Information Risk and Vulnerability Assessment for Google Apps: External Applications

Prepared for:

ACME

This Information Risk and Vulnerability Assessment for Google Apps (IRVA) Report provides a security score
based upon an audit of your Google domain conducted in ___________ 2013.

The score represents the application risk and vulnerability profile for ACME's Google Apps domain, comprised of the statistics, recommendations, and apps that had access to the domain during the audit period.

Date: ______, __, 2013

Account Manager:

Prepared By:

Overview

The objectives of this audit report are to:

- Review the overall Security Score for ACME's Google Apps domain
- Provide metrics and considerations that led to that analysis
- Discuss the general steps involved in mitigating the risk of using third-party applications, while maintaining a high level of functionality for end users.

Security risks related to third party applications, whether the result of intentional exploit by an external vendor or misuse/misunderstanding by internal users, could potentially result in a security incident, such as an inappropriate use or disclosure of PII, PCI, or intellectual property.

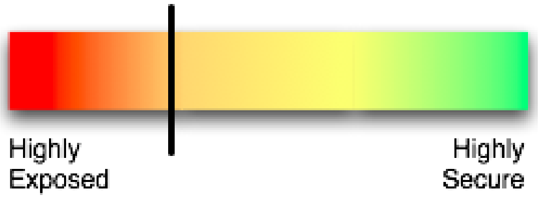
These security risks may be assessed in terms of their *capacity* for harm (based upon the amount of data loss or damage which would result from an exploit) as well as their *likelihood* of inflicting that harm (based upon the intended use of the application, the number of users who are running it, and the overall trustworthiness of the application vendor).

CloudLock was used to scan the Google Apps domain for ACME.com, and found the following apps statistics across the environment:

ACME's Security Score

Your CloudLock security score is:

33.4 (out of 100)



ACME's Security Score Breakdown

23,721	**508**	**120**
Total App Installs	Total Unique Apps	Total Apps with Domain Admin Access

What are our primary risk factors?

- **Number of applications:** ACME's Google Apps domain contains a high number of unique applications, comprising a very large number of installations; from a risk perspective, this reflects a wide range of potential exposure points
- **Apps with Admin access:** Over one hundred applications have domain admin access; this is statistically high, and represents a significant risk. Although these are "core" apps (e.g., Android login services, Chrome, and Google itself), it may be prudent to designate SuperAdmin access only to accounts used for administrative work, and separate daily email and work for those users from their administrative access and role.

How can we address them?

- **Evaluate and classify apps in use:** Ensure that privileged users (Google Admins) are using sanctioned productivity apps
- **Create an Acceptable Application Policy:** Since OAUTH is end-user controlled, and cannot be disabled, consider how you are informing end users of what is or is not an appropriate vendor and/or application, and socialize that policy within the organization.
- **Remove unneeded or inappropriate apps:** Based upon your classifications and (if implemented) AAP, determine which 3rd-party apps should not have access and remove them. Observed apps such as these may warrant investigation for productivity purposes, and for safeguarding the ACME Google Apps environment:

Business Productivity Tools	Social & Communication Tools	Gaming / Entertainment
● www.scheduleonce.com ● Scratchpad ● QuickOffice ● Lucidchart ● MindMeister ● sharethis.com ● sendwhenever.com ● Dropbox ● Floorplanner ● Gantter ● my.yahoo.com ● skillpages.com ● SlideRocket ● www.smartsheet.com ● Asana ● iDoneThis	● www.linkedin.com ● BeeJive IM ● www.tripit.com ● twitter.com ● IM+ ● badoo.com ● evite.com ● imo messenger ● Klout ● notesforgmail.com ● Plaxo ● Pinterest ● LiveJournal	● Google Play Movies ● www.wayn.com ● foursquare.com ● runkeeper.com ● WeVideo ● Gawker Media ● InnoGames ● “The BBC website” ● www.weddingpaperdivas.com

Application Risk Assessment

Application risk is directly related to the scope of access being provided to each app that is running within the ACME environment. While any application may have multiple access types, risk correlates to a number of factors, and should be reviewed in the following contexts:

- **Application Purpose** -- Is the app appropriate for accomplishing business needs?
- **Permission Type** -- Does the application only request permissions it clearly needs to operate?
- **Vendor Trustworthiness** -- Who developed the application? Are they a reputable source? Have they provided a clear privacy policy? Are they externally or self-certified (SSAE-16, TRUSTe, etc.)?
- **Usage and Roles** -- Is the application being used by users, admins, or both?

Application Access Type refers to the level of access that a third party has in a Google Apps domain.

For example, an application might request permission to view and update a user's contact list. This permission request is formally part of the application's authentication request that is presented to any user who enables that application and allows it to use his or her Google Apps credentials, and will be reflected within Apps Firewall under the "Access Scope" list.

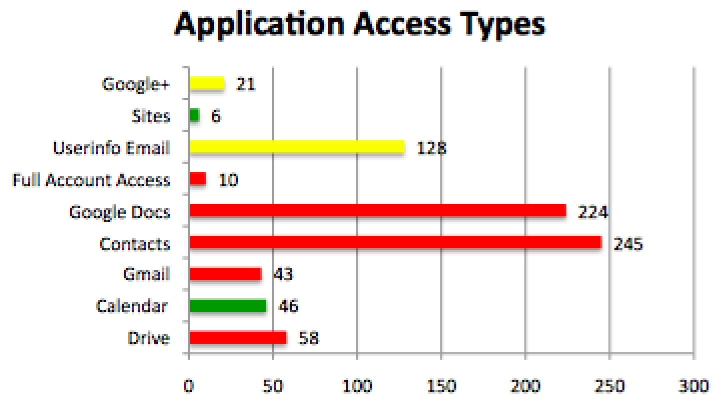
In general, applications should be reviewed for both *breadth* of access (that is, how many "access scopes" are requested) as well as *appropriateness* of access (in other words, do the requested scopes make sense in terms of the application's stated purpose). A full technical description of all of the Google APIs available to applications can be found at:

https://developers.google.com/gdata/docs/directory

For the purpose of this audit, the following application access types have been highlighted:

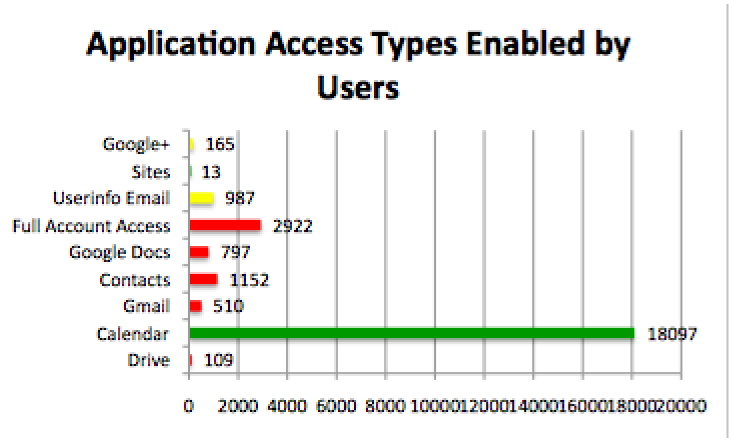
Category	What this means	Exposure Rating
Google Drive	Google Drive access permits an application to create, view, copy, and edit the contents of files stored in your Drive environment.	**High**
Calendar	Calendar access provides an application with the ability to create new events, edit or delete existing events, and search for events based upon specific criteria.	**Low**
Gmail	Applications with GMail access can read some or all content stored within GMail; applications granted Settings API access may modify user-level Google Mail settings for any of the users within your domain.	**High**
Contacts	Contacts API access allows an application to create new contacts, edit or delete existing contacts, and query for contacts that match particular criteria.	**High**
Google Docs	Applications granted Google Docs API permissions may create, retrieve, update, and delete Google Docs (including but not limited to text documents, spreadsheets, presentations, and drawings), files, and collections. It also provides some advanced features like resource archives, Optical Character Recognition, translation, and revision history.	**High**
Full Account Access	Full Account Access is the most permissive authorization scope available, allowing complete control over all aspects of an account, identical to what an interactive user could accomplish.	**High**
Userinfo Email	Applications with access to user information and profiles may retrieve and update profile information for users in a Google Apps domain, and perform operations on behalf of the domain administrator, such as modifying user profile photograpphs or executing bulk query and update requests. Note that profiles may never be created or deleted with this API.	**Med**
Sites	The Sites API allows client applications to access, publish, and modify content within a Google Site, as well as to upload and download files to Sites, including Sites created by the API itself.	**Low**
Google+	The Google+ API allows client applications to access, publish, and modify content with the Google+ application	**Med**

Risk Statistics and Metrics



Application Access Types:

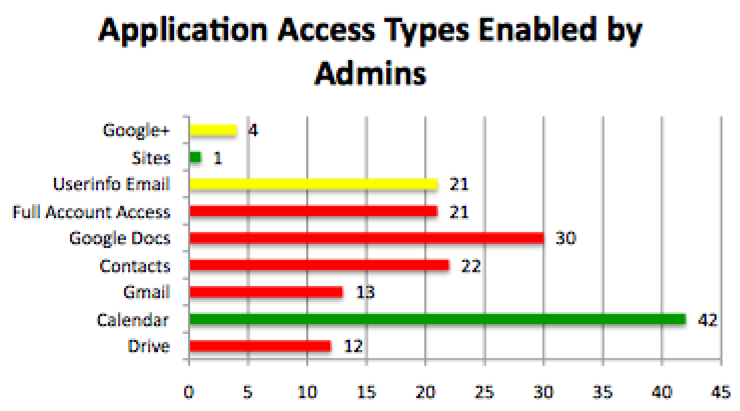
This chart shows the count of distinct applications with access to the domain, grouped by access type.



Application Access Types Enabled by Users:

This chart shows the count of all applications that have been granted access by end-users, grouped by application access type.

- 1029 Users with Google Chrome



Application Access Types Enabled by Admins:

This chart shows all applications that have been granted access by domain Administrators, grouped by application access type.

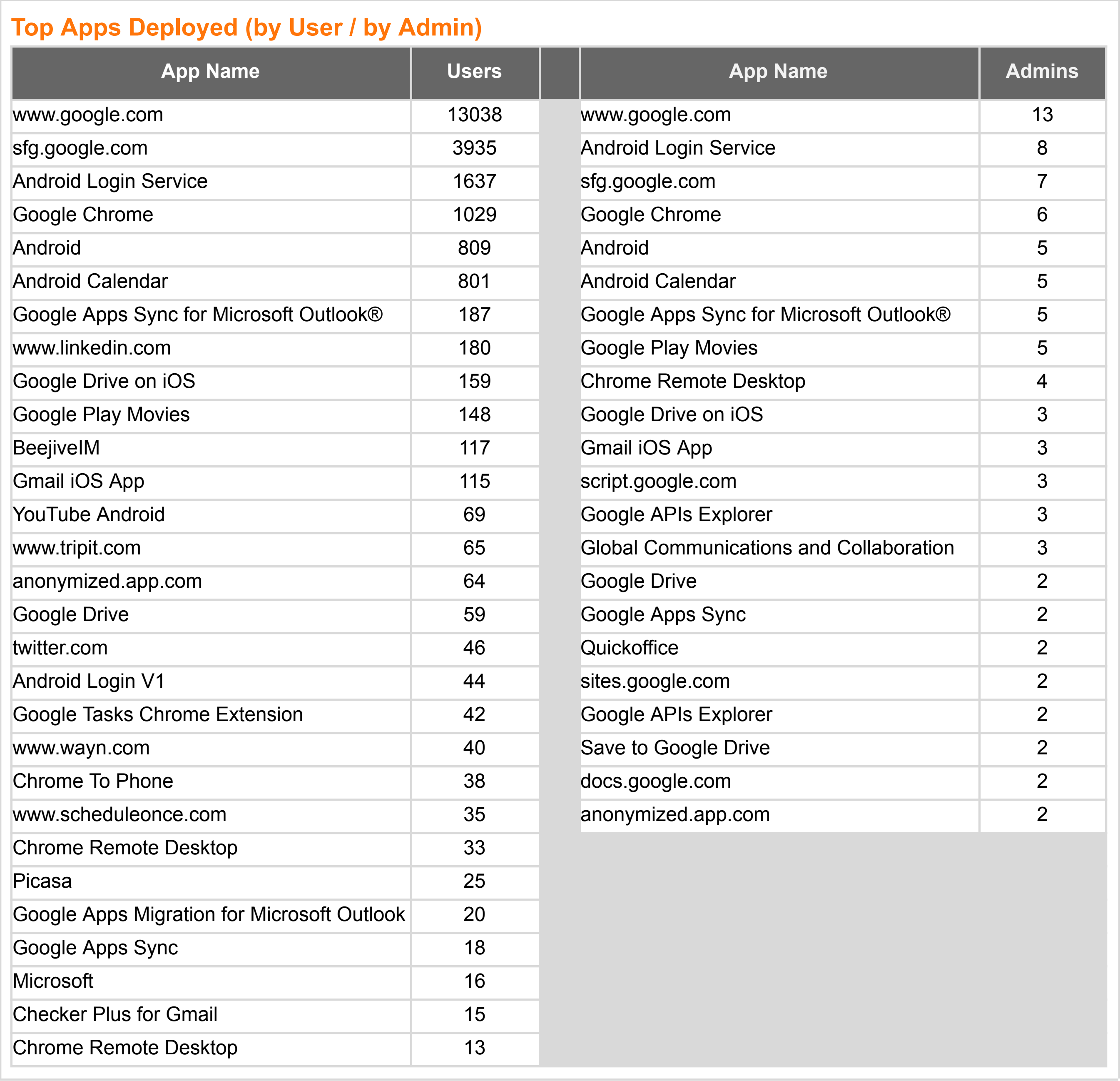
General Recommendations

When analyzing third party applications, both in general terms and as related specifically to ACME, the follow recommendations provide a framework for analyzing and responding to risk while maintaining functionality and flexibility for end-users:

1. Review Applications and their access types

- Applications that have full account access, drive/docs, gmail and/or contacts access should be vetted to determine security of the application
- Remove non productive apps, or those apps that may gain access to the Google Apps environment unnecessarily. e.g.: apps such as these may be candidates for review:

Top apps for users:



Top Apps Deployed (by User / by Admin)

App Name	Users		App Name	Admins
www.google.com	13038		www.google.com	13
sfg.google.com	3935		Android Login Service	8
Android Login Service	1637		sfg.google.com	7
Google Chrome	1029		Google Chrome	6
Android	809		Android	5
Android Calendar	801		Android Calendar	5
Google Apps Sync for Microsoft Outlook®	187		Google Apps Sync for Microsoft Outlook®	5
www.linkedin.com	180		Google Play Movies	5
Google Drive on iOS	159		Chrome Remote Desktop	4
Google Play Movies	148		Google Drive on iOS	3
BeejiveIM	117		Gmail iOS App	3
Gmail iOS App	115		script.google.com	3
YouTube Android	69		Google APIs Explorer	3
www.tripit.com	65		Global Communications and Collaboration	3
anonymized.app.com	64		Google Drive	2
Google Drive	59		Google Apps Sync	2
twitter.com	46		Quickoffice	2
Android Login V1	44		sites.google.com	2
Google Tasks Chrome Extension	42		Google APIs Explorer	2
www.wayn.com	40		Save to Google Drive	2
Chrome To Phone	38		docs.google.com	2
www.scheduleonce.com	35		anonymized.app.com	2
Chrome Remote Desktop	33			
Picasa	25			
Google Apps Migration for Microsoft Outlook	20			
Google Apps Sync	18			
Microsoft	16			
Checker Plus for Gmail	15			
Chrome Remote Desktop	13			

Scratchpad	13
GDrive	12
IM+	12
Quickoffice	11
Android Phone	10
attachments.me	10
anonymized.app.com	10

Privileged users should not pass their administrative credentials to any 3rd Party Apps without vetting the security of the app itself. Resources online including CloudLock, the Chrome Web Store or other ratings systems can be used to determine the security of the application.

2. Remove redundancy, and promote known-good applications
If there are applications that provide a redundant service, consolidate the application use to reduce the exposure level. Promote sanctioned applications, and remove non-approved applications from the domain.

3. Notify users who are running inappropriate or risk apps, and/or revoke those apps
Identify users who have authorized applications that are deemed insecure, inappropriate, or are otherwise not approved for use within the domain. Via CloudLock, inform them that such 3rd-party applications should not be used within the domain, and provide information on how to revoke access.

Appendix: List of Discovered Applications

App Name	Users	Admins	Access
anonymized.app.com	1	0	Google Calendar
anonymized.app.com	1	0	Google Docs
Activism	1	0	Userinfo Profile,Userinfo Email
anonymized.app.com	1	0	Google Docs
Affixa	2	0	Gmail Settings APIs,Gmail
Alto	1	0	Gmail,Userinfo Email
Analytics Tiles Pro	1	0	Userinfo Email,Google Analytics
Android	809	5	Paths Notifications Api,Google Voice,Personal Derived Data API
Android Calendar	801	5	Google Calendar
Android First Party Default Client	2	0	Google Calendar
Android Login Service	1637	8	Full Account Access
Android Login V1	44	1	Full Account Access
Android Phone	10	1	Full Account Access
animoto.com	1	0	YouTube
anonymous	1	0	Gmail
Anytodo	1	0	Tasks
api.cloudsponge.com	3	0	Contacts
app.gantter.com	1	0	Google Calendar,Google Docs,Contacts
appservicer.com	2	0	Google Sites
Asana	4	0	Userinfo Email,Userinfo Profile,Contacts
Astro Test	3	0	Drive API,Google Docs
attachments.me	10	0	Gmail
Attachments.me for Google Drive	7	0	Google Docs
Awesome Screenshot	2	0	GDrive Files,Userinfo Email
Backup Box	1	0	GDrive Files,Userinfo Email,Userinfo Profile,Google Docs
badoo.com	4	0	Contacts
Balsamiq Mockups	1	0	GDrive Files,Userinfo Email,Userinfo Profile
BeejiveIM	117	1	Userinfo Email,Google Talk
beta.unroll.me	1	0	Gmail,Contacts
bolinfest.com	1	0	Google Calendar
Cacoo	1	0	GDrive Files,Userinfo Email,Userinfo Profile
Cacoo for Hangouts	1	0	Google+ You
calendar.comcast.net	1	0	Userinfo Email,Contacts
carpoolworld	1	0	Userinfo Email
chameleon.teknision.com	2	0	Gmail
Checker Plus for Gmail	15	0	Contacts
Checker Plus for Google Drive	1	0	Drive API
Chrome Remote Desktop	33	4	Chrome Remote Desktop Directory,Userinfo Email,Google Talk
Chrome Remote Desktop	13	0	Chrome Remote Desktop Directory,Userinfo Email,Google Talk
Chrome to Mobile	8	1	Google Cloud Print,Userinfo Email,Userinfo Profile
Chrome To Phone	38	1	unknown

Chrome to phone for China	2	0	Userinfo Email
Cirrus gDrive	1	0	Drive API
Clarity regression	1	0	Google Docs
Clarity Regressions	1	0	Google Docs
Cloud Printer App for Mac	2	0	Google Cloud Print,Userinfo Email
Codecademy	2	0	Userinfo Email,Userinfo Profile
codejob	1	0	Userinfo Email
Codenvy	1	0	Google App Engine Admin Console
connect.kunlun.tw	1	0	Contacts
connex.io - automating your address book	1	0	Contacts
convio.net	1	0	Contacts
cs12.salesforce.com	1	0	Google Docs
cs3.salesforce.com	6	0	Google Docs
CSDN.NET	2	0	Userinfo Email
CtoCloud Application	1	0	Userinfo Email,Userinfo Profile,Google Calendar,Google Docs,Contacts
cube.bitrzr.com	2	0	Google Calendar,Google Docs,Contacts
dailybooth.com	1	0	Contacts
Do	1	0	Userinfo Email,Google Docs,Contacts
docs.google.com	2	2	Google Docs
docs.latexlab.org	1	0	Google Docs
Documents by Readdle	1	0	Drive API,Userinfo Email
DocuSign	1	0	GDrive Files,Drive API,Userinfo Email,Userinfo Profile
Doodle	1	0	Userinfo Email,Userinfo Profile
doodle.com	1	0	Google Calendar,Contacts
draw.io	1	0	GDrive Files,Userinfo Email,Userinfo Profile
Drive 2	1	0	Drive API,Userinfo Email,Userinfo Profile
Drive Notepad	3	0	GDrive Files,Userinfo Email,Userinfo Profile
Dropbox	8	0	Contacts
dev.api.ACME.com	2	0	Google Calendar
emailgame.baydin.com	1	0	Gmail,Google Calendar,Contacts
ES File Explorer	1	0	Userinfo Profile,Google Docs
Evernote	3	1	Contacts
evite.com	4	0	Contacts
Feed It Forward 2011	1	0	Contacts
feedly	8	0	Google Reader
File Manager	1	0	Google Docs
findbigmail.com	1	0	Gmail
Floorplanner	6	0	GDrive Files
FolderSync	1	0	Drive API
Form+	1	0	GDrive Files,Userinfo Email,Userinfo Profile,Google Docs,Google URL Shortener
foursquare.com	3	0	Contacts
Fox To Phone	3	0	unknown
FZTesting	1	0	Gmail,Google Calendar,Google Docs,Google Sites,Contacts
ga-api-javascript-samples.googlec	1	1	Google Analytics

ode.com			
gadgets.zoho.com	3	0	Userinfo Email,Google Docs
Gantter	6	0	GDrive Files,Userinfo Email,Userinfo Profile,Google Docs
anonymized.app.com	1	0	Drive API
anonymized.app.com	0	1	Groups APIs
anonymized.app.com	2	0	Google Sites
Gawker Media	2	0	Userinfo Profile
gcal2excel.com	1	0	Google Calendar
GCC Drive Admin Tool	0	1	Drive API
anonymized.app.com	0	1	Google Calendar
gCloud Print	1	1	Google Cloud Print
anonymized.app.com	2	0	Contacts
anonymized.app.com	1	0	Contacts
GDrive	12	0	Userinfo Email,Google Docs
GDrive	1	1	Drive API,Userinfo Email
GDrive Viewer	1	0	Drive API,Userinfo Email,Userinfo Profile
Glists	1	0	Tasks
Global Communications and Collaboration	2	3	Google Calendar
Global Communications and Collaboration	0	1	Google Calendar

