

Cloudy Security?

Accelerate Cloud Adoption and Safeguard the Business

Andy Land
Director of Cloud Security Products
October 1, 2015



Cloudy Security: So What's the Problem?

1 in **3**

Fortune 1000 employees
upload corporate
data to cloud apps

50%

of millennials
use third-party
cloud apps at work

1 in **4**

Fortune 1000 employees
use corporate log-in details for
cloud apps

60%

of employees know using
external apps is a violation of
their company's security policy

On behalf of IBM Security, Ketchum Global Research & Analytics (KGRA) conducted an online survey using the services of Ipsos Public Affairs. The survey interviewed 1,001 full-time employees at Fortune 1000 companies. The survey was fielded from July 27 to 31, 2015.

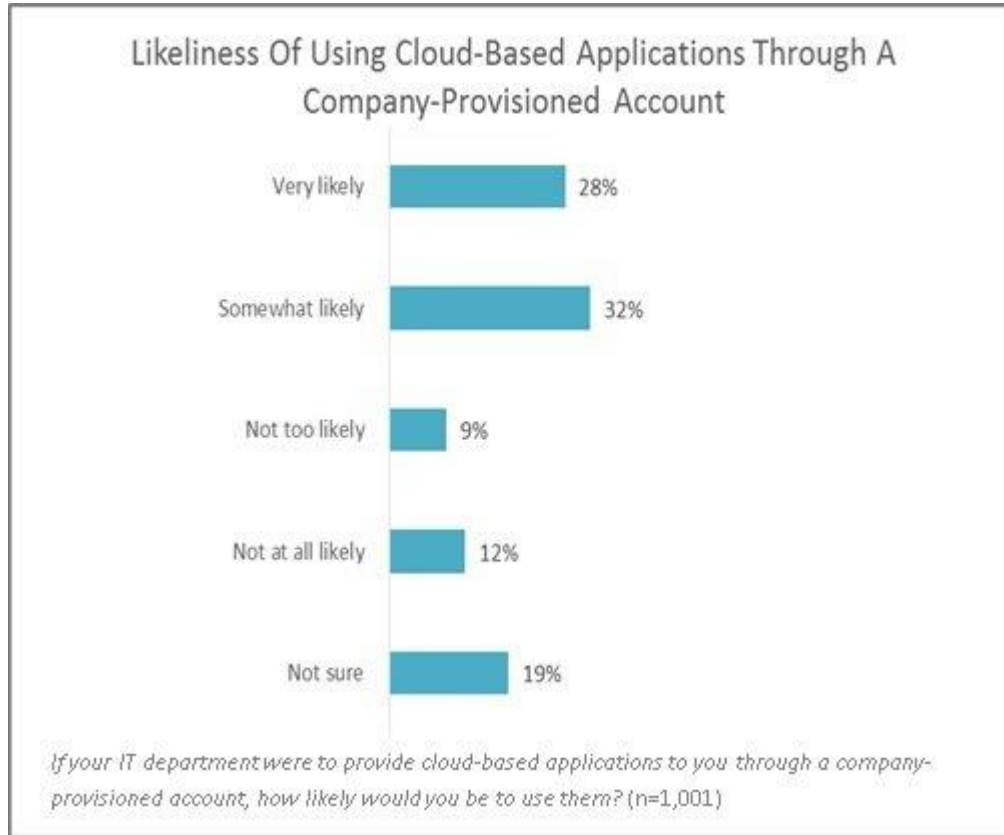
Cloudy Security: What are Employees Thinking?



- Access their data anytime, anywhere (45%)
- Ability to do jobs better and more efficiently (37%)
- External cloud apps are faster and more convenient than internal apps (26%)

On behalf of IBM Security, Ketchum Global Research & Analytics (KGRA) conducted an online survey using the services of Ipsos Public Affairs. The survey interviewed 1,001 full-time employees at Fortune 1000 companies. The survey was fielded from July 27 to 31, 2015.

Cloudy Security: If We Provide It, Will They Come?



60%
of Fortune 1000 employees
would likely use IT-approved
cloud apps.

75%
Nearly 75% of millennial
workers would use IT-
approved cloud apps.

On behalf of IBM Security, Ketchum Global Research & Analytics (KGRA) conducted an online survey using the services of Ipsos Public Affairs. The survey interviewed 1,001 full-time employees at Fortune 1000 companies. The survey was fielded from July 27 to 31, 2015.

Cloud is here to stay, are you ready to move with the business?



EMPLOYEES

- Look for better ways to get their jobs done
- Find cloud services quick and easy to use



IT OPERATIONS

- Wants to save money and reduce complexity
- Wants to automate and consolidate IT



YOUR BUSINESS

- Loses visibility and control over IT
- New risk requires new safeguards

Security and IT leaders face new challenges



“My team is not equipped to manage the increased employee usage and demand for cloud”

CISO / CIO:

How does my organization?

- Uncover “Shadow IT”
- Gain visibility of all cloud app usage
- Simplify connecting to approved apps
- Remove mobile blind spots
- Stop risky user behavior
- Quickly react to cloud threats
- Address compliance and governance concerns

Introducing IBM Cloud Security Enforcer



DETECT

Usage of cloud apps and actions

CONNECT

Users to approved cloud apps

PROTECT

Against cloud-related threats

A new SaaS solution to help securely deploy cloud services





DETECT

App usage and user activity

Good morning

All systems are running.
Here are some items that may need your attention.

- New Log Source**
Bluecoat0177282
- Open**
24 application requests
- Connected**
2 applications connected

Quick Insights

Last updated today at 8:23am

Past 30 Days

High Risk Applications

487

Total Applications

1.3k

Unique Users

10.2k

High Offenses

89

Applications

Unknown **527** ↗ Connected **996** ↗

High Risk Applications vs. Total Applications



Proxies

Beta

Proxy Users **1.4k** ↘ Proxies Online **5**

Proxy Latency by Data Center



Offenses

Active **1.3k** ↗ Hidden **37** ↘

High Offenses vs. Total Offenses



Users

Unknown **73** ↗ High Risk **723** ↘

Top Offenders

Application

Zippy Share Business

56 high alerts
1.2k total users

DETECT APPROVED / SHADOW APPS

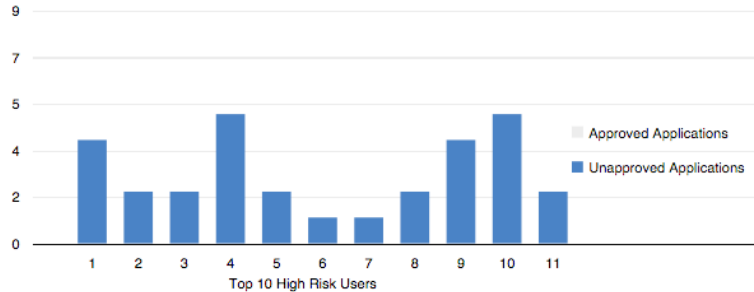
- Discover thousands of cloud apps
- View analytics and risk reports
- Chart progress over time



Users

Last updated Today at 4:51 AM

Past 30 days



High Risk
896

Rogue Activity
12k

Total Activity
13k

Search

Score	Name	Department
10.0	lula.paradiso@us.ibm.com	
10.0	camelia.mattsey@us.ibm.com	
10.0	nita.hotaling@us.ibm.com	
10.0	johnathon.liebowitz@us.ibm.com	

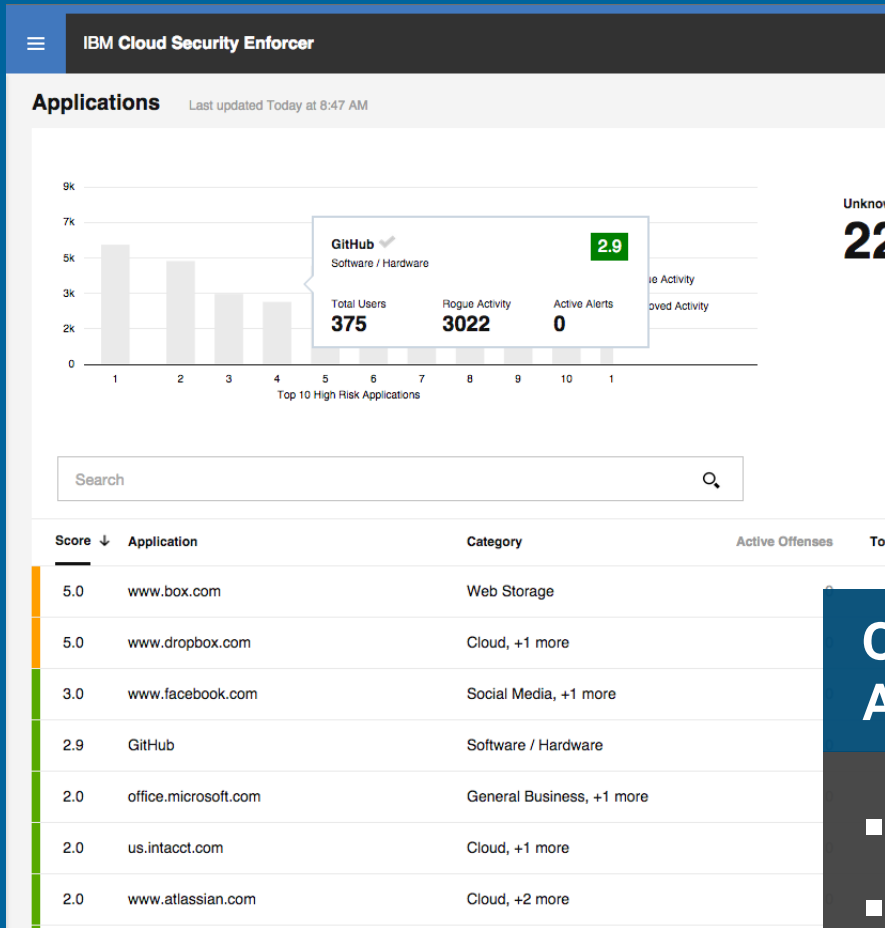
DETECT DETAILED USER ACTIVITY

- Correlate cloud activity to employees
- Identify suspicious activities and trends
- See and respond to priority alerts



CONNECT

Users to approved cloud apps



GitHub
Approved ✓ Connected ✓ Flagged

Score **2.9**

Overview **Connections** Users Offenses

Add a new connection

GitHub Connector Expand

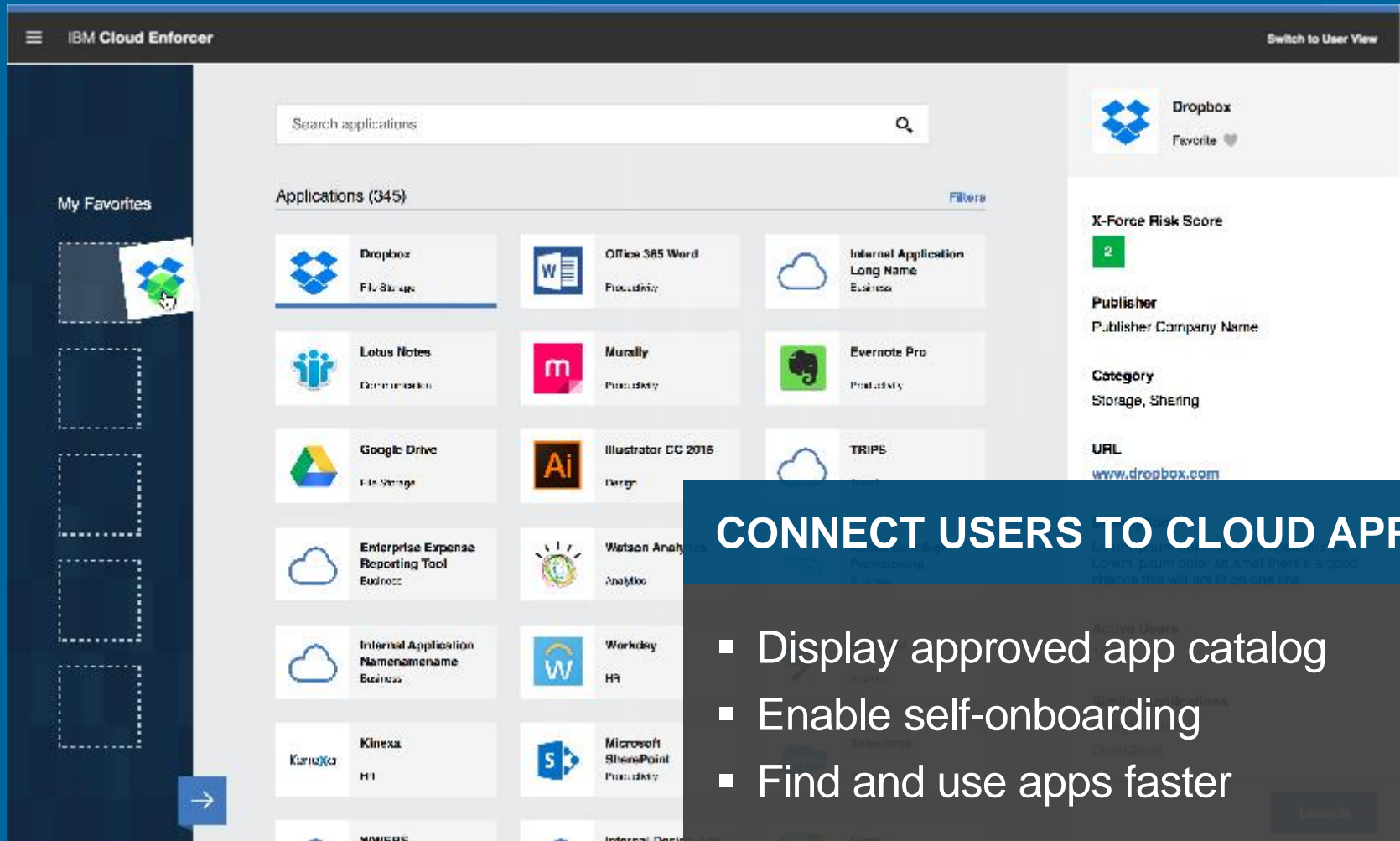
GitHub Connector for NA Dev Team Collapse

Last Utilized September 30, 2015

Enabled

CONNECT THE BUSINESS TO APPROVED APPS, DISABLE OTHERS

- On/Off toggles for cloud access
- Correct out of policy application usage



CONNECT USERS TO CLOUD APPS

- Display approved app catalog
- Enable self-onboarding
- Find and use apps faster



Protect

Against cloud-related threats

IBM Cloud Enforcer

Applications Last updated Today at 12:34pm ↻

Unknown **7k** Unapproved **3k**

Top Insight
The use of unapproved applica...

Internal Application Long Nomenclature **Score 8.6**
Approved ✓ Connected ✓ Flagged ⚑

Overview | Connections | Users | Offenses

Total Offenses **456** Total Users **12k** Rogue Activity **878**

X-Force Details [View in X-Force Exchange](#)

X-Force Risk Score 8.6
Malware Detected Yes (4)

Application IPs 72.21.192.019 (United States)
72.21.192.019 (Germany)
72.21.192.019 (Canada)
[+9 more](#)

Publisher Publisher Company Name
Category Business, Authorization

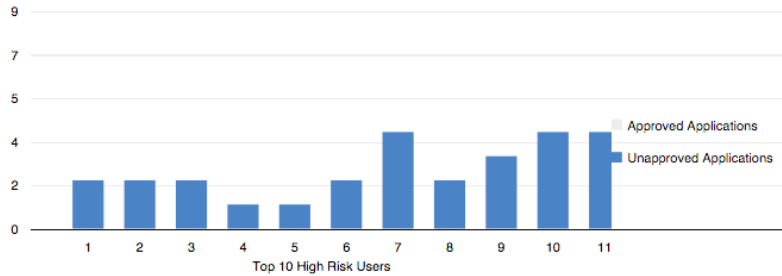
Score	Application	Category	Active Offenses ↓	Total Users
8.6	Office 365 Excel	Business, +2 More	125,256	872,000
8.6	Internal Application L...	Business, +1 More	456	12,000
5.9	Evernote	Productivity	406	1,500
6.7	Google Docs	Storage, +1 More	375	5,000
4.0	Adobe Acrobat	Business	275	500

PROTECT AGAINST RISKY APPS

- Understand cloud app reputation
- Prioritize apps based on past threats
- Limit interaction with unsafe apps



Users Last updated Today at 3:44 PM



High Risk
694

Past 30 days

Last active January 8, 2017 at 3:50 PM
antione.barbor@us.ibm.com
Flagged

Score 10.0

Overview Applications Offenses

Rogue Activity

Top 10 Applications [View Full List](#)

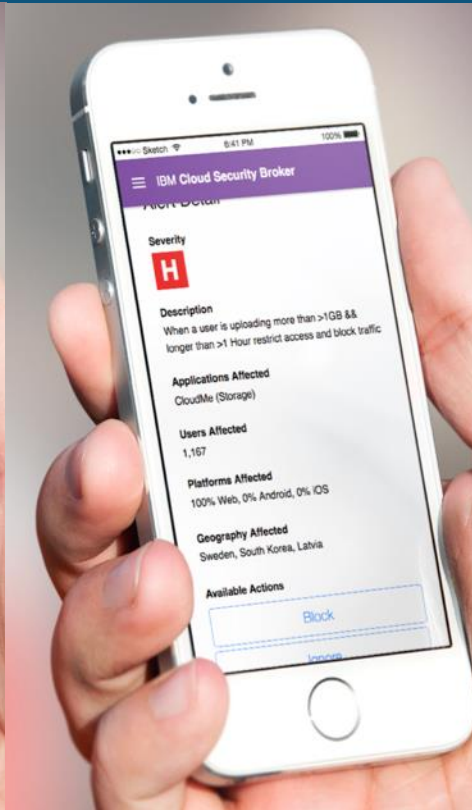
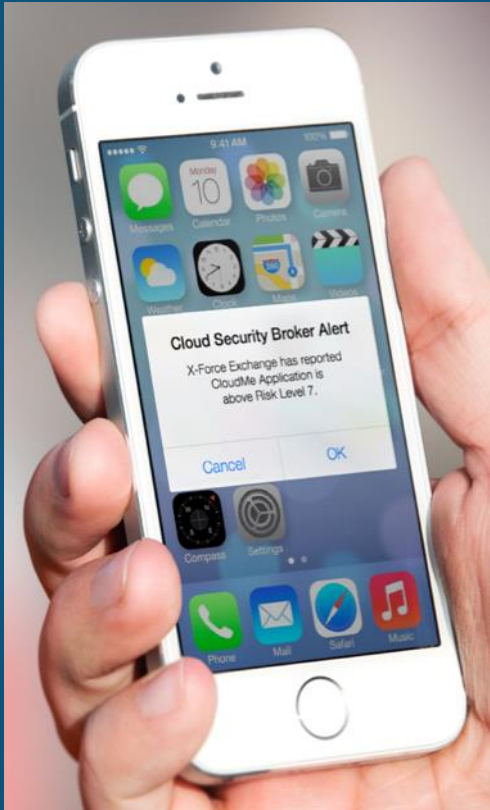
Score	Application	Rogue Activity	Last Accessed
7	Application Longname	11,201	15 May, 2015

Search

Score ↓	Name	Department
10.0	camelia.mattsey@us.ibm.com	
10.0	nita.hotaling@us.ibm.com	
10.0	antione.barbor@us.ibm.com	
10.0	shelba.osborn@us.ibm.com	
10.0	clint.rinde@us.ibm.com	
10.0	rubin.arnall@us.ibm.com	

PROTECT AGAINST RISKY BEHAVIOR

- Establish user risk ratings
- Address “rogue” cloud app usage
- Block specific actions to/from the cloud



PROTECT WITH RAPID RESPONSE TO THREATS

- Respond to new threats, in or out of the office
- Integrated with threat intelligence from IBM X-Force

PROTECT BY LIMITING ACCESS

- Block risky or unsanctioned apps on mobile devices
- Coach safe employee usage





IBM Cloud Security Enforcer

- 1 Industry's first solution to combine cloud discovery, access, and threat prevention
- 2 Connect users to Cloud apps in seconds
- 3 Protect against Cloud threats using IBM's network of threat intelligence
- 4 Speed cloud adoption, making your employees more productive

ibm.com/security/cloud-enforcer

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

THANK YOU

www.ibm.com/security



IBM Security

Intelligence. Integration. Expertise.

© Copyright IBM Corporation 2015. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and / or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.