ADALLOM

Cloud Usage Risk Report

October 2014

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.

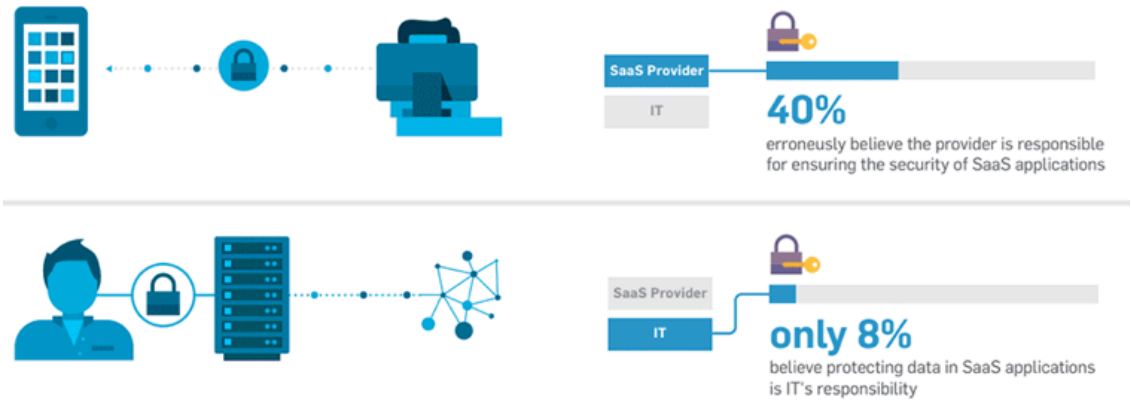


Figure 1: Adallom Infographic (source: Forrester survey - "SaaS Adoption Requires a New Approach To Information Security")

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

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.

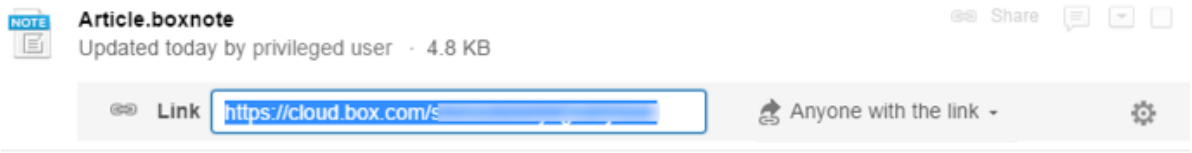
One example of consumer-driven circumvention are platform specific mobile apps that allow users to authenticate directly to the application. Another is direct access to the application through third party API. Neither of these scenarios necessarily represent malicious behavior by users; in some cases 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

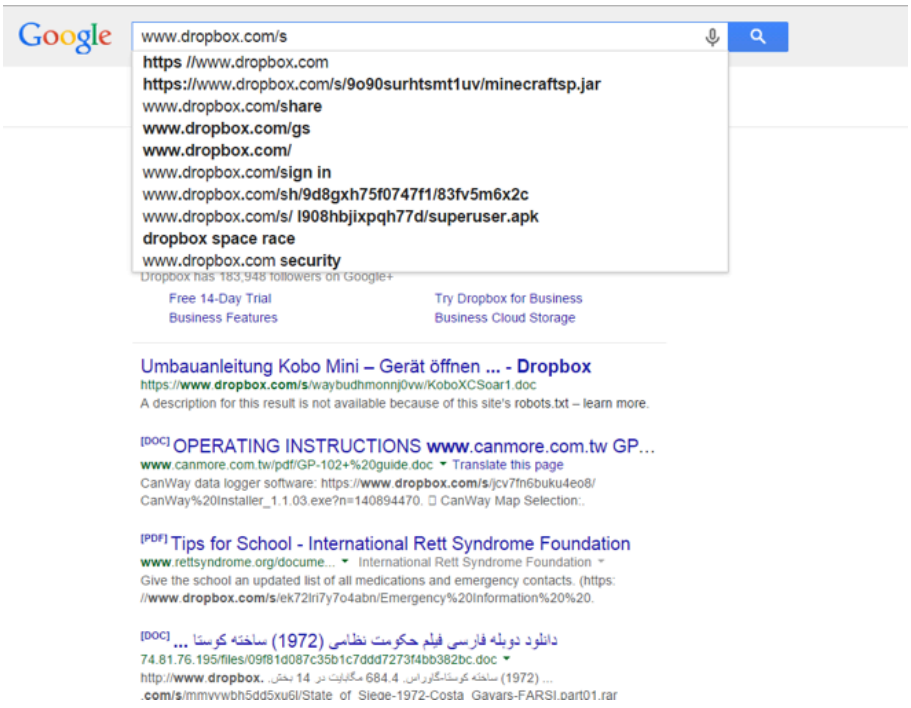
There are several reasons private enterprise data unknowingly winds up publicly accessible:

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.

	External Domain	Shared Files	Sharing Users	Risk Score
HIGH	gmail.com	11282	95	Risk of personal accounts usage Excessive share rate
	[redacted]	2209	6	Share to a single external account Excessive share rate Domain name does not resolve to website
	verizon.net	1369	1	Share to a single external account Excessive share rate Domain name does not resolve to website
	[redacted]	501	18	
MEDIUM	[redacted]	393	2	Excessive share rate
	[redacted]	364	2	Excessive share rate
	[redacted]	361	2	Excessive share rate
	google.com	229	7	
LOW	yahoo.com	46	6	Risk of personal accounts usage
	live.com	46	5	Risk of personal accounts usage

Excerpt from an Adallom Risk Assessment Report

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. [12] 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.

In many cases, even ostensibly well-governed organizations overlook critical risks.[14] 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." [2]

Figure 6: More data is stored in Salesforce than any other SaaS application, including corporate-approved cloud storage services

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

[1] S. Deshpande, N. MacDonald and C. Lawson, "Emerging Technology Analysis: Cloud Access Security Brokers," Gartner, 2014.

[2] A. Cser, "SaaS Adoption Requires A New Approach To Information Security," Forrester Consulting, 2014.

[3] F. Gilbert, P. Jones Harbour, D. Kessler, S. Ross and T. Trappler, "CSA Security Guidance Domain 3: Legal Issues: Contracts and Electronic Discovery," Cloud Security Alliance, 2011.

[4] S. Ragan, "Phishing attack uses data URI to target Google accounts," 13 May 2014. [Online]. Available: http://www.csoonline.com/article/2154202/social-engineering/phishing-attack-using-data-uris-to-target-google-accounts.html.

[5] Google, Inc., "Google Apps for Business (Online) Agreement," 22 July 2014. [Online]. Available: http://www.google.com/apps/intl/en/terms/premier_terms.html. [Accessed 8 October 2014].

[6] AbleBots, LLC, "Code Spaces : Is Down!," Code Spaces, 17 June 2014. [Online]. Available: http://www.codespaces.com. [Accessed 7 September 2014].

[7] A. Allan and F. Gaehtgens, "Align Your IAM Program With Your CIO's Priorities," Gartner, 2014.

[8] S. Chuang and D. Zumerle, "Managing Mobile Access to the Cloud," Gartner, 2013.

[9] D. Gilbert, "Dropbox and Box Users Accidentally Leaking Private Files Online," 6 May 2014. [Online]. Available: http://www.ibtimes.co.uk/dropbox-box-users-accidentally-leaking-private-files-online-1447352.

[10] L. Constantin, "More fake antivirus programs found in Google Play, Windows Phone Store," IDG News Service, 16 May 2014. [Online]. Available: http://www.pcworld.com/article/2156300/more-fake-antivirus-programs-found-in-google-play-windows-phone-store.html.

[11] A. Gonsalves, "What to avoid in Dropbox-related phishing attack," 6 June 2014. [Online]. Available: http://www.csoonline.com/article/2360670/malware-cybercrime/what-to-avoid-in-dropbox-related-phishing-attack.html.

[12] T. McClure and K. Kao, "Security Considerations for Online File Sharing," Enterprise Strategy Group (ESG), 2013.

[13] S. Krapes, "Use IAM Life Cycle Policies to Enforce Account Disabling and Deletion," Gartner, 2014.

[14] R. Mogull, "The Future of Security: The Trends and Technologies Transforming Security," Securosis, 2014.

ADALLOM

HQ
2390 El Camino Real, Suite 240
Palo Alto, CA 94306
+1 (650) 268-8322

www.adallom.com

R&D
Habarzel 21 Street, Building B
Tel Aviv, 6971001
Israel