are at confidential, undisclosed locations in order to guard against your data being targeted. These facilities are protected around the clock, and we use strong methods of entry protection to ensure that only our authorised personnel can have access to our servers.

Google has a dedicated security operations team who focus on maintaining the security of our code and platform. Internally, projects are subject to strong security reviews to check for vulnerabilities before deployment. On an ongoing basis, new code is reviewed by multiple developers to check for vulnerabilities. Google servers are also protected by multiple levels of firewalls to protect against attacks.



HEDLOC provides sales, support and services for Google Enterprise IT solutions

For more information visit www.hedloc.com.au/products/collaboration

Google Apps for Enterprise offers a user-friendly interface which operates email and data storage off remote servers, ensuring sensitive information is not stored on a local computer.

Even with all of these levels of protection, unknown vulnerabilities do emerge, and Google is equipped to respond swiftly to security alerts and vulnerabilities. Our security team audits our infrastructure for potential vulnerabilities, and works directly with our engineers to correct any known issues swiftly. We also believe that we cannot do this by ourselves, so we have engaged the larger security community through responsible disclosure. We work in close connection with some of the best security experts in the world to monitor for potential vulnerabilities, listen to identified issues, and correct them.

Evading Threats

Email viruses, phishing attacks and spam are amongst the biggest security threats within corporations today. Reports show that more than two-thirds of incoming mail is spam, and over forty new email viruses are born and distributed throughout the Internet each month. Keeping on top of this can be an overwhelming task, and even corporations with spam and virus filters struggle with keeping these constantly updated to deal with the latest threats.

Google Apps for Enterprise customers benefit from one of the strongest spam and phishing filters in the industry today. Google has developed a filter that learns from patterns in messages identified as spam, and this filter has been trained across billions of mail messages. As a result, we can very accurately identify spam, phishing stacks and viruses, and make sure that your inbox is protected.

Furthermore, through our web-based interface, we enforce virus protection to make sure that users don't spread a virus through your corporation. Unlike a client-based email program, messages are not downloaded to your desktop. Additionally, Gmail will not let a user open an attachment until our virus filters have scanned the attachment. As a result, email viruses cannot take advantage of client-side security vulnerabilities, and users cannot unknowingly open a document with a virus. These filters ensure that users are secure even within the world of email threats.

Safe Access

No matter how secure your data is within a datacenter, this data is no longer secure once it's downloaded to a user's local computer. Studies have shown that the average laptop has over 10,000 files and thousands of downloaded email messages. Imagine if one of these corporate laptops falls into the hands of a malicious user. Simply by mounting a disk, an unauthorised user can get access to your corporation's intellectual property and secrets.

The web-based design of Google Apps for Enterprise allows you to make sure that users have ready access to their data from anywhere while the data remains safely on your servers. Rather than emails being stored on a desktop, users have desktop-quality user interfaces to email while still using a web browser.

Similarly, applications such as Google Docs and Spreadsheets afford you a high level of control over your documents. These documents stay on the server, but the users get rich editing capabilities through the web browser. In addition, users have fine-grained control over who has access to these documents, and they can set up a list of editors and viewers. These permissions are enforced on any access to a document, allowing you to avoid the problem of an internal document getting forwarded outside your corporation by email. Finally, these products track changes at a fine-grained level, letting you have visibility into who made which changes and at what time.

Moreover, we protect the transmission of data on the wire, and make sure that users are accessing data securely without threat of confidential data being intercepted on the network. Google offers HTTPS access to all services within Google Apps for Enterprise, and the product can be set up to only allow HTTPS access. With this functionality, all user access to the data and all interactions are encrypted.



HEDLOC provides sales, support and services for Google Enterprise IT solutions

You have the control to use your existing authentication or log-in system for accessing Google Apps, as well as the power to shut off or delete accounts on demand.

Protecting Your Privacy

Google is very sensitive to a user's privacy, and we ensure with Google Apps for Enterprise that your information is not compromised. Google has a legally binding privacy policy that protects all of our services, and this can be found at; <http://www.google.com/privacypolicy.html>

We assure our users that we will not make this policy any less strict without written permission from our customers.

Giving You Control

In addition to providing these protections on your data, we give you the control to integrate your own security, access, auditing, and authentication methodologies into Google Apps for Enterprise. We provide a single sign-on API based on SAML 2.0, which will let you use your existing authentication mechanism to give users access to Google Apps. You can, for example, use your Active Directory authentication to log in as a user, and the password is not transmitted through Google servers for access to the web-based tools.

In addition, we provide an administration console and API to let you manage your users. You have the power to instantly shut off access to an account or delete an account on demand. This can also be tied to your internal processes for provisioning and deprovisioning a user through the API.

Also, we let you place a mail gateway in front of our mail system. This way, all incoming and outgoing mail goes through you, and gives you the ability to audit and archive mail, as well as put in place supervisory controls. If your corporation has a filter to ensure that confidential material does not get sent out of the enterprise, you can place this filter in front of Gmail.

Guarding Against Disaster

Google provides the ability for your enterprise to keep running in the event of a disaster. Google's datacenter architecture is designed to prevent failure, and we expect and design our software to keep running in the event of a failure.

Data is replicated multiple times across our clustered active servers, so, in the case of a machine failure, your data will still be accessible through another system. In addition, your email data is replicated across datacenters. As a result, if an entire datacenter were to fail or be involved in a disaster, a second datacenter would be able to immediately take over and provide services to your users.

Living Up To Your Trust

Google operates one of the largest networks of distributed datacenters in the world, and we go to great lengths to protect the data and intellectual property on these servers. These facilities are protected around the clock and we have a dedicated security operations team who focuses specifically on maintaining the security of our environment. The controls, processes and policies that protect the data have successfully completed a SAS 70 Type II audit. There are three main components to our security practices:



HEDLOC provides sales, support and services for Google Enterprise IT solutions

Data is replicated in numerous locations to ensure that, in the event of a disaster, your information is always accessible to you from an alternative server.

Protecting Your Privacy

People

Google employs a full-time information security team including some of the world's foremost experts in information, application, and network security. This team is responsible for the company's perimeter defense systems, security review processes, and customised security infrastructure, as well as for developing, documenting, and implementing Google's security policies and standards.

Process

Security is part of the Google DNA. Each application is built from the ground up with security in mind. Google applications go through multiple security reviews as part of the Secure Code development process. The application development environment is closely restricted and carefully monitored to maximise security. External security audits are also regularly conducted to provide additional assurance.

Technology

Google Apps data is fractured and obfuscated across multiple servers and disks, making it human-unreadable. Data is replicated in multiple data centers for redundancy and consistent availability. To reduce exploit risks, each Google server is custom-built with only the necessary software components, and the homogeneous server architecture enables rapid updates and configuration changes across the entire network when necessary.

Our commitment to keeping customer information safe – whether you are a consumer user or our largest enterprise customer – is part of our DNA, and we protect this information as rigorously as we protect our own sensitive corporate information. In fact, we use the very same services that we offer to our users for our own email, documents, project team sites and calendars.

Ever since the first Gmail users began trusting Google with their private information, keeping people's data safe has been one of our top priorities. Today, more than a million businesses, plus thousands of schools and organisations using Google Apps rely on us to safeguard their critical information.



HEDLOC provides sales, support and services for Google Enterprise IT solutions