



Comprehensive review of security and vulnerability protections for Google Apps

A Google white paper February 2007

Security of Google Apps



Securing network-based applications against would-be hackers is key to ensuring the success of any system. When it comes to email and collaboration, the importance is paramount. Google invests billions of dollars in technology, people, and process to ensure data in Google Apps is safe, secure, and private. Google's dedicated team of security professionals is responsible for designing in security from the onset, reviewing all design, code, and finished product to ensure it meets strict Google security and data privacy standards. The same infrastructure used to host Google Apps and secure hundreds of thousands of user's data is also used to manage millions of consumers' data and billions of dollars in advertising transactions. With Google Apps, information is safe and secure.

FOR MORE INFORMATION

Online www.google.com/a

Email apps-enterprise@google.com

INTRODUCTION	3
ORGANIZATIONAL AND OPERATIONAL SECURITY	3
Development Methodology	4
Operational Security	4
Security Community & Advisories	4
DATA SECURITY	4
Physical Security	4
Logical Security	5
Information Accessibility	5
Redundancy	6
THREAT EVASION	6
Spam and Virus Protection	6
Application & Network Attacks	6
SAFE ACCESS	7
End user protections	7
Giving You Control	7
DATA PRIVACY	8
CONCLUSION	8



Introduction

As part of the mission to organize the world's information, Google is responsible for the safekeeping of data for tens of millions of users. This responsibility is taken very seriously, and Google has gone to great lengths to earn and live up to the trust of its users. Google recognizes that secure products are instrumental in maintaining user trust and strives to create innovative products that serve users' needs and operate in their best interest.

Google Apps benefits from this extensive operational experience in producing secure and reliable products. Google's products and services combine advanced technology solutions with industry-leading security practices to ensure customer and user data is secure. Billions of dollars in capital are invested to ensure the most secure, reliable environment for data and applications. In particular, Google focuses on several aspects of security that are critical to business customers:

- Organizational and Operational Security – Policies and procedures to ensure security at every phase of design, deployment and ongoing operations.
- Data Security – Ensuring customer data is stored in secure facilities, on secure servers, and within secure applications.
- Threat Evasion – Protecting users and their information from malicious attacks and would-be hackers.
- Safe Access – Ensuring that only authorized users can access data, and the access channel is secure.
- Data Privacy – Ensuring that confidential information is kept private and confidential

This paper looks at Google's security strategy, which utilizes numerous physical, logical, and operational security measures to ensure the utmost in data security and privacy.

Organizational & Operational Security

The foundation of Google's security strategy starts with its people and processes. Security is a combination of people, processes, and technology, that when put together properly lead to safe and responsible computing. Security is not something that can simply be validated after the fact. Rather, it is designed into products, architecture, infrastructure, and systems from the onset. Google employs a full time security team to develop, document, and implement comprehensive security policies. Google's Security team is made up of some of the world's foremost experts in information, application and network security.

The security team is divided by functional area into perimeter defense, infrastructure defense, application defense, and vulnerability detection and response. Many come to Google with experience in senior information security roles at Fortune 500 companies. This team focuses a large amount of their effort on preventative measures to ensure that code and systems are secure from the onset, and is on call to dynamically respond to security issues

Development Methodology

Google's security posture is top of mind from the moment a product design is drafted. Google engineering and product teams receive extensive training in security fundamentals. Google's development methodology lays out a multi-step plan with ongoing checkpoints and full audits.

The Google Application Security team is involved in all stages of the product development lifecycle including design review, code audit, system and functional testing, and final launch approval. Google uses a number of commercial and proprietary technologies to ensure that applications are secure at every level. Google's Application Security team is also responsible for ensuring that secure development processes are followed to ensure customer safety.

Operational Security

Google's Security Operations team is focused on maintaining security of the operational systems including data handling and system management. These individuals routinely audit datacenter operations and conduct ongoing threat assessment against Google's physical and logical assets.

This group is also responsible for ensuring that all employees are appropriately screened and trained to conduct their job in a professional and secure manner. As appropriate, Google goes to great lengths to screen and verify an individual's background prior to joining the organization. All personnel responsible for maintaining security processes and procedures are thoroughly trained on the practices and continually updated on their training.

Security Community & Advisories

In addition to the processes described above, Google actively works with the security community, leveraging the collective wisdom of the world's best and brightest. This helps Google keep ahead of security trends, quickly react to emerging threats, and harness the expertise of those inside and outside the company. Google actively engages this larger security community through responsible disclosure. Visit <http://www.google.com/corporate/security.html> to find more information about this program and some of the key security experts with whom Google maintains ongoing dialog.

Even with all of these levels of protection, unknown vulnerabilities can emerge, and Google is equipped to respond swiftly to security alerts and vulnerabilities. The Google Security team audits all infrastructure for potential vulnerabilities, and works directly with engineering to correct any known issue immediately. Google Apps Premier Edition customers are notified of user-impacting security issues as soon as practicable via email.

Data Security

The security of company and user data is the mission of Google's Security and Operations teams. Google's business is built on user trust, and therefore this is one of the keys to continued success of Google as a corporation. All Google employees are instilled with the value of responsibility to the end user. Protecting data is at the core of what Google is all about. Google takes great care to protect the billions of dollars of consumer and advertising transactions; we apply that same care to Google's communication and collaboration technologies.

You can see that this is fundamental to who we are as a company by reviewing our code of conduct at <http://investor.google.com/conduct.html>.

Physical Security

Google operates one of the largest networks of distributed datacenters in the world, and goes to great lengths to protect the data and intellectual property in these centers. Google operates datacenters worldwide, and many Google datacenters are wholly owned and managed ensuring that no outside parties can gain access. The geographic locations of the datacenters were chosen to give protection against catastrophic events.. Only select Google employees have access to the datacenter facilities and the servers contained therein, and this access is tightly controlled and audited. Security is monitored and controlled both locally at the site, and centrally at Google's worldwide security operations centers.

The facilities themselves are engineered not only for maximum efficiency, but also for security and reliability. Multiple levels of redundancy ensure ongoing operation and service availability in even the harshest and most extreme of circumstances. This includes multiple levels of redundancy within a center, generator-powered backup for ongoing operations, and full redundancy across multiple dispersed centers. State of the art controls are used to monitor the centers both locally and remotely, and automated failover systems are present to safeguard systems.

Logical Security

In web-based computing, the logical security of data and applications is as critical as physical security. Google goes to extremes to ensure that applications are secure, that data is handled in a secure and responsible way, and that no external unauthorized access to customer or user data can be achieved. To achieve this goal, Google uses a number of industry standard techniques as well as some unique, innovative approaches. One such approach is leveraging special purpose technology as opposed to general-purpose software.

Much of Google's technology is written to provide special purpose capabilities as opposed to general purpose computing. For example, the web server layer is specially designed and implemented by Google to only expose the capabilities required for operation of specific applications. Therefore, it is not as vulnerable to the wide range attacks that most commercial software would be susceptible to.

Google has also made modifications to core libraries for security purposes. Because the Google infrastructure is a dedicated application system rather than a general purpose computing platform, a number of the services provided by the standard Linux operating system can be limited or disabled. These modifications focus on enhancing the capabilities of the system needed for the task at hand and disabling or removing any exploitable aspects of the system that aren't required.

Google's servers are also protected by multiple levels of firewalls to protect against attacks. Traffic is inspected as appropriate for attempted attacks, and any attempts are dealt with to protect users' data.

Information Accessibility

Data such as email is stored in an encoded format optimized for performance, rather than stored in a traditional file system or database manner. Data is dispersed across a number of physical and logical volumes for redundancy and expedient access, thereby obfuscating it from tampering. Google's physical protections described above ensure that no physical access to servers is possible. All access to production systems is conducted by personnel using encrypted SSH (secure shell). Specialized knowledge of the data structures and Google's proprietary infrastructure would be required to get meaningful access to end user data. This is one of many security layers to ensure security of sensitive data within Google Apps.

Google's distributed architecture is built to provide a higher level of security and reliability than a traditional single-tenant architecture. Individual user data is dispersed across a number of anonymous servers, clusters, and datacenters. This ensures that data is not only safe from potential loss, but also highly secure.

User data is only accessible with appropriate credentials, ensuring that there is no possibility of one customer having access to another customer's data without explicit knowledge of their login information. Not only does this proven system serve tens of millions of consumer users with email, calendaring, and documents on a daily basis, but is also used by Google as the primary platform to serve its 10,000+ employee base.

Redundancy

The application and network architecture run by Google is designed for maximum reliability and uptime. Google's grid-based computing platform assumes ongoing hardware failure, and robust software failover withstands this disruption. All Google systems are inherently redundant by design, and each subsystem is not dependent on any particular physical or logical server for ongoing operation.

Data is replicated multiple times across Google's clustered active servers, so, in the case of a machine failure, data will still be accessible through another system. In addition, user 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 users.

Threat Evasion

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, new email viruses are born and distributed throughout the Internet each day. Keeping on top of this can be an overwhelming task, and even corporations with spam and virus filters struggle with keeping these constantly up to date to deal with the latest threats. In addition, network-based applications are the target of malicious attacks attempting to tamper with data or bring down the service. Google's world-class threat evasion protects users from attacks on the data and within the content of their messages and files.

Spam and Virus Protection

Google Apps customers benefit from one of the strongest spam and phishing filters in the industry today. Google has developed advanced technology filters that learn from patterns in messages identified as spam, and these filters are trained continually across billions of mail messages. As a result, Google can very accurately identify spam, phishing attacks, and viruses, and ensure sure that users' inboxes, calendars, and documents are protected.

Through Google's web-based interface, virus protection blocks the threat of unknowing users spreading a virus through the corporation or internal network. Unlike traditional client-based email applications, messages are not downloaded to the desktop. Rather, they are scanned on the server for viruses and Gmail will not allow a user to open an attachment until it has been scanned and any threat mitigated. As a result, email viruses cannot take advantage of client-side security vulnerabilities, and users cannot unknowingly open a document with a virus.

Application & Network Attacks

In addition to filtering the content of data for spam and viruses, Google is continuously protecting itself and customers against malicious attacks. Hackers are always looking for ways to pry into web-based applications or bring them down. Denial of service, IP spoofing, cross site scripting, and packet tampering are just a few of the types of attacks that are used against networks daily. Google, being one of the world's largest providers

of web-based services has gone to great lengths to protect against these and other threats. All software is scanned using a variety of commercial and proprietary network and application scanning packages. The Google Security team also works with external parties to test and enhance Google's infrastructure and application security posture.

Safe Access

No matter how secure data is within a datacenter, this data is vulnerable 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 unauthorized user can get access to your corporation's intellectual property and secrets. Google Apps allows companies to mitigate this risk by avoiding the local storage of data onto users' laptops.

End User Protections

The web-based design of Google Apps allows you to make sure that users have ready access to their data from anywhere while the data remains safely on Google's servers. Rather than emails being stored on a desktop or laptop, users have desktop-quality, highly interactive interfaces for email, calendars, and instant messaging while still using a web browser.

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

Google Apps also protects the transmission of data on the wire, to ensure users are accessing data securely without threat of confidential data being intercepted on the network. Access to the web-based administrative console to Google Apps as well as most end-user applications is offered through a Secure Socket Layer (SSL) connection. Google offers HTTPS access to most services within Google Apps, and the product can be set up to allow only HTTPS access to key services such as email and calendar. With this functionality, all user access to the data and all interactions are encrypted.

At no time does Google use cookies to store passwords or customer data on the user system. Cookies are used for session information and user convenience, but at no time is that information sensitive nor can it be used to break into a user's account.

Giving You Control

In addition to providing these protections on company and user data, Google gives businesses the control to integrate corporate security, access, auditing, and authentication methodologies into Google Apps. Google Apps provides a single sign-on API based on SAML 2.0 which lets companies use existing authentication mechanisms to let users access Google Apps. Businesses can, for example, use Active Directory authentication to log in a user, and the credentials are not transmitted through Google servers for access to the web-based tools. This also allows companies to continue to enforce their password strength and change frequency policies.

In addition, Google provides an administration console and API for user management. Administrators 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.

With respect to email and instant messaging, Google also provides the facility to place a mail gateway in front of the mail system. In this configuration, all incoming and outgoing mail goes through the customers system, and this gives you the ability to audit and archive mail, as well as put supervisory controls in place.

Data Privacy

Google is very sensitive to company and user privacy, and realizes that the data housed within applications is confidential and sensitive. Google ensures with Google Apps that information is not compromised. Google's legally binding privacy policy that protects all services can be found by visiting <http://www.google.com/privacypolicy.html>. Per this policy and related policies for the individual services contained within Google Apps, at no time will Google employees access confidential user data. Google also ensures that this policy will not be altered in any potentially damaging way without express written consent from the customer and/or user.

Conclusion

Google Apps provides a secure and reliable platform for your data, bringing you the latest technologies and best practices for datacenter management, network application security, and data integrity. When you entrust your company's information with Google, you can do so with confidence, knowing that the full weight of Google's technology and infrastructure investment is brought to bear to ensure the security, privacy, and integrity of your data.

For more information about Google Apps, go to <http://www.google.com/a> or email apps-enterprise@google.com.