IBM Security

Intelligence. Integration. Expertise.

IBM

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%

Accessibility

Helps me do my job

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

Cloud Access Security Brokers (CASB)

Gartner®

"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	▪ Automated alerting and reporting based on custom rules and risk indicators ▪ Logging and monitoring of all activities and transactions ▪ Machine learning/algorithmic analysis of usage patterns
Compliance	▪ User activity and transaction monitoring ▪ SaaS 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 Standard ▪ Ability 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	▪ Granular access control based on enterprise access control policies ▪ Heuristics and user/device behavior baselines for anomaly detection ▪ Malware detection/monitoring
Data Security	▪ Preserving application functionality (via integration with SaaS provider APIs) while implementing encryption and tokenization APIs ▪ Web application firewall as part of CASB platform ▪ Mobile 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

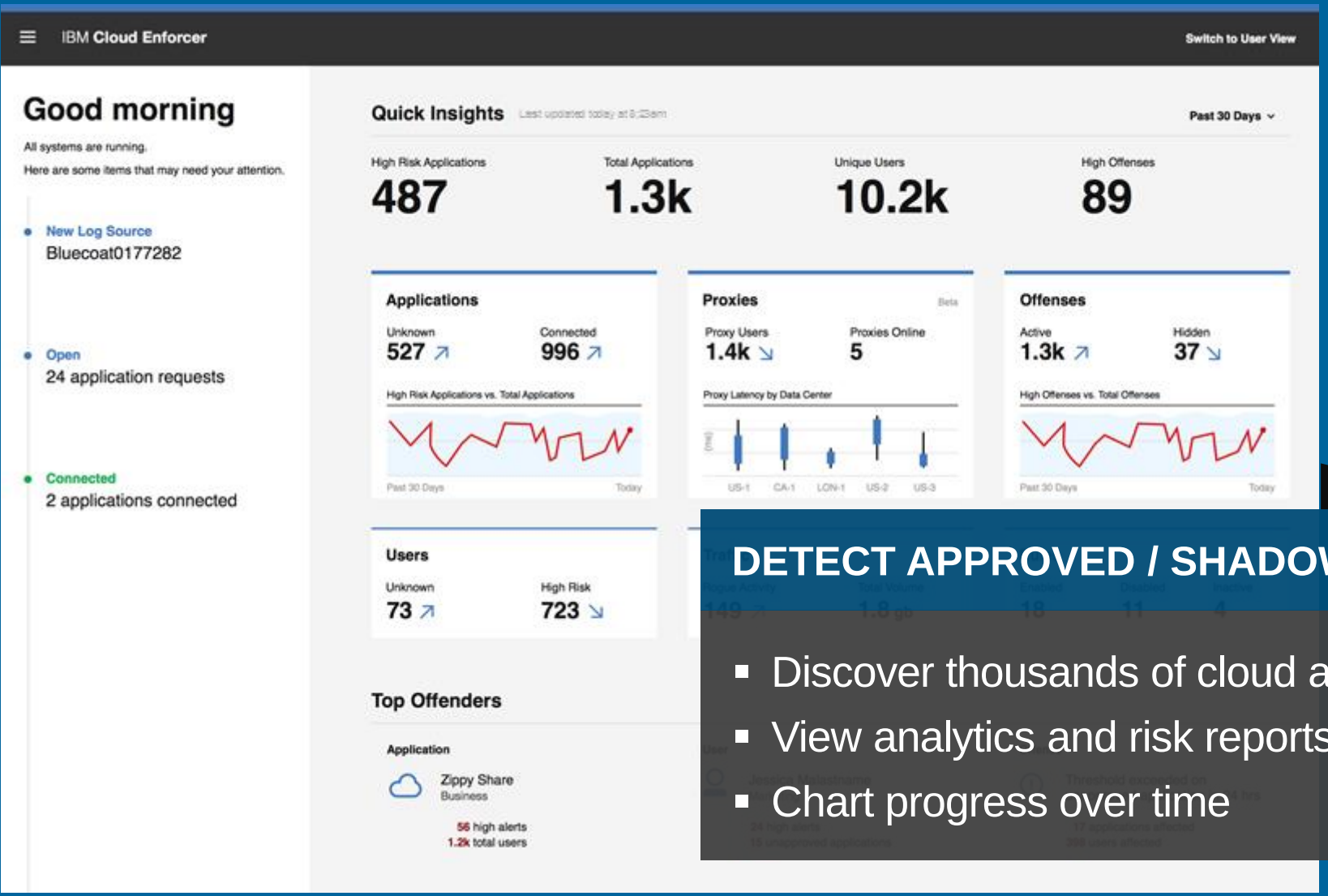
PROTECT
Against cloud-related threats

IBM Cloud Security Enforcer

Adopt the Cloud but Without The Risk

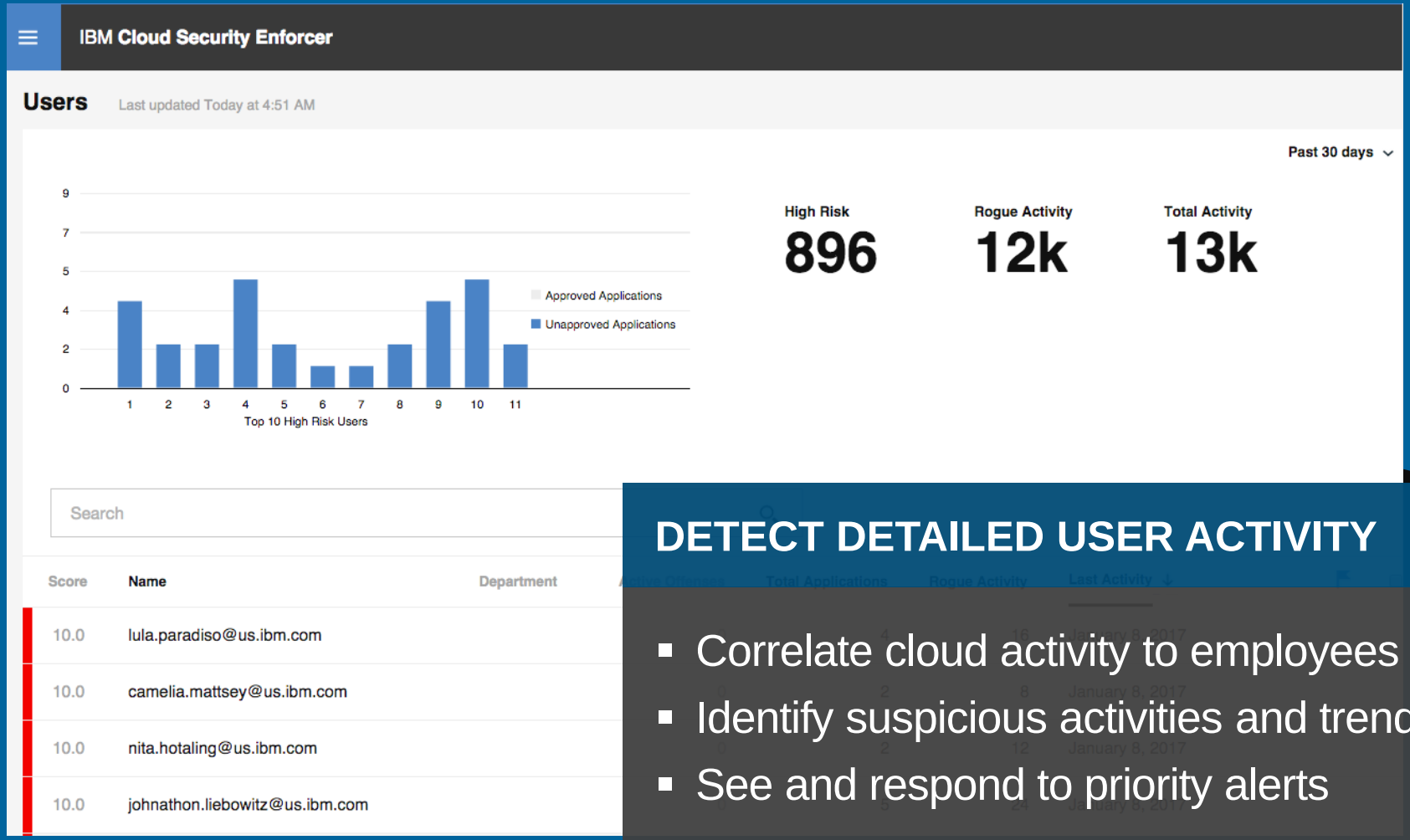
DETECT

App usage and user activity



DETECT APPROVED / SHADOW APPS

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

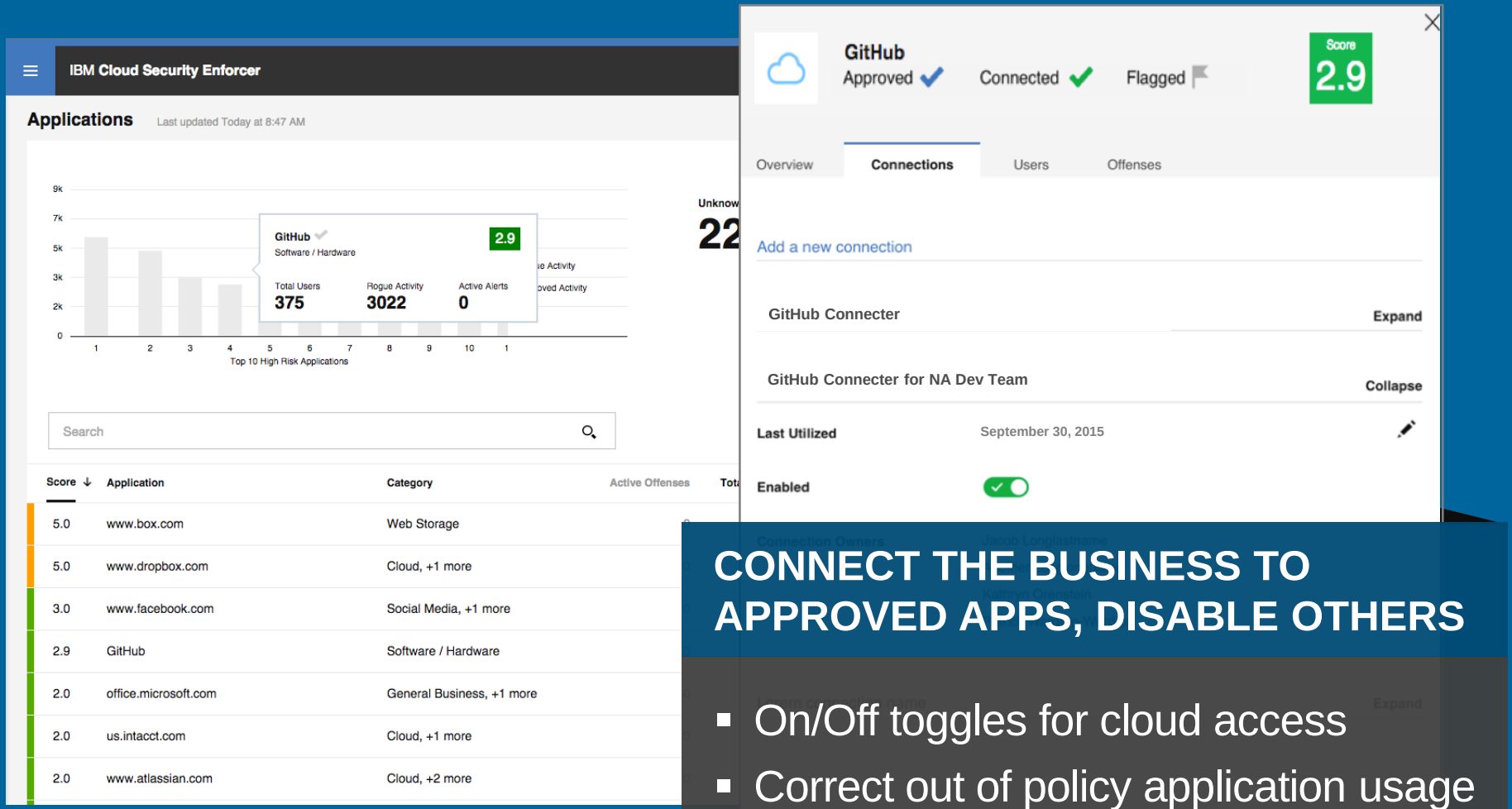


DETECT DETAILED USER ACTIVITY

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

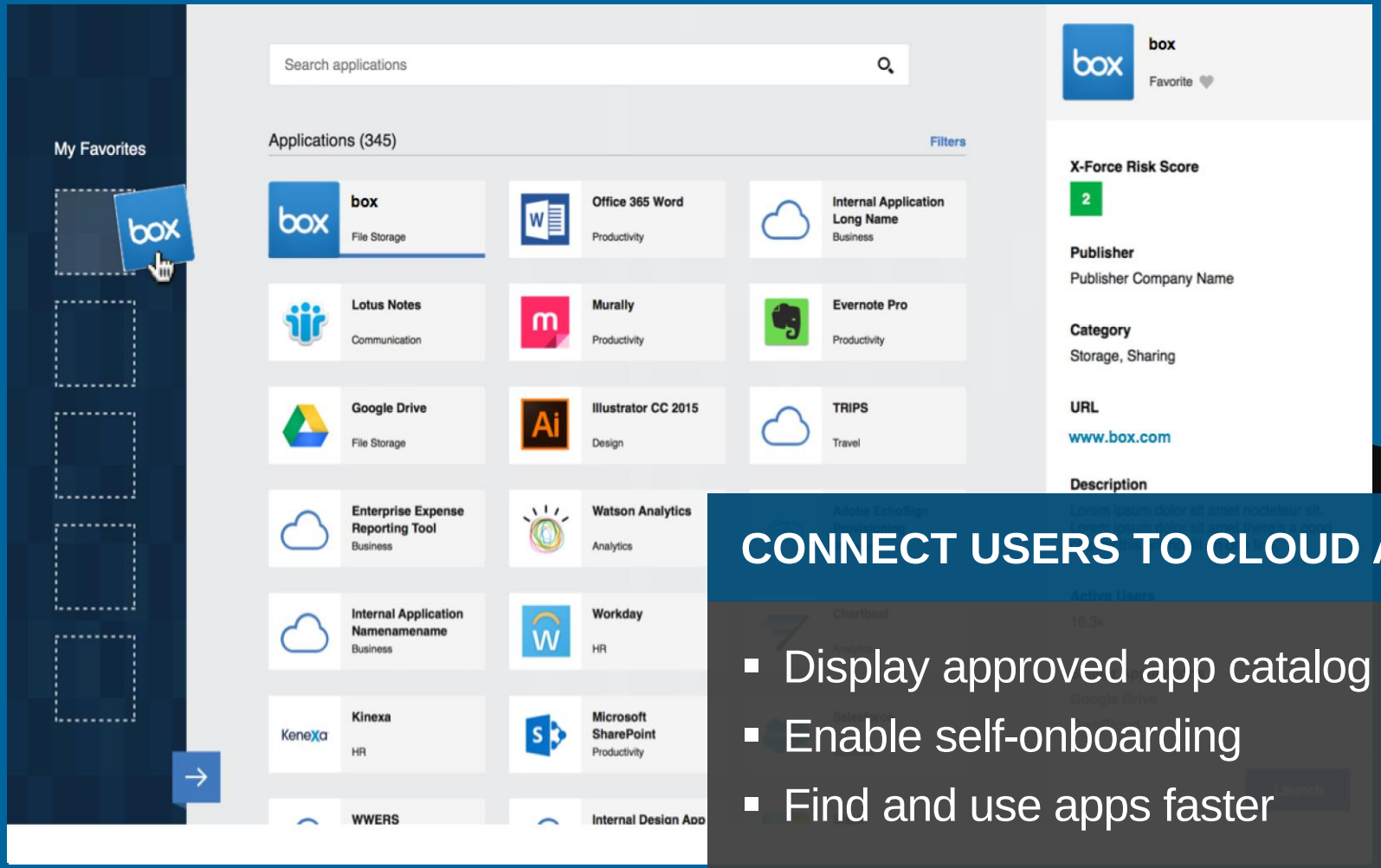
CONNECT

Users to approved cloud apps



CONNECT THE BUSINESS TO APPROVED APPS, DISABLE OTHERS

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

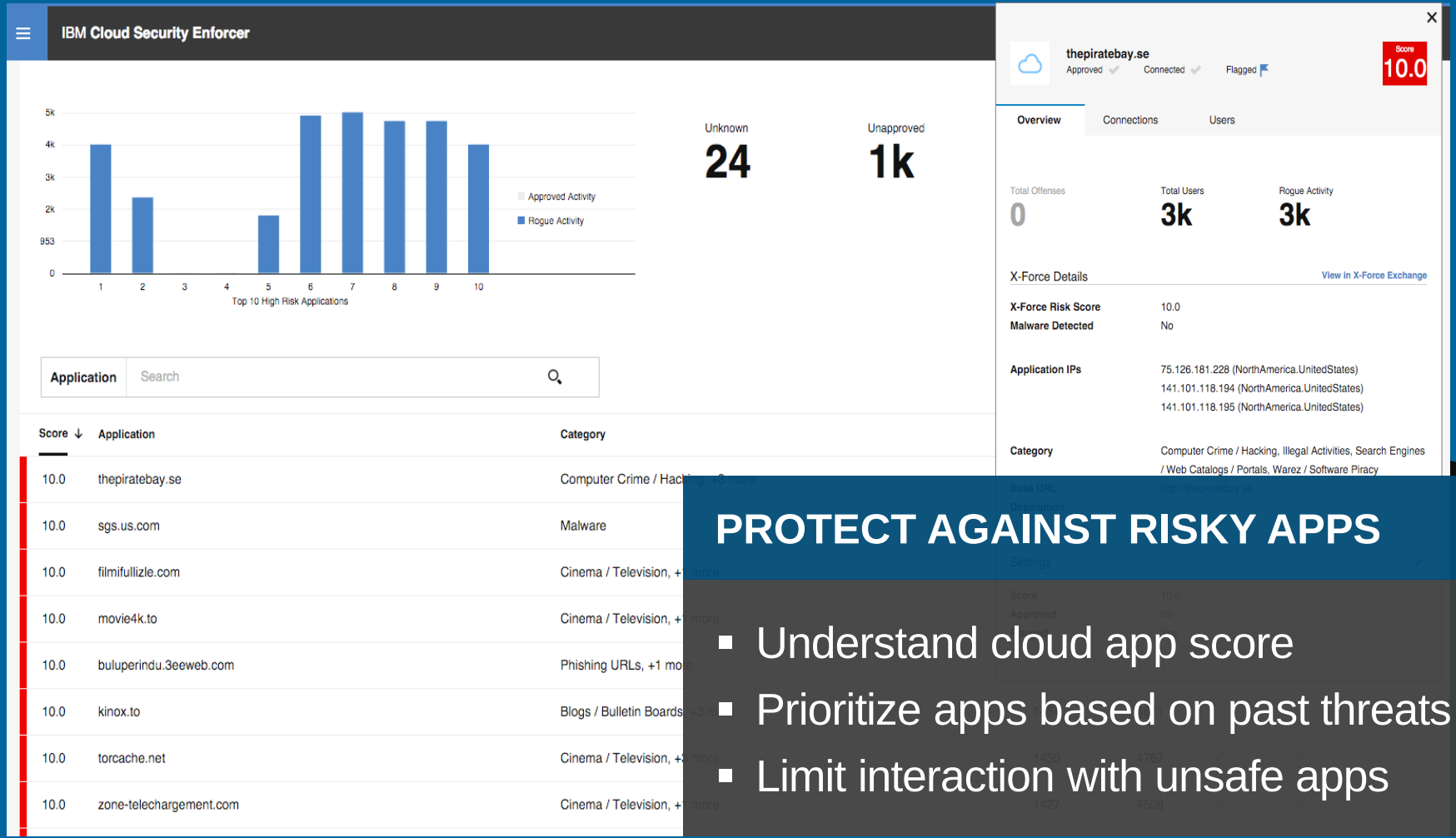


CONNECT USERS TO CLOUD APPS

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

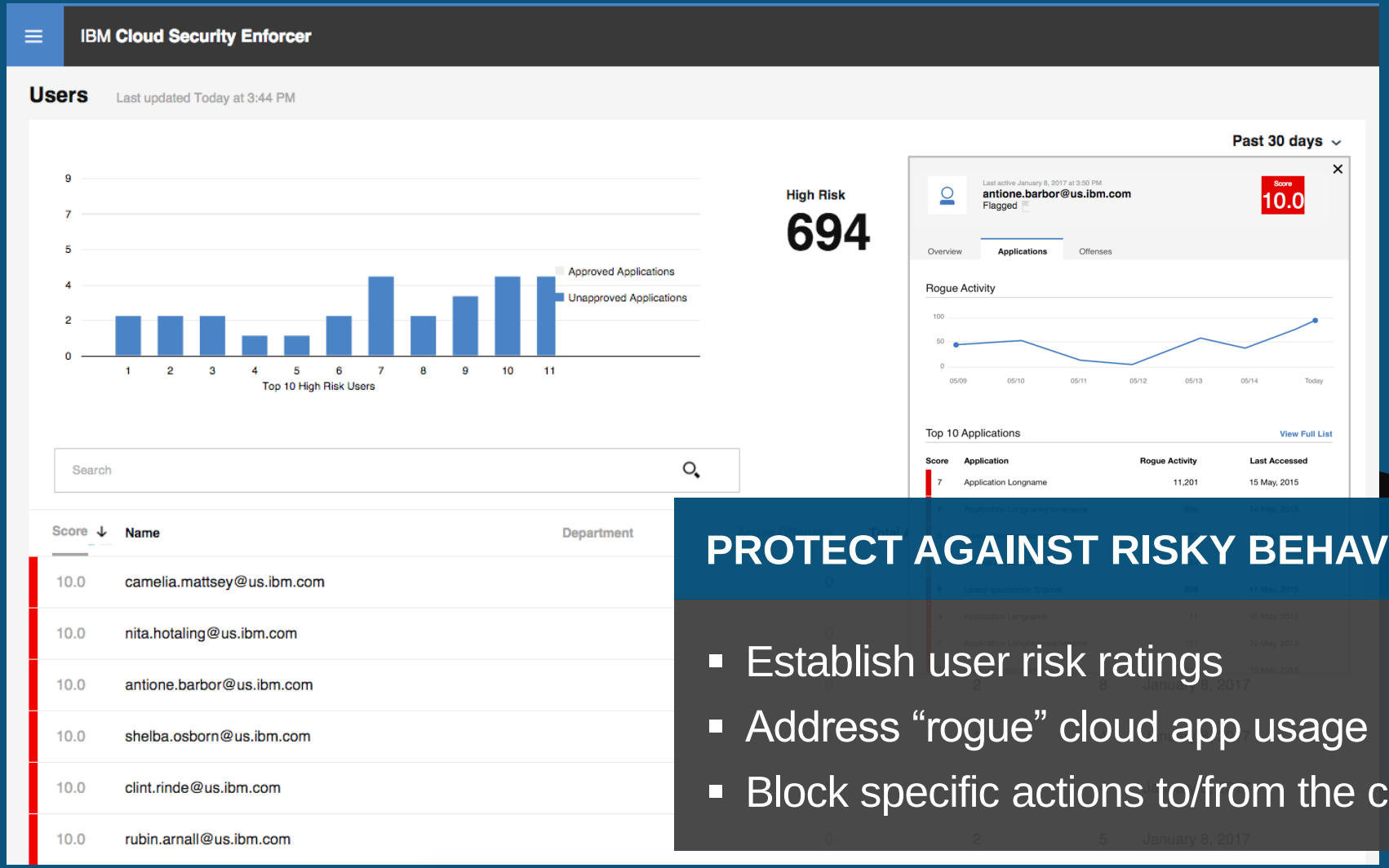
Protect

Against cloud-related threats



PROTECT AGAINST RISKY APPS

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



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	CONNECT	PROTECT		
Discovery and Visibility	**Identity and Access Control**	**Cloud Event Correlation**	**Threat Prevention**	**Policy Enforcement**
• 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	• Federated cloud SSO • Connectors to popular cloud apps • Simplified access controls • Self-service catalogs • Delegated administration	• User activity and traffic monitoring • Behavioral analysis and correlation to company policies • Alerting, reporting, and auditing	• Intrusion Prevention and global threat intelligence from IBM X-Force • Threat signatures, network analysis, and zero-day threat protection	• 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.

IBM Security

Intelligence. Integration. Expertise.

IBM

BACKUP

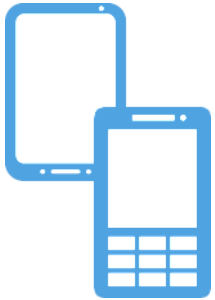
Mobile apps a big concern

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

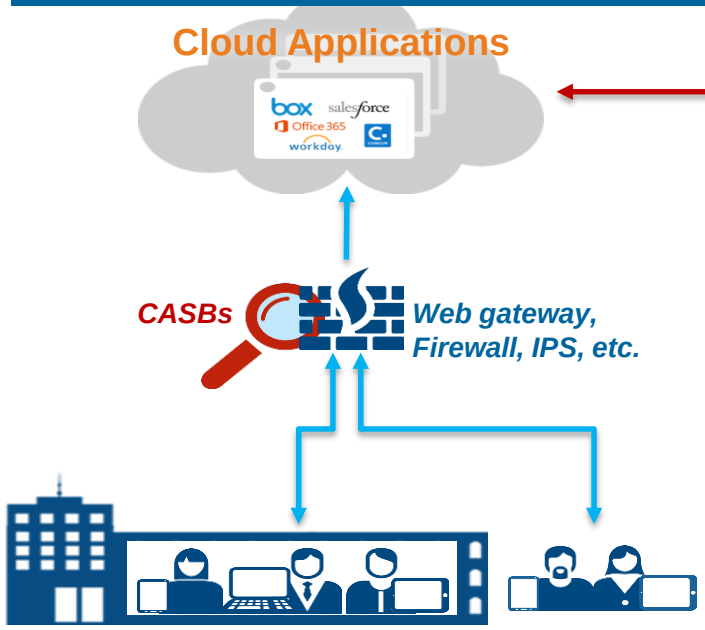
46% say their smartphone is something they couldn't live without

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

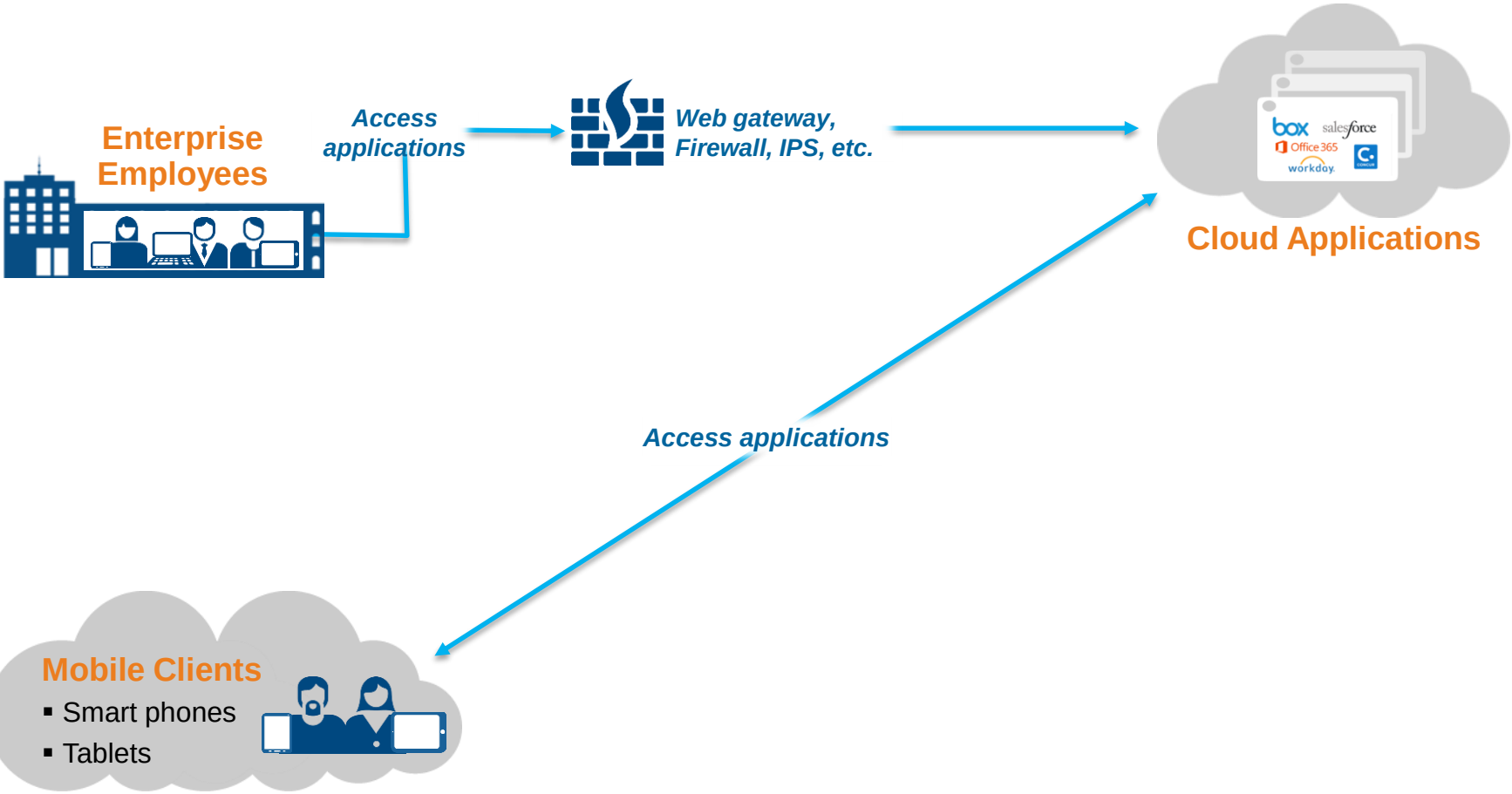


"Blind spots" still exist for mobile usage

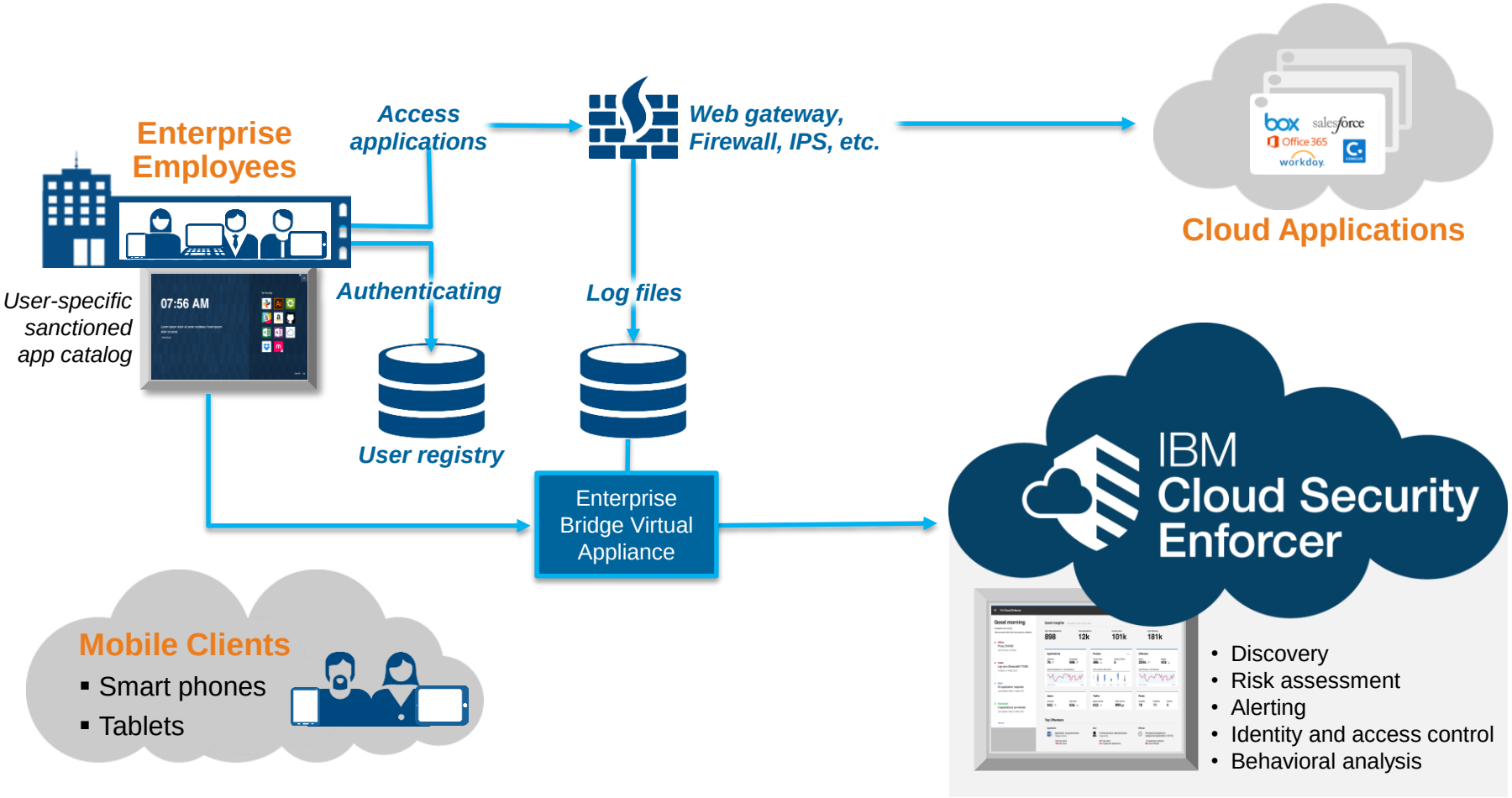
Mobile users can go directly to cloud apps – creating the "mobile blind spot"

- 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

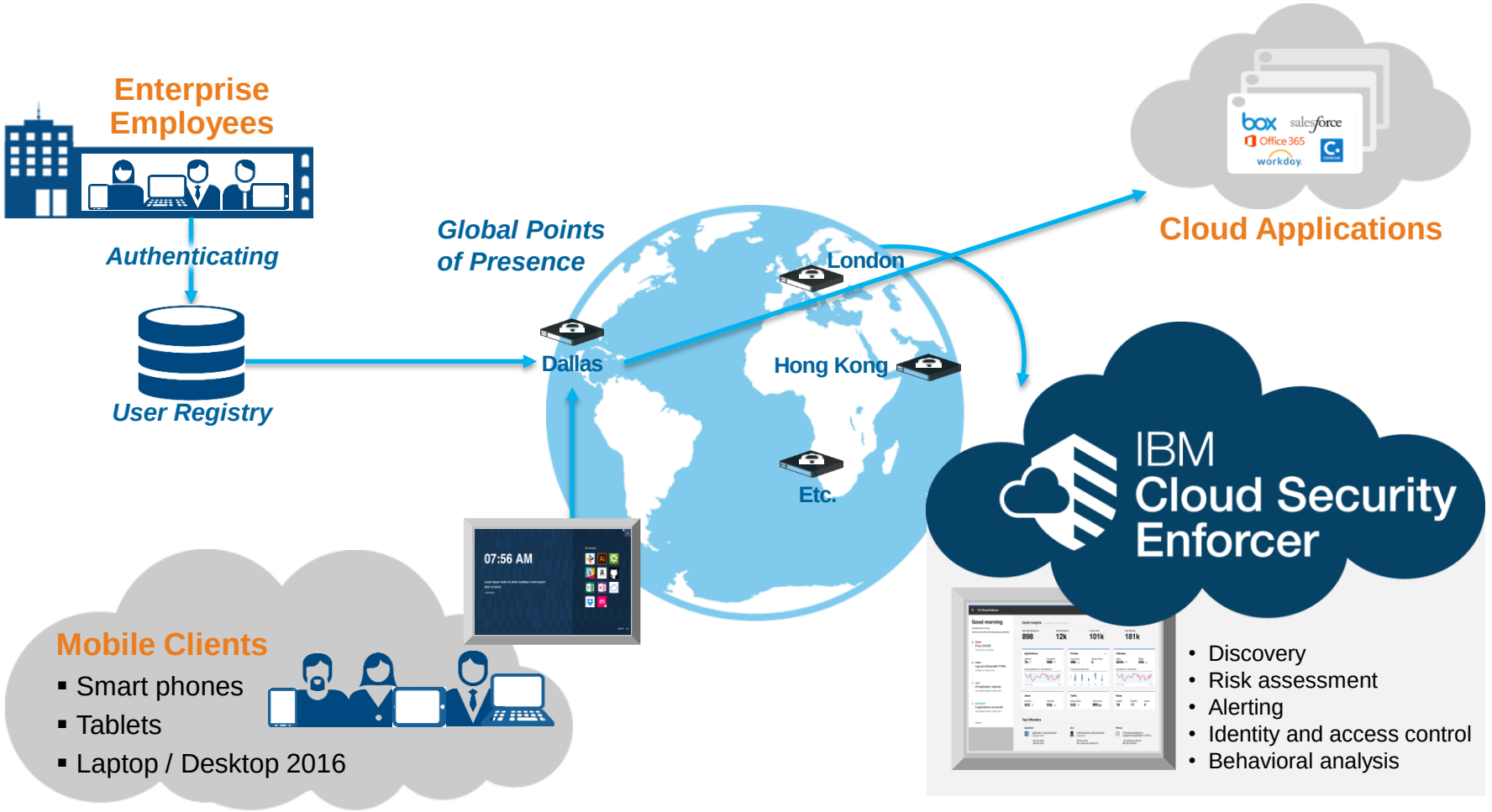
Cloud Application Usage Today



In-enterprise application visibility and control

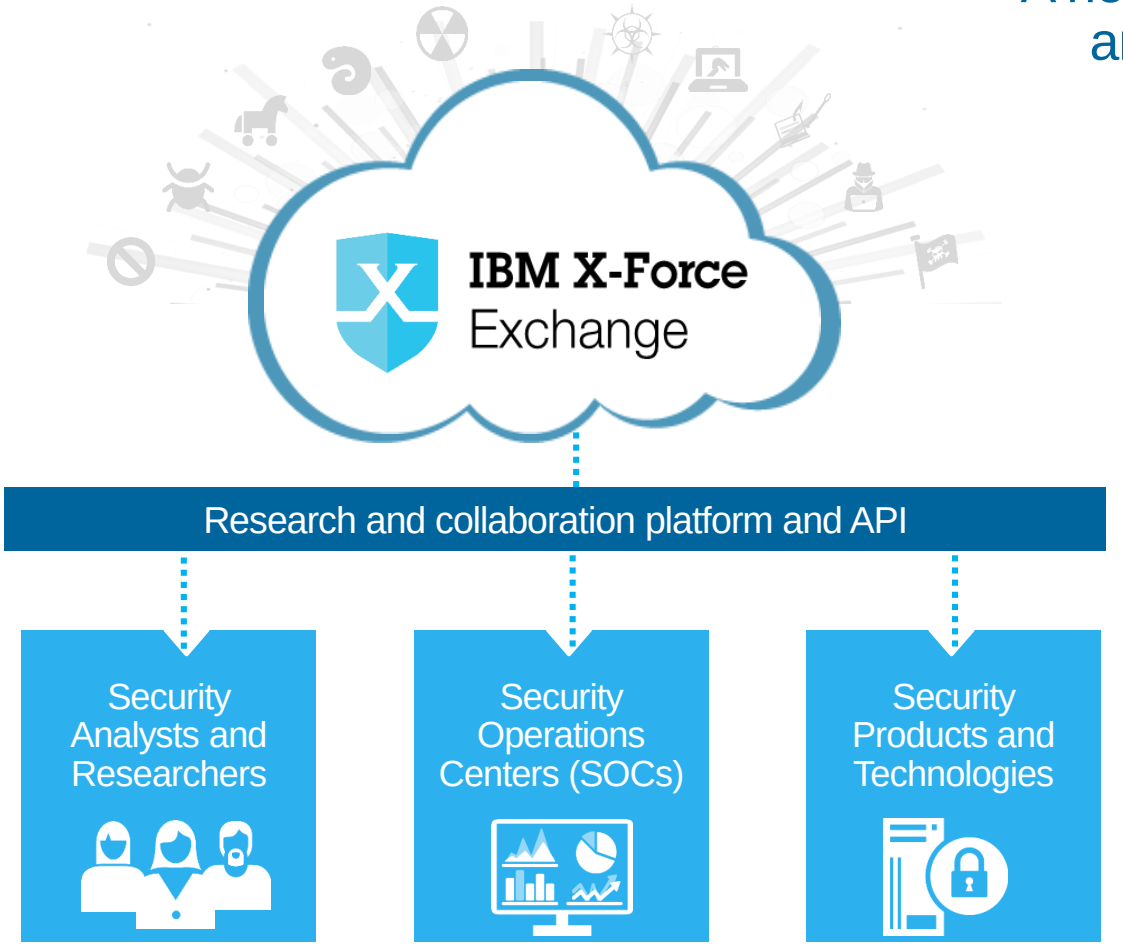


Mobile application visibility, control and protection



IBM X-Force Exchange

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



- 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

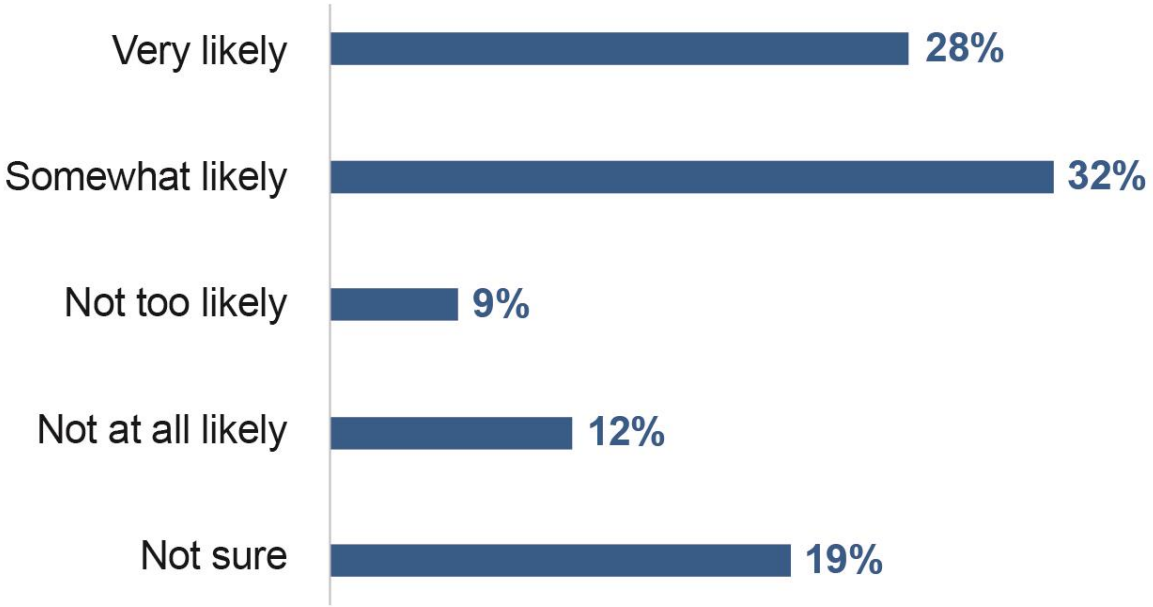
Cloud-based threat intelligence sharing platform

Real-time sharing of Trusteer intelligence

Intelligence databases dynamically updated on a minute-by-minute basis

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.