

carahsoft.

Welcome to the

Carahsoft-ATARC Federal Cloud Marketplace Forum

Wednesday, July 24, 2019

Featuring FedRAMP Solutions & Successes



 **ATARC**

Getting to Success



Petko Stoyanov

*Chief Technical Strategist, Public
Sector and Cloud Compliance,
McAfee*



Getting to Cloud Smart

Petko Stoyanov

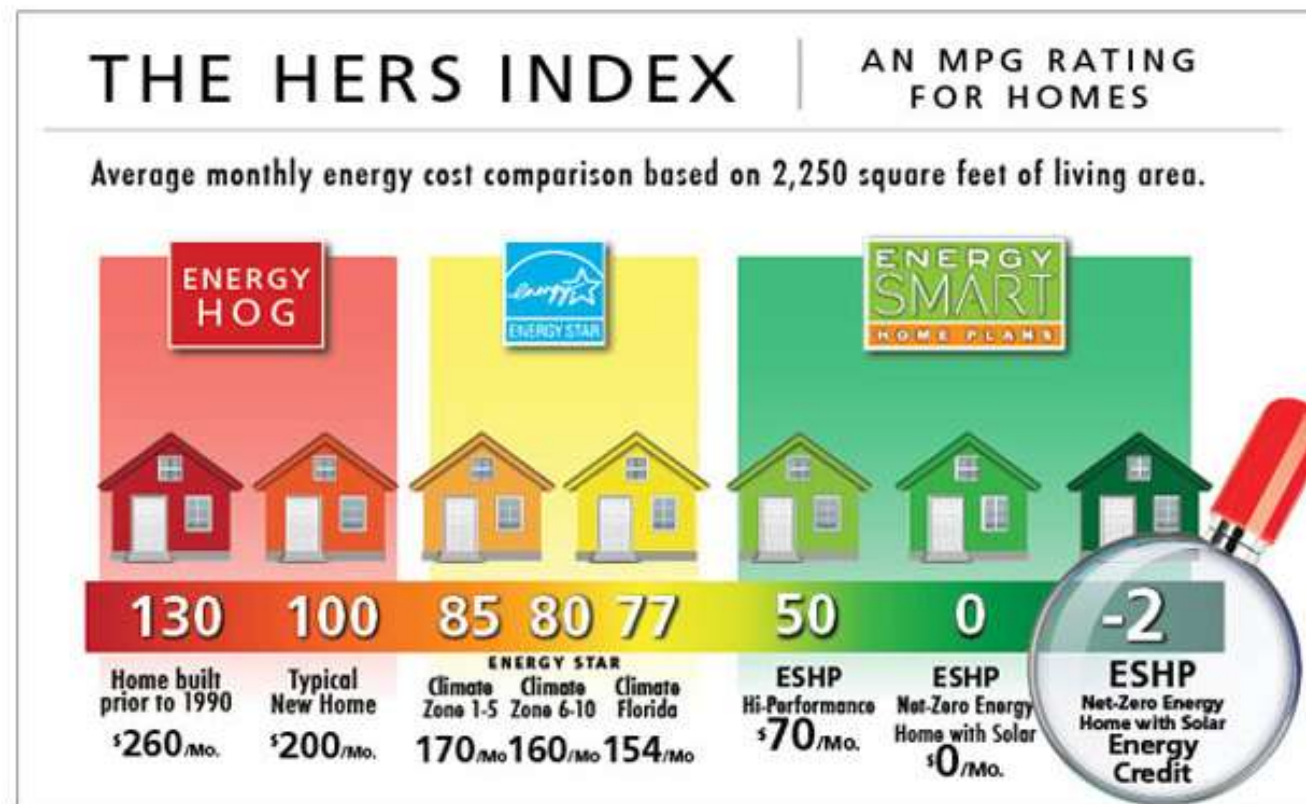
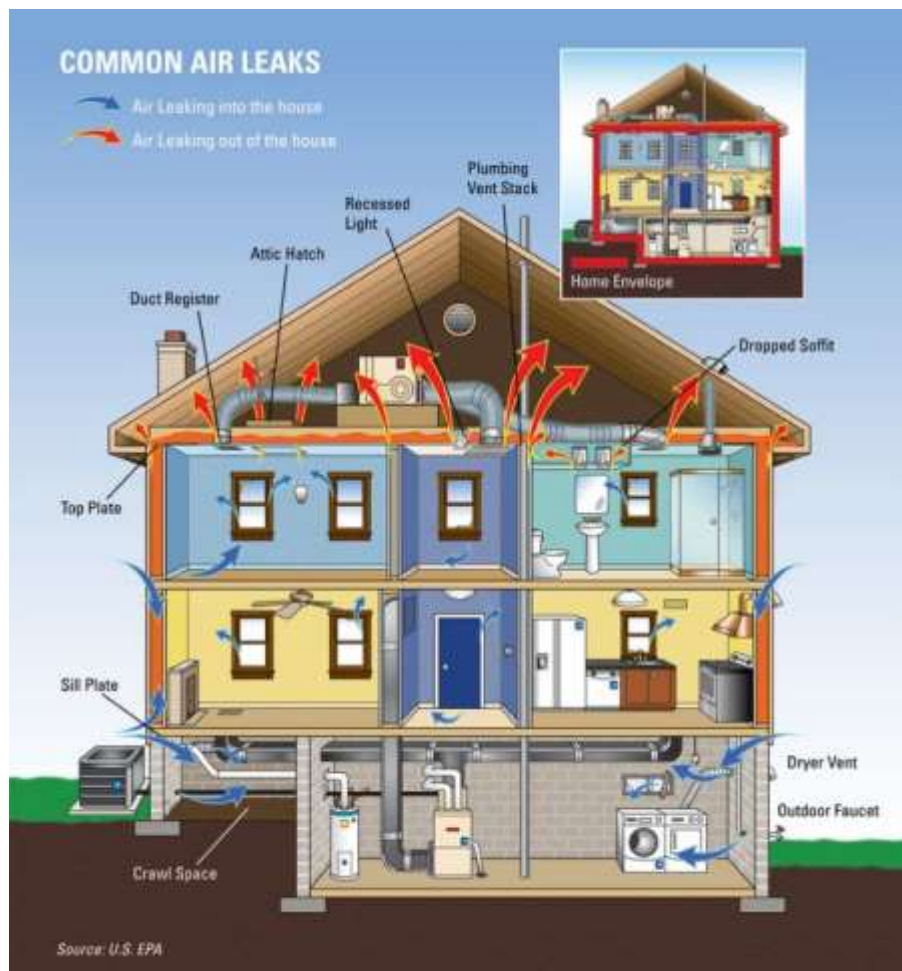
Chief Technical Strategist

- Public Sector & Cloud Compliance



Who has a leaky house?

How do you know?



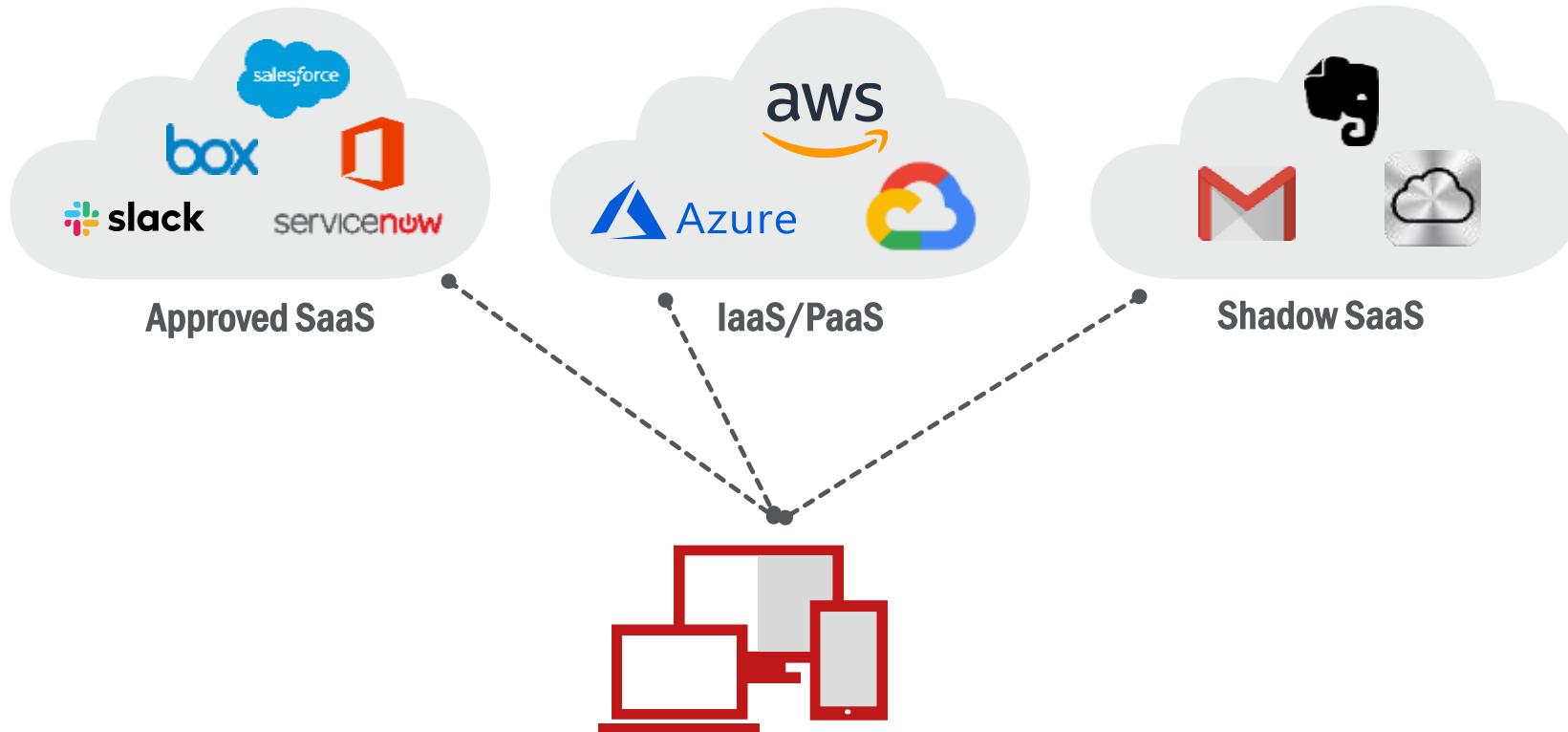
Source: <https://energysmarthomeplans.com/hers-index/>

Customer Drivers for Cloud Adoption

1 SaaS
Business Agility

2 IaaS/PaaS
Business Transformation

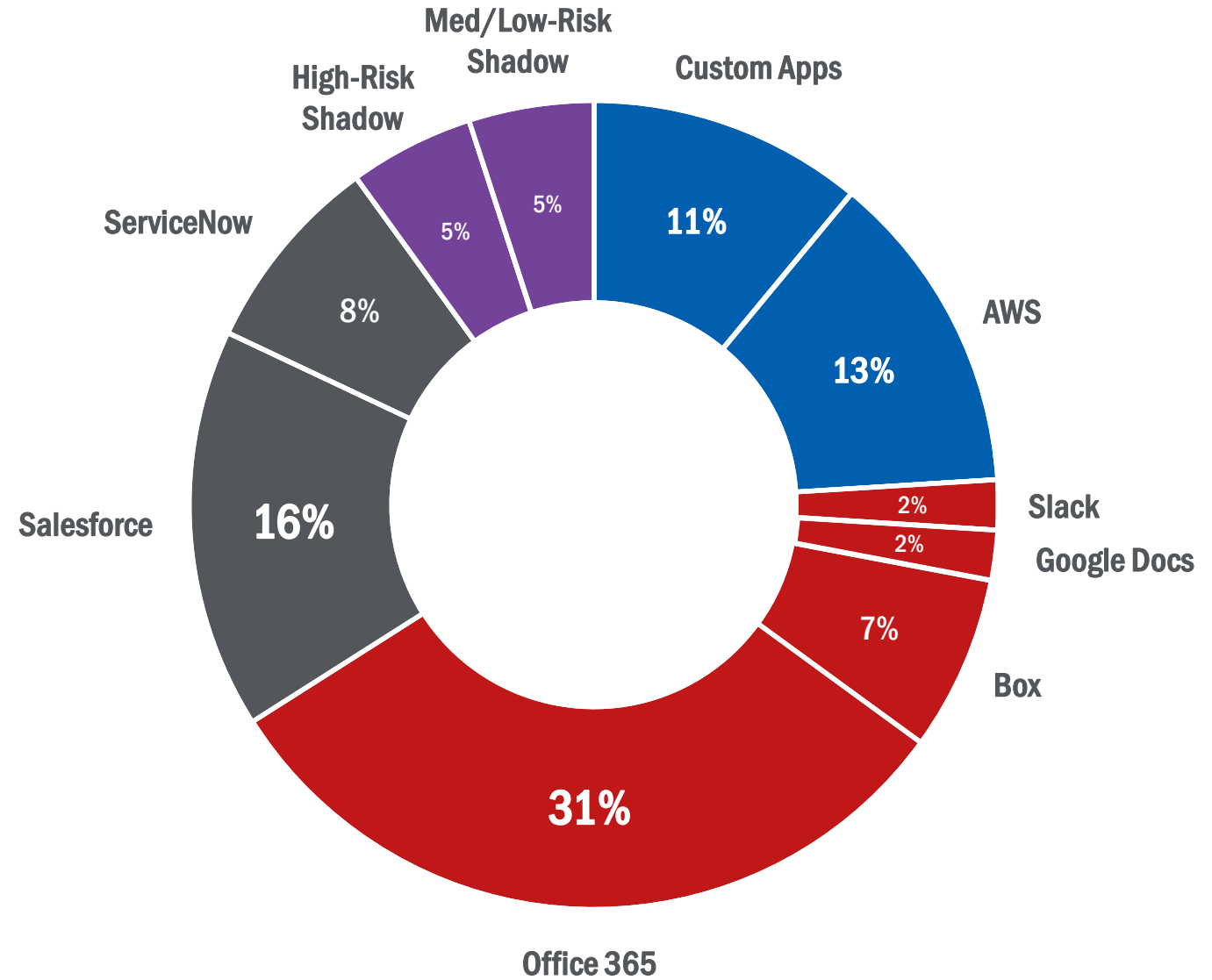
3 Consumer
Personal Productivity



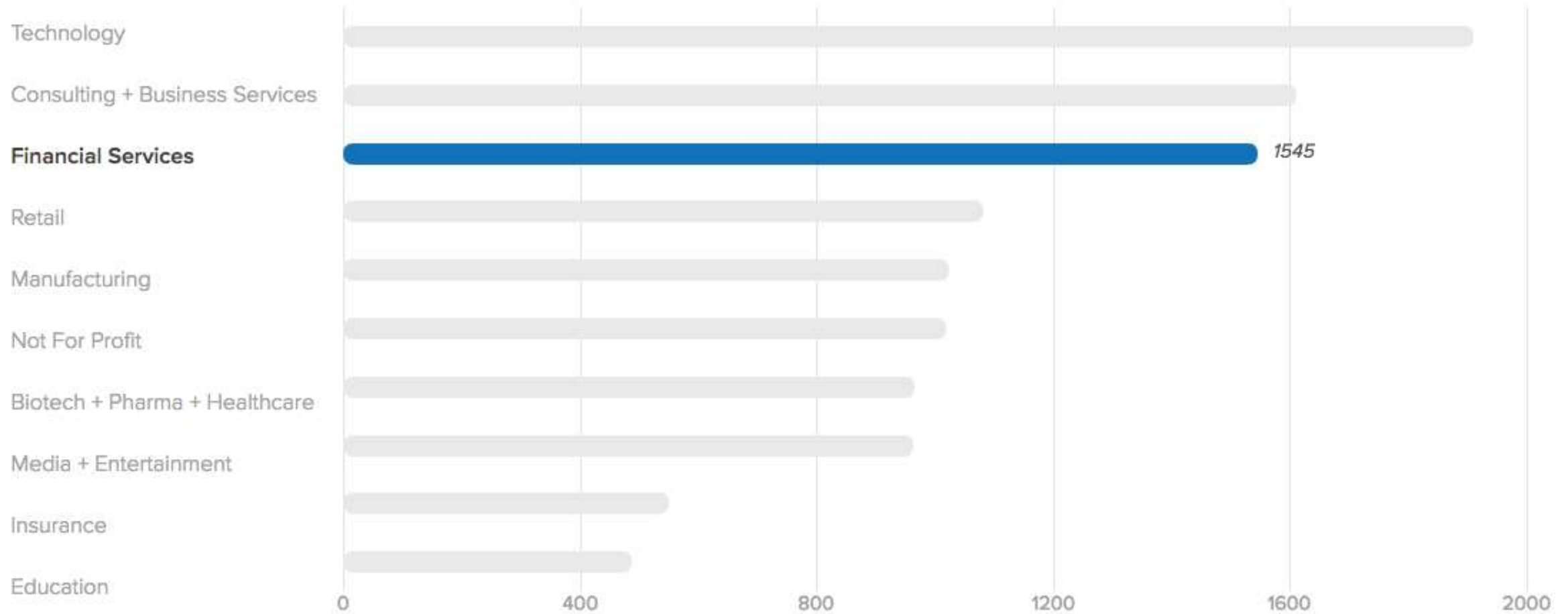


Visibility

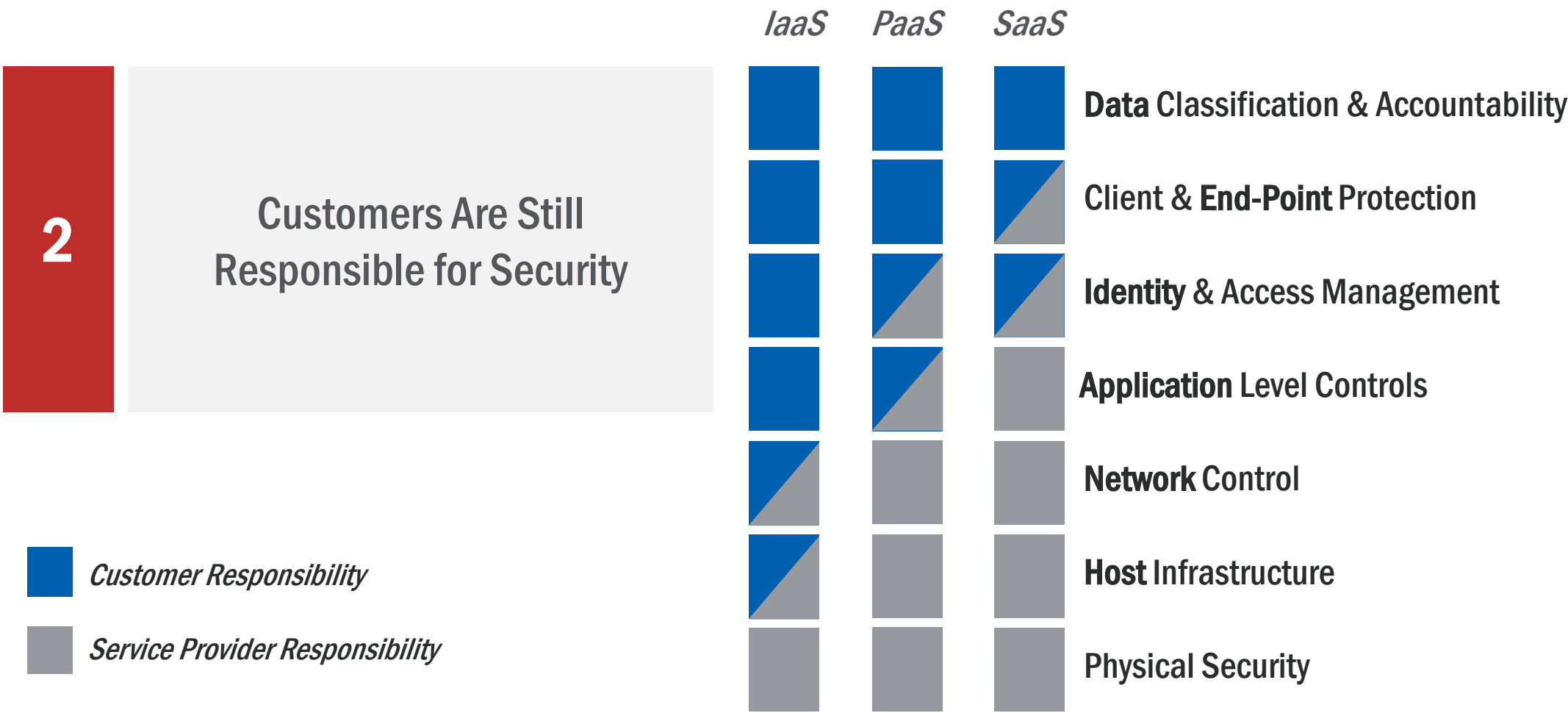
Where is enterprise sensitive data in the cloud?



The average Financial Services organization uses **1,545** cloud apps



The Cloud (First) Enterprise Challenges



Cloud Shared Responsibility Model

Most Cloud Apps are not Enterprise-ready



Support multifactor authentication



Specify that customer owns all data uploaded



Delete data immediately on account termination



Encrypt data at rest



Encrypt data with customer-managed keys



McAfee MVISION Cloud





McAfee - MVision Cloud



MVISION Cloud



MVISION ePO



MVISION Endpoint



MVISION Mobile



MVISION EDR

600+ customers including 30% of the Fortune 100





Why McAfee MVISION Cloud?

Enabled collaboration while keeping internal-only data internal.

- Real-time enforcement
- Context- and content-aware policies

AMERICAN EXPRESS

McAfee (Skyhigh) customer since 2016

63,500 Employees

Why McAfee MVISION Cloud

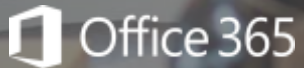
- Data Loss Prevention
- Collaboration Control
- Governance

Project Champion

- Todd Fennel (VP, InfoSec)
 - Won CSO50 Award for use of MVISION Cloud to accelerate business



Shadow IT



salesforce





CAESARS
ENTERTAINMENT®

Prevent Data Loss due to usage of Personal Devices

**Enable BYOD while preventing data loss from
Salesforce, ServiceNow, O365, Box, and Google via
lost or stolen devices.**

- **Check for device certificate, confirm user/device mapping**
- **Limit access based on device or location**
- **Block access or limit to view-only**





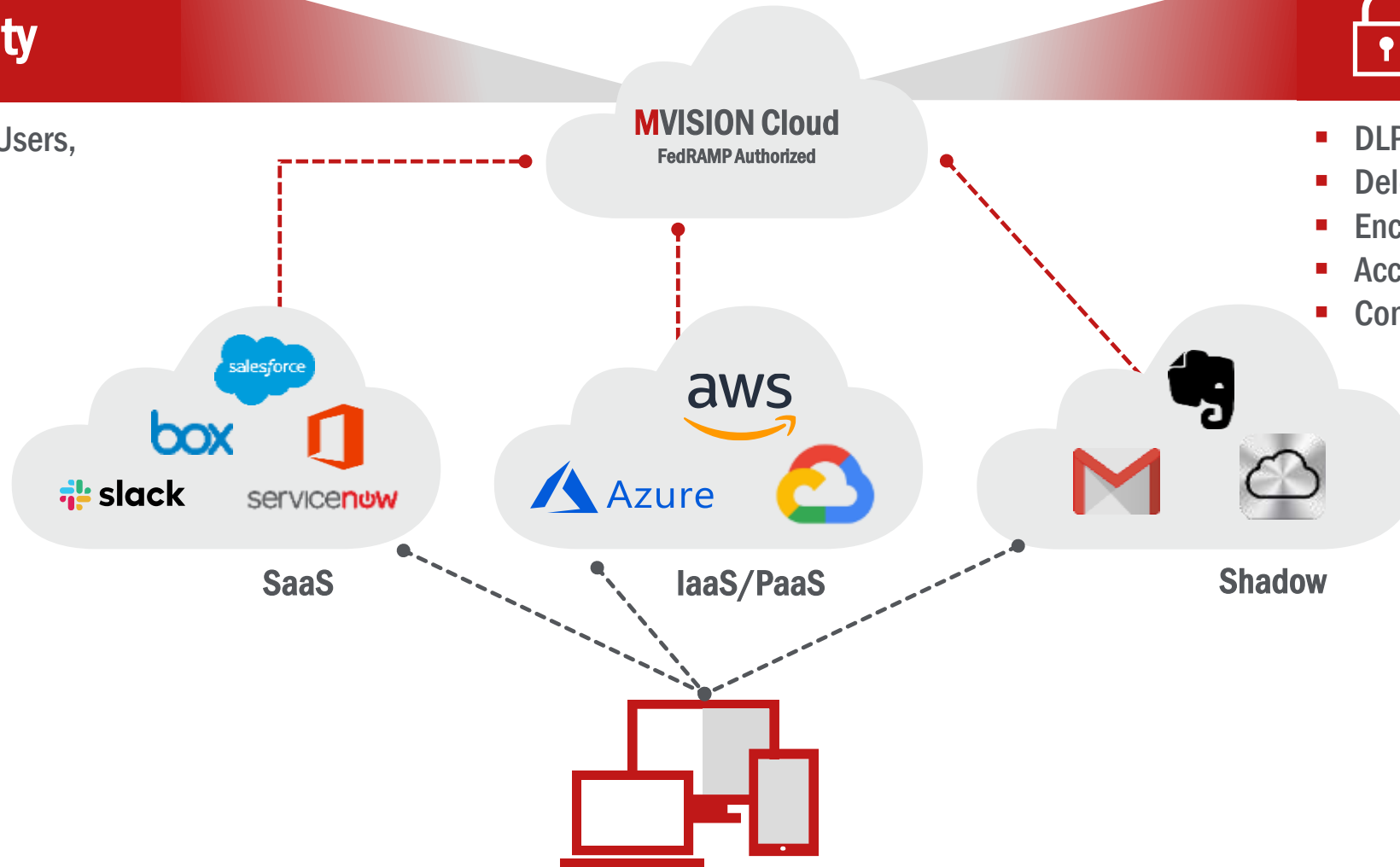
Visibility

- What: Data, Apps, Users, Devices
- Who
- Where
- When



Control

- DLP
- Delete/Quarantine
- Encryption
- Access
- Configuration



Apps: Name, Configuration, Posture, Risk

Workloads: Details, Location, Posture

Data: Classification, Tagging, Metadata

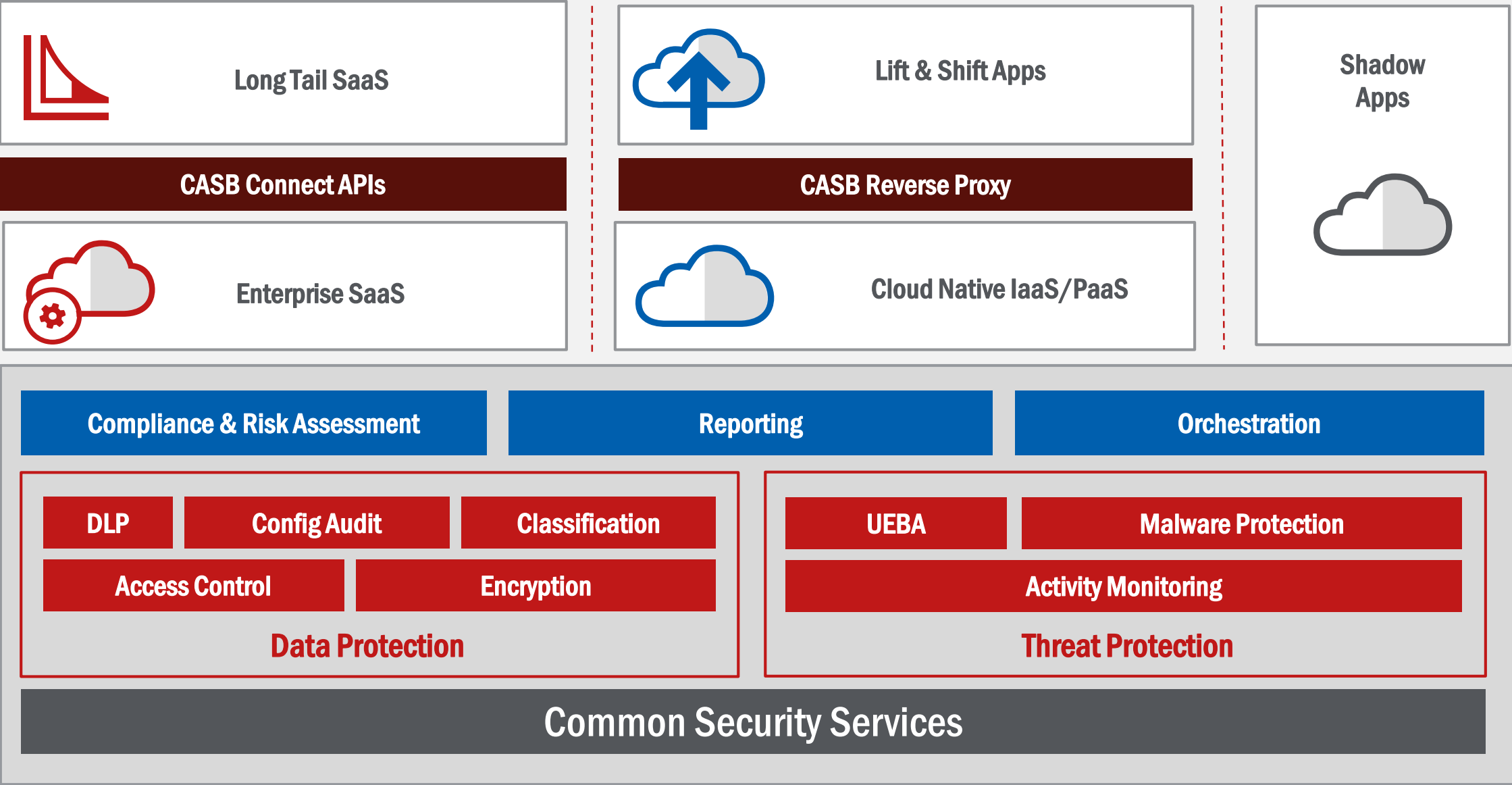
Users: Role, Activity, Collaborators

Activities: Access, Read, Write, Download, Upload...

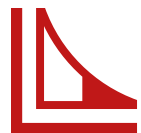
Device: Managed, Unmanaged

Location: Where, When

McAfee **M**VISION Cloud protects *ALL* customer data in the cloud



McAfee **M**VISION Cloud protects *ALL* customer data in the cloud



Long Tail SaaS



Enterprise SaaS

MVISION Cloud



Webex Teams



GitHub

okta



EGNYTE

@workplace

jive

ctera

ShareFile
by citrix

onelogin

aprimo

smartsheet

SAP Concur

ATLASSIAN zendesk

Office 365

SharePoint
Online

Microsoft Teams

Exchange

box

OneDrive

Google Drive

slack

salesforce

workday

servicenow

Thank You

Ask us about a
Shadow IT Assessment

Petko Stoyanov

<https://www.linkedin.com/in/Petko-Stoyanov/>

**Thanks again to our
speakers, sponsors and
participants.**

**See more at:
carahsoft.com/FedRAMPFForum
carah.io/fcmf**