



Cloud Data Security & Compliance

Who's speaking today



● Maurizio Costa (*m.costa@sinergy.it*)

- Tech Account Manager Security from **Sinergy**
- >15 years in information security
- CISA, ISO 27001 LA, ISO 22301 LA, PMP

● Giuseppe Marullo



- Senior Systems Engineer from **Symantec**
- >18 years in information security
- CISSP, GCFA, CSSA

Agenda



- Cloud Phenomenon
- Cloud Security Challenge (privacy & compliance)
- Cloud Security Controls
- Cloud vs on-premise Security Stack
- Why CASB solutions (UBA, business related, ...)
- CASB solution details
- O365 use case
- What can we cloud see (visibility & reporting)

Cloud Adoption: how is it going?



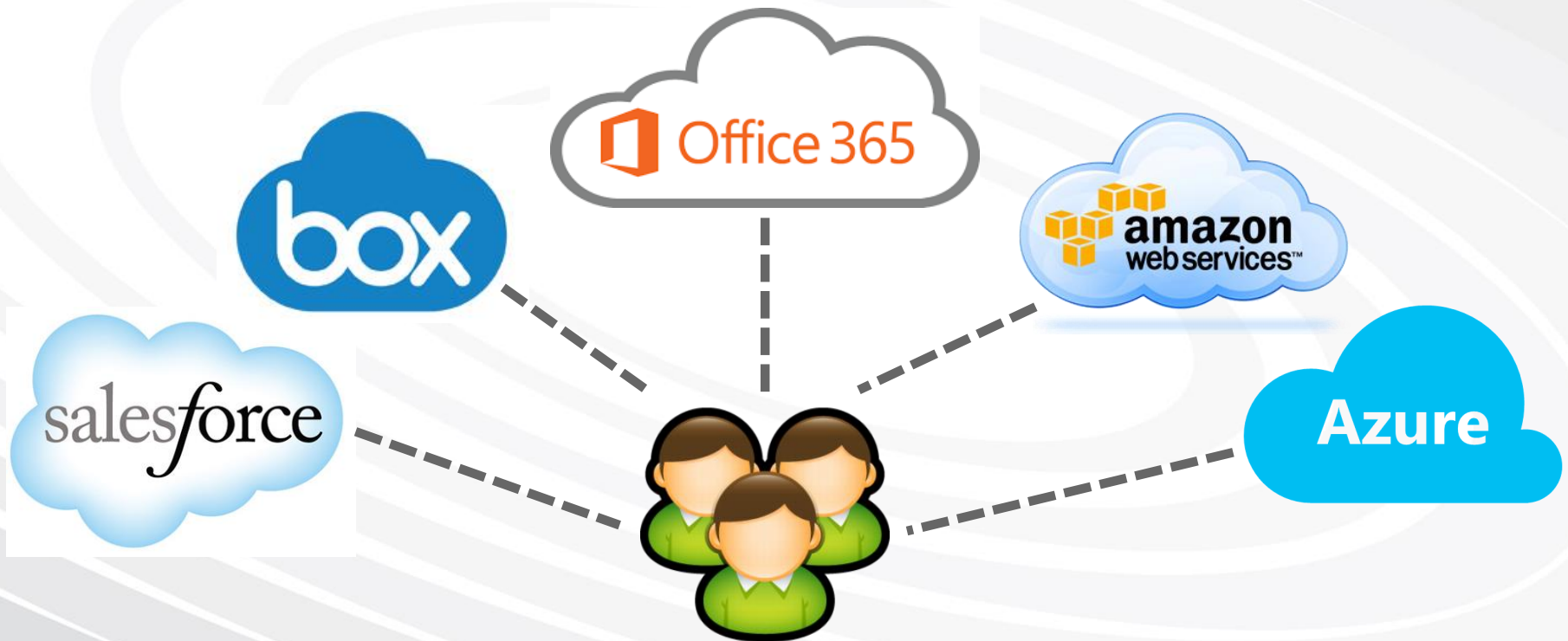
Cloud Adoption: why is it happening?



SILICON VALLEY



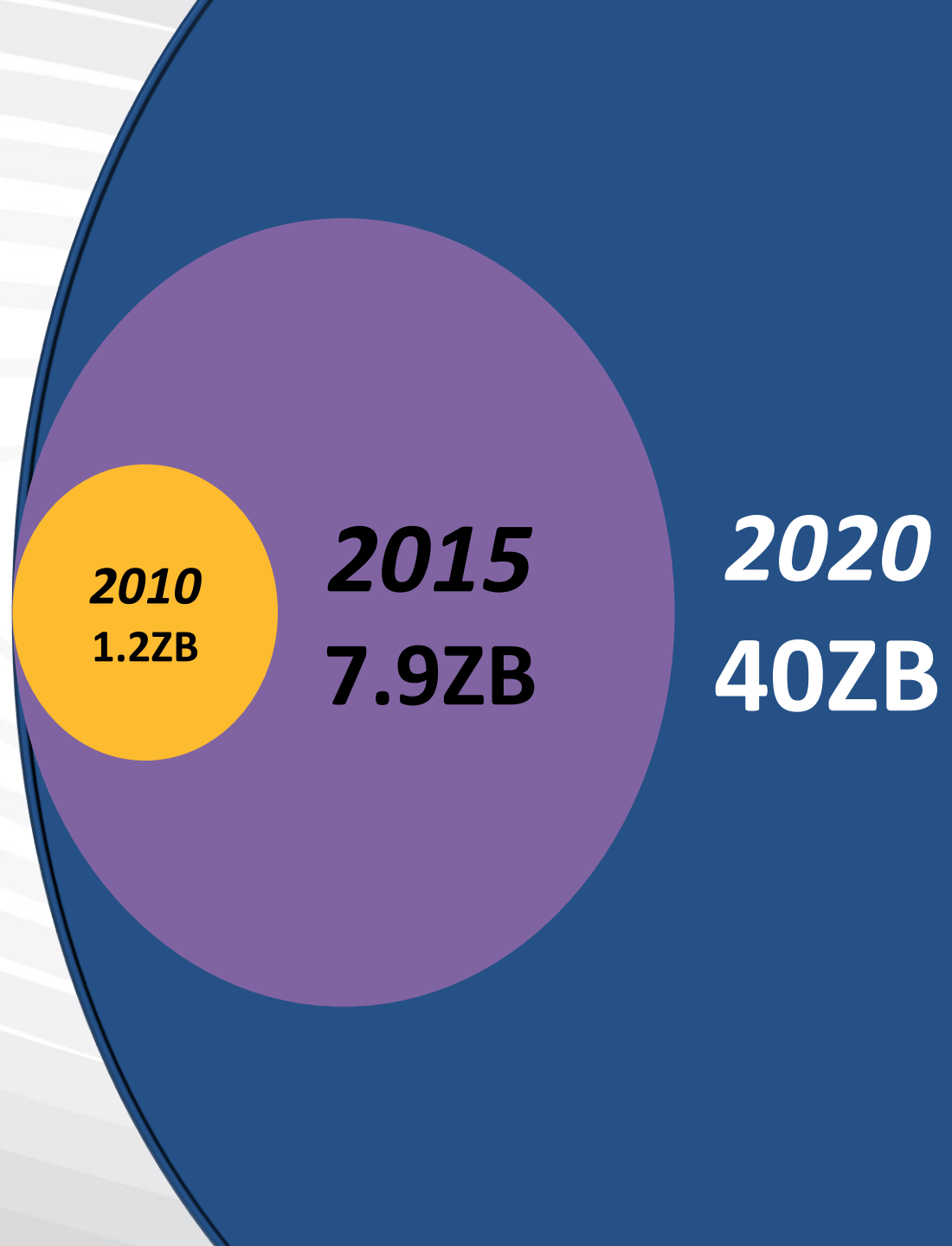
Applications and Data are Moving to the Cloud



**Information is
exploding**

“zettabyte”

ZB = $\times 10^{21}$



2017 Cloud computing trends



- IDG Enterprise's 2016 Cloud Computing Survey
 - Cloud technology is becoming a staple to organization's infrastructure as 70% have at least one application in the cloud.
 - This is not the end as 56% of organizations are still identifying IT operations that are candidates for cloud hosting.
 - On average, organizations will invest \$1.62 million in cloud computing, with enterprise organizations leading the spending.
 - Lowering total cost of ownership, replacing on-premise legacy technology and enabling business continuity are the top business goals driving cloud investments

Privacy & Compliance: User Perspective / 1



Keeping your data safe and secure

88%



Delivering quality products / services

86%



Delivering great customer service

82%



Treating their employees and
suppliers fairly

69%



Being environmentally friendly

56%



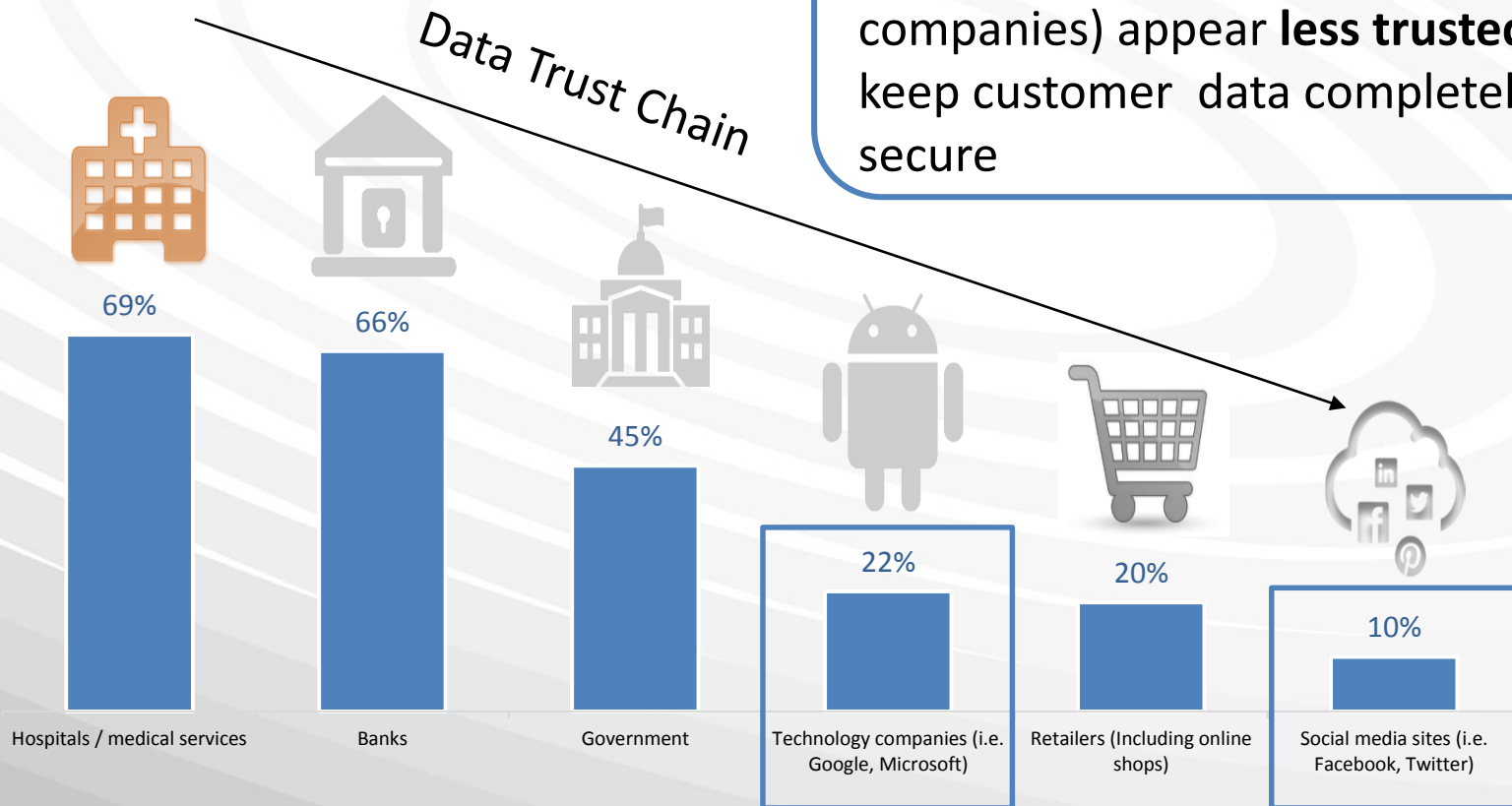
Symantec State of Privacy Report 2015

<https://www.symantec.com/content/en/us/about/presskits/b-state-of-privacy-report-2015.pdf>.

Privacy & Compliance: User Perspective / 2

Not all Organisations have the same level of Consumer Trust for Securing Data

Organisations whose **business models** are based on **data** (tech companies and social media companies) appear **less trusted** to keep customer data completely secure



Privacy & Compliance: Regulations



Drivers & Challenges for Data Privacy & Compliance



Drivers

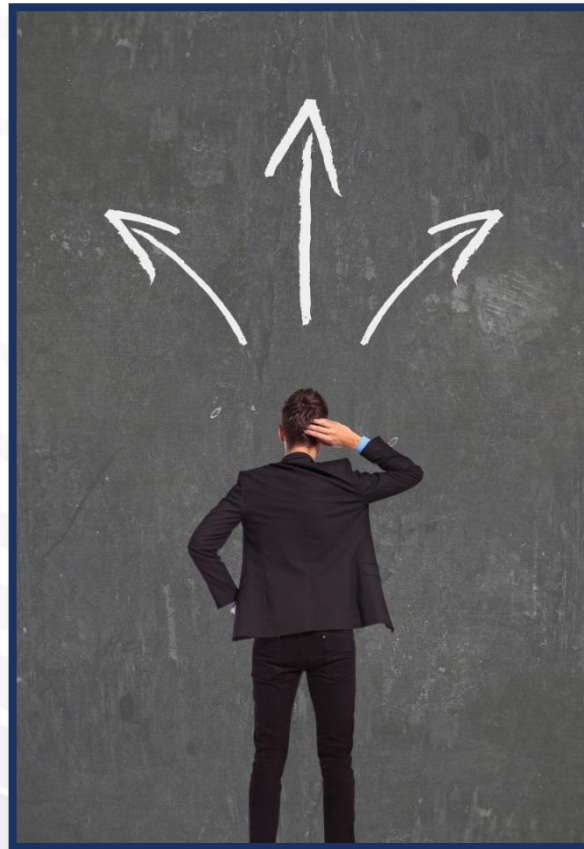
Regulations

Press Headlines

Reputation

Customer Trust

Business
Opportunity



Challenges

Lack of Visibility

Data Growth

Evolving Threat
landscape

Lack of Business
Ownership

Emerging
Technology

Cloud: Security is about the data (not the network)



● Identity

- How do I authenticate, provision, de-provision users across my clouds?

● Shadow IT

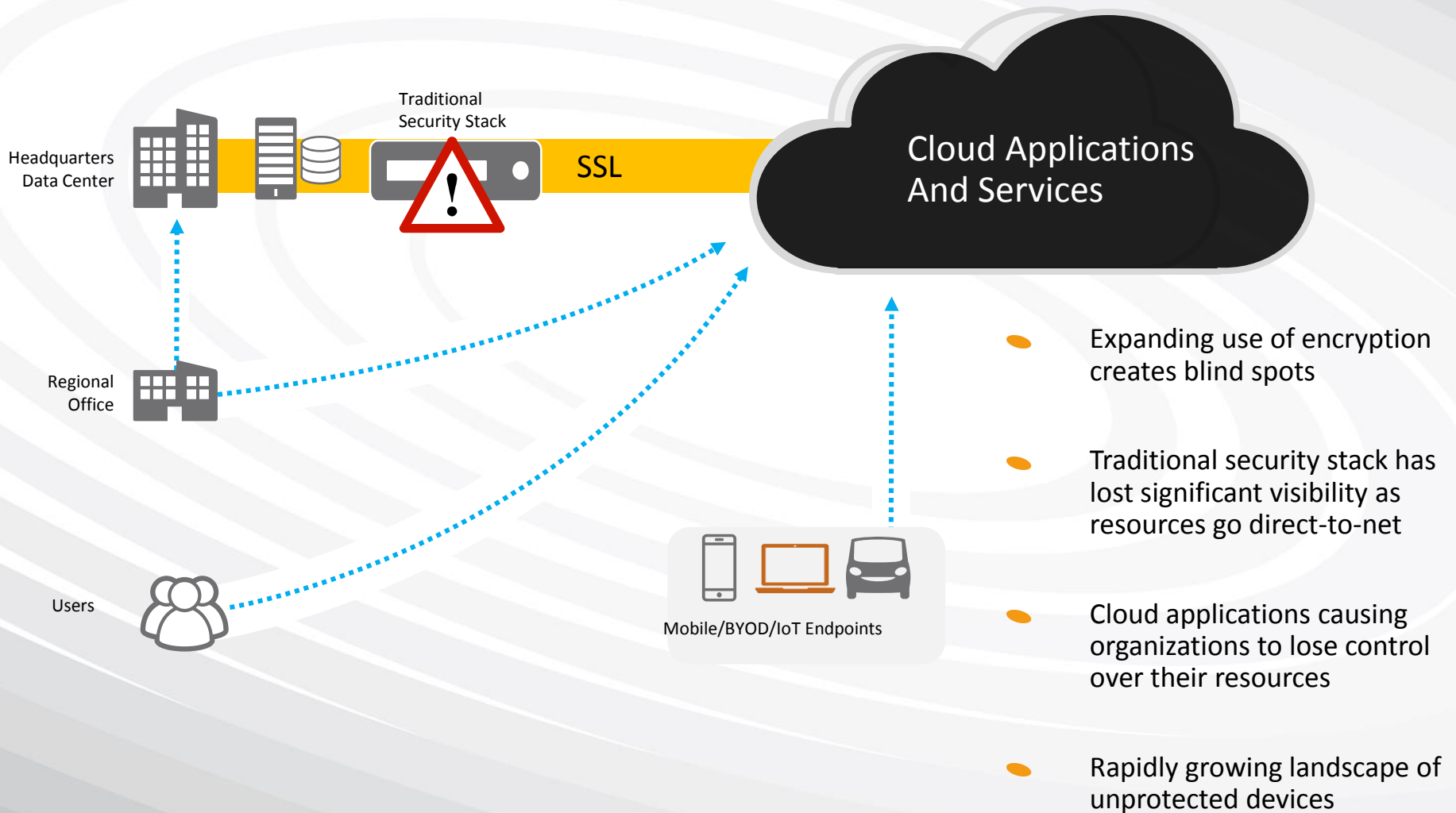
- What unauthorized risky cloud service are being used?

● Data Protection – Shadow Data

- What are my users storing in the cloud?
- What are they downloading from the cloud?
- What are they sharing in the cloud?

"SaaS security is identity and data centric not network centric"

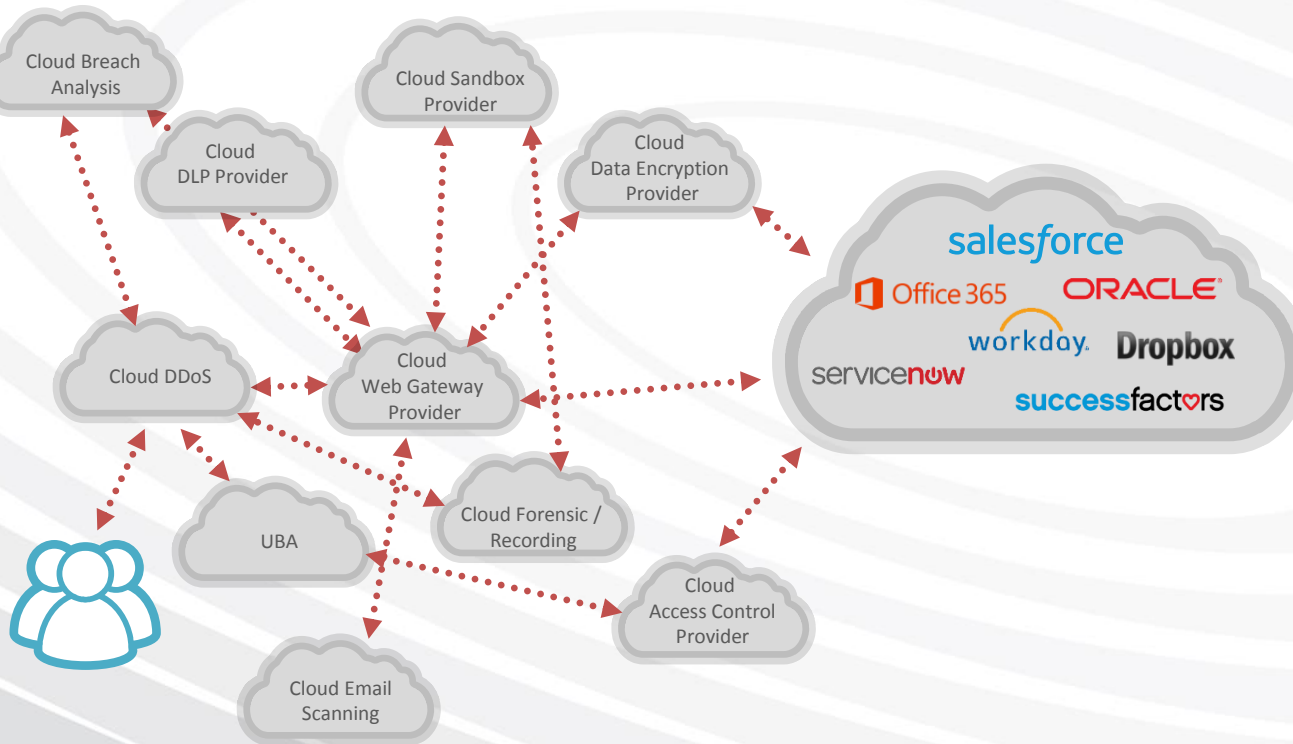
Traditional Security Stack Challenges



Cloud Security Stack Challenges



Complications of Cloud Adoption



- Who owns the Comprehensive Service Level Agreements?
- Single Pane of Glass?
- Redundancy & High-Availability?
- Vendor Compatibility?

Gaining Control of the Cloud



- **Visibility**

- ...know what is running / stored where...

- **Authentication**

- ...ensure only right users can access the right apps/data...

- **Data Protection**

- ...safeguard my data everywhere and at all times...

- **Secure Environment**

- ...ensure the environment is protected from malware and advanced threats...

- **Adaptive Security**

- ...security stays in-sync and scales with my constantly changing Cloud environment...

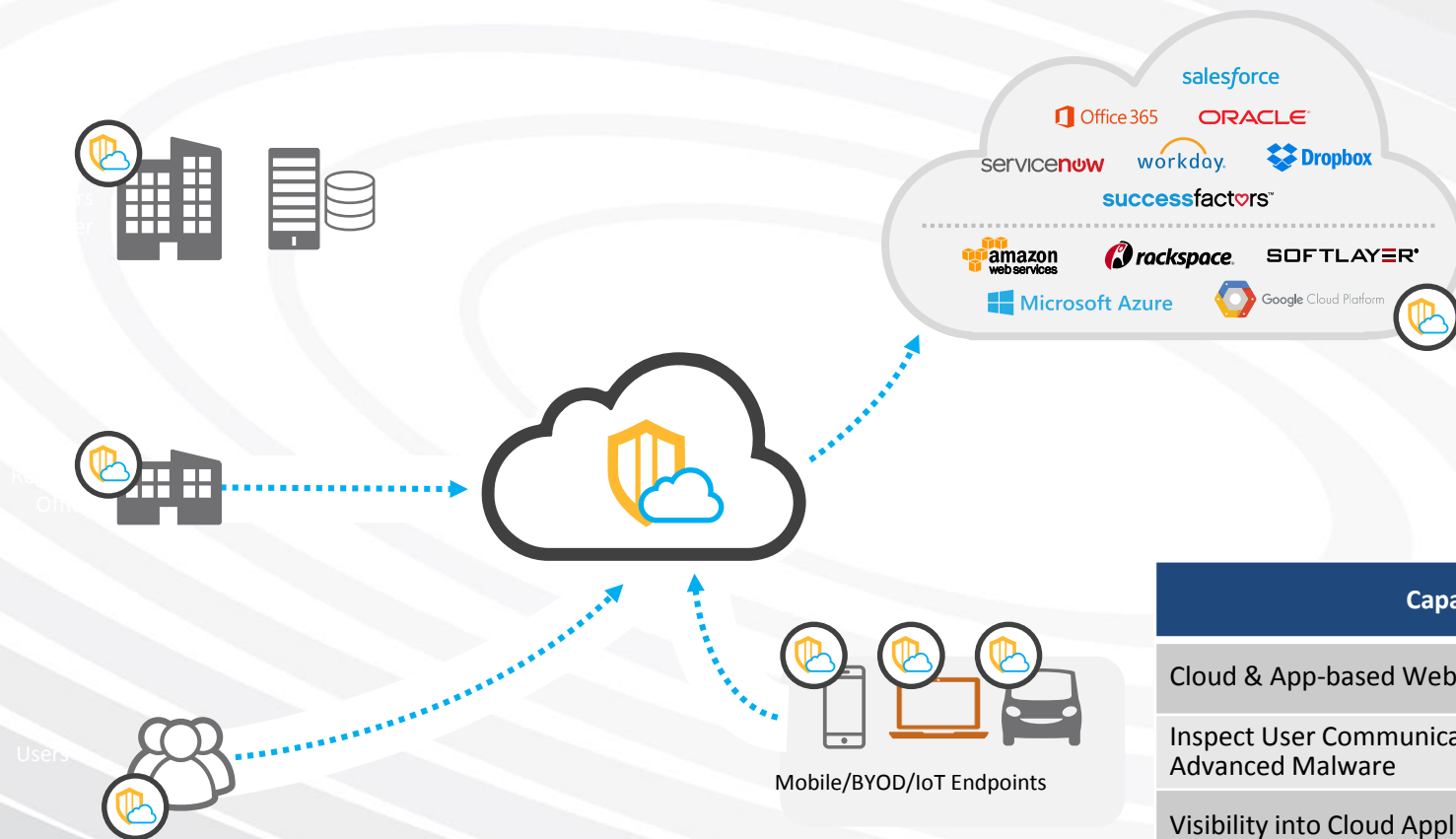
- **Automation**

- ...be able to automatically apply the right security with minimal human intervention...

- **Ease of Use**

- ...manage my complex hybrid world from single control point...

Cloud Security Access Brokers CASB



Capability
Cloud & App-based Web Traffic Cleansing
Inspect User Communication for Advanced Malware
Visibility into Cloud Application Usage by Users
User-Centric DLP
User-Based Cloud Application Authorization
Audit Acceptable-Use with Real-Time Analytics

CASB Benefits

- Minimise Cloud Risk
 - Understand and Control your Cloud Usage
 - Know your Data
 - Harmonise Security Policies
 - Control Migration to the Cloud
- Ensure Compliance
 - Protect Data in and for the Cloud
 - Audit Cloud Activity
- Maximise Benefit from Cloud Usage
 - Build and Maintain Trust
 - Choose the Right Cloud(s)
 - Secure Digital Transformation



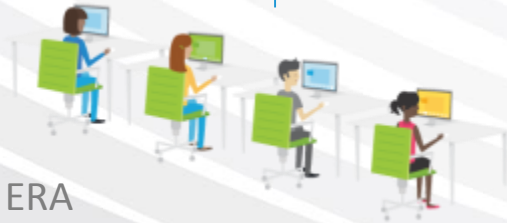
Tectonic Shift in the Market



Enterprise



Unmonitored Activities
Bypass Traditional Security



CLOUD ERA

Traditional Security Stack

Risk Assessment

IDS/IPS

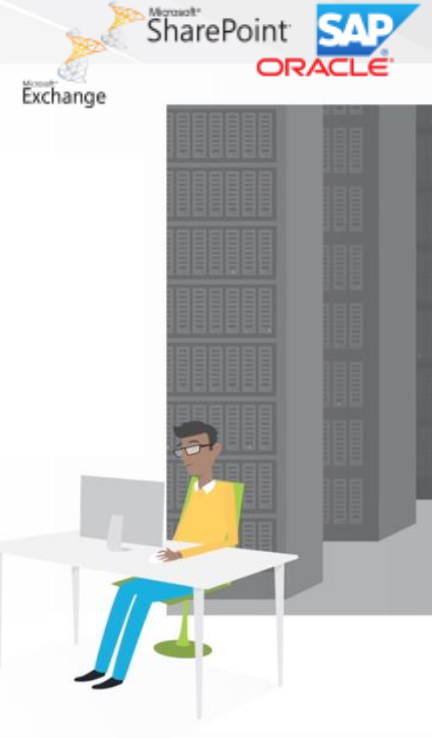
Firewall

SWG

DLP

SIEM

PRE-CLOUD ERA



New Security Stack for Cloud Apps



Enterprise

Traditional Security Stack



Risk Assessment

IDS/IPS

Firewall

SWG

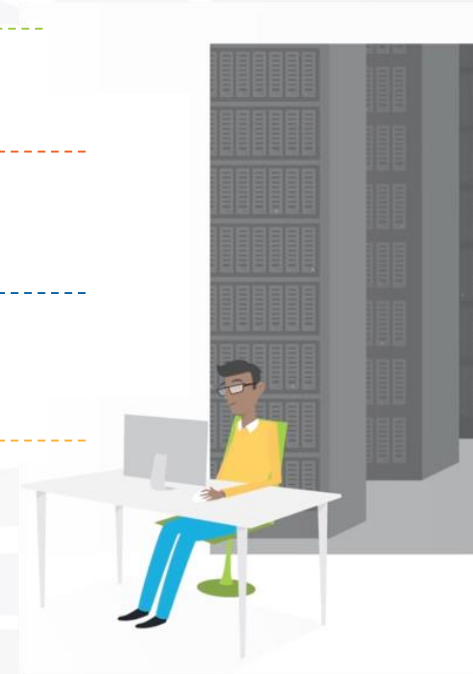
DLP

SIEM

Unmonitored Activities
Bypass Traditional Security

CLOUD ERA

PRE-CLOUD ERA



CASB Components



Shadow IT Audit

- Solution for Shadow IT Analysis
- Leverages log data from NG Firewalls, SWGs, etc.
- On-prem SpanVA appliance helps aggregate and anonymize log data
- Tight integration with ProxySG and WSS



Securlets™

- API-based solution for sanctioned cloud apps
- Custom app dashboard
- Protect, Detect & Investigate
- Current Securlets with DLP scanning: Office 365, Box, Dropbox, Salesforce, Google, AWS
- Other Securlets: ServiceNow, Yammer, AWS, DocuSign, Jive



CASB Gateway

- Gateway solution for unsanctioned and sanctioned cloud apps
- Protect, Detect & Investigate
- Real-time policy enforcement
- Works with Reach Agent to enforce device-level policies
- Current Gatelets with DLP Scanning: around 57
- Total Gatelets: around 75

Audit

Protect

Detect

Investigate

API Coverage for Cloud Apps

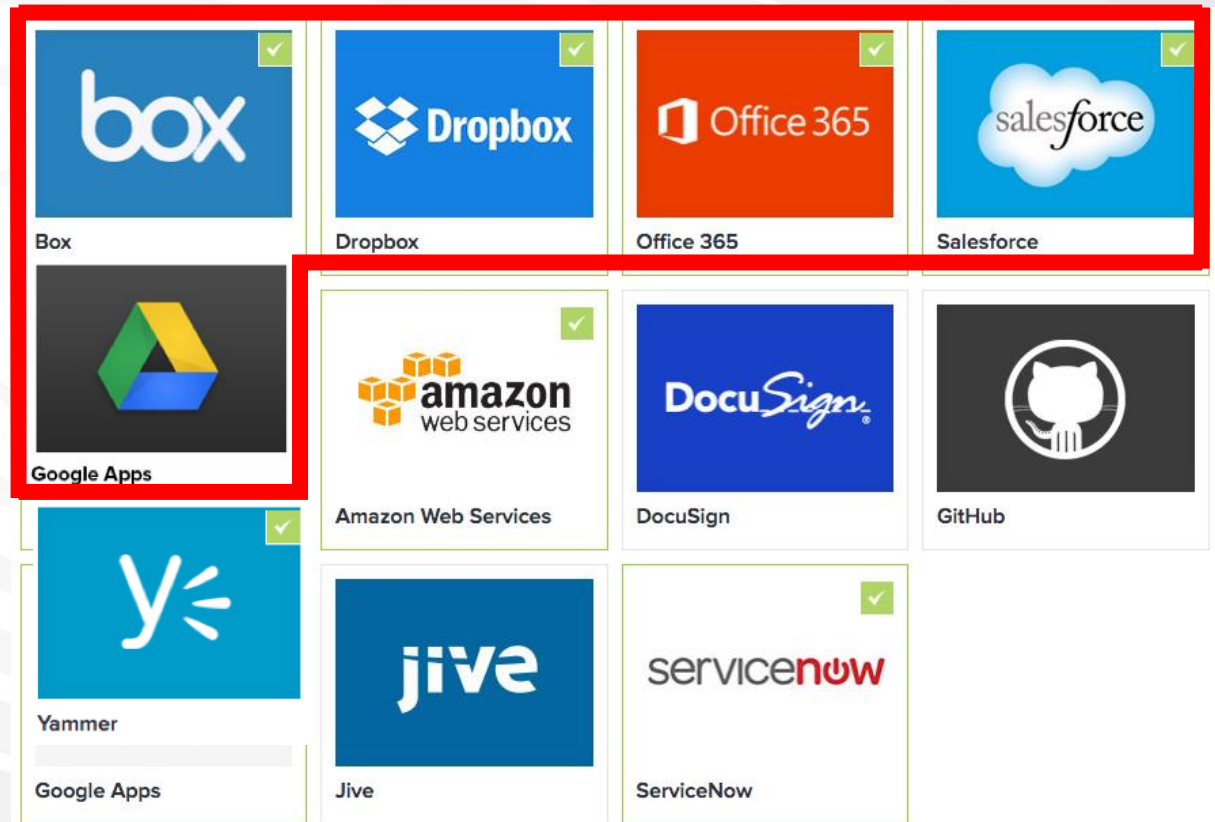


11

Total

5

With DLP



Gateway Coverage for Cloud Apps



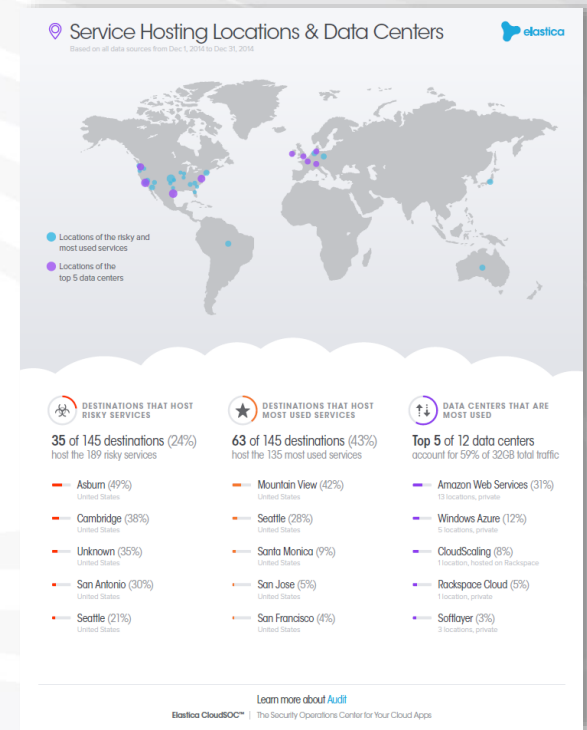
Gateway Coverage
for Cloud Apps:

70 + 57

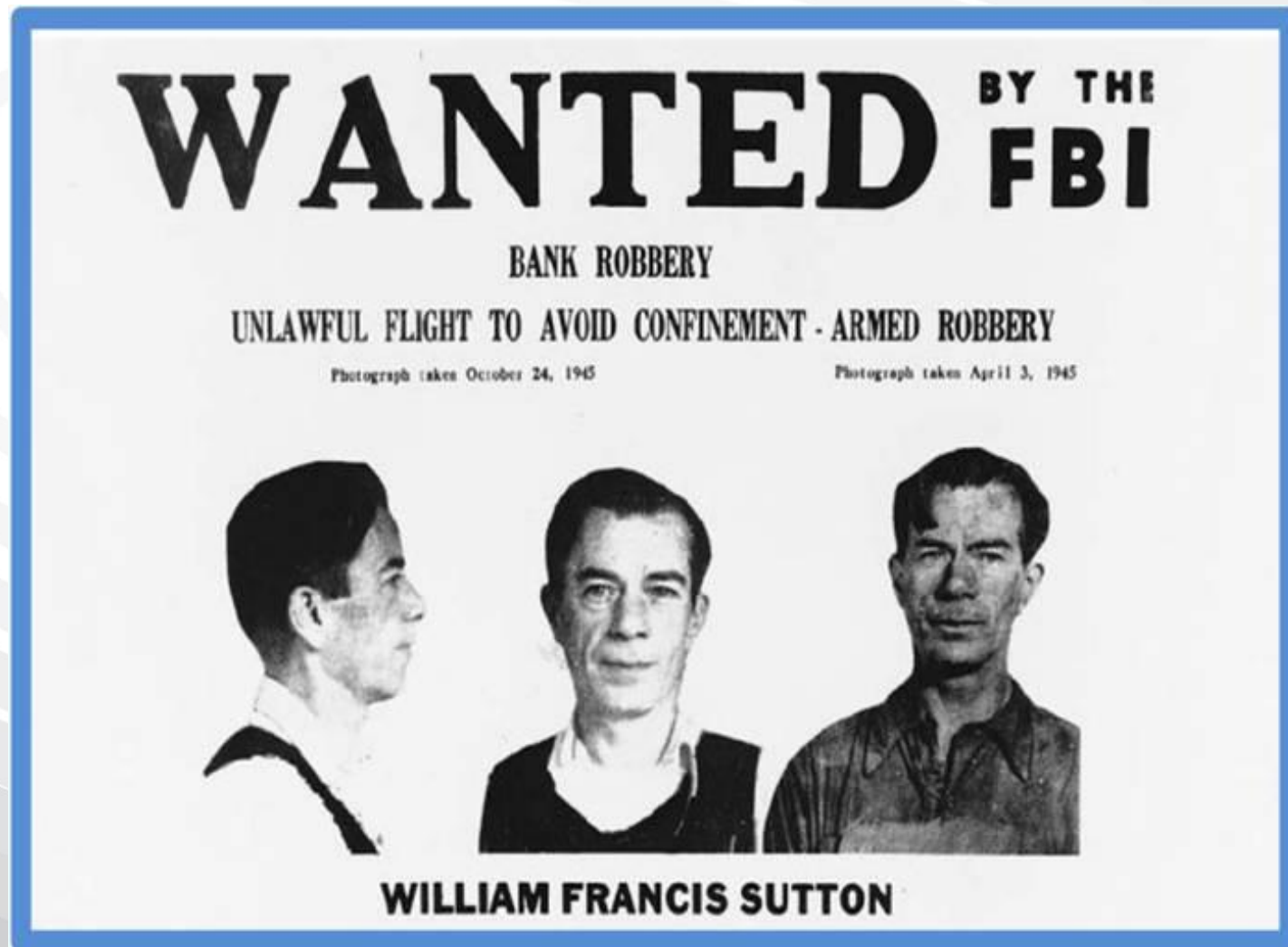
Total With DLP

Box	Dropbox	Microsoft Dynamics	Gmail	GroupDocs	Hightail
Evernote	Google Drive	Office 365	Huddle	IBM Connections	iCloud
OneDrive Personal	Salesforce	Sites	IDrive	IntraLinks	Jive
SugarSync	SurveyMonkey	Yammer	Joyent	Just Cloud	MailerLite
4Shared	4Sync	Acrobat.com	MediaFire	Microsoft Azure	OneHub
AIM Mail	Alfresco	Amazon CloudDrive	OneUbuntu	Outlook.com	OwnCloud
Amazon Web Services	Amazon WorkDocs	Bitcasa	Oxygen Cloud	Podio	Rackspace Cloud
BV ShareX	cCloud	CentralDesktop	RapidShare	SafeSync	SeaCloud
Cloud Provider	CloudMe	Concur	ShareFile	Slack	SmartFile
Confluence	Copy	Cubby	Soonr	Synclivity	Uploaded
Digital Ocean	DocuSign	Egnyte	WatchDox	WebCargo	Workshare
FilesAnywhere	Flow	Ftopia	Wuala	Xero	Yahoo Mail
			Zoho Docs	DigitalBucket	

Deep Usage Analysis and Reporting

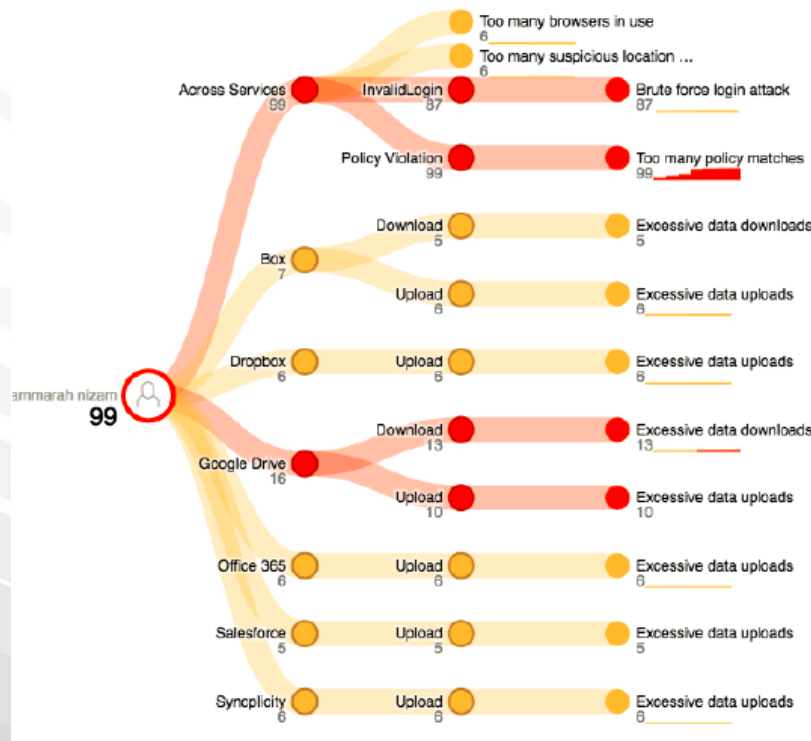


User Behavior Analysis



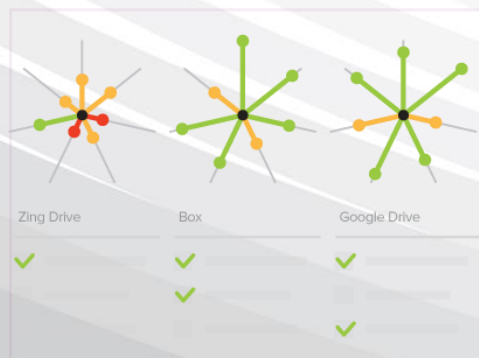
User Behavior Analysis

- User's behavior threshold could trigger blocking or further rules



Determine the apps that are best for your business

- View Business Readiness Rating based on 60+ metrics across 7 categories
- Customize prioritization of metrics to tailor analysis to your organization
- Perform side-by-side comparative analysis of alternative apps







Business Readiness Rating™

38

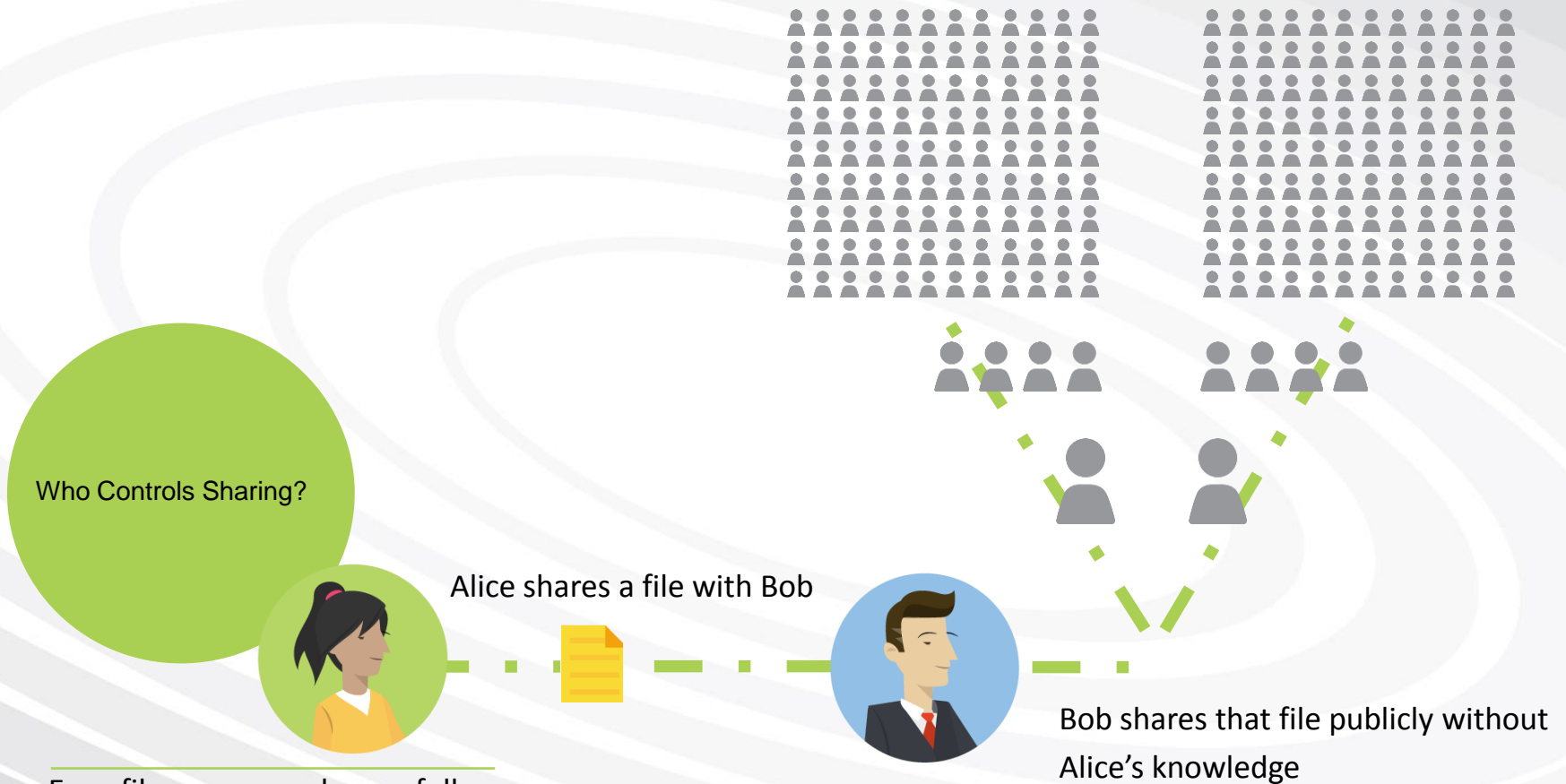
SUB CATEGORY	IMPORTANCE	
Federated Identity Management ⓘ	<input type="range"/>	Don't care
Brute-force protection ⓘ	<input type="range"/>	Must have

Office 365 provides base security, but you still need...



REQUIREMENT	BECAUSE	HOW
 <p>Automated classification</p>	Compliance mandates require identification of sensitive data	Leverage data science to automatically understand content without involving humans
 <p>User visibility and control</p>	Users are the biggest threat that can bypass your security controls	Real-time awareness of access and actions
 <p>Analysis of risky behavior</p>	This is not readily seen just by A/V scanning or APT systems	Per user-graph of “normal” behavior vs. risky behavior
 <p>Data protection / attack mitigation</p>	Before, during, and after a breach requires fast response	Complete lifecycle solution

Office 365 use case



Alice shares a file with Bob

Bob shares that file publicly without Alice's knowledge

Even file owners no longer fully control how their files are shared

Office 365 use case



Using Office 365



Alice

Shared



Payroll.docx



with Bob

But it's
not that
simple

From an
Unmanaged
Device

?

From an
Anomalous
Location

?

?

The File
Contains
PII Risk

Bob is an
External
Collaborator

Get your (free) cloud risk assessment



Inbound risky content shared with employees (e.g. malware, IP, etc)



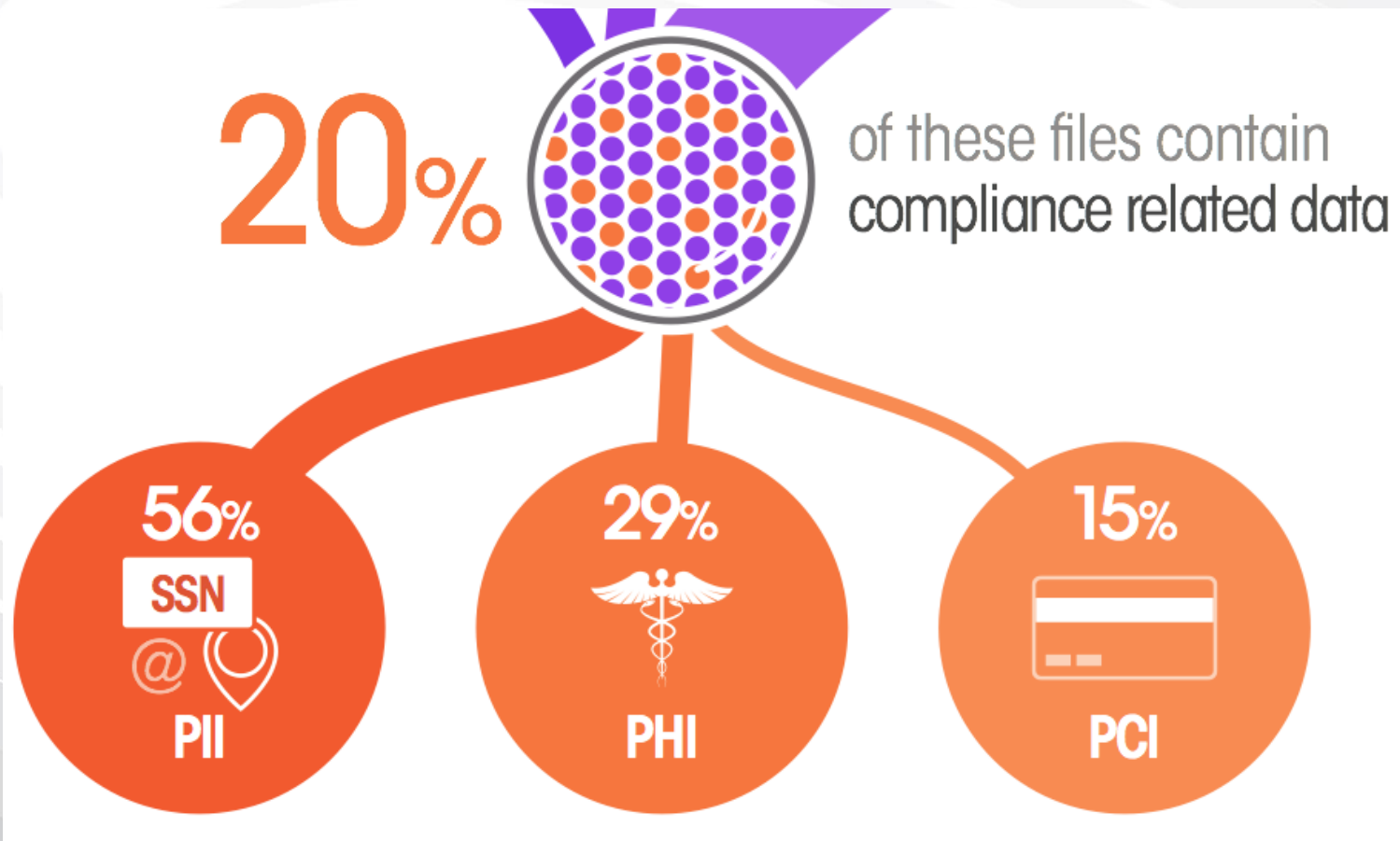
External and public content exposures, including compliance risks

Risky users and user activities

From Cloud Risk Assessment



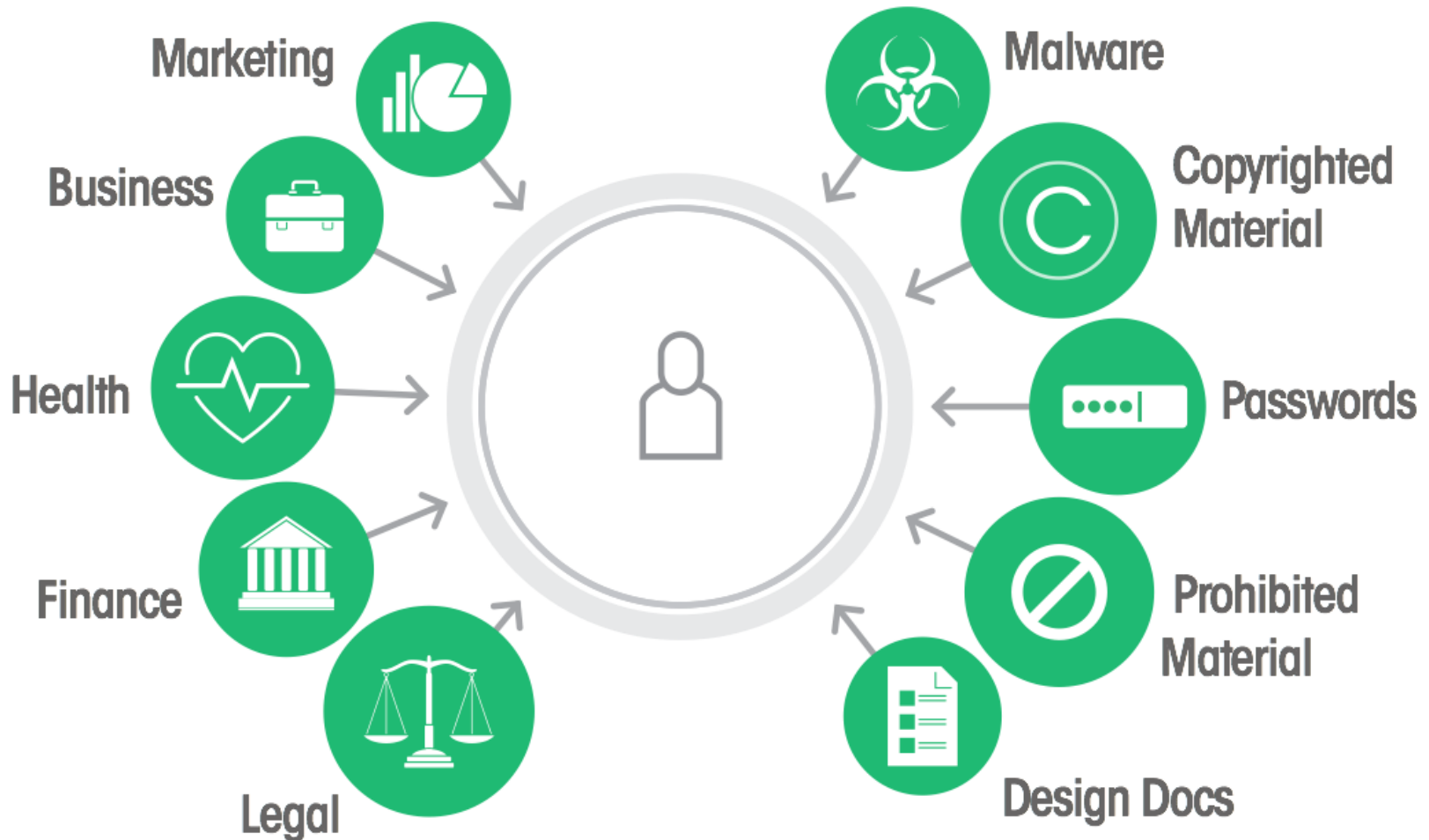
External and public content exposures, including compliance risks



From Cloud Risk Assessment



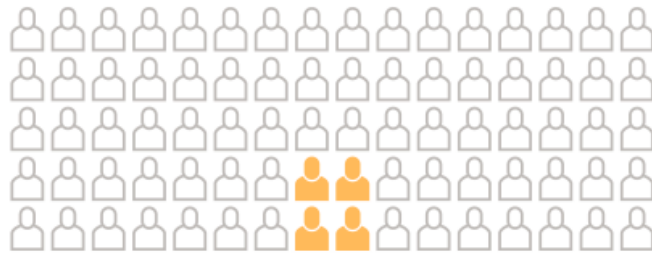
Inbound risky content shared with employees (e.g. malware, IP, etc)



From Cloud Risk Assessment



Risky users and user activities



5% of the users are responsible for



85%
of the total
risk exposures



www.sinergy.it

Marketing@sinergy.it