

DATAWATCH

*Avoiding the riptide of
corporate data exposure*



As adoption of cloud and mobile grows, businesses are able to operate more flexibly and efficiently. However, the practices of the modern business world present a number of risks to corporate data.

With bring your own device (BYOD), employees can access corporate data and perform their job duties remotely through personal devices. This renders traditional security tools like corporate firewalls ineffective—particularly when data is accessed through unsecured WiFi.

Cloud applications enable mass sharing and breed productivity, but also allow data to be exposed to inappropriate parties. Extensive sharing increases the risk of data exfiltration and gives malware more opportunities to infect organizations.

Bitglass' Threat Research Team tested two real-world scenarios—public WiFi use and sharing of data from within a cloud app—to uncover the risks posed by users' data-related habits.



PUBLIC WATERS

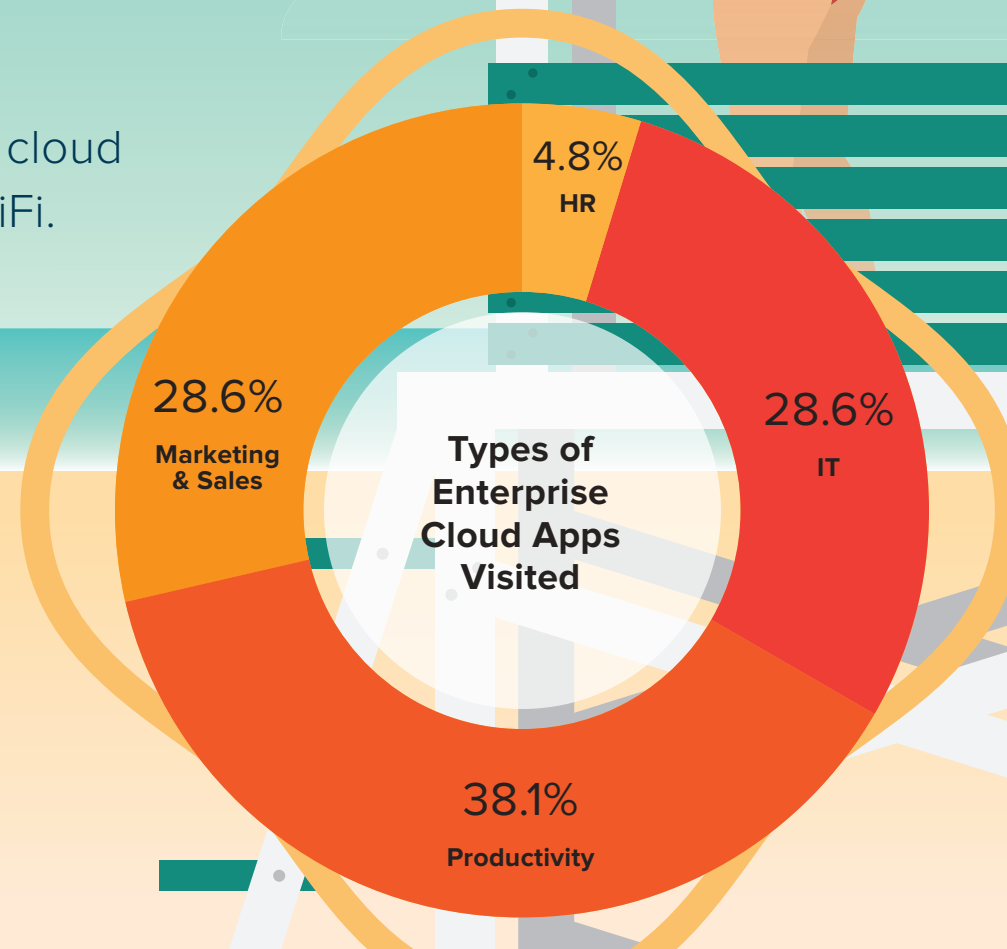
Of the world's many employees, a large number are likely to connect to unsecured public WiFi and access enterprise cloud applications. By setting up unsecured WiFi hotspots in random public spaces and monitoring traffic through a packet sniffer, Bitglass was able to observe the browsing behaviors of a sample of the general public.

One in five individuals connected to Bitglass' unsecured WiFi.

11.2% accessed enterprise cloud applications like Office 365, Salesforce, Adobe Marketing Cloud, and ADP.

At **38.1%**, productivity apps were the enterprise cloud apps most commonly visited over unsecured WiFi.

Visits to sites like Facebook and YouTube dominated the traffic. However, users also accessed personal banking domains like Wells Fargo, Chase, Bank of America, Capital One, and Citibank. Two connected devices even navigated to malware hosts. Had a malicious hacker done the same as Bitglass, credentials and much more could easily have been stolen via deep packet inspection.



SHARING THE BEACH

Like public WiFi, cloud apps introduce a heightened risk of data leakage. Through excessive sharing, employees can leave massive volumes of corporate data exposed to unauthorized users. What's more, cloud data sharing can facilitate the spread of malware. Bitglass analyzed customers' cloud applications to uncover information about data sharing.

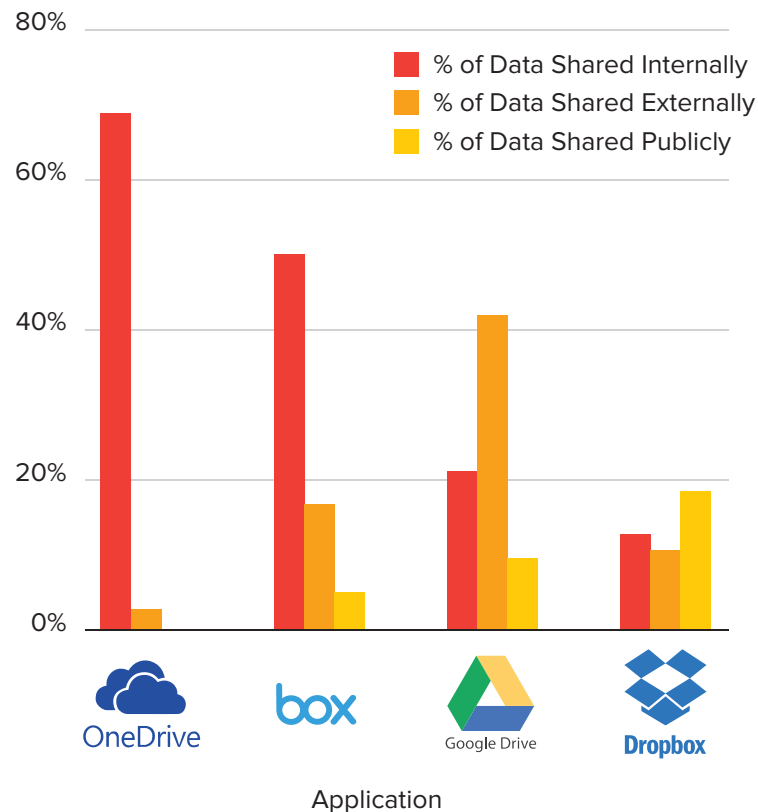
72% of data stored in Box, Google Drive, and OneDrive is shared in some capacity.

On average, organizations have **69.5%** of OneDrive data shared internally.

51.3% of data stored in Google Drive is shared with individuals outside of the enterprise—significantly more than data in other apps.

At **18.9%**, more corporate data is publically available in Dropbox than any other app.

Volume of Shared Cloud Data



The same results held true when considering numbers of files instead of amounts of storage—Office 365 is widely used for internal sharing but not external sharing, Google Drive is widely used for both external and internal sharing, and Dropbox is the SaaS app with the most publically shared documents.

CREDENTIALS ADRIFT

Large amounts of shared data and shared files indicate the potential for the proliferation of malware, as well as how easily one set of stolen credentials can lead to extensive data theft. **Digital Shadows** gathered and analyzed data on leaked credentials on the Dark Web—the results suggested that leaked credentials should be a growing concern. With malicious intent, corporate and personal credentials can easily be stolen.



97% of organizations have some form of stolen credentials available to the public online.

Average number of leaked employee credentials

1,800 in financial services

3,400 in healthcare



METHODOLOGIES

Public WiFi

Bitglass' Threat Research Team set up an open WiFi access point for two-hour increments at random times of day in random public spaces. This was done in order to see how many people would connect and what websites they would visit on an unsecured network. Of the 834 people in the public spaces, 187 unique devices connected to the unsecured WiFi and were monitored. Bitglass only collected source and destination IPs and packet headers—no sensitive data was tracked or saved. Destination IPs were run through Bitglass in order to identify threats and destinations deemed risky by Bitglass' algorithm.

Sharing and Malware

Via API crawling, Bitglass analyzed enterprise customers' storage data to uncover the average volume of data and files at rest in their cloud apps. Using Bitglass' analytics engine, the team looked at data shares and which applications were most prone to excessive sharing. Bitglass customers may exhibit greater comfort storing sensitive data in cloud apps because they have Bitglass deployed. However, the fact remains that average employees are the ones sharing data, they tend not to consider sharing best practices, and even one set of compromised credentials can lead to a large amount of corporate data access.





KEEPING EYES ON YOUR DATA

Public WiFi use is a major challenge for organizations because unmanaged devices are so common. The best way to solve this challenge is to control access from unmanaged devices and limit access in risky contexts.

As for external sharing, the sheer volume of sensitive data shared out of widely used SaaS applications should be a point of concern for organizations. In addition to utilizing native security features, they should adopt a third-party solution that provides greater visibility and control over data in the cloud.

Whether it's ransomware, careless insiders, hackers, or other threats, enterprises are faced with many security concerns. Rather than turning a blind eye or relying on traditional security measures, firms must search for one complete solution to protect cloud data.

ABOUT BITGLASS

Bitglass' Total Cloud Security Platform is the only secure access service edge offering that combines a Gartner-MQ-Leading cloud access security broker, the world's only on-device secure web gateway, and zero trust network access to secure any interaction. Its Polyscale Architecture boasts an industry-leading uptime of 99.99% and delivers unrivaled performance and real-time scalability to any location in the world. Based in Silicon Valley with offices worldwide, the company is backed by Tier 1 investors and was founded in 2013 by a team of industry veterans with a proven track record of innovation and execution.











Phone: (408) 337-0190

Email: info@bitglass.com

www.bitglass.com

APPENDIX

Application (on Average)	GB of Corporate Data	GB of Data Shared Internally	GB of Data Shared Externally	GB of Data Shared Publicly	% of Data Shared Internally	% of Data Shared Externally	% of Data Shared Publicly	% of All Data Shared
	128.2	64.7	21.3	6.7	50.5%	16.6%	5.2%	72.3%
	811.2	118.5	92.3	153.6	14.6%	11.4%	18.9%	44.9%
	801.1	167.2	333.5	77.7	20.9%	41.6%	9.7%	72.2%
	208.6	145.0	6.6	0.6	69.5%	3.1%	0.3%	72.9%

Application (on Average)	Count of Corporate Files	Count of Files Shared Internally	Count of Files Shared Externally	Count of Files Shared Publicly	% of Files Shared Internally	% of Files Shared Externally	% of Files Shared Publicly	% of All Files Shared
	63,087	21,044	5,780	669	33.4%	9.2%	1.1%	43.6%
	176,953	17,571	12,647	20,396	9.9%	7.1%	11.5%	28.6%
	102,232	30,379	12,673	1,967	29.7%	12.4%	1.9%	44.0%
	175,232	109,517	5,006	72	62.5%	2.9%	0.04%	65.4%