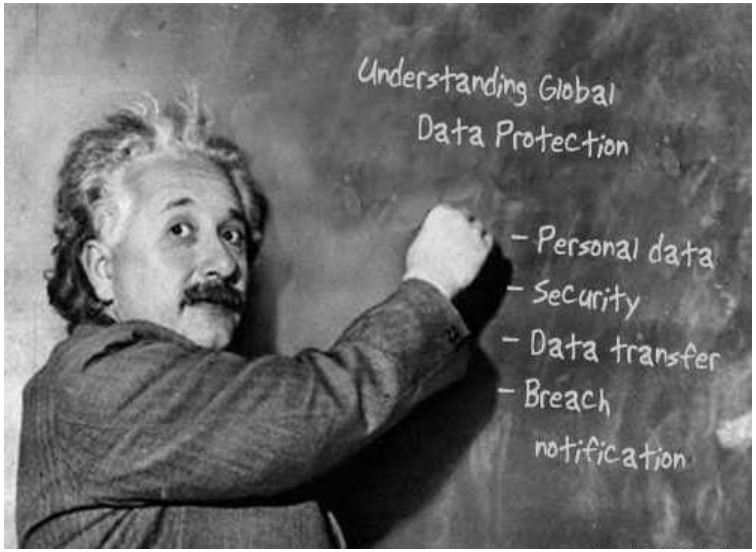
CipherCloud®
Trust in the Cloud™

Understanding Global Data Protection Laws

Willy Leichter
Global Director, Cloud Security

Agenda

- Cloud benefits and inhibitors
- Changing IT landscape
- Compliance basics
- Overview of global protection laws
- Microsoft/Ireland legal challenge
- Best practices to meet compliance
- Recommendations



Changing IT Challenges

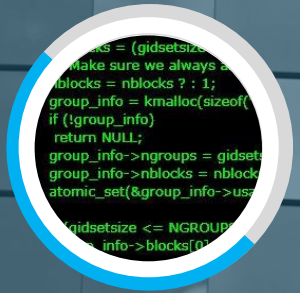
Protecting data instead of just infrastructure

Disappearing network perimeter

Managing the proliferation of cloud services

Surveillance and forced disclosure risks

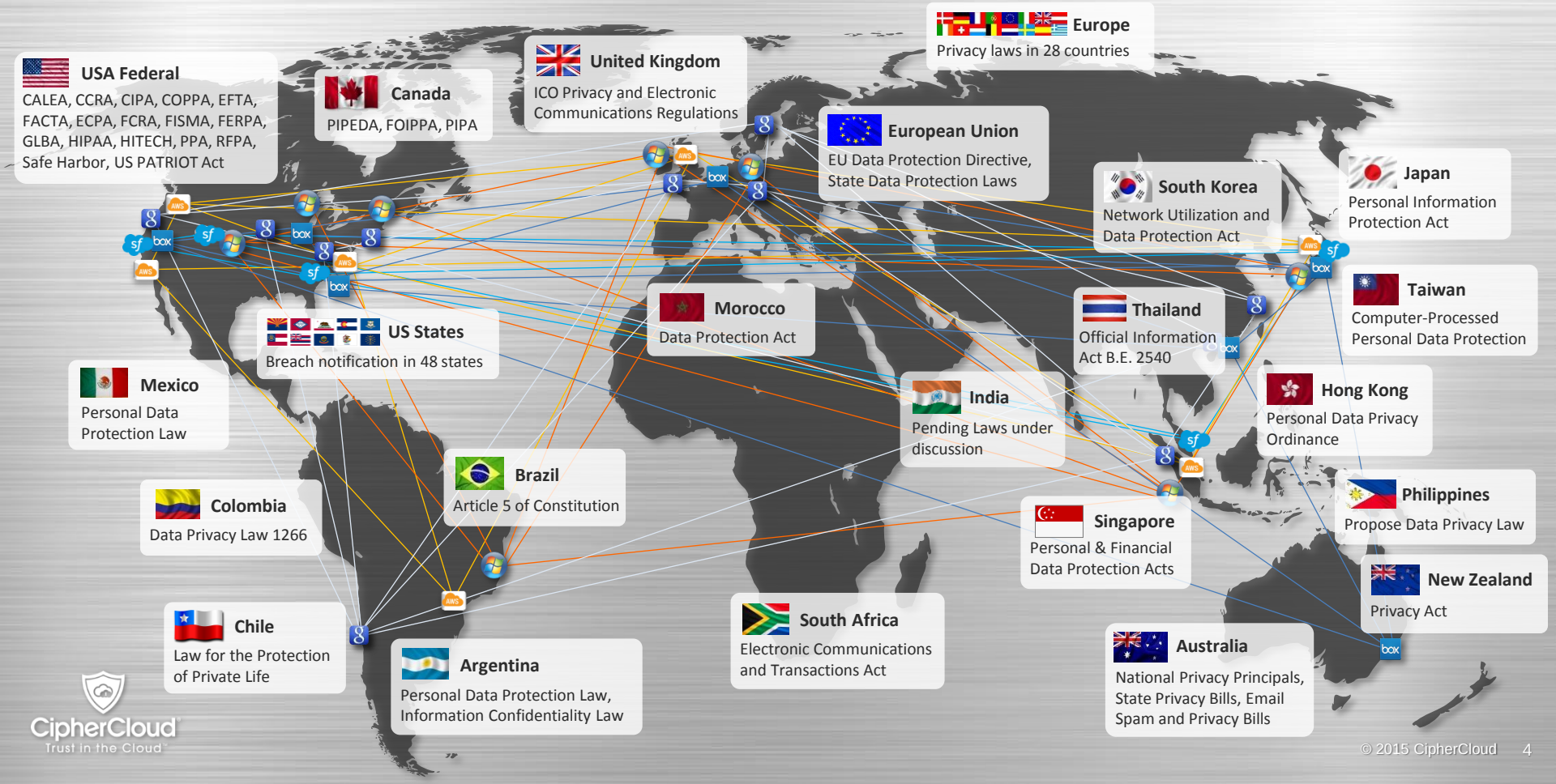
Complying with data protection and residency laws



Using legacy tools against emerging cloud threats

©CipherCloud | All rights reserved

Where Cloud Data Resides and What Laws Might Apply

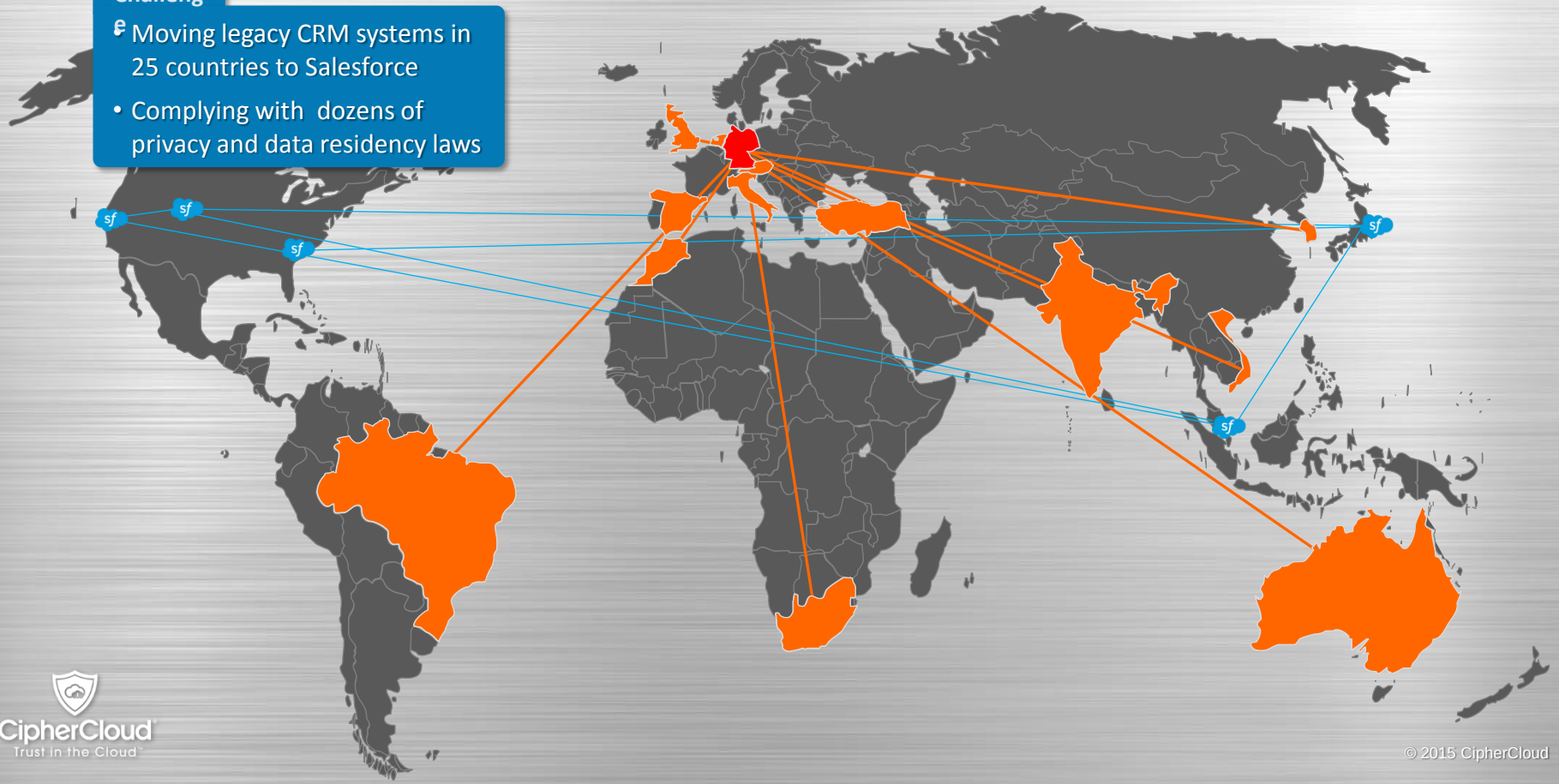


CipherCloud
Trust in the Cloud

Customer Example: Global Telco

Challeng

- Moving legacy CRM systems in 25 countries to Salesforce
- Complying with dozens of privacy and data residency laws



CipherCloud
Trust in the Cloud

Legacy Compliance Models Don't Work in the Cloud

Legacy Protection Model

- Location of data determines what laws apply
  - Legal sovereignty over physical media or files
- Data owners control infrastructure security
- Transfer and processing of data is controlled (in theory…)
- Regulators focus on location, certification, perimeter security

Reality in the Cloud

- Data won't and shouldn't stay in one location
  - Distributed computing
  - Cross-region backups
  - Third-party processing
- Many people can access the data
  - Remote command-and control
  - Support & services
- Customer ask the wrong questions
  - Datacenter location
  - Infrastructure security

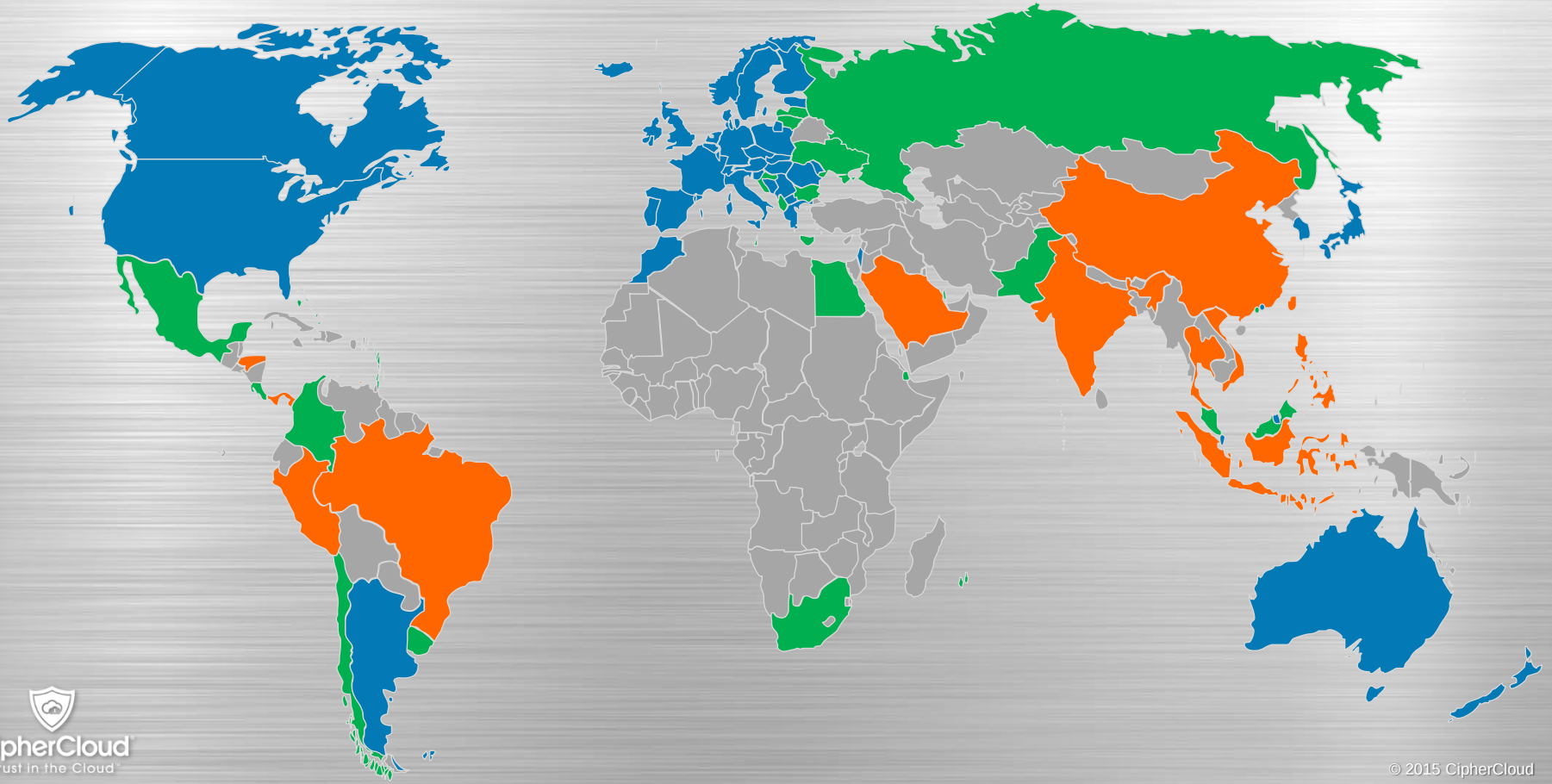
Global Compliance Basics

- **Data Owner/Controller**
  - Always responsible, regardless of location
- **Data Processors & Sub-Processors**
  - Cloud providers with access to private data
  - Extensive contractual requirements for data owner
- **Data Residency/Sovereignty**
  - Must assure data doesn't go to regions with weaker privacy protections
- **Data Transfer**
  - Strict requirements if data goes to a specific region with weaker controls

Global Compliance Resource Center

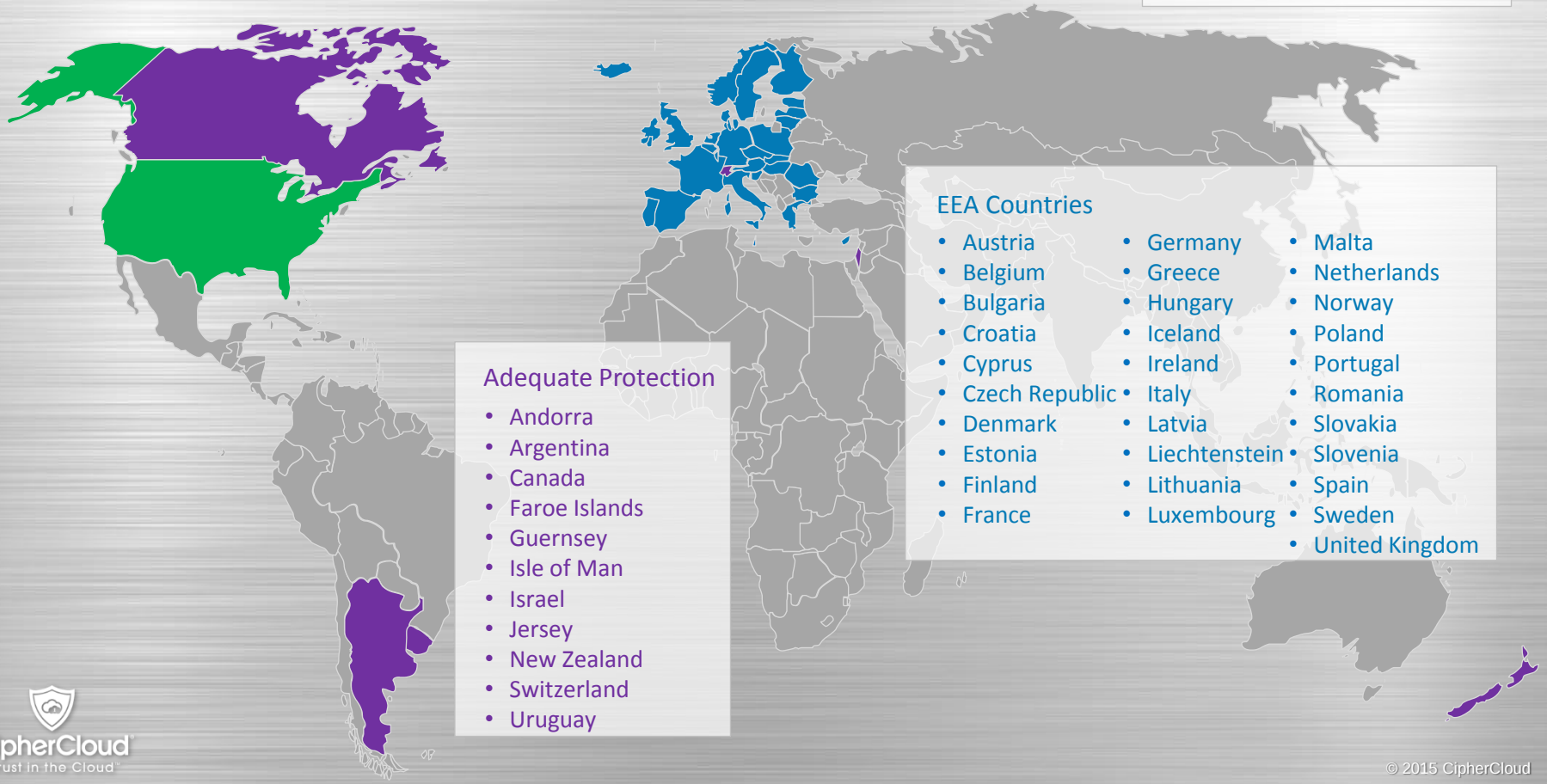
- **Details on data protection laws in 83 countries**
  - Summaries of laws
  - National authorities and links
  - Security requirements
  - Definitions of personal and sensitive data
  - Data transfer restrictions
  - Breach notification requirements
- **Content on industry-specific regulations**
  - Financial services
  - Payment card industry (PCI)
  - Healthcare
- **ciphercloud.com/global-compliance-resource-center**
  - Dynamic interactive map
  - Downloadable book (PDF)

Overall Levels of Restrictions



CipherCloud
Trust in the Cloud

EEA and Safe Harbor



Adequate Protection

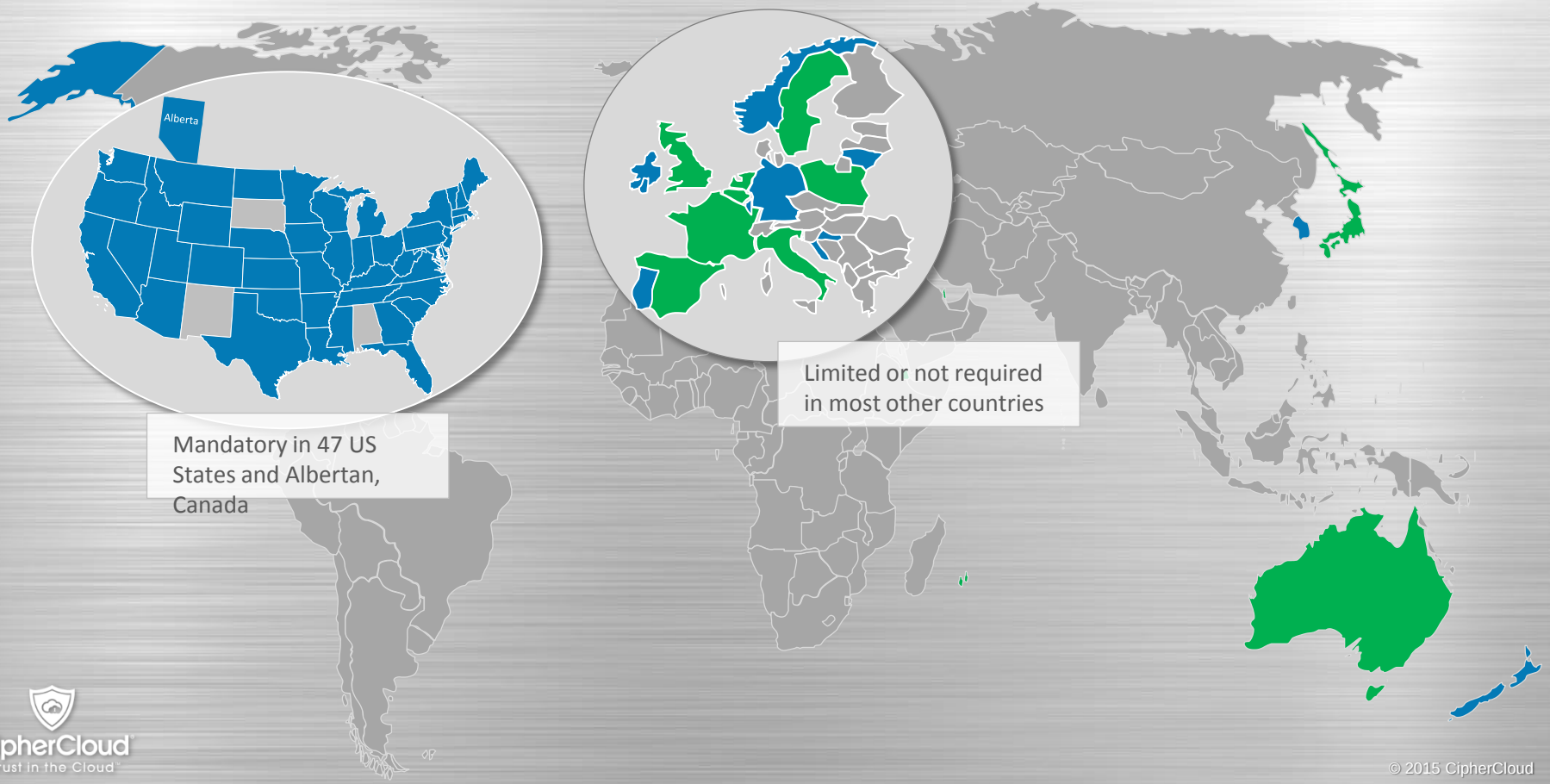
- Andorra
- Argentina
- Canada
- Faroe Islands
- Guernsey
- Isle of Man
- Israel
- Jersey
- New Zealand
- Switzerland
- Uruguay

EEA Countries

- Austria
- Belgium
- Bulgaria
- Croatia
- Cyprus
- Czech Republic
- Denmark
- Estonia
- Finland
- France
- Germany
- Greece
- Hungary
- Iceland
- Ireland
- Italy
- Latvia
- Liechtenstein
- Lithuania
- Luxembourg
- Malta
- Netherlands
- Norway
- Poland
- Portugal
- Romania
- Slovakia
- Slovenia
- Spain
- Sweden
- United Kingdom

CipherCloud
Trust in the Cloud

Breach Notification Requirements



CipherCloud
Trust in the Cloud

Does Data Residency = Data Sovereignty?

Cloud providers control data across borders

- Regional datacenters are rarely autonomous
- Redundant backup data centers only in US
- Central “command and control” can usually access data residing in any country

SLAs are usually not binding on location

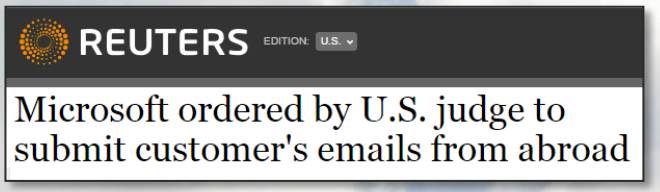
- Data often spread across multiple datacenters
- Best practices call for backups in other regions

US court rulings challenge data residency

- Data “controlled” by US cloud providers can still be subject to US subpoenas
- Microsoft ruled to release data stored in Ireland to US law enforcement

Primary Microsoft datacenter locations

The Microsoft / Ireland Case



"It is a question of control, not a question of the location of that information"

- Judge Loretta Preska, chief of the US District Court in Manhattan

"Warrant requires the company to provide documents it controls, regardless of location"

-U.S. Justice Department

"They have total control of those records, can produce them here, and that's all that matters."

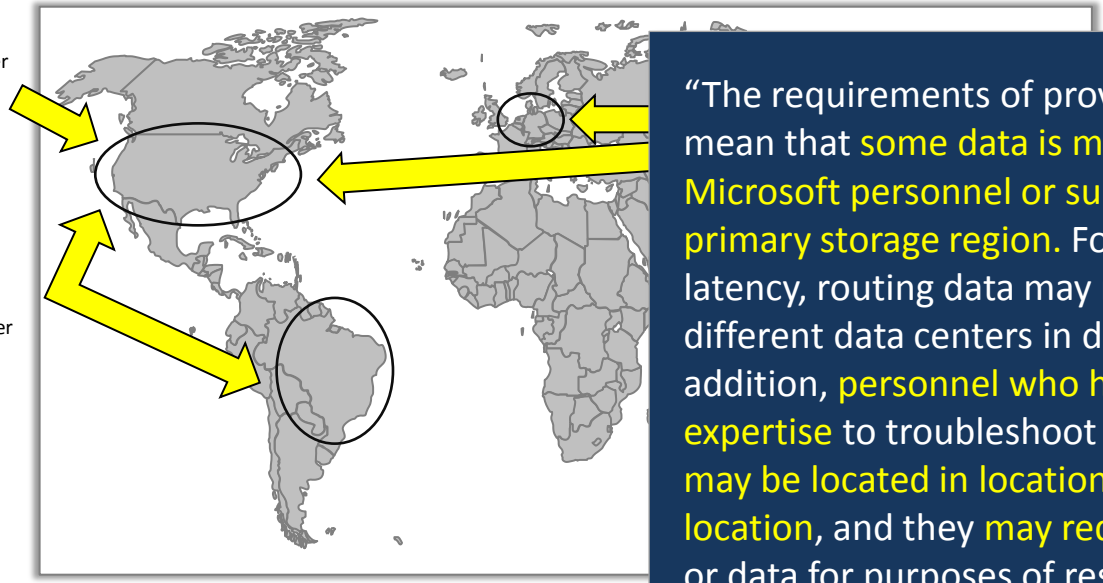
- Federal prosecutor Serrin Turner

Weak SLAs Don't Help

Microsoft – standard SLAs for South American cloud customers

SharePoint Online, Exchange Online and Lync Online Datacenter locations for South American customers.

SharePoint Online, Exchange Online and Lync Online Datacenter locations for Brazilian customers.



"The requirements of providing the services may mean that some data is moved to or accessed by Microsoft personnel or subcontractors outside the primary storage region. For instance, to address latency, routing data may need to be copied to different data centers in different regions. In addition, personnel who have the most technical expertise to troubleshoot specific service issues may be located in locations other than the primary location, and they may require access to systems or data for purposes of resolving an issue."

- Microsoft standard cloud SLAs

What Are Your Practical Options?

1. Just say 'NO' to the Cloud

- Not viable or recommended
- Makes you less competitive
- Limits access to latest technology

2. Ignore the problem

- Your users will use cloud anyway
- Hope (and pray) you're not the next data breach time bomb

3. Focus on protecting data - not just infrastructure

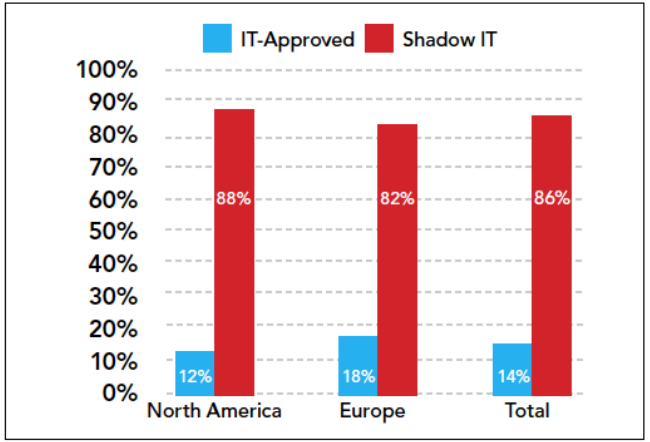
- Technology solutions exist
- It's possible to control sensitive data and benefit from the cloud

Cloud Use is Inevitable

NA 1,245

EU 981

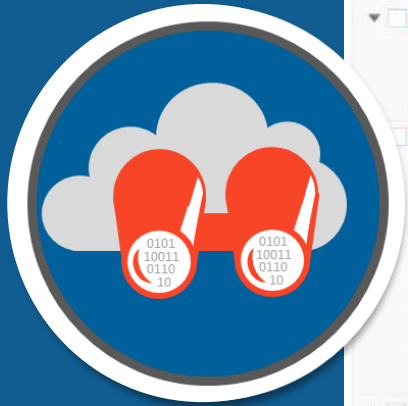
Average # of cloud apps per organization



"The average global enterprise utilizes over 1,100 cloud applications"

"86% of cloud applications used by enterprises are unsanctioned Shadow IT"

Cloud Discovery & Risk Assessment



Drill-down details on all apps, risk and user activity

Granular trend analysis

Advanced multi-criteria filtering

Cloud Data Loss Prevention

CipherCloud
Trust in the Cloud™

My Favorites | Activity Monitoring | Anomaly

Filter By | Filter text | Filter | Last Week

Violated Policies by Object

Top Violated Po

Vio

1

0

Credit Card | GLB Act | NDC Code | PCI | SSN

Account | User

Last Rendered: 19:48:27 PM

salesforce 14

Search...

Home | Chatter | Files | Leads | Accounts

Magen Kenney

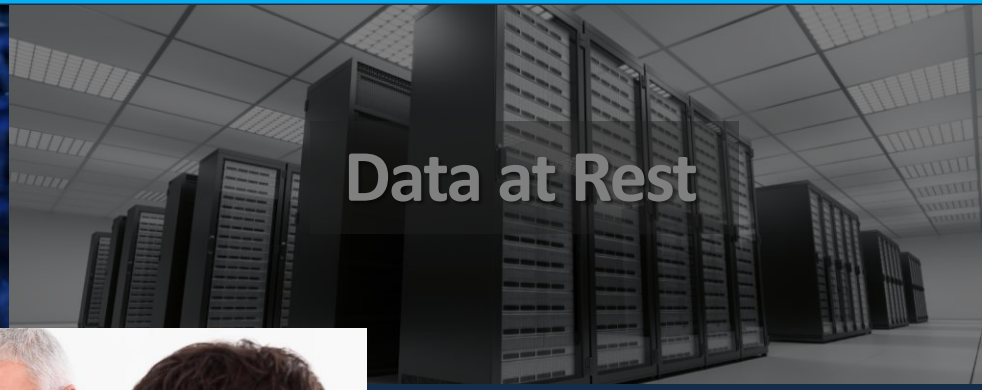
I'm working on a Credit Memo.

TO: Stan Crawford, Customer Service
FROM: Laura Jacobson, Western Accounts
SUBJECT: NanoSystems Acquistion
DATE: February 18, 2013
CC: Vincent Dimarco, CFO

Stan,
As we discussed, we need to issue a refund for the molecular failed FDA testing. In order to expedite this, here's a list of credit card numbers for a direct refund:
David Welsh, Secure Nontech, VISA 5466160038201172
Cindy Meyers, Ocean Detection, VISA 6011 0009 9013 9420
Bill Johnson, Metro Tech, 3530 1113 3330 0000
Jagadeesh Jambur, Axway, 3566 0020 2036 0500
Briggs Humbolt, Avery Systems, 5555 5555 5555 4440

Regards,
Laura

Where Should You Protect Your Data?



Vulnerabilities

- Account hijacking*
- Forced disclosure
- Data breaches*
- Malicious insiders*
- Insecure APIs*
- Shared technology*

* Top Threats

cloud security alliance SM

CipherCloud Encryption Model

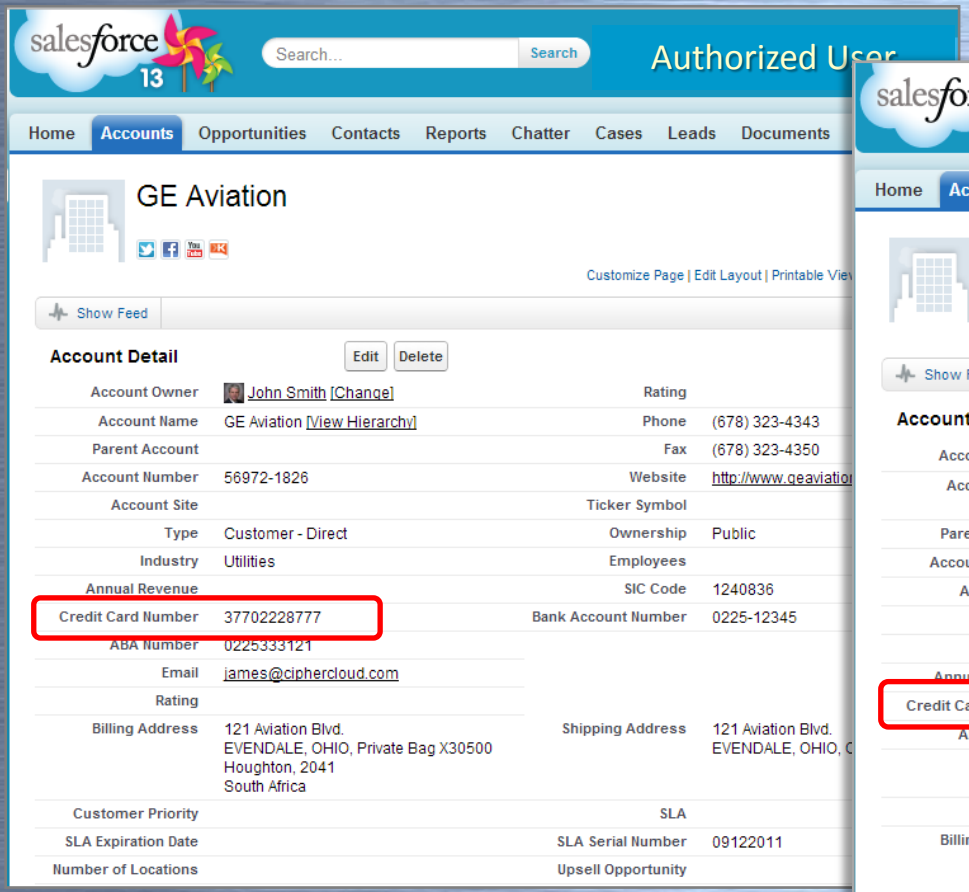
- Encryption or tokenization at the enterprise gateway
- Minimal latency
- Integrated malware detection

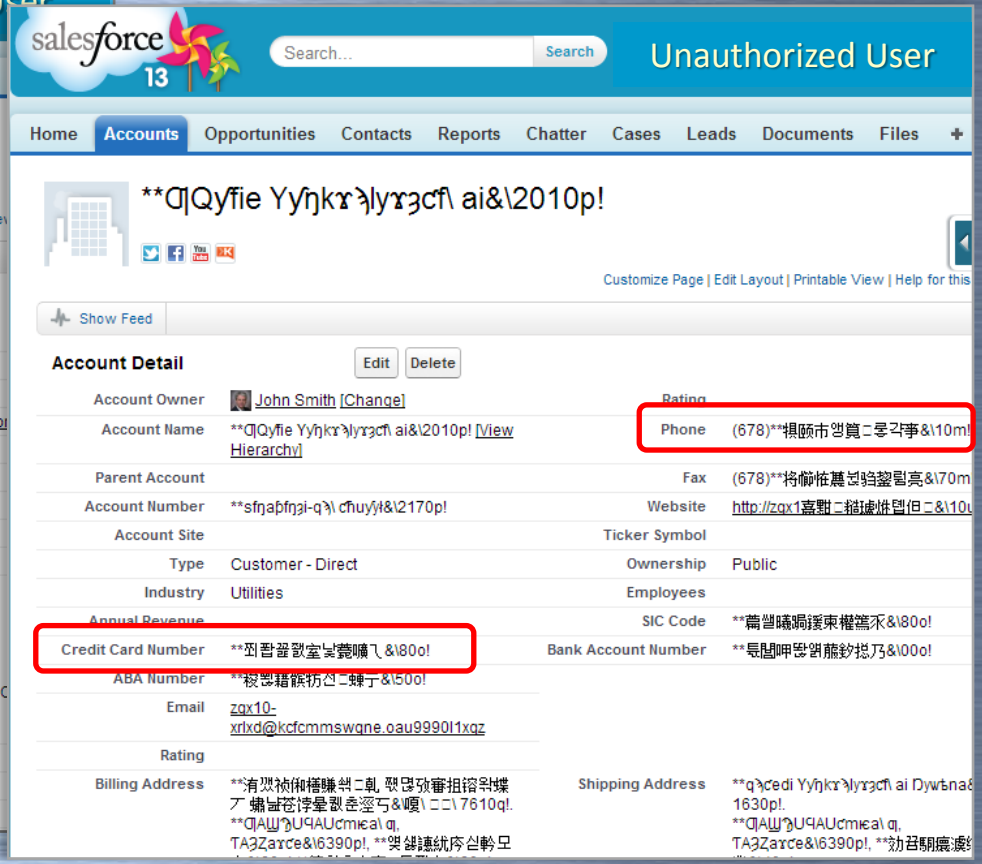
Encrypted data is indecipherable to unauthorized users

Transparent to users
Preserves application functionality

Encryption keys never leave the enterprise

Granular Field-Level Control





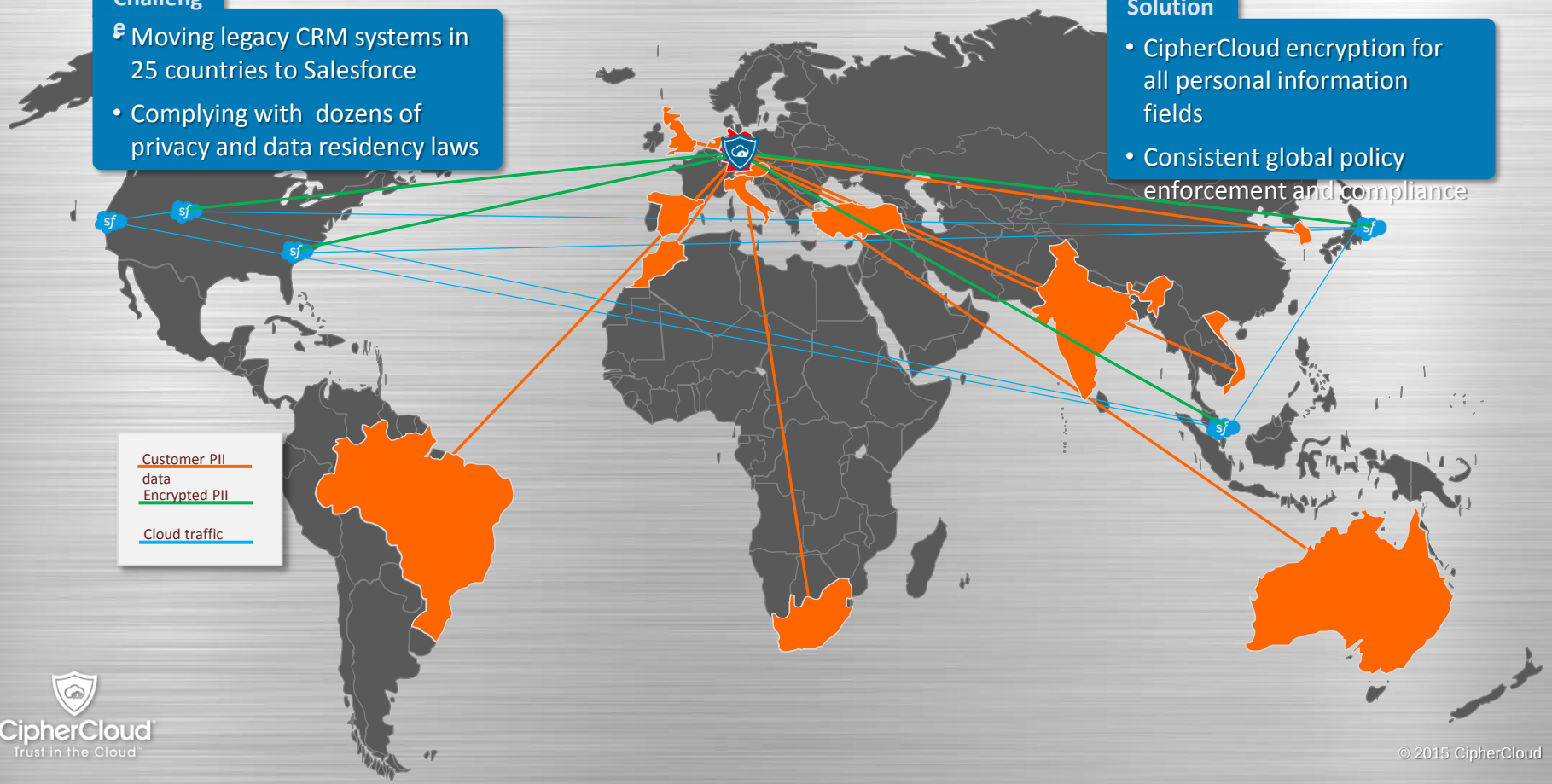
Customer Example: Global Telco

Challeng

- Moving legacy CRM systems in 25 countries to Salesforce
- Complying with dozens of privacy and data residency laws

Solution

- CipherCloud encryption for all personal information fields
- Consistent global policy enforcement and compliance



CipherCloud
Trust in the Cloud

Compliance Arguments for Cloud Encryption

- **Prevents Cloud Providers from being Data Processors**
  - Widely accepted for US and many global data protection laws
  - Still debated in Europe – especially Germany
    - Some believe any encryption to be “pseudo-anonymization”
- **Improves Controller compliance even if Cloud Provider is not exempt**
  - Important added layer of security
  - Widely accepted for US data protection laws
- **Aligns with upcoming data privacy laws**
  - Significantly stiffer penalties and legal enforcement
  - Important added layer of security
  - Widely accepted for US data protection laws

Upcoming EU Data Protection Requirements

Core principles all supported by advanced data protection

- Data Minimization
- Data Portability
- Privacy by Design & Default
- Privacy Impact Analysis

Balancing Cloud Benefits with Compliance Requirements

Top 3 US Bank's Consumer Self-Service Loan Origination Portal

Largest Hospital Chain Meets HIPAA & HITECH in the Cloud

German Cosmetics Giants Meets International Security Regulations

Top Canadian Bank Safeguards Proprietary Information in the Cloud

Non-Technology Leader Trust Sensitive Data in Cloud Email

Major European Telco Consolidates Call Centers for 25 Countries

Global Leader in Customer Loyalty Moves Email to the Cloud

UK Education Organization Deploys Global Cloud-Based Portal

Large Pharmaceutical Company Uses Encrypted Email

Major Wall Street Firm Adopts Cloud Applications with Confidence

Genomics Testing Leader Protects Patient Data while Using the Cloud

New Zealand Bank Collaborates in the Cloud and Meets Compliance

Medical Audit Leader Launches Cloud-Based Customer Portal

Credit Reporting Giant Deploys Cloud Collaboration with DLP Controls

Government-Owned Mortgage Backer Protect PII Data in the Cloud

Recommendations

- **Avoiding the cloud is no longer viable, or desirable**
- **IT must move beyond the perimeter model to stay relevant**
  - Focus needs to be on protecting data – not infrastructure
- **Compliance requires more than cloud provider assurances**
  - You're responsible for the data – you must be proactive
- **Security and privacy challenges are solvable**
  - Strong encryption can assure exclusive access to data located anywhere
  - But keys must be retained by the data owner
- **Encryption is becoming and established best practice**
  - Not applying encryption is increasingly hard to justify
- **Work with companies that understand data protection and have deep integration with cloud applications**

About CipherCloud

Company

3.8+ Million Active Users

13 Industries

25 Countries

7 Languages

13 Patents

525+ Employees

Solutions

DISCOVER — Cloud Discovery, Cloud DLP

PROTECT — Strong Encryption, Tokenization

MONITOR — Activity Monitoring, Anomaly Detection

salesforce AppExchange Program **PARTNER**

servicenow amazon web services™

box Office 365

Customer

5 out of 10 Top US Banks

3 out of 5 Top Health Providers

Top 2 Global Telecomm Company

3 out of 5 Top Pharmaceuticals

40% of Global Mail Delivery

Largest US Media Company

Questions?

Willy Leichter
Global Director, Cloud Security
CipherCloud™
Trust in the Cloud

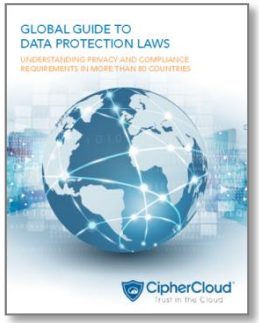
wleichter@ciphercloud.com
Twitter: @WillyLeichter

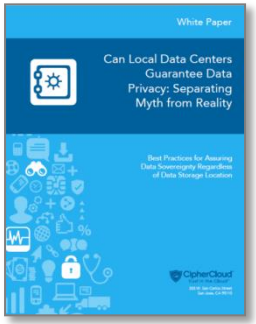
For additional information :

- Website: www.ciphercloud.com
- Twitter: @ciphercloud
- Email: info@ciphercloud.com
- LinkedIn: www.linkedin.com/company/ciphercloud
- Phone: +1 855-5CIPHER

Global Compliance Resource Center: Online Map, Guide, Whitepapers & More

www.ciphercloud.com/resources/global-compliance-resource-center





Quiz

How do you pronounce the name of the German BDSG data protection act:

Bundesdatenschutzgesetz