

Bringing Cloud out of the Shadows

Accelerate Cloud Adoption and Safeguard the Business



How many IT directors are in your organization?



**HR
Manager**



**Web
Master**



**Marketing
Guy**

Shadow IT makes anyone an IT Director

1 in 3

1 in 4

50%

60%



1

Accessibility



2

Helps me do my job



3

Speed / convenience

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

The right tools are essential



NO! I CAN'T BE BOTHERED TO SEE ANY PESKY SALESMAN . . . I'VE GOT A BATTLE TO FIGHT!

Cloud Access Security Brokers (CASB)



“By 2020, 85% of large enterprises will use a cloud access security broker product for their cloud services”

Emerging Technology Analysis: Cloud Access Security Brokers

CASB Pillar	Big Rocks: Major Differentiating Features
Visibility	<ul style="list-style-type: none">Automated alerting and reporting based on custom rules and risk indicatorsLogging and monitoring of all activities and transactionsMachine learning/algorithmic analysis of usage patterns
Compliance	<ul style="list-style-type: none">User activity and transaction monitoringSaaS API-based monitoring reporting capabilities that map to regimes such as the U.S. Health Insurance Portability and Accountability Act and the Payment Card Industry Data Security StandardAbility to search for cloud apps by risk attribute (for example, availability of encryption standards, two-factor authentication and certifications earned) and take deployment decisions that align with compliance mandates
Threat Prevention	<ul style="list-style-type: none">Granular access control based on enterprise access control policiesHeuristics and user/device behavior baselines for anomaly detectionMalware detection/monitoring
Data Security	<ul style="list-style-type: none">Preserving application functionality (via integration with SaaS provider APIs) while implementing encryption and tokenization APIsWeb application firewall as part of CASB platformMobile and cloud DLP functionality

If I Told You IBM is Now in the CASB market, You Might Think...



Who did IBM partner with/buy?



This is probably just a “Frankenstein” of IBM products, right?



This is so un-IBM

What was IBM's Approach?

1 We looked at existing solutions in the market

2 We looked at our existing portfolio

3 We adopted a new attitude

4 We innovated

5 We moved *fast*

Introducing IBM Cloud Security Enforcer

CASB, IDaaS, & Threat Prevention



DETECT

Usage of cloud apps and actions

CONNECT

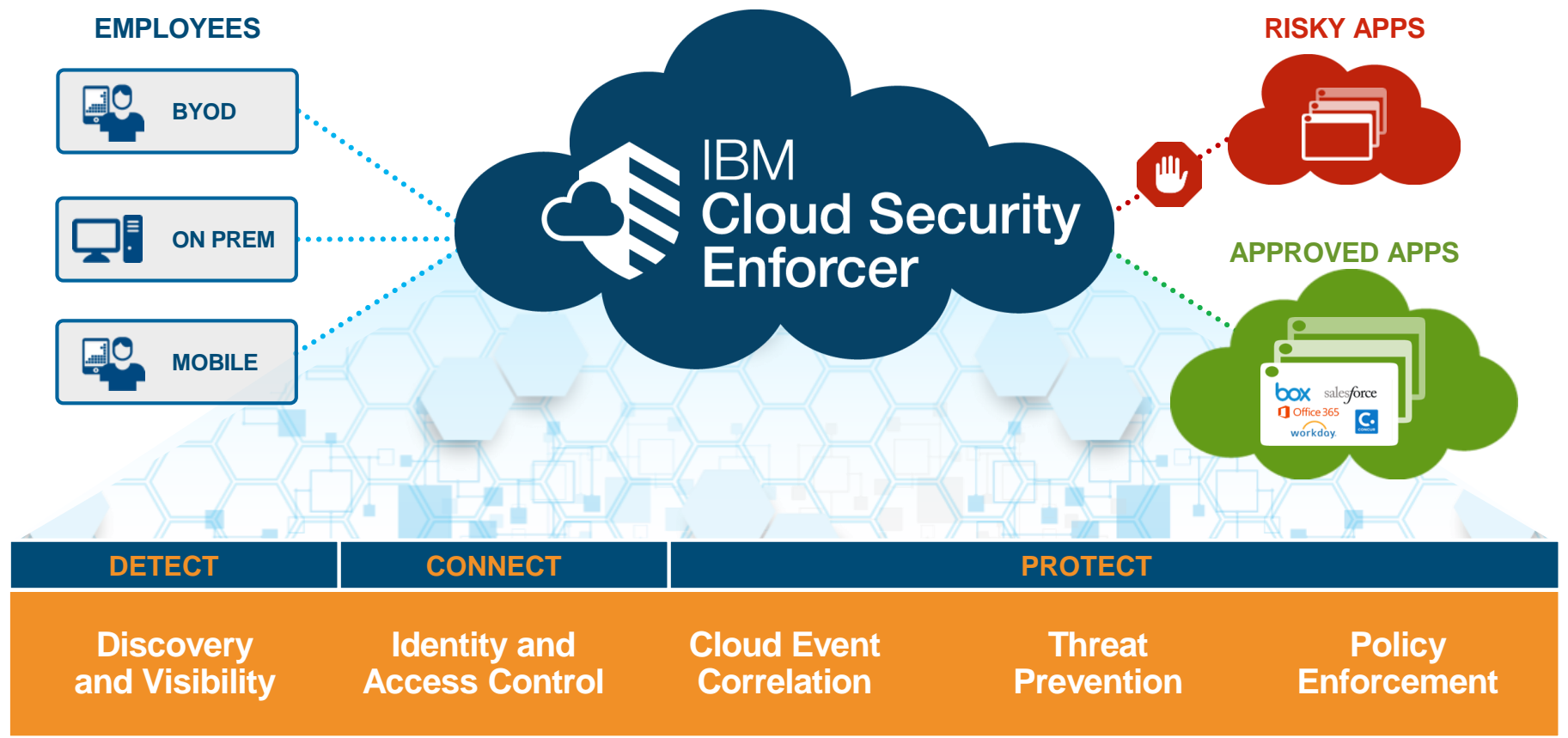
Users to approved cloud apps

PROTECT

Against cloud-related threats

IBM Cloud Security Enforcer

Adopt the Cloud but Without The Risk





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	Connected
527 ↗	996 ↗

High Risk Applications vs. Total Applications



Proxies

Beta

Proxy Users	Proxies Online
1.4k ↘	5

Proxy Latency by Data Center



Offenses

Active	Hidden
1.3k ↗	37 ↘

High Offenses vs. Total Offenses



Users

Unknown	High Risk
73 ↗	723 ↘

Top Offenders

Application

Zippy Share Business

56 high alerts
1.2k total users

DETECT APPROVED / SHADOW APPS

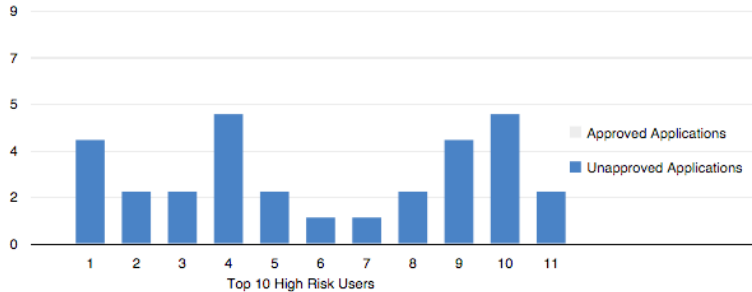
- Discover thousands of cloud apps
- View analytics and risk reports
- Chart progress over time



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	

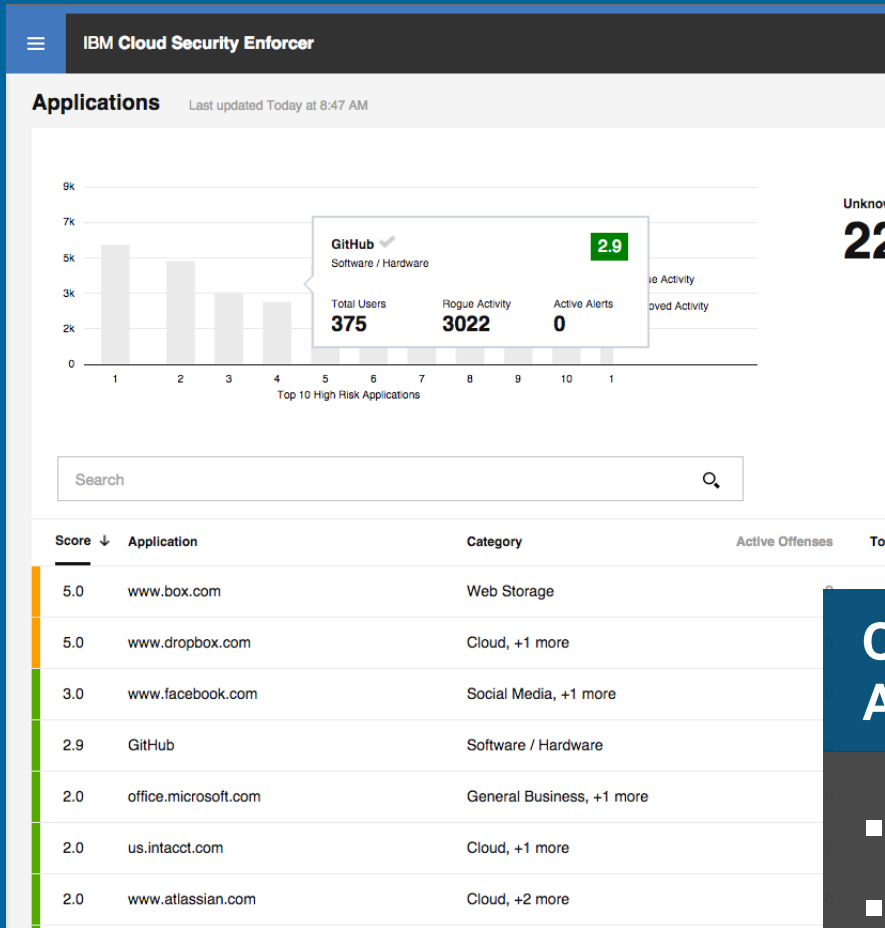
DETECT DETAILED USER ACTIVITY

- 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

Search applications

Applications (345) Filters

box
File Storage

Office 365 Word
Productivity

Internal Application Long Name
Business

Lotus Notes
Communication

Murally
Productivity

Evernote Pro
Productivity

Google Drive
File Storage

Illustrator CC 2015
Design

TRIPS
Travel

Enterprise Expense Reporting Tool
Business

Watson Analytics
Analytics

Internal Application Nomenclature
Business

Workday
HR

Kinexa
HR

Microsoft SharePoint
Productivity

WWERS

Internal Design App

box
Favorite

X-Force Risk Score
2

Publisher
Publisher Company Name

Category
Storage, Sharing

URL
www.box.com

Description

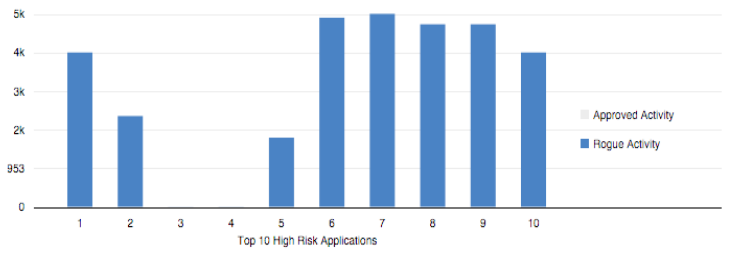
CONNECT USERS TO CLOUD APPS

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



Protect

Against cloud-related threats



Unknown **24** Unapproved **1k**

Application Search

Score ↓	Application	Category
10.0	thepiratebay.se	Computer Crime / Hack...
10.0	sgs.us.com	Malware
10.0	filimifullizle.com	Cinema / Television, +
10.0	movie4k.to	Cinema / Television, +
10.0	buluperindu.3eeweb.com	Phishing URLs, +1 mo
10.0	kinox.to	Blogs / Bulletin Boards
10.0	torcache.net	Cinema / Television, +
10.0	zone-telechargement.com	Cinema / Television, +

thepiratebay.se
 Approved ✓ Connected ✓ Flagged F

Score 10.0

Overview | Connections | Users

Total Offenses: **0** | Total Users: **3k** | Rogue Activity: **3k**

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

X-Force Risk Score: 10.0
Malware Detected: No

Application IPs: 75.126.181.228 (NorthAmerica.UnitedStates), 141.101.118.194 (NorthAmerica.UnitedStates), 141.101.118.195 (NorthAmerica.UnitedStates)

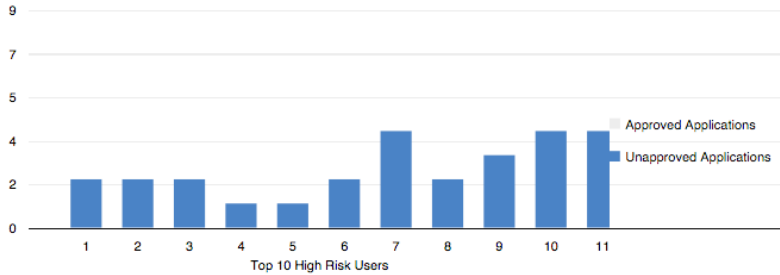
Category: Computer Crime / Hacking, Illegal Activities, Search Engines / Web Catalogs / Portals, Warez / Software Piracy

PROTECT AGAINST RISKY APPS

- Understand cloud app score
- 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

Integrating leading IBM security technology into a single platform



DETECT

Discovery and Visibility

- Risk scoring for 1000's of apps
- Continuous stream of cloud activity data
- Mapping of network data to specific users
- Mobile integration to uncover blind spots

CONNECT

Identity and Access Control

- Federated cloud SSO
- Connectors to popular cloud apps
- Simplified access controls
- Self-service catalogs
- Delegated administration

PROTECT

Cloud Event Correlation

- User activity and traffic monitoring
- Behavioral analysis and correlation to company policies
- Alerting, reporting, and auditing

Threat Prevention

- Intrusion Prevention and global threat intelligence from IBM X-Force
- Threat signatures, network analysis, and zero-day threat protection

Policy Enforcement

- User coaching
- Redirection for out-of-policy usage
- Policy and anomaly rule implementation

Key takeaways



IBM Cloud Security Enforcer

- 1 Industry's first solution to combine cloud discovery, identity & access, and threat prevention
- 2 Connects users to Cloud apps in seconds
- 3 Protects against Cloud threats using IBM's network of threat intelligence

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.

BACKUP



Mobile apps a big concern

Millennials and their smartphones...

87%

have their smartphone at their side, day and night

78%

spend over 2 hours a day using their smartphones

68%

consider their smartphone to be a personal device



[Source: "55 US Mobile Facts Every Marketer Needs For 2015" by Heidi Cohen, December 2014](#)

By 2017, mobile devices will make up **87%** of Internet-enabled technology total sales

[Source: Lander Blog, "Five Online Marketing Trends for 2014, April 2014](#)

46% say their smartphone is something they couldn't live without

[Source: "6 facts about Americans and their smartphones" by Pew Research Center, April 2015](#)

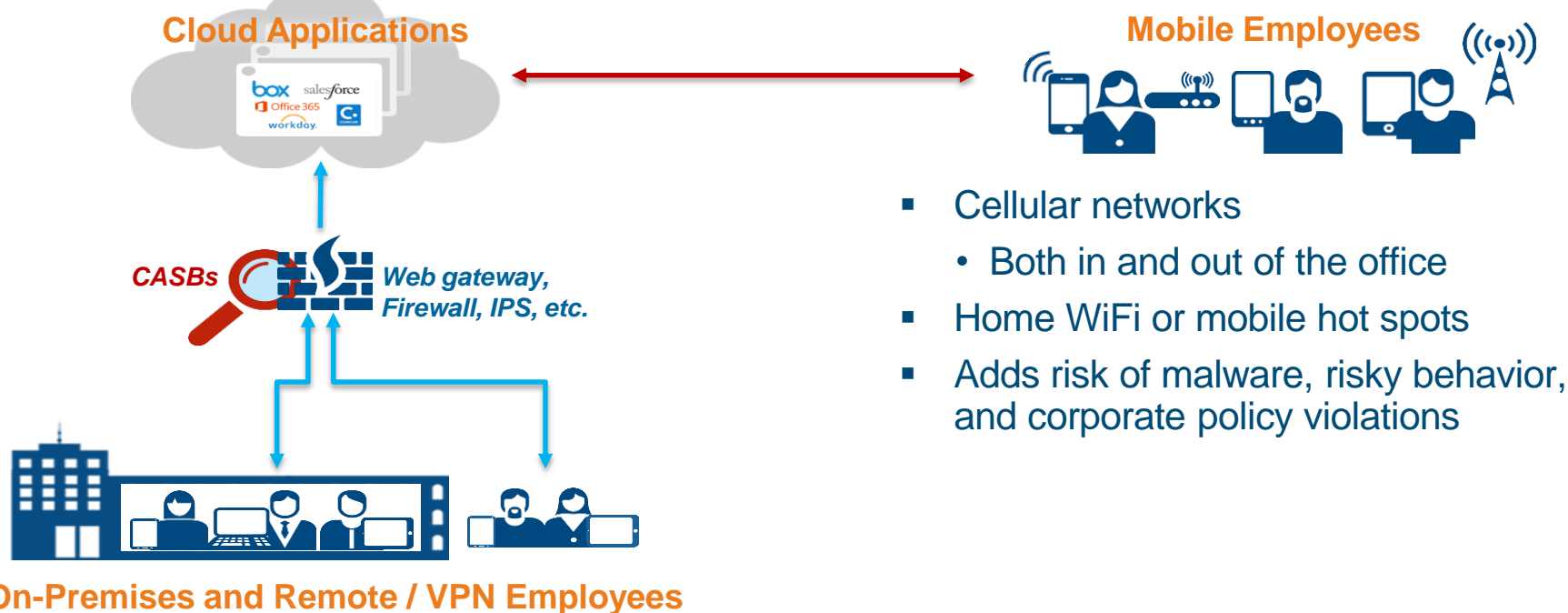
How Can You Protect What You Can't See?

CASBs are an important visibility

CASBs collect cloud app usage details on traffic going through corporate gateways

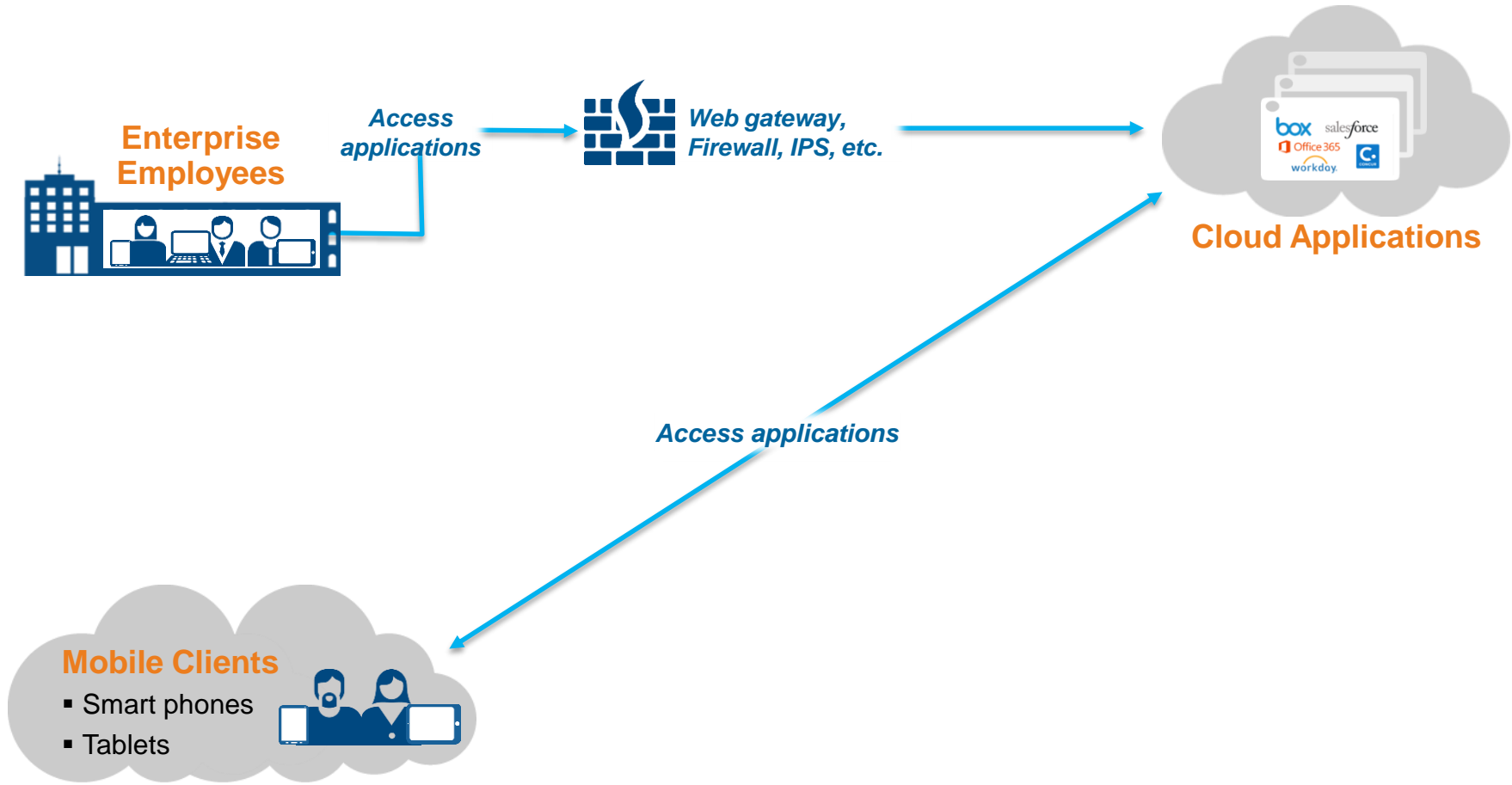
"Blind spots" still exist for mobile usage

Mobile users can go directly to cloud apps – creating the "mobile blind spot"

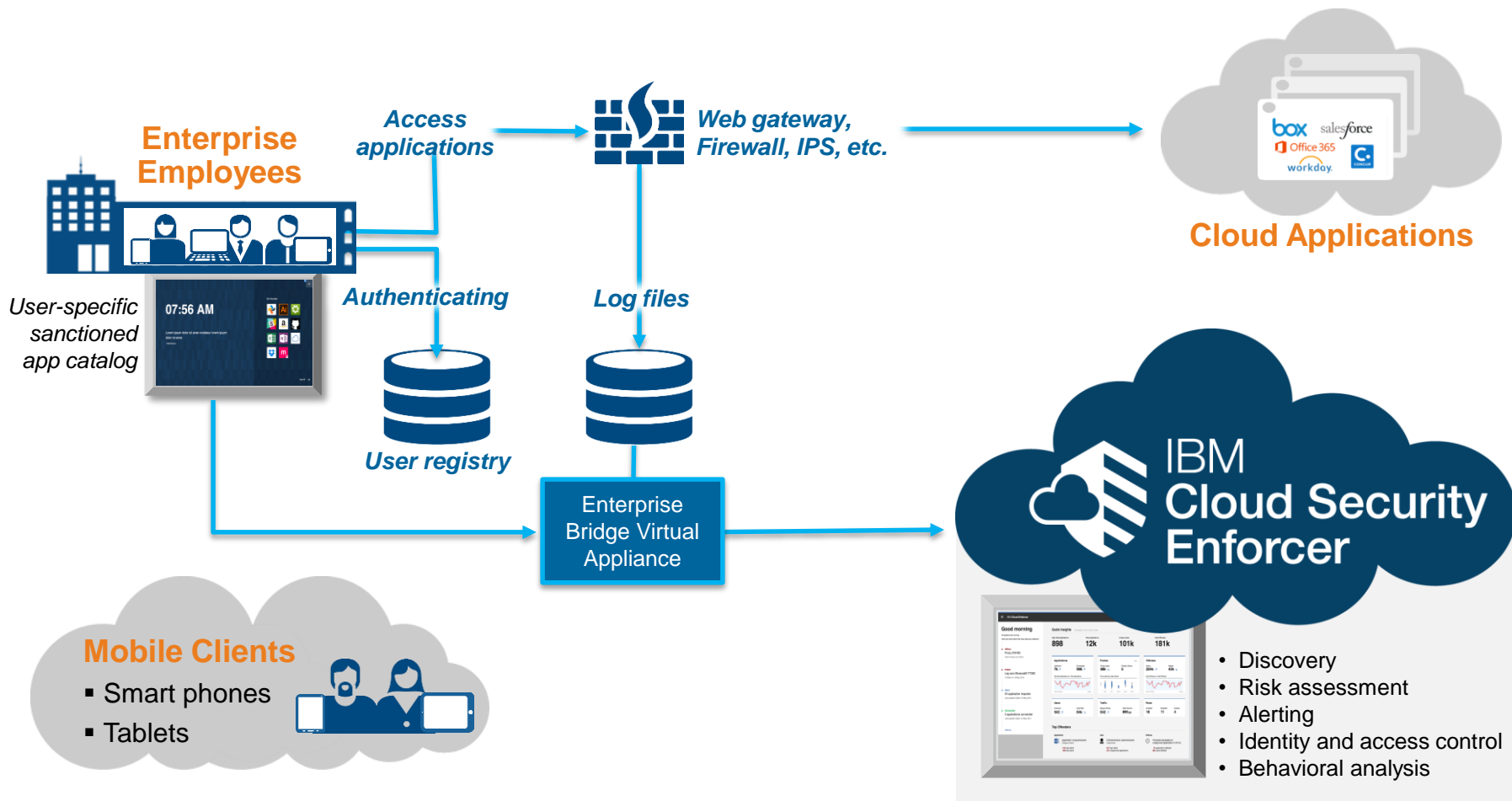


- Cellular networks
 - Both in and out of the office
- Home WiFi or mobile hot spots
- Adds risk of malware, risky behavior, and corporate policy violations

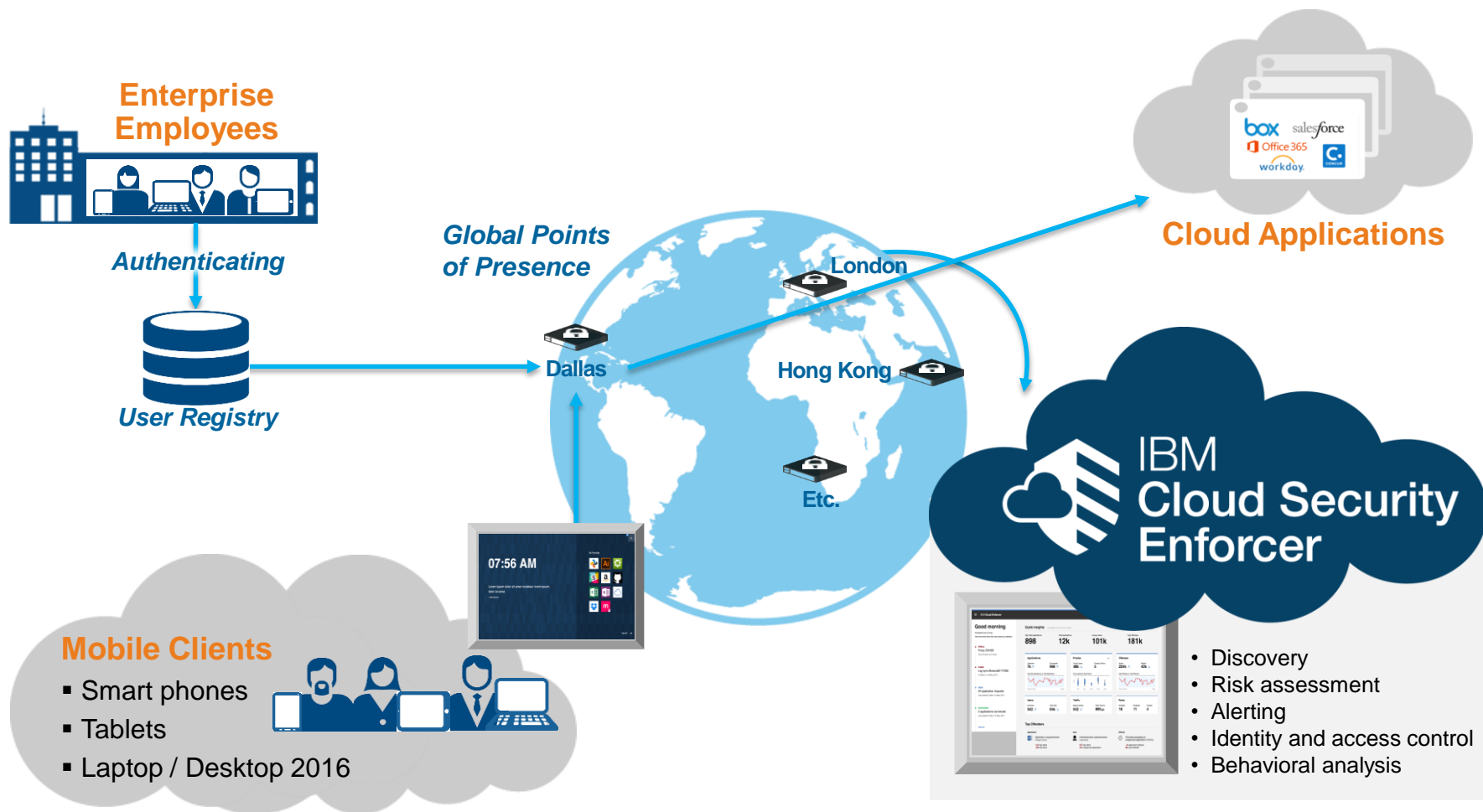
Cloud Application Usage Today



In-enterprise application visibility and control



Mobile application visibility, control and protection



IBM X-Force Exchange



A new platform to consume, share, and act on threat intelligence

Research and collaboration platform and API

Security Analysts and Researchers



Security Operations Centers (SOCs)

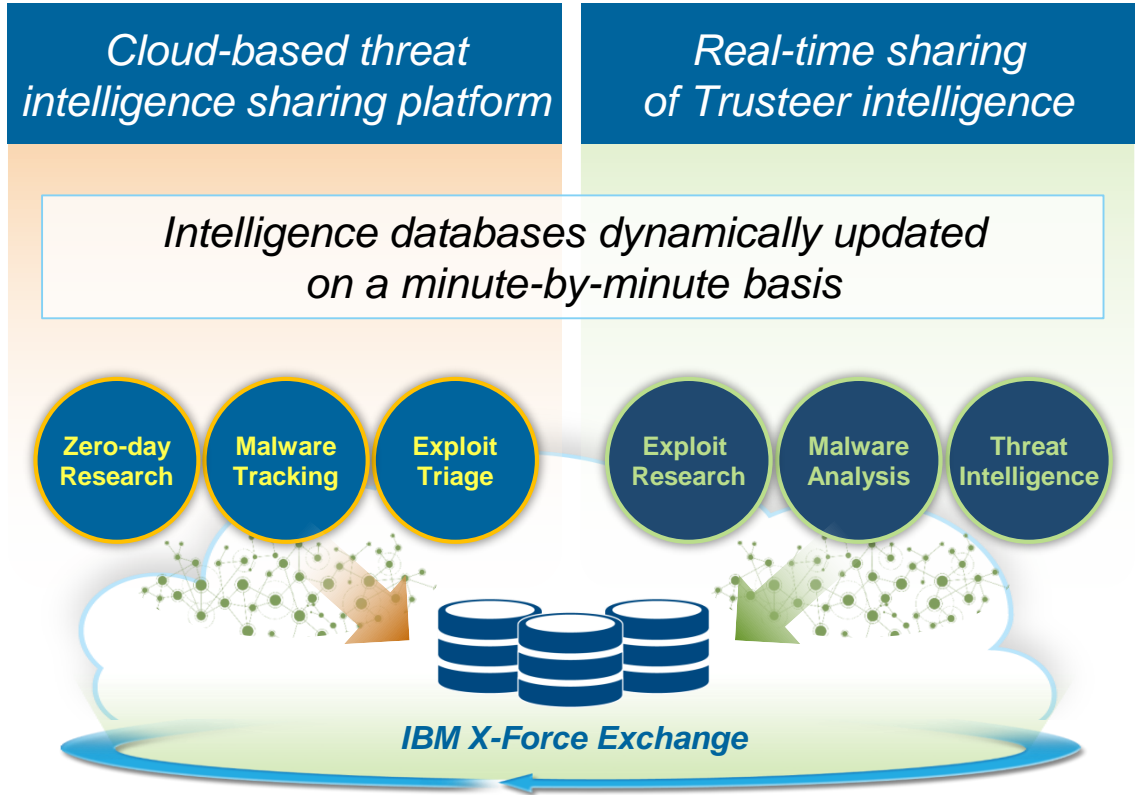
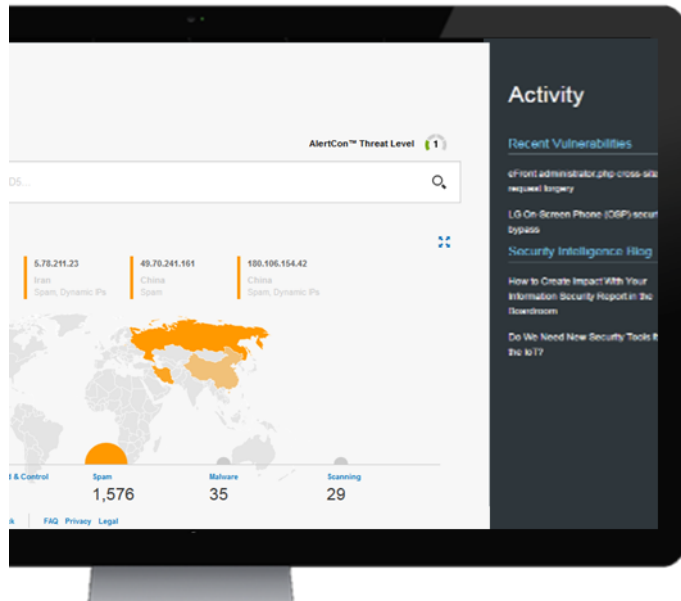


Security Products and Technologies



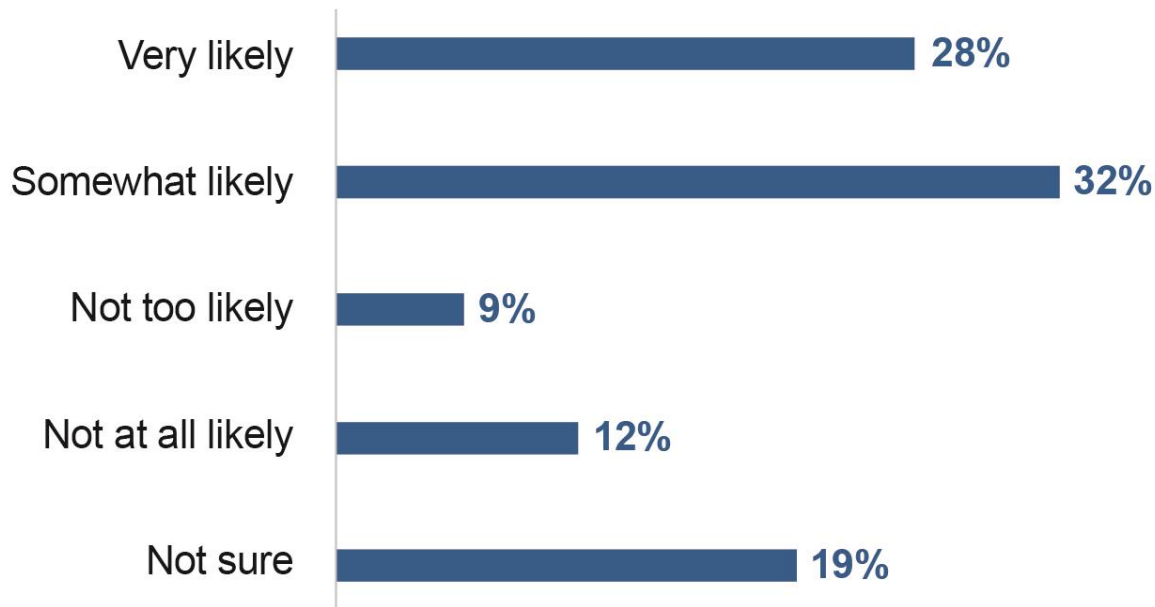
- Anonymized threat information from monitoring **15B+ security events** daily
- Real-time global threat intelligence from **270M+** endpoints
- Data based on threat monitoring of **25B+** web pages and images
- One of world's largest database of **89K+** vulnerabilities
- Deep intelligence on **8M+** spam and phishing attacks
- Reputation data with **860K+** malicious IP addresses

Join the IBM X-Force Exchange



Cataloging 88K+ vulnerabilities, 25B+ web pages, and data from 100M+ endpoints

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.