Cloud Usage Risk Report

November 2014
Executive summary

The Adallom Cloud Risk Report is published annually, detailing actionable insights and information mined from the Adallom subscriber base. This specific report incorporates analysis of cloud application usage for over one million enterprise SaaS enabled users traversing four dominant SaaS platforms: Salesforce, Box, Google Apps, and Office 365 between October 2013 and October 2014.

This report is the first of its kind to detail application usage patterns and risky behaviors for the top SaaS applications used by businesses. The key findings in this report reaffirm the need for a new approach to data governance, risk management, and security in the context of cloud adoption. Perimeter and endpoint security solutions provide minimal protection against new, emerging, and largely unknown risks. Therefore, enterprises need to proactively invest in new controls like Identity and Access Management (IAM) solutions and Cloud Access Security Brokers.

Key findings include:

- **In the cloud zombies are real:** 11% of all enterprise SaaS accounts are “zombies,” inactive assigned users that are at best eating up the cost of a license, and at worst increase the attack surface of the organization.

- **More admins, more problems:** Every administrative account represents a real and present risk to the enterprise. In some SaaS applications Adallom recorded an average of 7 administrators out of every 100 users.

- **80% of companies have at least one former employee whose SaaS application credentials have not been disabled:** De-provisioning continues to plague organizations, credential creep makes the problem unwieldy.

- **19% of users bypass Identity and Access Management controls:** Rebalancing the enterprise security portfolio from exclusively preventative controls to blended risk management based compensating controls is necessary.

- **5% of an average company’s private files are publicly accessible:** The productivity gains of SaaS adoption come at the cost of reduced legacy control effectiveness and purview, it’s time to refresh enterprise governance controls.

- **The average company shares files with 393 external domains:** Accountability and liability for the distribution of enterprise data, especially privileged data continue to challenge IT in the cloud era.

- **29% of employees share an average 98 corporate files with their personal email accounts:** Personal sharing of enterprise data manifests both governance and security risks.

- **Think of the orphans:** An average of 6% of files in cloud services are orphans. Of those, approximately 70% were created by users outside the company, and 30% by terminated employees or former contractors.

- **37% of our customers discovered they stored more cloud data in Salesforce than any other cloud storage service:** Although Salesforce has a secure storage layer, its information governance controls are limited.
Introduction

When it comes to the protection of enterprise data in the cloud, the SaaS providers’ focus is on security, not “risk”: SaaS providers’ investments in security are largely directed toward certifications, compliance and audits/testing of their infrastructure that all increase their “trustability” in the eyes of their customers. [1]

It’s not reasonable to expect your SaaS provider to protect your users from malware or phishing attacks, even if those attacks specifically target their service. That’s not to say the provider won’t do everything within their power to help you - their security teams rank among the best, but they could never be accountable for the security posture of your organization or its employees.

A recent Forrester survey found that a majority of IT decision makers placed accountability for a data breach on SaaS providers. [2] This is a misplacement, as in reality, companies are responsible for user activities and data, even in the cloud. According to the Cloud Security Alliance guidelines:

“When data is transferred to a cloud, the responsibility for protecting and securing the data typically remains with the collector or custodian of that data.” [3]

The Forrester survey findings clearly indicate that the broad IT community is still grappling with the boundaries between provider and customer liability.

An example that may aid in edifying the shared responsibility model is a phishing attack which targeted Google Apps users discovered recently by security experts at BitDefender. [4] The attack employed the data URI feature to conceal the true origin of the phishing page. Once breached, attackers could have gained access to sensitive company data, including user emails, drive and company shared files. Furthermore, compromised accounts could be used to further infiltrate the affected company by sending phishing emails and infected emails from the compromised employee’s corporate email account.

With access to a person’s Google account, attackers could cause a lot of damage very quickly – from compromising email and documents to expanding the attack to the victim’s social circle via email or social tools, like Google+.

There is no doubt this kind of attack poses a great risk to enterprise data in the cloud; the problem lies in delineating accountability for mitigation should such an attack take place. In the aforementioned scenario, the Google Apps Terms of Service clearly state:

“Customer will use commercially reasonable efforts to prevent unauthorized use of the Services and to terminate any unauthorized use. Customer will promptly notify Google of any unauthorized use of or access to the Services of which it becomes aware.” [5]

The only reasonable interpretation of this clause is that the customer is expected to prevent unauthorized usage of the service. This clause encompasses most of the possible user attack scenarios, from identity theft (compromised insider) to internal threat.
(malicious insider), as in the cloud everything falls under the broad definition of "unauthorized usage" because the “insider” is the attack vector. Specifically, the BitDefender phishing attack described above is classified as “unauthorized usage," and a Google Apps customer affected by it is liable for any damage caused while Google itself is indemnified.

The fact that the majority of SaaS adopting companies do not understand they are responsible for SaaS security means that these companies are left unprotected and their data is at great risk.

SaaS risk management is a very different competency, which is why Cloud Access Security Brokers are an important complement to the likes of endpoint and perimeter security controls. Adallom Labs has compiled the insights in this report from over a million users traversing through the Adallom service.

In the cloud, zombies are real

At Adallom, we refer to user accounts which haven’t been active over a period of three months as “zombies”. Not all zombies are bad – in some cases, such as sabbaticals, maternity leave, or disability – this inactivity is not unusual, but even in those cases there are best practices such as account suspensions that keep the user’s data active while preventing a would-be hijacker from taking over the account during the user’s absence.

An inactive account does not only represent a security risk, it’s also a financial burden on the company. In many of the organizations we protect, we often see double digit percentages of zombies – these are licenses which the company is paying for even though they aren’t being used.

The most dangerous kind of zombies are “Zombie Admins” – because privileged accounts are the preferred and most targeted attack vector for threat actors. A compromised account with administrative capabilities may allow an attacker to gain substantial access to valuable corporate information. Specifically, in administrative panels for cloud applications, a privileged account wields a lot of power.

Figure 2: 11% of enterprise SaaS users are zombies that have access to the application, but have not been active for three months or longer
More admins, more problems

Different cloud services have varied ratios of administrators to users. The higher the ratio, the greater the likelihood of one of those privileged users being a zombie admin.

Within our Adallom customer community, we find that Salesforce has the highest ratio of privileged users to non-privileged users.

One of the biggest issues in cloud services is that these privileged users are often what we call "super admins" – meaning they have complete and unrestricted access to the service. A compromised “super admin” account represents a much greater threat to an organization because it has access not only to view and edit privileged data, but also to modify access rights of other privileged users.

A well-documented recent example of such a scenario is Code Spaces: The company’s Amazon EC2 control panel access credentials were compromised through a phishing attack. The attackers then made extortion demands of company officials. Upon realization that somebody had access to their administrative control panel, Code Spaces changed their EC2 passwords. However, they quickly discovered the attackers had created backup logins, and once recovery attempts were noticed, the attackers began deleting artifacts from the panel. By the time Code Spaces finally managed to get their panel access back, most of their data, backups, machine configurations and offsite backups were either partially or completely deleted.

The Amazon Web Services administrative portal is itself delivered as-a-Service, much like the administrative portals of Google Apps, Box, Salesforce, and Office 365. Customers, not vendors, are responsible for risk management. While most enterprise SaaS providers have built-in support for two-factor authentication and IP restrictions that can be used with user accounts, sophisticated attackers can circumvent those controls through session hijacks and targeted malware.

Using Adallom, one of our customers found over 100 Salesforce users with administrator privileges. We gave them visibility into which users were using administrative functions, and the users who were never actually logging in (the zombies). We worked with their sales operations team on enabling delegated admin user groups within Salesforce so that not every admin was a “super admin,” thus significantly reducing their attack surface.
80% of companies have at least one former employee whose SaaS application credentials have not been disabled

Enterprise user de-provisioning continues to be the dark side of an organization’s user access provisioning process. When it comes to removing access due to a changing job role or an employee (more often a contractor) departing the organization, IT is notified to revoke access through a semi-automated policy-driven process infamous for its gaps.

Focusing attention on the problem and making executive management aware of the risks posed by having “orphaned” accounts within the organization’s business systems is a crucial component of a prudent risk management strategy. There is plenty of supporting evidence which documents the high costs to organizations through data loss, reputation and monetary costs due to errant user access management. [7]

Fortunately, the de-provisioning threat has been reduced significantly through Identity and Access Management (IAM) tools such as Centrify, Okta, or Ping. Onboarding an IAM service is a best practice, but doing so should be complemented with Cloud Access Security Brokers.

19% of users bypass Identity and Access Management controls

Although SaaS providers offer security features such as two factor authentication and IP restrictions, there are many ways for the security to fail. IAM and Single Sign-On tools go a long way toward centralized access control, but there are many mechanisms built in to standard user workflows that yield non-malicious circumvention.

One example of consumer-driven circumvention are platform specific mobile apps that allow users to authenticate directly to the application. Another is direct access to the application through third party API. Neither of these scenarios necessarily represent malicious behavior by users; in some cases users are not even aware that they are bypassing the IAM mechanism. Unfortunately, in the event of a breach, circumvention does not move liability from the shoulders of the organization to the user. IT still has a responsibility to protect the integrity of the data in the services that power the business. [8] The challenge is how to function in the face of such disruptive forces.

Changing the strategy is not just about satisfying employees. IT can also benefit. By embracing and aligning itself with a risk management model that accounts for circumvention, rather than maintaining the slower, provable inefficient pace of prevention-based security. While no perfect solution exists, a combination of third-party tools and attention to where data is stored can create a security environment sufficient to meet the assessed risk level of many organizations.
5% of an average company’s files are publicly accessible by anyone on the internet

There are several reasons private enterprise data unknowingly winds up publicly accessible:

1. The “anyone with this link” problem

Ideally, to share a document with specific people, we expect users to share the file exclusively with the recipient’s email address. However, problems have arisen for users who would not (or could not) create an account on the file sharing service in question. These users were unable to access the shared documents. When the complaints began, savvy users gleaned a different security setting to solve the problem – sharing files using the ‘Anyone with the link’ setting. That works, but now anyone who had the link could share the link which makes documents easier to share, but less secure.

2. Enabling anonymous access and indexing (aka “crawlability”)

Some SaaS applications allow search engines to index (or crawl) documents contained within them, and lack of awareness over the governance of search engine indexed documents has already made headlines several times over the past few years. [9]

This functionality is usually globally controllable, and often disabled by default – but we are consistently surprised by the quantity of organizations that have public crawling enabled.
3. Unnecessarily privileged third-party applications

Enterprise SaaS providers often feature marketplaces for third party ecosystem applications built on their platform. Whether installed by administrators, or end users, these applications can request and be granted privileged access that allows them to upload, download, edit, and delete files and data.

In the consumer space, there have already been scenarios where malicious ecosystem applications have tricked users into handing over access to privileged data \[10\] – and we are currently investigating several such apps in enterprise SaaS marketplaces.

Governance over third party SaaS ecosystem application access becomes increasingly difficult as SaaS platforms intersect with each other. For example, there are already cross-platform third party applications that integrate services like Dropbox with Salesforce, or Google Drive with Huddle – meaning a compromised account in one cloud service could become an attack vector into another. It’s a best practice to know what third party ecosystem applications have access to enterprise data in the core platform, and develop a risk appetite strategy for the access privileges those apps are granted.

The average company shares its files with 393 external domains

Sharing files with third parties is an important and beneficial feature of enterprise SaaS applications, however there are risk ramifications that are concurrent with these benefits.

Some SaaS providers install a local device agent in order to synchronize between user devices and the Web, which often means users are unaware of the full spectrum of data being synchronized to the SaaS provider.

Inadvertent sharing is a real danger for enterprises with an increased uptake of services such as Office 365, Box and Google Drive. For governance and security purposes, it’s crucial to understand where corporate files are stored and who they are being shared with.

Malicious threat actors have already used malicious file sharing with employees as a successful attack vector for malware distribution, clandestinely exploiting file sharing as a mechanism for gaining access to enterprise resources.\[11\]
9

Adallom assigns risk scores to external domains based on a comprehensive heuristic scale, including factors such as their Alexa score, whether any Adallom subscriber has ever interacted with them, when they registered, and the sensitivity of the data being shared relative to the risk score of the domain it’s being shared with.

### 29% of employees share an average 98 corporate files with their personal email accounts

Personal sharing can happen unintentionally via the aforementioned sync agents – for example, employees who use Google Drive for personal as well as enterprise storage may have their data segregated in the cloud but integrated on their local device, such that when they move files from one folder to another on the local device, corporate files accidentally sync to their personal Google Drive in the cloud.

When personal sharing is intentional, the act is rarely malicious. In fact, we consistently see “malicious insiders” as the least likely scenario for data exfiltration. In some cases, personal sharing of corporate data is done for productivity purposes (sometimes at the expense of data governance policy circumvention). For example, many Office 365 users prefer editing a document in a local version of Word 2013 over of Word Online.

Any variety of personal sharing manifests both governance and security risks. Once corporate data is moved to a user’s personal cloud or physical drive, any attestation, DLP, or eDiscovery controls become largely moot.

Encryption is often thought of as a solution to this problem, but third party encryption tools are given more gravitas than they deserve. The theory is that only authorized personnel and programs see decrypted information. But encryption controls are not designed to know if the user has been compromised or has granted someone else access to the key.

Most enterprise SaaS providers encrypt data in transit as it flows between their data centers and user devices, as well as “at rest” on their servers. Those providers who aren’t doing so are certainly moving in that direction, and can be persuaded to move faster by their customers (a good use of your time!).

Beyond vendor provided encryption, the focus in SaaS should be attestation, not encryption. What’s needed is a clear and actionable audit trail of all user activities in SaaS applications with direct correlation to which data - structured and unstructured - has been exchanged, shared, or otherwise interacted with.

<table>
<thead>
<tr>
<th>External Domain</th>
<th>Shared Files</th>
<th>Shared Users</th>
<th>Risk Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>gmail.com</td>
<td>11382</td>
<td>95</td>
<td></td>
</tr>
<tr>
<td>hotmail.com</td>
<td>2366</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>verizon.net</td>
<td>1389</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>email.com</td>
<td>501</td>
<td>18</td>
<td></td>
</tr>
<tr>
<td>google.com</td>
<td>299</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>outlook.com</td>
<td>361</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>hotmail.com</td>
<td>366</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>google.com</td>
<td>299</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>yahoo.com</td>
<td>46</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>live.com</td>
<td>46</td>
<td>5</td>
<td></td>
</tr>
</tbody>
</table>

Excerpt from an Adallom Risk Assessment Report

Copyright ©2014 Adallom Inc.
Think of the orphans

Previously in this report, we discussed the notion of “orphan” users whose accounts persist beyond their termination. However, “orphaned” files are an entirely different risk that is often unseen or overlooked in the enterprise. Orphan files are files that have no owner. This can happen when files are owned by users or groups that have been deleted. It can also happen when external users share files with internal users through temporary access on the corporate sanctioned SaaS drive.

Among our customers, an average of 6% of files in cloud services are orphans. When we research their origin, we find that approximately 70% were created by users outside the company, and 30% by terminated employees or former contractors.

The danger of having a file or folder owned by a non-existent user or group ID is that someday, that user or group ID could be assigned to a newly created user or group, members of which would be automatically able to access the file.

Orphan files also create a governance problem because they don’t have a clear provenance and attestation trail, which means that they might violate retention policies. In the event of an eDiscovery query or regulatory compliance audit, orphan files could be troublesome, especially if they contain privileged data.[13]

Adallom provides a “single pane of glass” view into orphan files across SaaS services and can be used to establish origin, age, and ownership along with governance capabilities that allow proper custodianship and control.

37% of our customers discovered they stored more cloud data in Salesforce than anywhere else.

Figure 4: Average of 6% of files in Adallom cloud services are orphans which have no owners

Figure 5: More data is stored in Salesforce than any other SaaS application, including corporate-approved cloud storage services
In many cases, even ostensibly well-governed organizations overlook critical risks. For example, one of our customers, prior to engaging with us, had spent nearly a full year on a Shadow IT control project intended on standardizing their enterprise file storage, sharing, and sync on a single sanctioned vendor – Box. However, shortly after deploying Adallom, the security team found that although employees had largely standardized on Box for file storage, nearly forty percent of their enterprise files in the cloud were stored in Salesforce. They had simply never considered Salesforce, an enterprise SaaS vendor that was sanctioned for CRM, as a cloud storage provider.

Although Salesforce has a storage layer, its information governance controls are limited. For example, it’s impossible to create a DLP policy for data in Salesforce without using a third party solution. So while it’s obvious that the Salesforce platform can be trusted with data retention, when it comes to managing files inside of Salesforce, it’s a best practice to integrate an enterprise storage governance solution from the Salesforce AppExchange. Consider Box for Salesforce for governance, along with a Cloud Access Security Broker for risk management, such as Adallom for Salesforce.

Takeways On Protecting SaaS Applications

“A whopping 92% of respondents to our survey indicated a belief that their existing security controls are either effective or very effective in protecting their digital assets in SaaS applications,” wrote Andras Cser, Forrester VP, Principal Analyst Serving Security & Risk Professionals. “Unfortunately, security professionals with this mindset are rolling the dice with their sensitive data. Perimeter and endpoint protections provide minimal protection against new, emerging, and largely unknown threats; they are ineffective when the endpoint is unmanaged and off premise.”

Being prepared means understanding organizational accountability for protecting enterprise data in SaaS applications, and adding a Cloud Access Security Broker to a prudent defense-in-depth architecture; which is why we emphasize the proactive service component of our cloud security solution. Adallom not only provides the visibility, governance, and protection capabilities of our platform, but we act as an extension of our customers’ security and risk management teams. This gives them actionable insights into compliance risks and external threats, as well as engages business units in their organization to jointly improve the company’s cloud security posture.
References


