CloudLock Whitepaper

Security Best Practices for Evaluating Google Apps Marketplace Applications

At a Glance

Intended Audience:

- Security Officers
- CIOs of large enterprises evaluating Google Apps Marketplace applications

Takeaway

- Readers will learn how to assess the trustworthiness of applications and vendors on the Google Apps Marketplace.

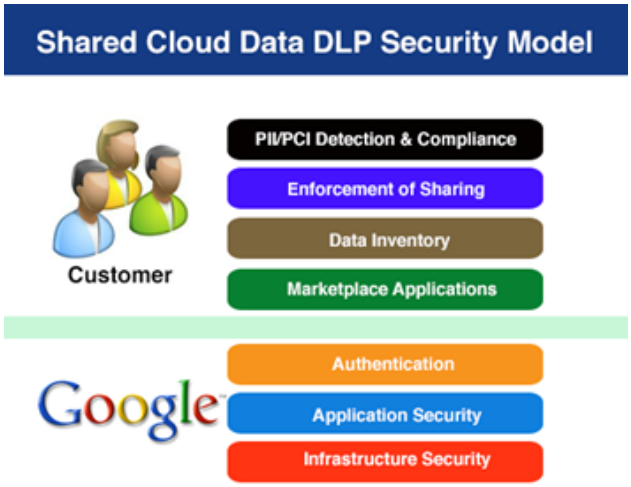
In This Whitepaper:

Introduction

Customers care about the security of their data in the cloud, and security of customer data is obviously important to Google, which is why Google has invested in completing numerous security audits and certifications such as FISMA, SSAE 16, and recently, ISO 27001.

As organizations move their data to the cloud, the most important security question to answer becomes:

"Can I trust the cloud provider to secure and protect my data at least as well as my organization can?"



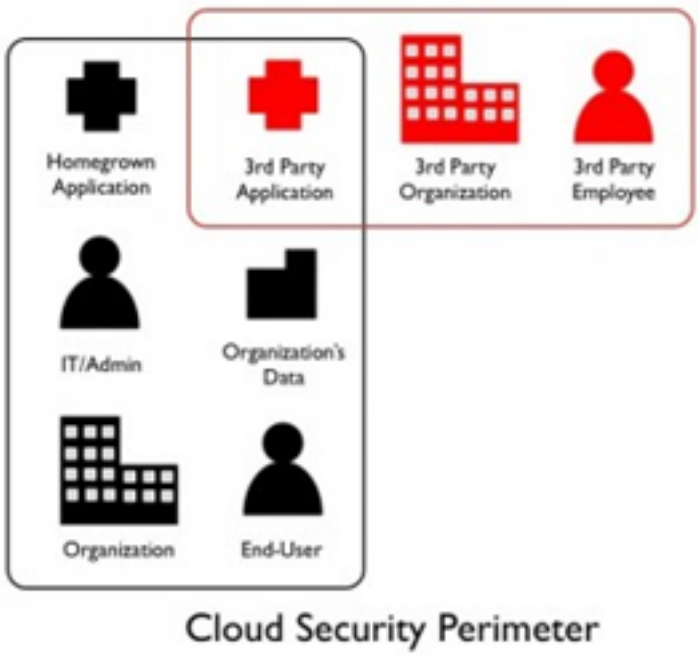
In the case of the Google Apps - the answer is a clear yes. However, the responsibility of protecting data rests not only with Google, but rather is shared between the application provider and the customer.

In the following whitepaper, we will detail the importance of evaluating the security of Google Apps Marketplace applications and vendors, and will give tools to assess the trustworthiness and security of both.

The Importance of Evaluating the Security of Marketplace Applications

One might argue that the real value of Google Apps is not contained to messaging and collaboration, but rather in the ability to transform the way businesses consume applications. This transformation is demonstrated and driven by the Google Apps Marketplace, offering hundreds of applications, broken down into multiple categories, which any Google Apps customer can add to their domain with a click of a mouse.

With great power comes great responsibility, and as enterprise IT Security professionals know, adding Google Apps Marketplace applications extends the security perimeter of the organization to include that application, and the company behind it (including the employees).



With this new method of consuming applications, businesses must understand how to do so securely, without putting their business at risk. Since 'installing' a marketplace application extends the security perimeter of the organization to include the application provider, there are multiple stakeholders that must be considered when evaluating a third-party marketplace application. They can include:

- Internal auditors
- Legal and compliance teams
- Customers (If your company hosts customer data)
- Partners

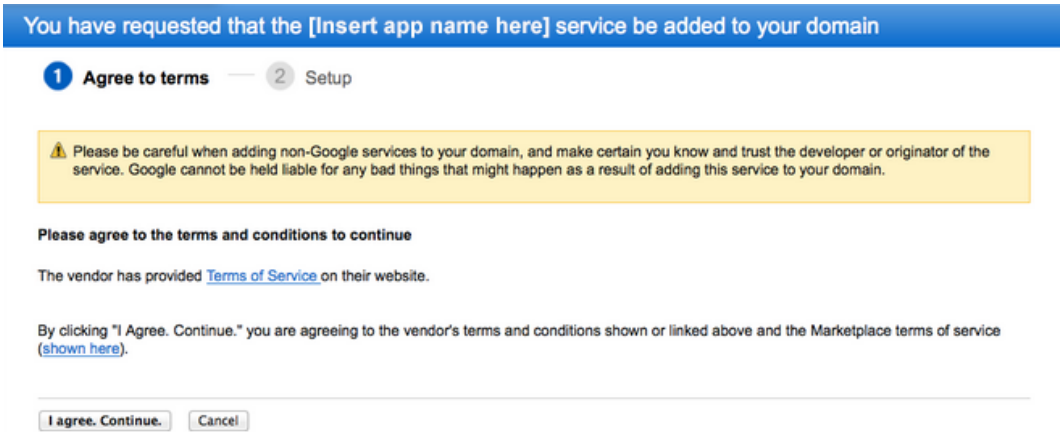
Technical Explanation of Installing a Marketplace Application

Technically speaking, adding non-Google services (aka “installing” marketplace applications) to a domain, is really granting privileges for that application to access the domain and end-user data. Different applications require access to different data repositories, for example:

- Calendar (Read/Write)
- Contacts (Read/Write)
- Docs (Read/Write)
- Groups Provisioning (Read Only)
- Spreadsheets (Read/Write)
- User Nicknames (Read only)
- User Provisioning (Read only)

Adding an application with the above data access requirements to a domain means that the application and whomever controls it (the developers and anyone who has access to that environment) can access, write to, and read the domain’s data.

Installing a marketplace application is, in essence, granting super admin access to the domain, to non-employees, and non-Google employees. This is the reason Google provides a security warning as part of the installation process:



Google reminds customers that it is their responsibility to trust and verify 3rd party (non-Google) services they would like to add to their domain.

How do customers trust and verify 3rd party applications?

Assessing the Trustworthiness of the Marketplace Application Provider

With the introduction of Google Drive, enterprises can now offer cloud-based alternatives to other forms of collaboration and fully embrace the collaboration benefits of Google Apps as Google Drive lets users drive more content more easily and securely into Google Docs.

Now that we've established the security implications of adding marketplace applications to an organization's domain, the question remains: how can one determine a trust level?

Here's a quick checklist that any organization can use in evaluating whether to add a marketplace application to their domain:

Trust / Controls	Run Away	Low Trust	Trustworthy	Most Trustworthy
SSAE 16 Audited				√
System Security Plan (SSP)			√	√
Ongoing Application Vulnerability Scanning			√	√
Customer Security Assessment		√	√	√
Application is strategic to the vendor		√	√	√

Here's an explanation around each of the security controls and its impact on the level of trustworthiness of the marketplace application provider. Highly trustworthy 3rd party application vendors will be able to provide the security assurances customers require proactively:

- **SSAE 16 Audited** - Having this means that a 3rd party auditing company has reviewed and attested to the security controls reported by the application vendor
- **System Security Plan (SSP)** - A system security plan is a 'must have' to be considered even somewhat trustworthy. Just having an SSP isn't enough, as anyone can write their own, and security officers should look for independent verification of the controls, procedures and processes reported in the SSP
- **Ongoing Application Vulnerability Scanning** - A standard practice for any cloud-based application
- **Customer Security Assessment** - In lieu of an industry standard security audit, prospective customers should demand the app provider to respond to a security assessment that will capture the controls they have in place. These include employee background checks, documented and implemented policies and procedures, change management, monitoring, and vendor self-audit verification
- **Application is Strategic to the Vendor** - If the app is not strategic to the vendor's core business, chances are that the necessary investment in security controls have not taken place. And security does require an ongoing investment (as anyone who's gone through a security audit will testify)

In summary, security of customer data should be important to everyone.

Security Assessment Template for Non-Audited Vendors and Applications

When a Marketplace application provider does not have independent validation of their security practices, the responsibility for assessing the level of maturity and security practices instead falls on the prospective customer.

The security assessment questionnaire can be broken to the following areas:

- Security
  - Physical Security
  - System Security
  - Network Security
- Development & Testing Procedures
- Change Management
- Incident and Problem Management
- Service Support
- Data Management

The following is a table of security controls we've collected from doing numerous security assessments with large organizations across the world. This list is by no means all-inclusive but should represent a good baseline for any organization with a need to assess a 3rd party cloud solution.

Audited Control	**Detailed Controls to be Audited**
Company Structure	• Overview of company structure (high level) • Overview of company IT support structure
IT Policies & Standards	Provide the following documents: • Corporate IT Security Policy • Security Incident Policies and Procedures • Patch Management Policies and Procedures • Capacity and Availability Policies and Procedures • Configuration Management Policies and Procedures • Change and Release Management Policies and Procedures • Backup and Retention Policies and Procedures • Building and IT Access Policies and Procedures • Staff Background Check Policies and Procedures • Data Retention and Destruction Policies • SLA Terms and Conditions • OLA Terms and Conditions • List any Industry best practices / security audits your company currently has (e.g SSAE 16, ISO etc)
Technical Information	• Architecture - Please provide an overview diagram of production technical architecture relating to the provision of the proposed service • Please provide details of how you ensure continuous delivery of service.

Network Security	• Are industry-standard firewalls deployed? Where are they deployed? How does your company keep the software for firewalls current? • Is administrative access to firewalls and other perimeter devices allowed only through secure methods or direct serial port access? What protocols and ports are allowed to traverse the network and firewall? • Does your company use intrusion detection systems (IDSs)? How long are IDS logs kept? Does your company use an intrusion prevention system (IPS)? • Does your company engage 3rd party security service providers to perform ongoing vulnerability assessments and quarterly scans? If not, what ongoing vulnerability assessments do you perform against your systems? • Does your company have a workflow diagram of the process for network system failure? If so, please provide. Does the service require a direct or indirect interface with our IT core systems?
Physical Security	• Where are the hosting centers located? • Describe the data center's physical security, disaster recovery, backup retention and redundancy. • Who has physical access to host servers? (Data centre staff, other employees, vendors etc.)? • Provide a copy of the process to allow access to the infrastructure.
Systems Security	• Are file permissions (ACLs) set on a need-to-access basis only? • How are operating systems kept up to date? How does your company keep abreast of software vulnerabilities? What is the procedure for installing software updates? • Are audit logs implemented on all relevant systems that store or process critical information? • How often are these logs reviewed? How long are access logs retained for? Who reviews the logs? • How many characters must the service / system password have? Are alphanumeric passwords required? How frequently must passwords be changed? Can passwords be reused within 12 months? • Please provide information on how sensitive and confidential information of the service / system is stored and in what form (i.e. encrypted). • Please provide information in how sensitive and confidential information is stored within backups (i.e., encrypted form). How is this handled and who has access to the media? • Do you have a Data Retention and Destruction Policy? • Please provide information on how passwords are stored within the system / service (i.e., plain text, hashed, etc), and who has access or visibility of these through whatever means (i.e., the password 'file', though a user interface). • Please provide information on how encryption keys are managed and handled. • Please define the encryption standards and versions used by the system / service. • Please provide information on which web pages are secured and by what technology i.e., HTTPS, SSL. • Please indicate all external access methods to the system / service i.e., ftp.

Software Life-Cycle Development	• Is there a ‘standalone’ development environment? • Is there a ‘standalone’ test environment? • Please provide an overview of test and development environments and the degree to which they are consistent with the production environment. • Is segregation of duties implemented for all developers / testers from production systems? • Is only code that is tested and approved rolled into production? • Please provide detail on what Common Off The Shelf (COTS) components comprise the systems / service being proposed. Please confirm that the agreements they are under provide you the right to incorporate them in the system / service. • What open standards are utilized? Please indicate where open systems are utilized within the system / service. Please confirm that the agreements they are under provide you the right to incorporate them in the system / service. • Please provide details of the documentation customer will receive prior to launch i.e., support documentation, developed code, schemas, code based work DTDs. • Please provide details of where Intellectual Property (IP) rights for the application development / service lie. • Will functional testing, load testing & performance tuning be completed by launch?
Change Management	• How will Quality Assurance be carried out before delivery of the system / service? • Are all changes tested prior to release into production? • Please provide details of the working procedures release management of source-code, version tracking, release and rollback. simple real time configuration change.
Incident and Problem Management	• Are incident and problem procedures in place? Are they tested regularly? • What are the procedures for problem prioritization, problem tracking, escalation and resolution including details of any logging systems?
Service Support	• Please provide details of the key staff employed to provide the system and service, including details of their relevant experience, qualifications / certifications and length of service.

Takeaways

When evaluating third-party applications from the Google Apps Marketplace, it is important to understand the security implications of allowing an application provider to have access to organizational data. Using the assessment templates for both audited and non-audited vendors included in this document will provide a clear understanding of whether a Google Apps Marketplace application or vendor can be trusted with your domain's data.

1. Evaluate how a Google Apps Marketplace application extends your security perimeter.
2. Understand which stakeholders should be involved when considering a third-party application.
3. Determine what type of data access will be needed by the application being considered.
4. Assess whether the application provider has the necessary audits and security procedures in place.
5. If the vendor does not have independent validation of their security processes, ask them to complete a thorough security assessment questionnaire.

About CloudLock

CloudLock helps enterprises extend their data loss prevention (DLP) security practices and policies to the cloud. CloudLock's suite of security applications give businesses the controls and visibility they need to take advantage of the collaboration benefits of public cloud offerings, without sacrificing on security. The largest Google Apps customers in the world trust CloudLock to secure their data. For more information about the company or reseller opportunities call (781) 996-4332 or visit cloudlock.com.