16 CLOUD APPS YOU NEED TO KNOW IF EMPLOYEES ARE USING

One of the biggest risks that companies face today is the growing popularity and availability of cloud-based applications – shadow IT. These applications can be used by any of your employees and they share huge amounts of data that fly under the radar of your security team. The danger lies in the fact that these cloud applications are also prime avenues for exposing sensitive or regulated data to third parties.

To make matters worse, it's very difficult to keep cloud apps secure because of the sheer number of employees in your company using them. It's even more difficult to detect data misuse because it can be hidden within the huge amounts of data stored in these apps. This makes identifying, targeting, and flagging specific apps crucial to keeping your company's data safe.

To help you, below is a list of 16 cloud apps (and reasons why they are high risk) used by your employees, that every organization needs to know about.

COLLABORATION APPS:

Skype is an extremely popular telecommunications cloud application used by your employees (especially for global companies) that provides video chat and voice calls between devices via the internet. Skype can be a dangerous app for your employees to use because it appears to be easy to hijack a Skype account through the user's email address. Once a hacker has access, any account that has had previous credit purchases can be used to activate an auto-payment.

Your employees use Yammer as a private social network that enables employees to collaborate across business applications, departments, and locations. Unfortunately, Microsoft Yammer Social Network Service can be vulnerable to multiple persistent script code injection web vulnerabilities.

DEVELOPMENT APPS:

Atlassian: Your developers and project managers use Atlassian as a hosted tool for collaboration, content sharing, and project and issue-tracking. Unfortunately, in February 2015, Atlassian suffered a data breach with roughly 2% of its users having names, email addresses,

and encrypted passwords stolen by the attackers. These could be the names, email addresses, and passwords of your employees.

GitHub is a cloud application used by your programmers and developers and known for its powerful collaboration, code review, and code management for open source and private projects. However, GitHub suffered an attack in March 2015 and endured 5 days of distributed denial service (DDoS) attacks from China. DDoS attacks have the ability to floods servers and slow down your systems. Could your company deal with days of slowed systems?

Your employees use SourceForge as a web-based source code repository. It's also a place for your software developers to manage open-source software development. Unfortunately within the last 10 years, SourceForge has faced critical attacks on its developer infrastructure, databases, and download mirror servers for its repository.

FILE SHARING APPS:

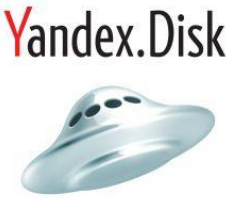
Despite being one of the most popular cloud storage services in the world, Dropbox does not offer the same level of security as an enterprise-level solution. The service is designed for personal and small business use and employees using Dropbox to store corporate documents outside of the enterprise level security could be leaving it vulnerable to more sophisticated attacks. In March 2015, a new ransomware attack called "Pacman" was identified that uses a phishing attack and utilizes Dropbox as a delivery mechanism. It only takes one click to infect a workstation and the victim has 24 hours to pay the ransom in Bitcoin.

As a consumer based cloud storage service, Google Drive suffers from some of the same security concerns as Dropbox. Google recently announced a greater focus on cloud security in their applications, but the results of that may still be further down the road. In contrary, in November 2014, Google Drive was exploited in a sophisticated phishing attack where cyber criminals published a modified version of the legitimate Google Drive login page to steal email credentials from users. Considering the popularity of Google Drive, if something like this were to happen again, there's a good chance your employees could be effected.

MyPCBackup is one of the most popular backup solutions for Androids. However, this automatic backup app can be extremely dangerous for your employees who have access to sensitive materials. Firstly, if your employees access company files on a device with MyPCBackup, they may not realize a copy is being uploaded to the cloud. Secondly, the sheer amount of data being stored on MyPCBackup makes it extremely difficult to detect any type of data misuse.

Panoramio is a geolocation photo sharing application used by your employees and owned by Google that can be accessed in Google Earth and Google Maps. It allows your employees to learn more about a given area by viewing the photos taken there. Unfortunately in 2008, Panoramio suffered a Spam attack that created thousands of accounts and comments on the photos that contained malicious links. If this happens again and your employees were to click a malicious link, then your security team would be confronted with a number of possible security problems.

WeTransfer is free cloud-based file sharing application and is a popular way to send files that are too large to send over email. Unfortunately what many of your employees don't understand is that the service is not designed to send the files securely.



Your employees use Yandex.Disk for storage, syncing, sharing, preview, and to integrate with other Yandex services. This is a risky cloud app for your employees to use because files are synced between all of the user's internet-enabled devices which may be connected to a personal network.

As a way to send, receive, digitally sign and synchronize files, YouSendIt offers solutions for personal use and businesses. While the business class version of the software may or may not be secure enough for your company – that might not be the version your employees are using. If they are using the cloud app without your knowledge or without you setting it up, they may be using the far less secure consumer-facing version to send sensitive corporate documents.

OTHER APPS:

Your marketers and content editors use Chartbeat, a web analytics app, to gain insights in real-time to be able to make decisions on what type of content to promote. Not long ago, the web traffic monitoring company was hit by a phishing attack carried out by the Syrian Electronic Army. It was reported that Chartbeat's clients' dashboards were viewed by unauthorized parties and numerous passwords were reset. These could be your company's dashboards being viewed and passwords being reset by third parties.

Your employees may download LogMeIn to their work computers to make it easier to work from home or access their stations remotely. Unfortunately, LogMeIn opens them up to remote access that could potentially harm your systems. While remote access is a good way to make your workforce more efficient, it should be carefully secured and monitored by you.

Your employees use tools like Snag It or Jing to easily take screen shots or screen recordings of their work or job functions. Unfortunately, if they are using a personal account, the pictures they take on the secure network at work will be accessible from their unsecure home network – leaving your company's data vulnerable.

This cloud application is a free, closed source BitTorrent site. Without your supervision, your employees could be using this site to download questionable torrents which could leave your system vulnerable. They could also use the service to upload torrents of sensitive information. In March 2015, employees from various companies complained that the latest update of software used for torrent downloading was silently installing a piece of unwanted software.

Do any of these apps look familiar? They should, because they are being used in your organization whether you have approved them or not.

It's important to note that employees are not using these cloud apps to intentionally leak data (for the most part, anyway). They are simply using them for convenience – to get work done. In the absence of "business-grade" file sharing and collaboration tools, cloud apps like these are viewed as a necessity. The problem occurs when they are used to "conveniently" store and transfer highly sensitive data like credit card numbers, social security numbers, health records and other types of PII. From there, you're only one weak password or lost device away from a potentially crippling data breach. These cloud apps are easy to use, but they are even easier to breach.

Of course, the initial reaction from many organizations would be to discourage the use of these cloud apps (which most do) or to block them outright. While this makes sense in theory, blocking apps sets a bad precedent and hampers productivity.

A more practical strategy would be to implement enterprise software such as ObserveIT that provides out-of-the-box reports to give your organization a clear understanding of the risks of Shadow IT and how employees are interacting with cloud applications across the company. ObserveIT allows you to quickly audit the types of applications that employees run on their desktops and laptops, such as cloud file-sharing or backup apps, torrent apps, screen capture apps or Web conferencing apps.

observe it

OBSERVEIT FEATURE HIGHLIGHTS

- **Screen capture recording** *plus* **video activity analysis** for searchable, text-based logging of all user activity
- **Real-time alerts** provide immediate awareness of suspicious, dangerous and out-of-policy behavior
- **Advanced keylogging** enables keyword searching to instantly find any on-screen mouse or keyboard action
- **Records actions in *all* system areas and *all* apps –** zero-gap recording of all commercial, legacy, bespoke and cloud apps plus all system areas
- **Supports all connection methods**, including local login, Remote Desktop, Terminal Services, PC Anywhere, Citrix, VMware, VNC, Dameware, etc.
- **SIEM, NMS** and **IT ticketing system** integration for better security and easier investigations – including direct links to session replay and user activity logs
- **Privileged User Identification**, without requiring password rotation or check-in/check-out
- **Threat detection console** detects and pinpoints suspicious activity
- **DBA Activity Audit** monitors and audits all SQL queries executed by DBAs against production databases
- **Pre-built and customizable audit reports** can be exported to Excel or XML, or scheduled to run automatically for email delivery

TRUSTED BY 1200+ CUSTOMERS

ING — *Auditing and compliance*

Coca-Cola — *Third-party monitoring*

UPS — *Privileged user monitoring*

SIEMENS — *Rapid incident response*

OBSERVEIT

IDENTIFY AND MANAGE USER-BASED RISK

Start monitoring in minutes, free:
www.observeit.com/tryitnow