



ISOAG Meeting November 1, 2017

Welcome to CESC



Welcome and Opening Remarks

Michael Watson

November 1, 2017



ISOAG October 11, 2017 Agenda

- | | |
|---|--|
| I. Welcome & Opening Remarks | Mike Watson, VITA |
| II. An AWS Security & Compliance Primer | Tim Andersen, Amazon Web Services |
| III. EY Building Trust in the Cloud | Gregory William & Ilyah Simuni, Ernest & Young |
| IV. Ransomware | Gregory Bell, DBHDS |
| V. Outsourced IT Security Audits | John Musgrove |
| VI. Upcoming Events | Mike Watson, VITA |
| VII. Partnership Update | NG |

AWS Security & Compliance

A Primer

Tim Anderson
Program Manager,
WWPS Security & Compliance Business
Acceleration Team
Amazon Web Services
tdander@amazon.com
Nov 17



Agenda

- Overview of AWS
- How we practice security
- Shared Security Model
- Assurance Programs – NIST Alignment
- GovCloud – When it makes sense
- How we can help

AWS Overview

AWS Global Infrastructure

16 Regions – 44 Availability Zones – 87 Edge Locations

Region & Number of Availability Zones

AWS GovCloud EU
(2)

Ireland (3)
Frankfurt (3)
London (2)

US West
Oregon (3)
Northern California (3)

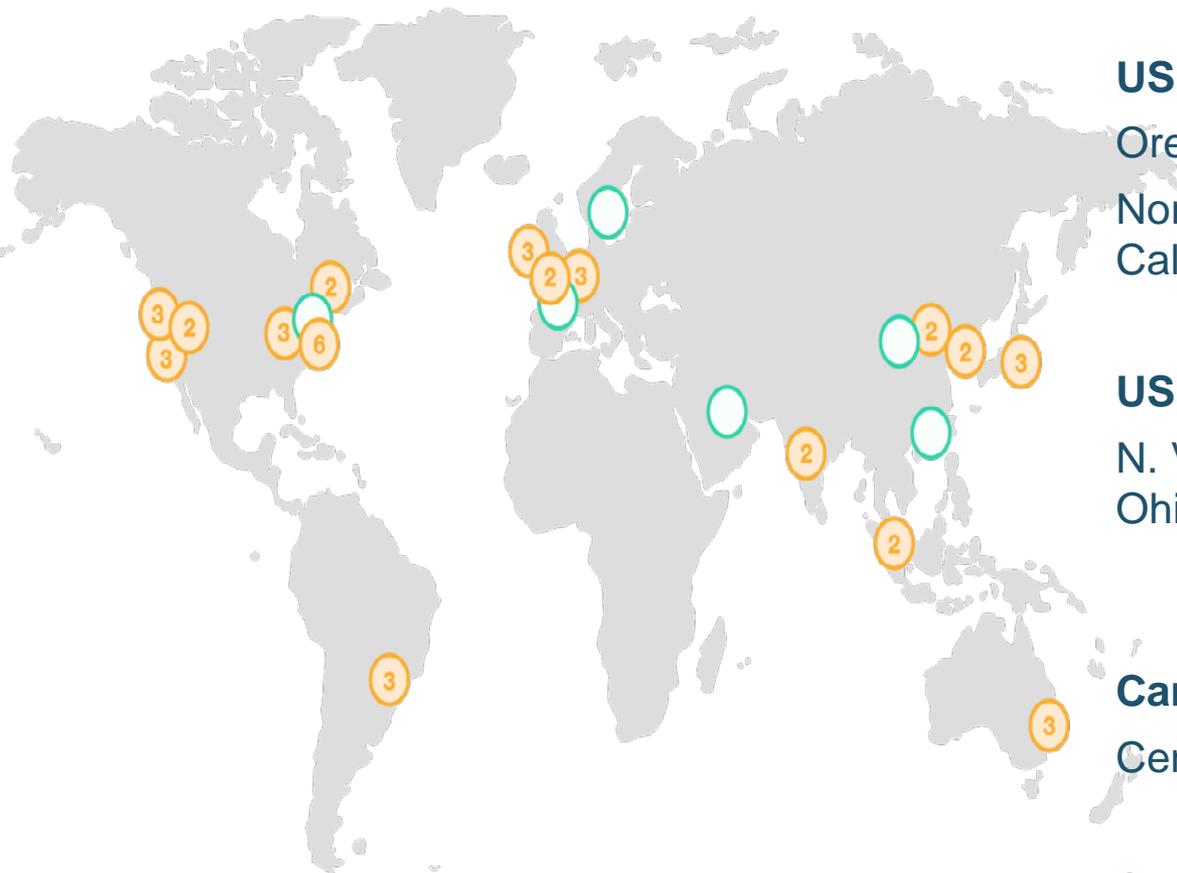
US East
N. Virginia (6),
Ohio (3)

Canada
Central (2)

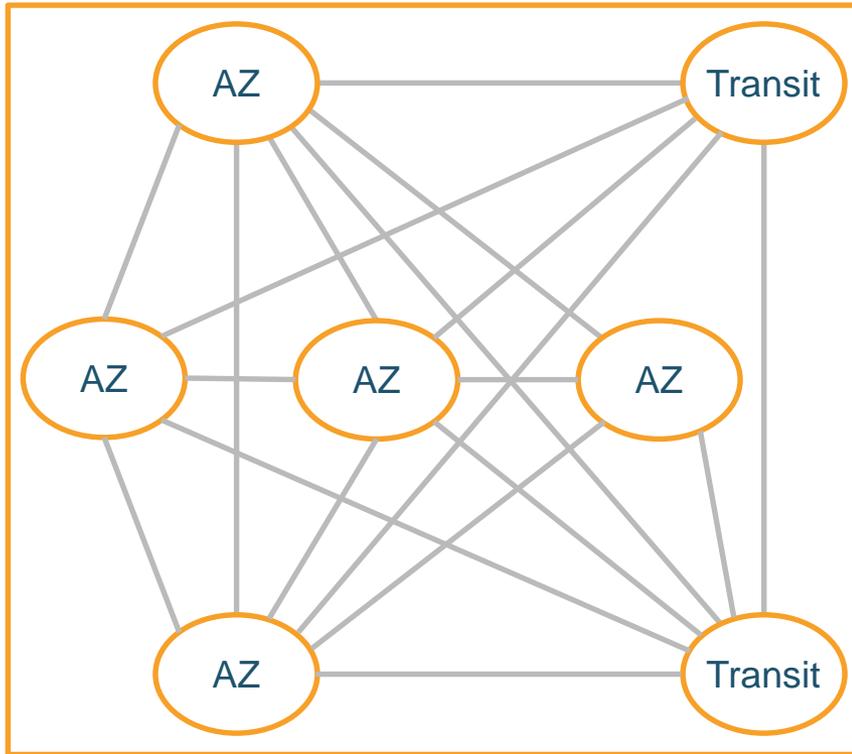
South America
São Paulo (3)

Asia Pacific
Singapore (2)
Sydney (3),
Tokyo (3),
Seoul (2),
Mumbai (2)

China
Beijing (2)

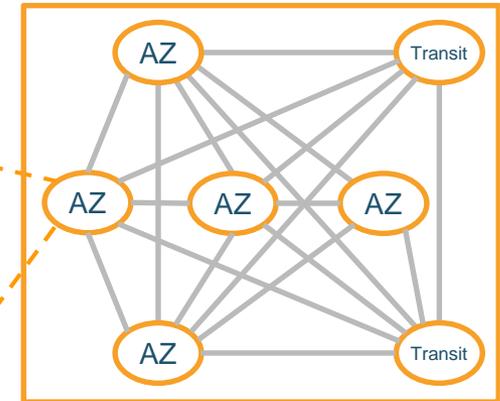
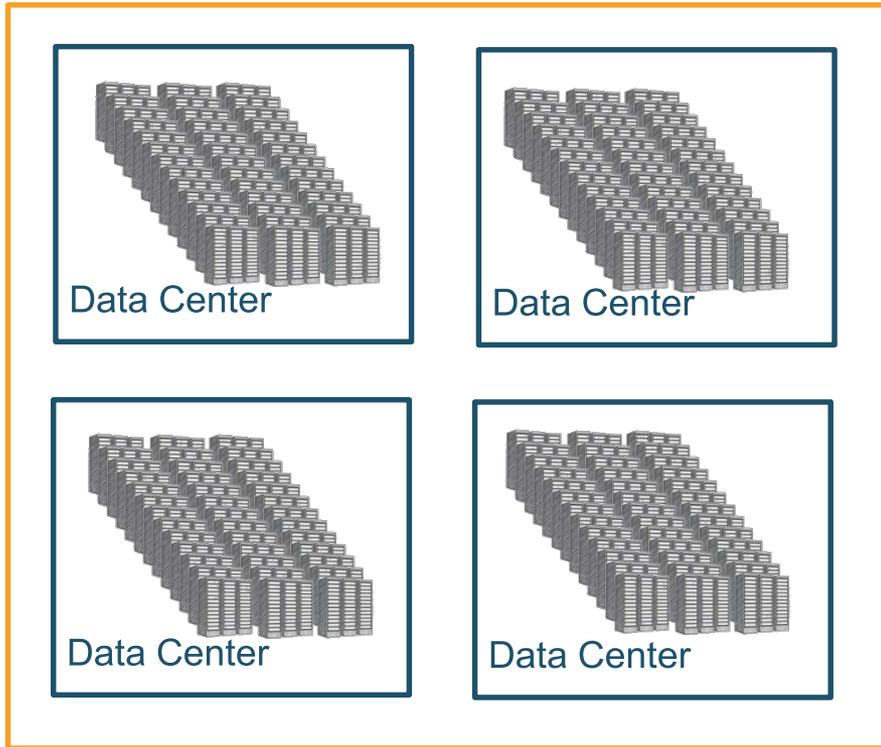


Example AWS Region



- Mesh of Availability Zones (AZ) and Transit Centers
- **Redundant** paths to transit centers
- Transit centers connect to:
 - Private links to other AWS regions
 - Private links to customers
 - Internet through peering & paid transit
- Metro-area DWDM links between AZs
- **82,864** fiber strands in region
- AZs <2ms apart & usually <1ms
- **25Tbps** peak inter-AZs traffic

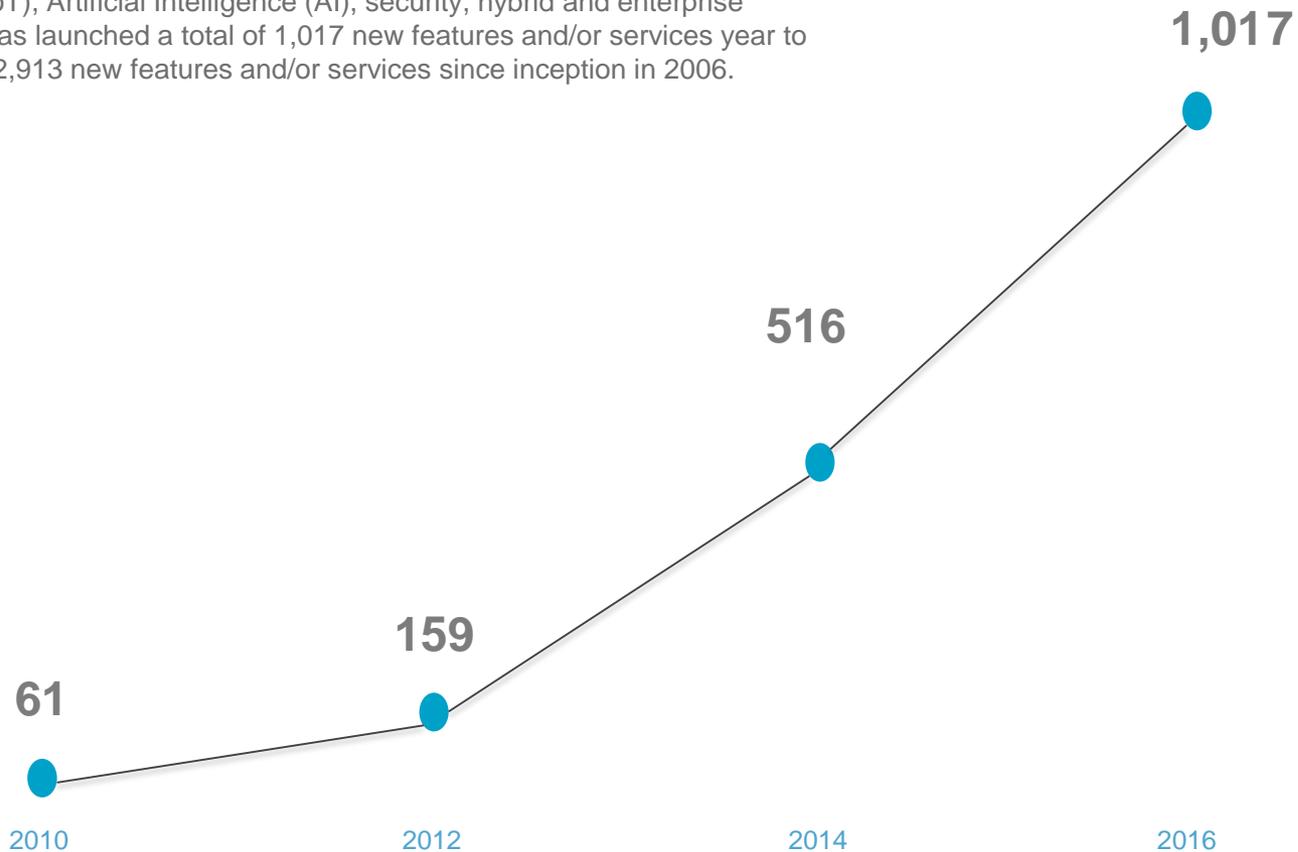
Example AWS Availability Zone



- 1 of 44 AZs world-wide
- All regions have 2 or more AZs
- Each AZ is 1 or more DC
 - No data center is in two AZs
 - Some AZs have as many as 6 DCs
- DCs in AZ less than $\frac{1}{4}$ ms apart

AWS Pace of Innovation

AWS has been continually expanding its services to support virtually any cloud workload, and it now has more than 90 services that range from compute, storage, networking, database, analytics, application services, deployment, management, developer, mobile, Internet of Things (IoT), Artificial Intelligence (AI), security, hybrid and enterprise applications. AWS has launched a total of 1,017 new features and/or services year to date* - for a total of 2,913 new features and/or services since inception in 2006.



2,913

GovCloud **Import/Export Snowball**

AWS Storage Gateway

Amazon Cognito

AWS OpsWorks

AWS CodeDeploy

Amazon ElastiCache

Amazon Config

Amazon CloudTrail

CodeCommit

EC2

Container Service

Amazon Kinesis

CloudHSM

Elasticsearch Service

AWS Elastic Beanstalk

Amazon SES

Elastic Transcoder

EC2 Container Registry

Amazon WorkMail

AWS CodePipeline

AWS Certificate Manager

Amazon EFS

Amazon Route 53

Redshift

Lambda

Identity & Access Management

AWS CloudFormation

Amazon AppStream

AWS Device Farm

Dynamo DB

QuickSight

Directory Service

Amazon RDS for Aurora

AWS Data Pipeline

AWS WAF

RDS for MariaDB

AWS Mobile Hub

Amazon SWF

Amazon API Gateway

AWS KMS

Amazon SNS

WorkSpaces

WorkDocs

AWS IoT

CloudWatch Logs

Mobile Analytics

CloudSearch

Amazon Machine Learning

AWS Direct Connect

AWS Service Catalog

Glacier

Amazon Inspector



How does AWS practice security?

Security is the foundation of everything we do

Security is Job Zero



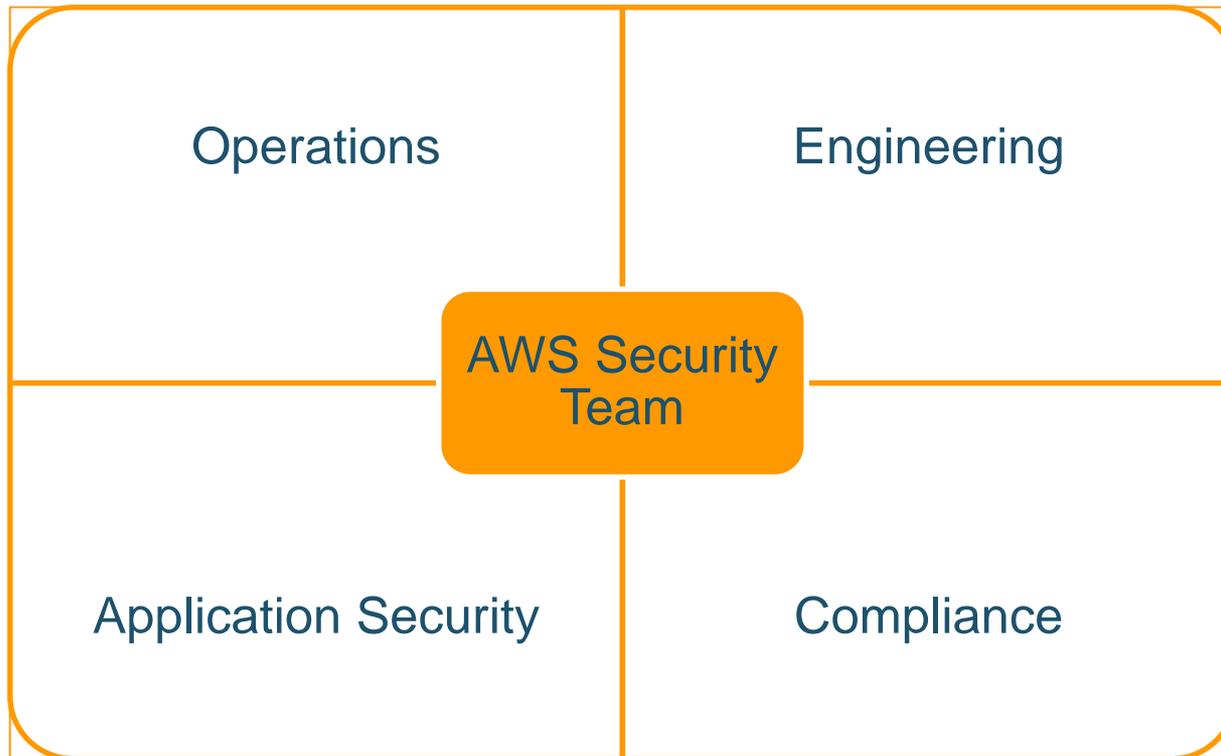
Physical Security

Network Security

Platform Security

People & Procedures

What does our Security Team look like?



Our Culture:

- Everyone is an owner
- When the problem is “mine” rather than “hers” there’s a much higher likelihood I’ll do the right thing
- Measure constantly, report regularly, and hold senior executives accountable for security - have them drive the right culture.
- Measure, measure, measure
 - 5 min metrics are too coarse
 - 1 min metrics are barely OK

Our Culture:

- Saying “no” is a failure
- Apply more effort to the “why” rather than the “how” Why is what really matters ask the “five whys”
- Decentralize - don’t be a bottleneck - Produce services that others can consume through hardened APIs
- Test, CONSTANTLY
 - inside/outside
 - Privileged/unprivileged
 - Black-box/white-box
 - Vendor/self

Our Culture:

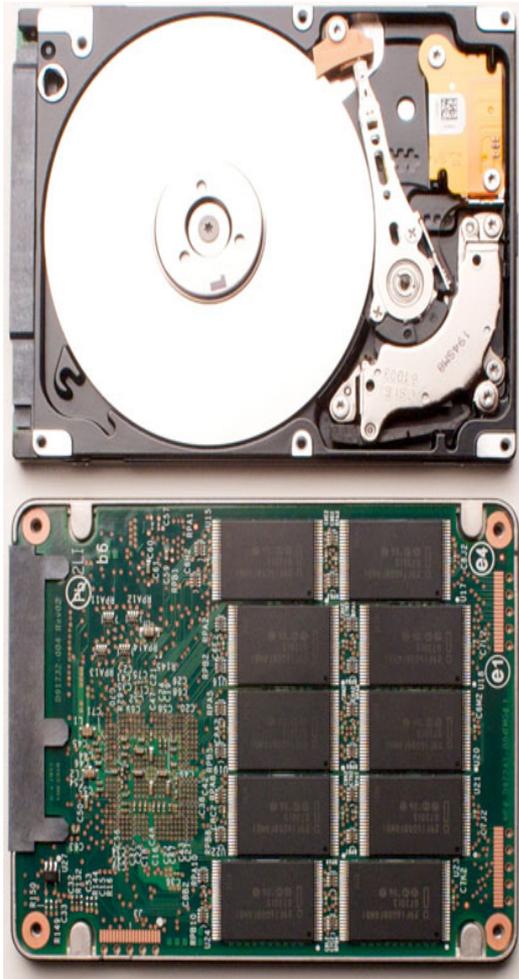
- Proactive monitoring rules the day
 - What's "normal" in your environment?
 - Depending on signatures == waiting to find out WHEN you've been had
- Collect, digest, disseminate, & use intelligence
- Make your compliance team a part of your security operations
- Base decisions on facts, metrics, & detailed understanding of your environment and adversaries

Operating principles

- Separation of Duties
- Different personnel across service lines
- Least privilege

Technology to automate operational principles

- Visibility through automation
- Shrinking the protection boundary
- Ubiquitous encryption

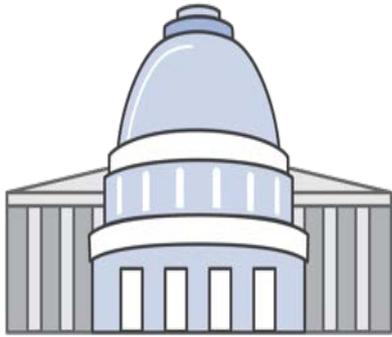


From this

To This



AWS in the Public Sector



2,300+

government
agencies



7,000+

educational
institutions



22,000+

nonprofit
organizations

Government and Education Worldwide



Access a deep set of cloud security tools

Networking



Amazon VPC



AWS Direct Connect



VPN connection



Security Groups



Flow logs



AWS Shield



AWS WAF



Route table

Compliance & Governance



AWS Service Catalog



AWS Trusted Advisor



AWS CloudFormation



AWS CloudTrail



Amazon EC2 Systems Manager



Amazon CloudWatch



AWS Config



AWS Artifact



Amazon Inspector

Identity



IAM



AWS Directory Service



AWS Organizations



Active Directory integration



Temporary security credential

SAML Federation



Encryption



AWS KMS



AWS CloudHSM



Client-side encryption



AWS Certificate Manager

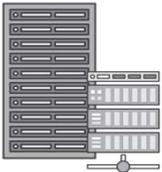
AWS Partners Focused on Public Sector



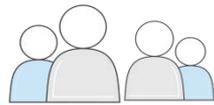
What our customers say

The security paradigm shifted

Traditional Infrastructure



Equipment



Resources and Administration



Contracts



Cost

- Big Perimeter
- End-to-End Ownership
- Build it all yourself
- Server-centric approach
- Self-managed Services
- Static Architecture - De-centralized Administration
- Focus on physical assets with multiple (manual) processes

AWS Cloud



No Up Front Expense
Pay for what you Use



Improve Time to Market & Agility



Scale Up and Down



Self-Service Infrastructure

- Micro-Perimeters
- Focus on your core value and on protecting Data
- Service-Centric
- Continuously Evolving
- Central Control Plane (API)
- Greater automation

Rob Alexander CIO of Capital One Bank



“And of course, security is critical for us. The financial services industry attracts some of the worst cyber criminals. So we worked closely with the AWS team to develop a security model which, we believe, allows us to operate *more securely* in the public cloud than we can even in our own datacenters.”

re:Invent Keynote 2015

<https://youtu.be/0E90-ExySb8>

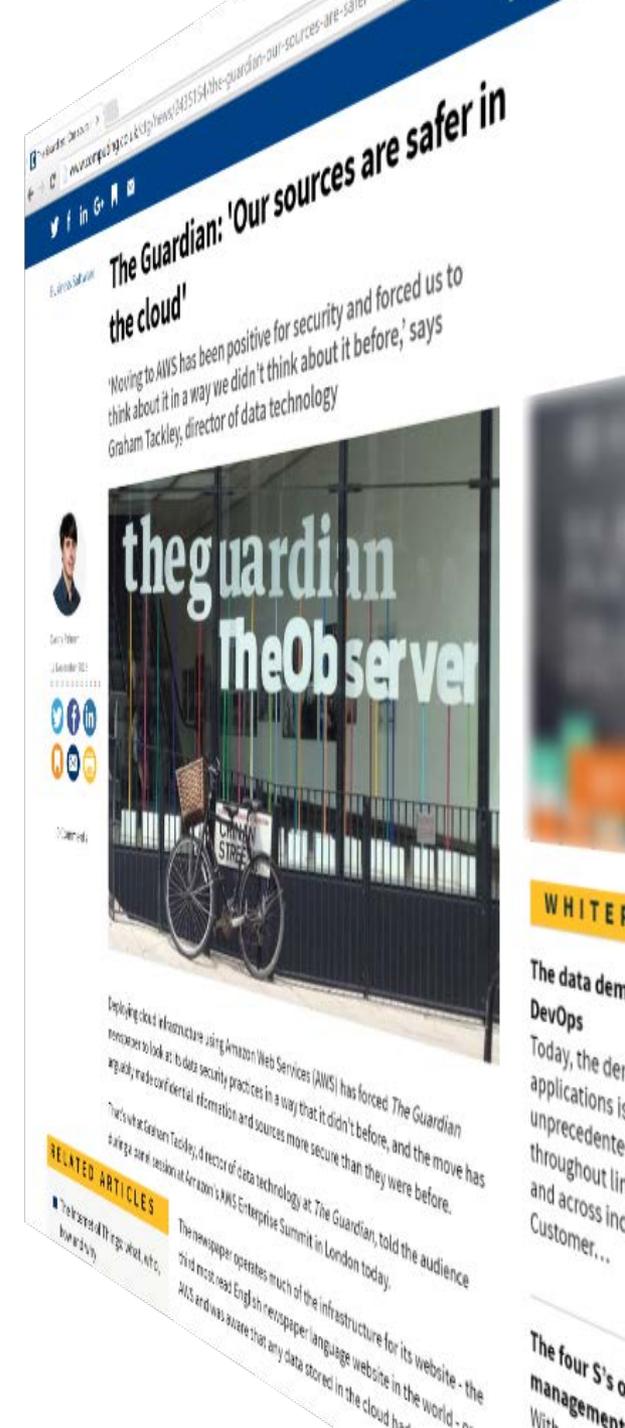


David Rogers UK MoJ CTO

“You should probably start engaging with the idea that the cloud can be considerably more secure than the private cloud or your own data centre, and start engaging with the risks that are building in the spaces where you haven't moved to the cloud yet.”



The Guardian: <http://bit.ly/1HXS321>
(emphasis added)



Improving your security with AWS...



“From a physical and logical security standpoint, I believe that, if done right, public cloud computing is as or more secure than self-hosting.”

– Steve Randich, EVP and CIO, Financial Industry Regulatory Authority, USA

FINRA now deploying multiple Hadoop-based and Redshift-based analytics apps core to their regulatory mission

- Multi-petabyte clusters growing by terabytes per day
- Core apps in full production since January 2015
- Half way thru 2 year plan to go “all in” to the AWS cloud



Financial Industry Regulatory Authority

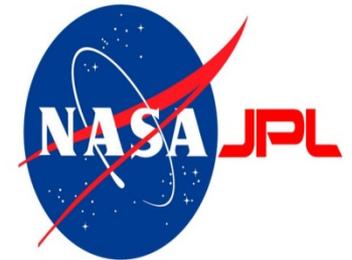
Improving security with the cloud

For more details, see Re:Invent 2013 presentations by NASA JPL cyber security engineer Matt Derenski (<http://awsps.com/videos/SEC205E-640px.mp4>)

“Based on our experience, I believe that we can be even more secure in the AWS cloud than in our own datacenters.”



Tom Soderstrom, CTO, NASA JPL



Shared Security Model

It is always YOUR data!

- 📦 Customer chooses **where to place data**
- 📦 AWS regions are geographically isolated by design
- 📦 **Data is not replicated to other AWS regions** and doesn't move unless customer chooses to move it
- 📦 **Customers manage access** to their customer content and AWS services and resources
- 📦 **Customers choose how their content is secured**

AWS Customer Agreement

<https://aws.amazon.com/agreement/>

<https://aws.amazon.com/compliance/data-privacy-faq/>

Cloud Security is a Shared Responsibility

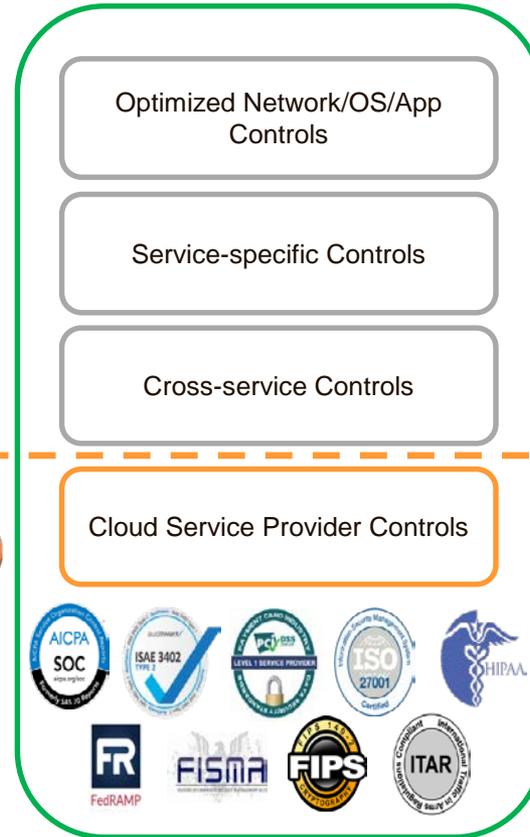
Customers and Partners implement their own Application and Service controls

Multiple customers with:

- FISMA/ICD-503 ATOs
- DIACAP/RMF ATOs

AWS obtains industry certifications & third party attestations:

- SAS-70 Type II / SOC 1 / SOC 2
- ISO 27001/ 2 Certification
- Payment Card Industry (PCI)
- Data Security Standard (DSS)
- DoD PA
- FedRAMP JAB P-ATO & Agency ATOs
- HIPAA
- ITAR



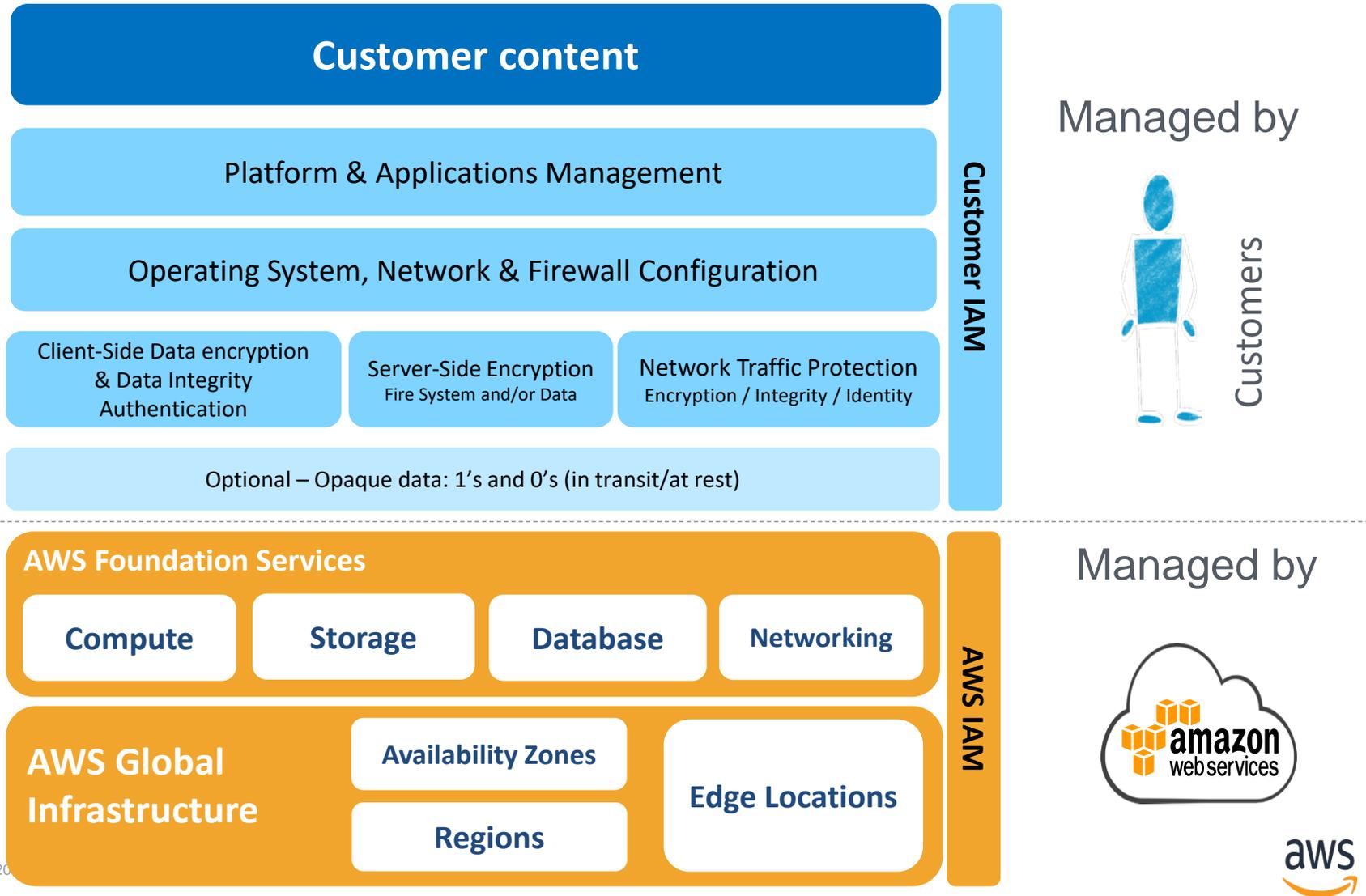
Compliance *in* the Cloud

Compliance *of* the Cloud

<https://aws.amazon.com/compliance>
awscompliance@amazon.com

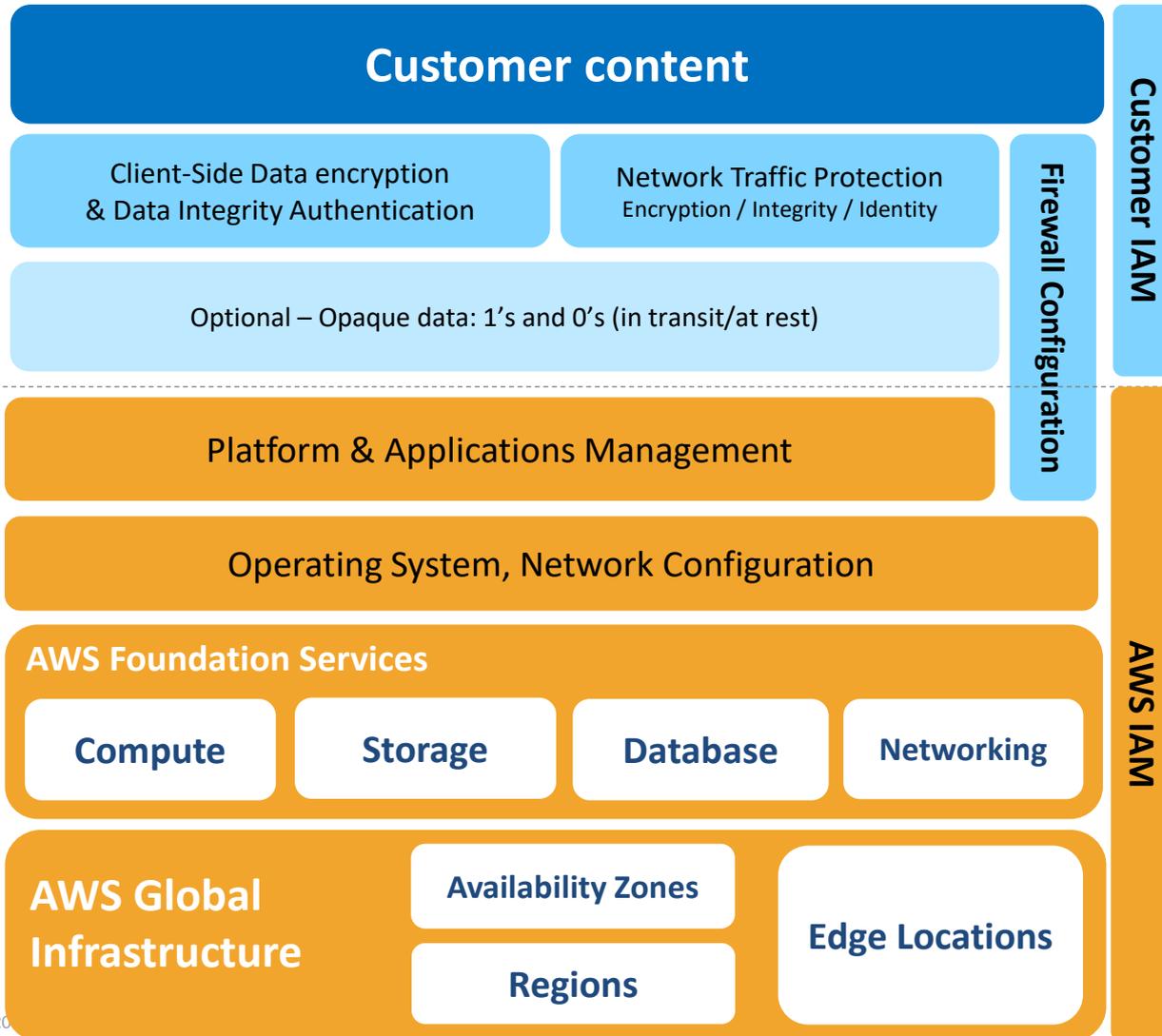
Shared Security Model: Infrastructure Services

Such as Amazon EC2, Amazon EBS, and Amazon VPC



Shared Security Model: Container Services

Such as Amazon RDS and Amazon EMR



Managed by



Customers

Managed by



Shared Security Model: Abstracted Services

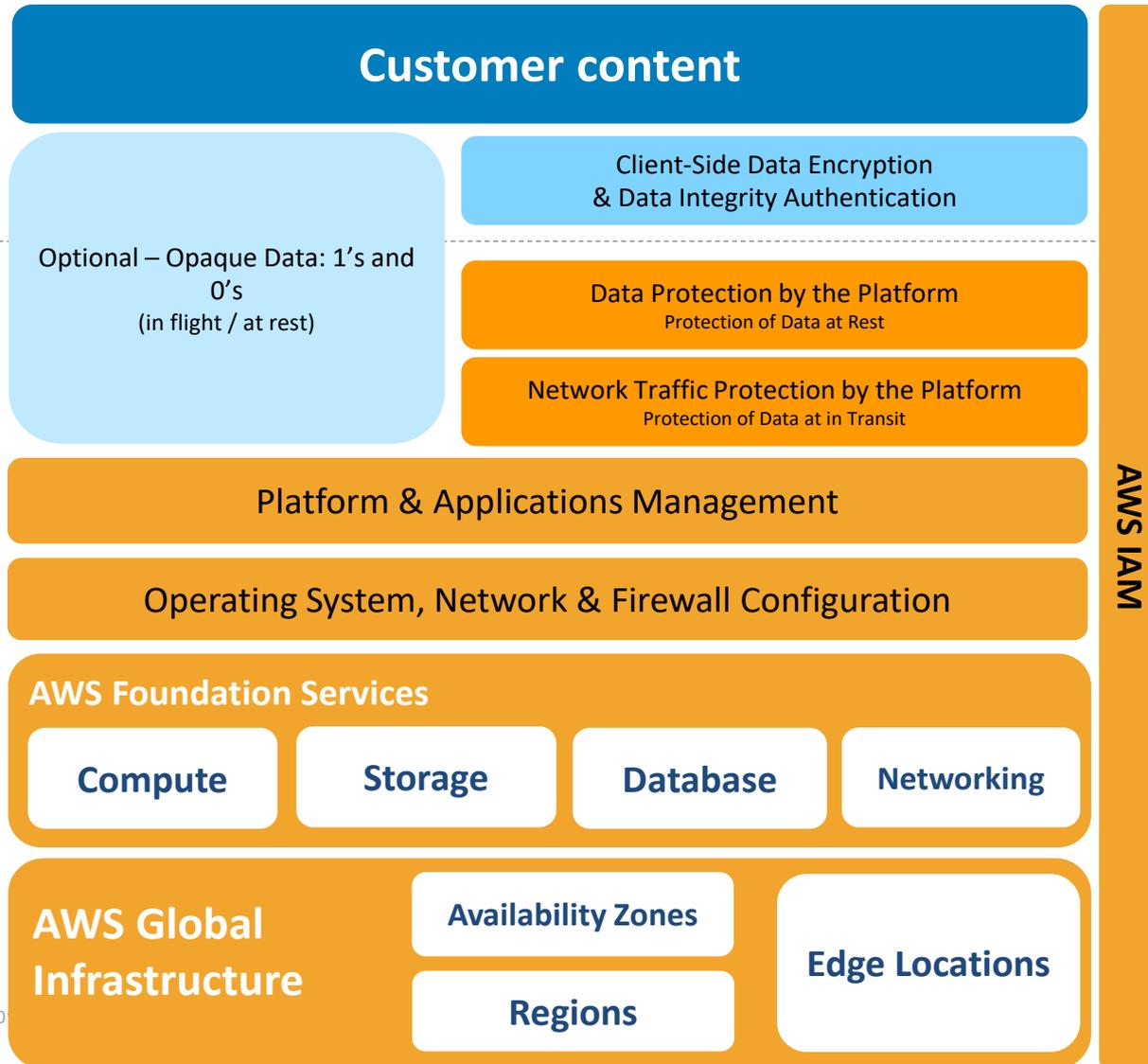
Such as Amazon S3 and Amazon DynamoDB

Managed by



Customers

Managed by



Security Assurance

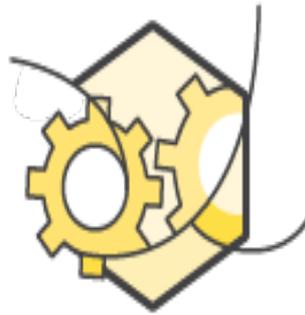
Security is Our No. 1 Priority



Designed for
Security



Constantly
Monitored



Highly
Automated



Highly
Available



Highly
Accredited

<https://aws.amazon.com/security/>

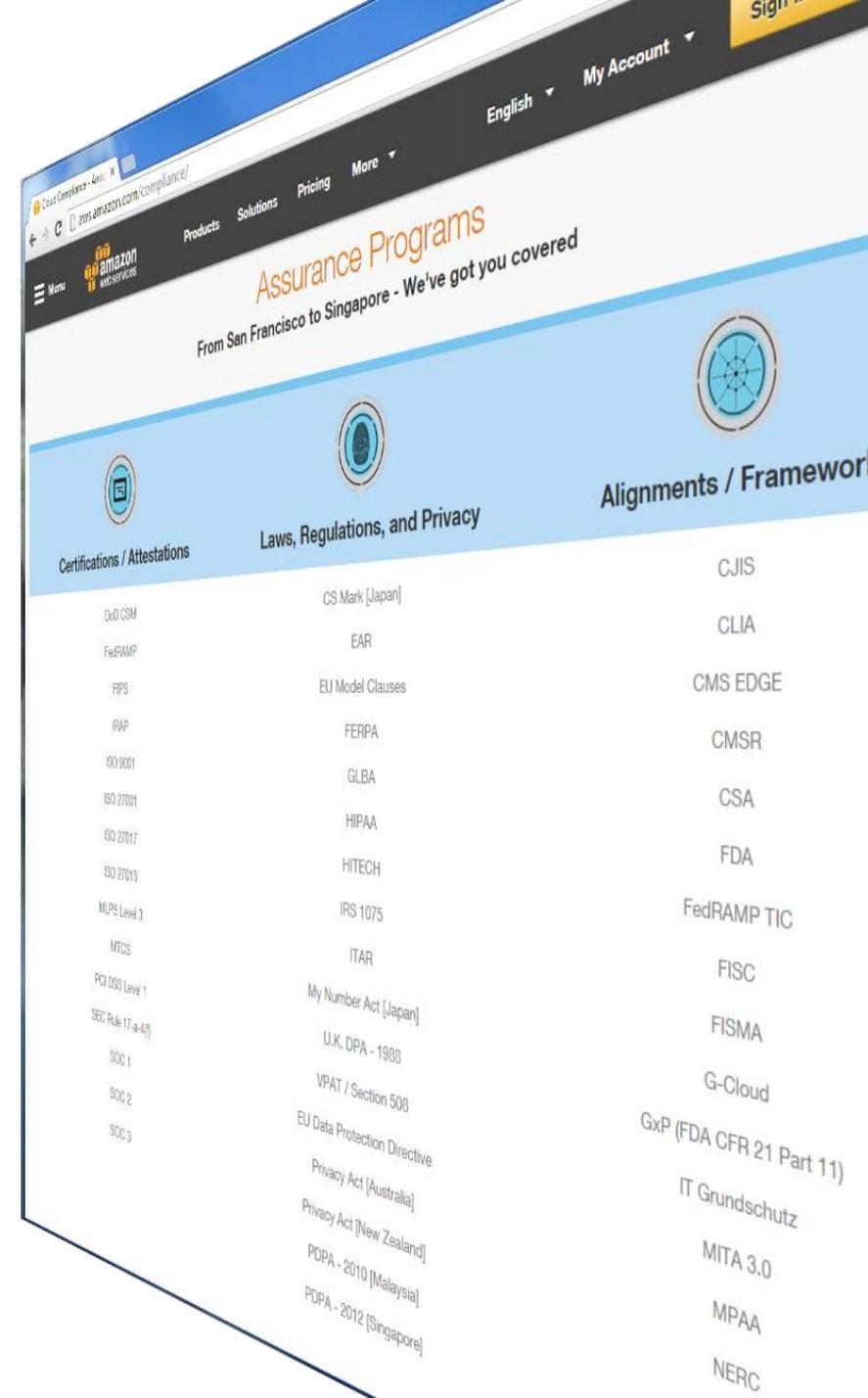
Architected for Government Security Requirements



And many more...

Role of compliance and 3rd party auditors

- Vendor claims alone are not enough
- Testing, auditing and certification by multiple teams of 3rd-party pros provides needed validation
- Far more numerous and rigorous processes than any gov't agency or corporation accepts



NIST Alignment

NIST Aligned Frameworks

NIST

SP 800-53 (rev 4)
SP 800-171



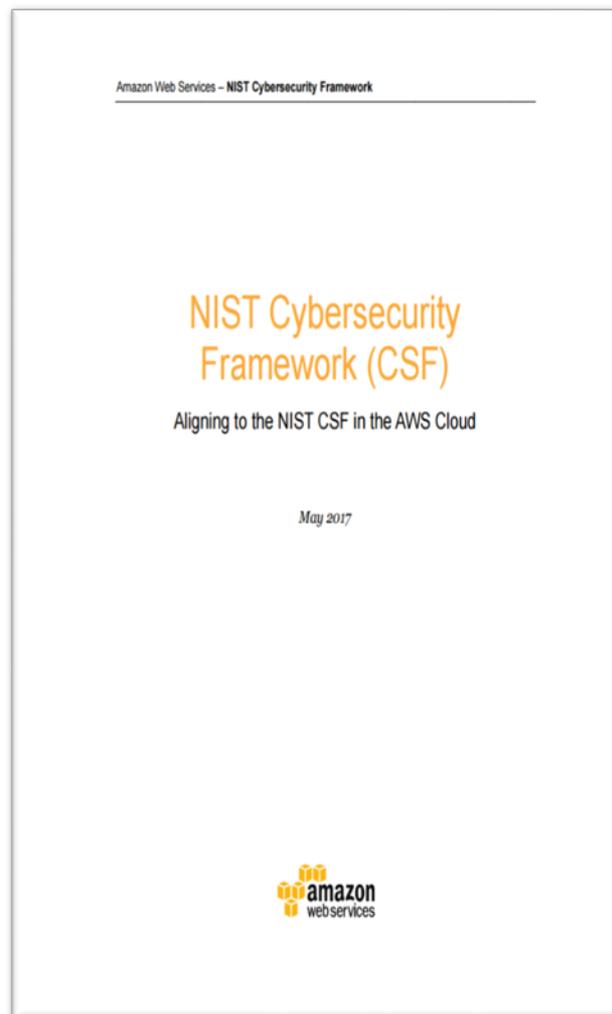
And many more...

<https://aws.amazon.com/compliance/>

Aligning to the NIST CSF in the AWS Cloud

AWS accomplishes two goals in aligning with the CSF:

- **Security *in the cloud***- Assesses the NIST CSF against AWS Cloud offerings that both public and commercial sector customers can use to align to the NIST CSF to improve the security measures that the customer implements and operates. We provide a [detailed breakout of AWS services and associated customer and AWS responsibilities](#) to facilitate alignment with the NIST CSF.
- **Security *of the cloud***- Provides a third-party auditor attestation that AWS services conform to NIST CSF risk-management practices (i.e., security *of the cloud*), assuring customers that their data is protected across AWS.



“But Where Can I Find the Controls AWS meets?”

In the AWS FedRAMP Package!

Available for both AWS Partners & Customer Agencies

AWS FedRAMP package covers:

- AWS infrastructure
- Underlying management of services
- Inherited controls
- Shared controls



Assists in documenting security of workloads built on AWS

This is how we see evidence about Security OF the Cloud!

What You Get in the AWS FedRAMP Security Package



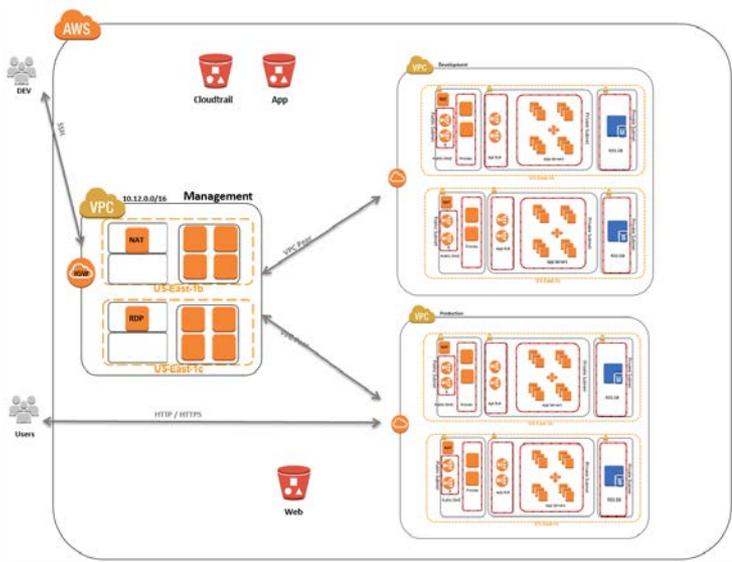
#	FedRAMP Security Package Document	Federal Agency	State, Local, Education	Vendors & Contractors
1	System Security Plan (SSP)	✓	✓	
2	Security Assessment Plan (SAP)	✓	✓	
3	Control Implementation Summary (CIS)	✓	✓	✓
4	FIPS-199 Categorization	✓	✓	✓
5	Control Tailoring Workbook (CTW)	✓	✓	
6	Security Assessment Report (SAR)	✓	✓	
7	Authority to Operate (ATO)	✓	✓	✓
8	User Guide	✓	✓	✓
9	Customer Responsibility Matrix (CRM)	✓	✓	
10	Configuration Management Plan (CM Plan)	✓		
11	Contingency Management Plan (CMP)	✓		
12	E-Authentication Plan	✓		
13	PTA/PIA	✓		
14	Rules of Behavior	✓		
15	Incident Response Plan (IRP)	✓		
16	Policies	✓		
17	Security Controls Summary			✓
18	SSP Template			✓

AWS Enterprise Accelerator Quick Start Web Site

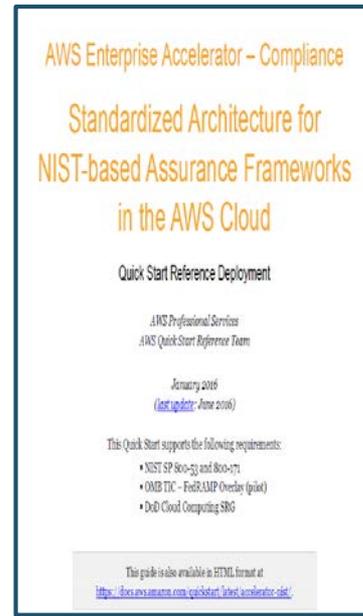
The screenshot shows a web browser window with the URL <https://aws.amazon.com/quickstart/#compliance>. The page features a dark navigation bar with the Amazon Web Services logo, "AWS re:Invent", and a language selector set to "English". The main heading is "Compliance (AWS Enterprise Accelerators)". Below this, three columns of content are displayed:

- PCI DSS:** Includes a PCI logo, the text "Standardized AWS architecture that supports PCI DSS compliance", and a "Learn more »" link.
- NIST:** Includes the NIST logo, the text "AWS architecture that supports NIST, DoD, FedRAMP standards", a "Learn more »" link (highlighted with a dashed blue box), and "View guide | Deploy" links.
- NIST High-Impact:** Includes the NIST logo, the text "AWS architecture for NIST high-impact controls, featuring Trend Micro", and "Learn more »" and "View guide | Deploy" links.

Enterprise Accelerator Quick Start Packages: *What's in the Box?*



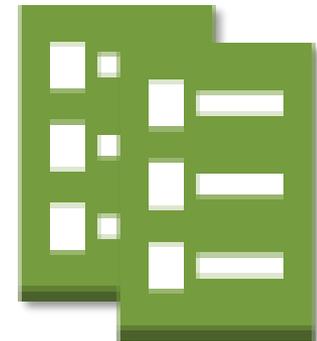
Architecture Diagram



Deployment Guide

NIST SP 800-53 rev4 Controls					OISS Inclusive 1255 Control Selection				FedRAMP Control Selection		DoD Cloud SRG Control Selection		
Family	Control (Id)	Control (Sub-part)	Title	Description	Priority	Control Identifier	Confidentiality	Integrity	Availability	FedRAMP	FedRAMP	DoD Cloud SRG	Level of
						System	System	System	System				
AUDIT AND ACCOUNTABILITY	AU-12	AL-2	AUDIT GENERATION	The information system:	F1	X	X	X	X	X	X	X	X
AUDIT AND ACCOUNTABILITY	AU-13	AL-2a	AUDIT GENERATION	Provide audit record generation capability for the auditable events defined in AU-2 as a program, organization-defined information system component.			X	X	X	X	X	X	X
AUDIT AND ACCOUNTABILITY	AU-12	AL-2b	AUDIT GENERATION	When the system organization-defined personnel or role is able to audit, the auditable events are to be audited by specific components of the information system, and			X	X	X	X	X	X	X

Security Controls Matrix (SCM)



AWS CloudFormation Templates





AWS GovCloud – When it makes sense

GovCloud (US) - Isolated AWS Region



Intended for customers with strict regulatory and compliance requirements and sensitive data or workloads

August 2011

Available to qualified customers



NIST
SP 800-53 (rev 4)
and
SP 800-171



Compliance

Safeguard sensitive data/systems

Addresses multiple US Government regulations and security requirements

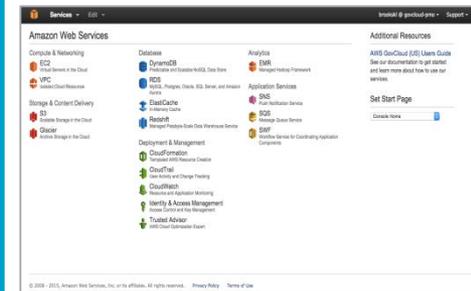
GovCloud (US) distinguishing features



Data, network, and machine isolation from other regions (also separate AZs, service endpoints)

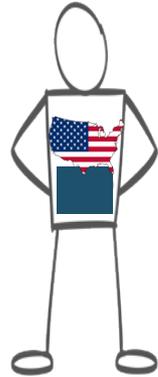


Separate IAM (unique credentials)

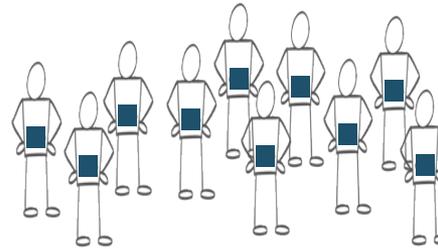


Dedicated GovCloud Management Console

GovCloud (US) – Region Features



Managed by US
Citizens on US
soil



“Community Cloud”
with vetted account
holders

GovCloud (US) – Access Requirements



Account holder must be a **US Person**
(US Citizen or a Green Card holder)



US entity incorporated to do business in
the United States and is **based on US soil**



Can handle **export control data**

Learn more: <https://aws.amazon.com/govcloud-us/getting-started/>

AWS GovCloud (US) is compliance in the Cloud



International Traffic and Arms Regulation



FedRAMP
Moderate and High



DOD Cloud Security Req's
Guide IL 2,4 and 5



Criminal Justice Information
Service Security Policy



IRS – 1075
(Section 6103 (p))



Federal Information
Processing Standard Pub



SP 800-53 (rev 4)
SP 800-171



Defense Federal
Acquisition Regulation
Supplement

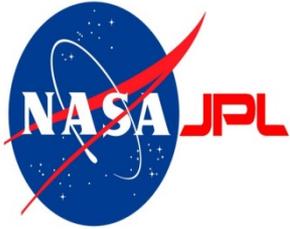
GovCloud Similarities to other AWS Regions

Same architecture, same services

- Same technical/security architecture as other regions
- Same services, although typically launched after US East launch
- AWS > Global Infrastructure > [Region Table](https://aws.amazon.com/about-aws/global-infrastructure/regional-product-services/) for parity in US regions
(<https://aws.amazon.com/about-aws/global-infrastructure/regional-product-services/>)

Just another AWS region in terms of billing

- Unique 12 digit “account number” (for authentication purposes)
- Linked with a standard AWS account (1-to-1 relationship)



You are not alone, we are here to help you!

Main resources

AWS Cloud Security <https://aws.amazon.com/security/>

AWS Cloud Compliance <https://aws.amazon.com/compliance/>

AWS Whitepapers <https://aws.amazon.com/whitepapers/>

AWS Quick Starts <https://aws.amazon.com/quickstart/>

Cloud Security Resources <https://aws.amazon.com/security/security-resources/>

AWS Security Blog <https://aws.amazon.com/blogs/security/>

Security and Compliance
Workshops

CISO/CIO RoundTable
Sessions

Security Blog Reviews

PubSec Compliance
Packages

Training and certification

AWS Training and Certification <https://aws.amazon.com/training/>

AWS Security Fundamentals <https://aws.amazon.com/training/course-descriptions/security-fundamentals/>

Security Operations on AWS training

<https://aws.amazon.com/training/course-descriptions/security-operations/>

Qwiklabs: Security on AWS <https://amazon.qwiklabs.com/quests/22>

AWS Auditor Learning Path

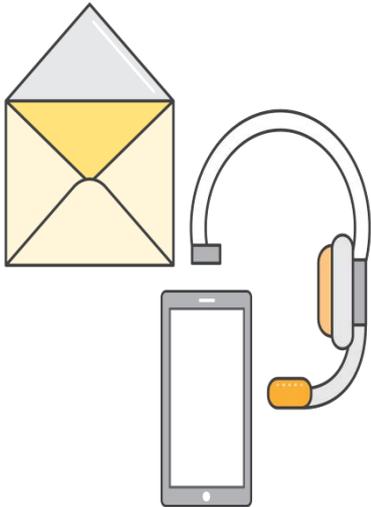
<https://aws.amazon.com/compliance/auditor-learning-path/>

AWS Support



Account Team

- Your Account Manager is your advocate
- Solutions Architects have a wealth of expertise
- Well-Architected Framework



Recommended tiers of support

- **Business** – Phone/chat/email support, 1 hour response time
- **Enterprise** – 15 min response time, dedicated Technical Account Manager, proactive notification and driving operational efficiency

Professional Services



AWS Professional Services

- Enterprise Security Architecture
- Policy & Controls Mapping
- SOC Design

AWS Partner Network

- Over 600 certified AWS Consulting Partners worldwide

Q & A

Thank you!

Tim Anderson
tdander@amazon.com

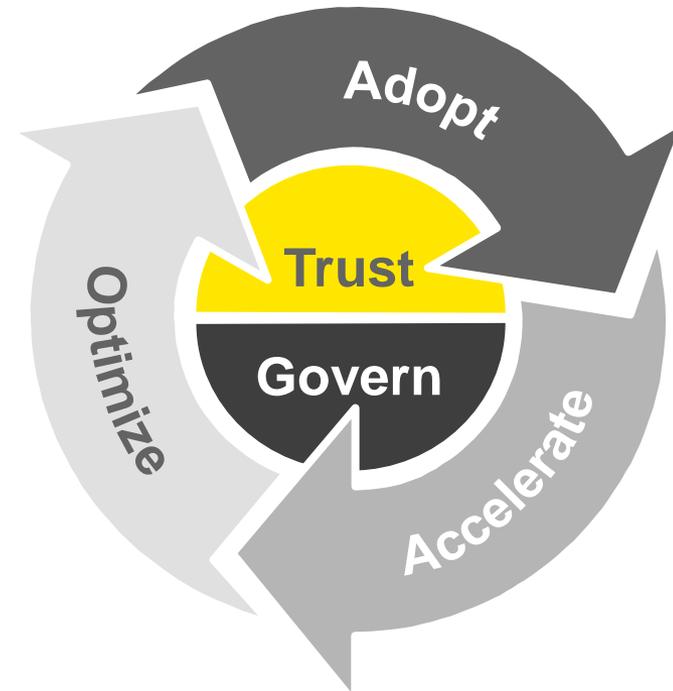
Building trust in the cloud

Creating confidence in your cloud ecosystem

ISOAG Meeting – November 1, 2017

Contents

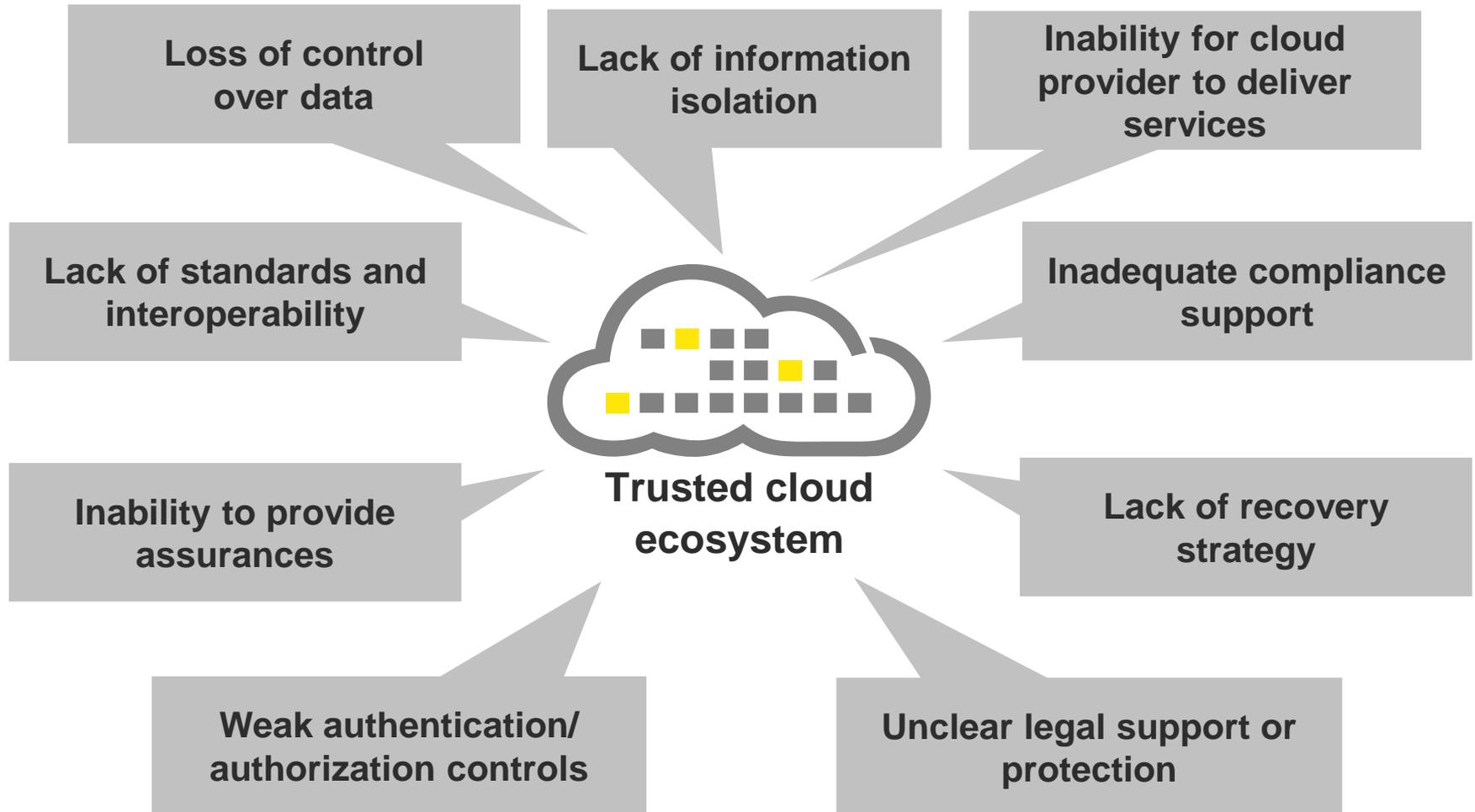
The EY Cloud Framework



- 1** **Why:** the need for a trusted cloud ecosystem
- 2** **How:** how to build “trust” in the cloud

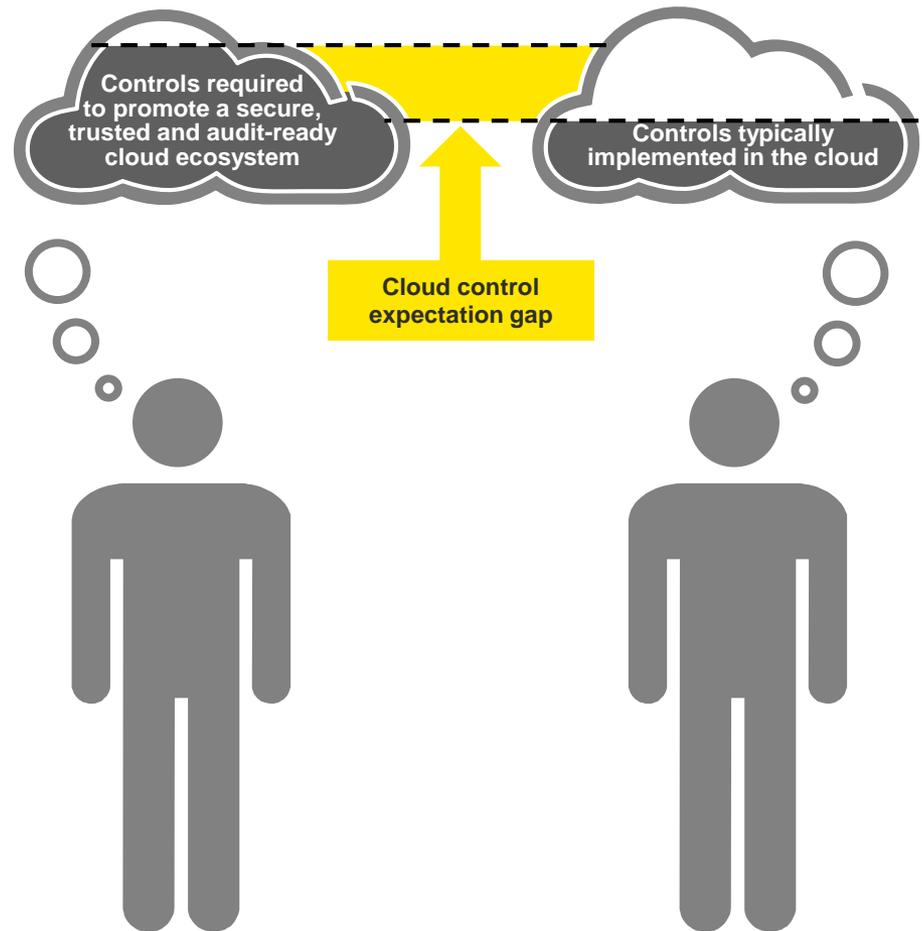
Why: the need for a trusted cloud ecosystem

There are many barriers and risks to achieving a trusted cloud ecosystem

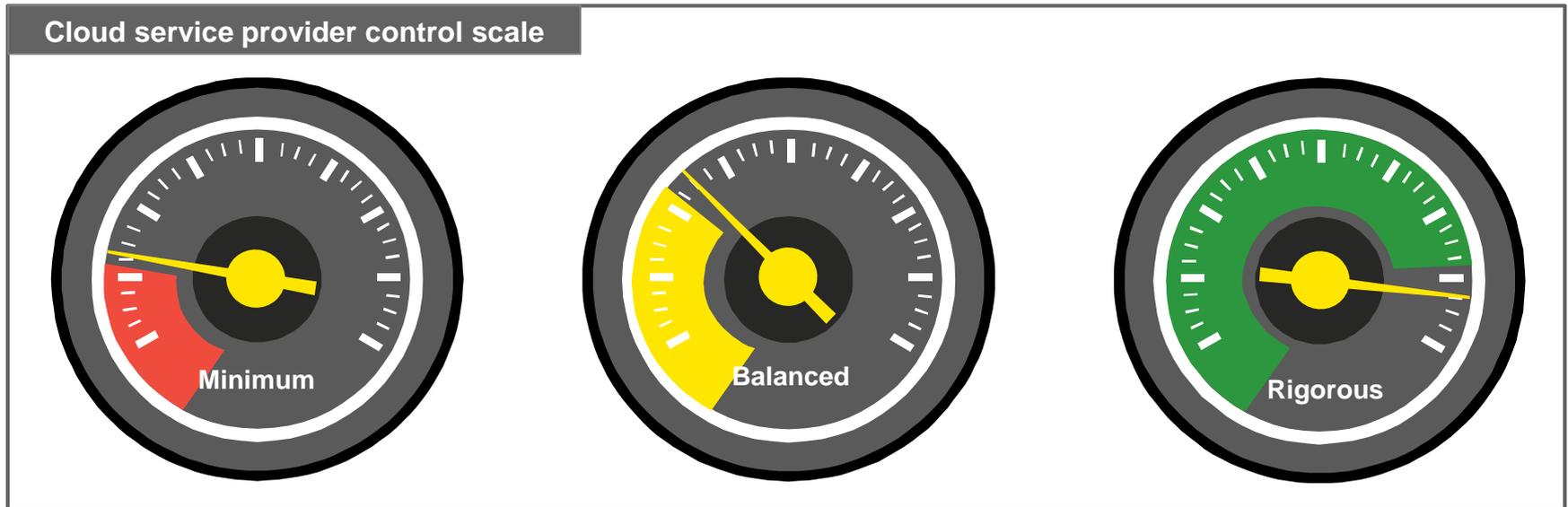


Fighting to close the “cloud control expectation gap”

- ▶ Companies have made significant moves to cloud-based solutions.
- ▶ Adopters of cloud solutions expect cloud service providers to deliver all the necessary controls to address the confidentiality, integrity and availability of their data.
- ▶ However, we have seen a much slower adoption of the controls necessary to promote a secure, trusted and audit-ready environment.
- ▶ As a result, the gap between what cloud controls we *think we have in place* and the controls we *typically implement in the cloud* is widening.
- ▶ This exposes adopters of cloud technologies to unmitigated risk.

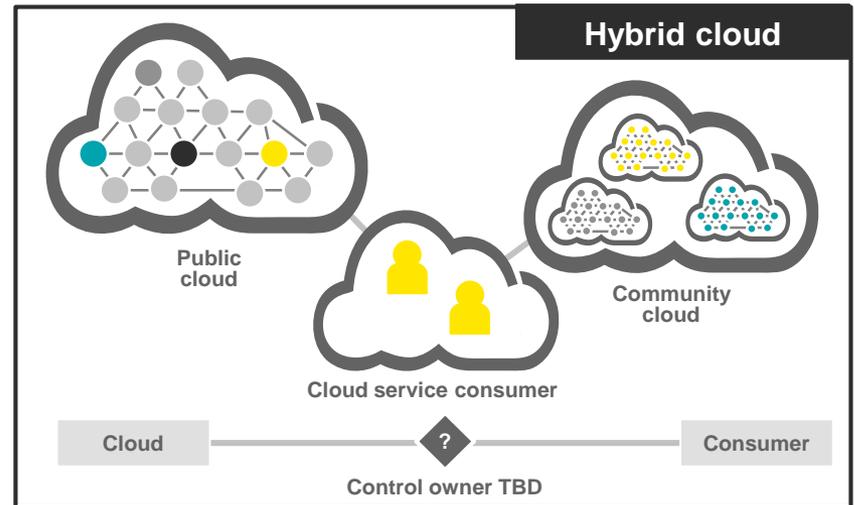
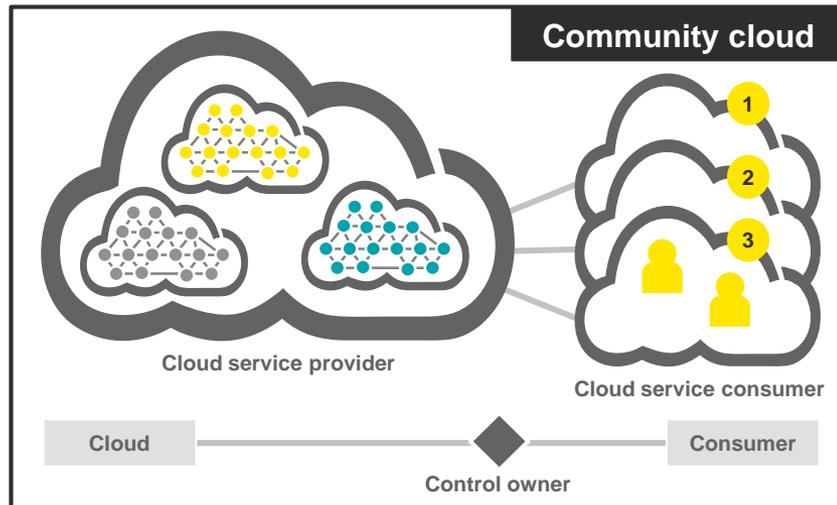
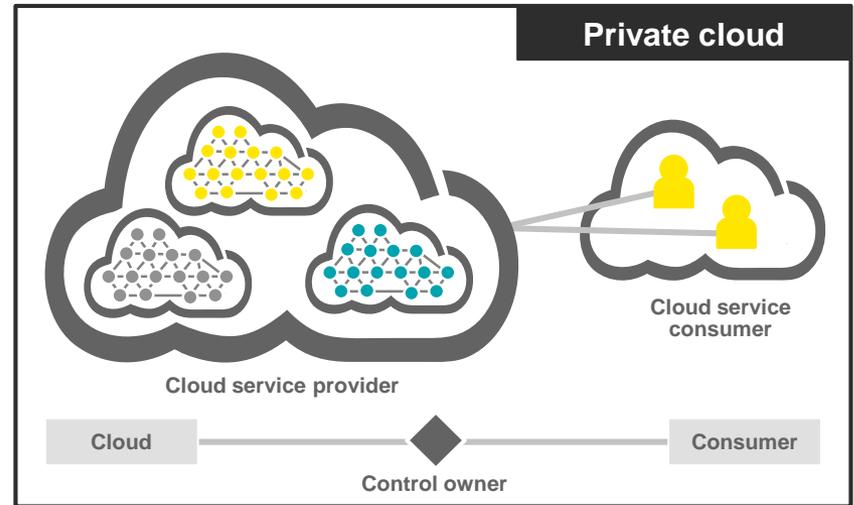
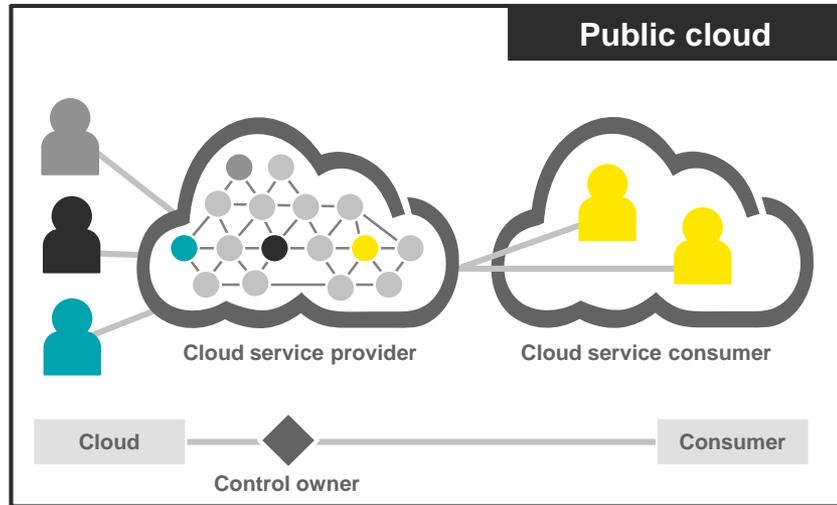


The type of cloud you choose: it shifts the controls you need

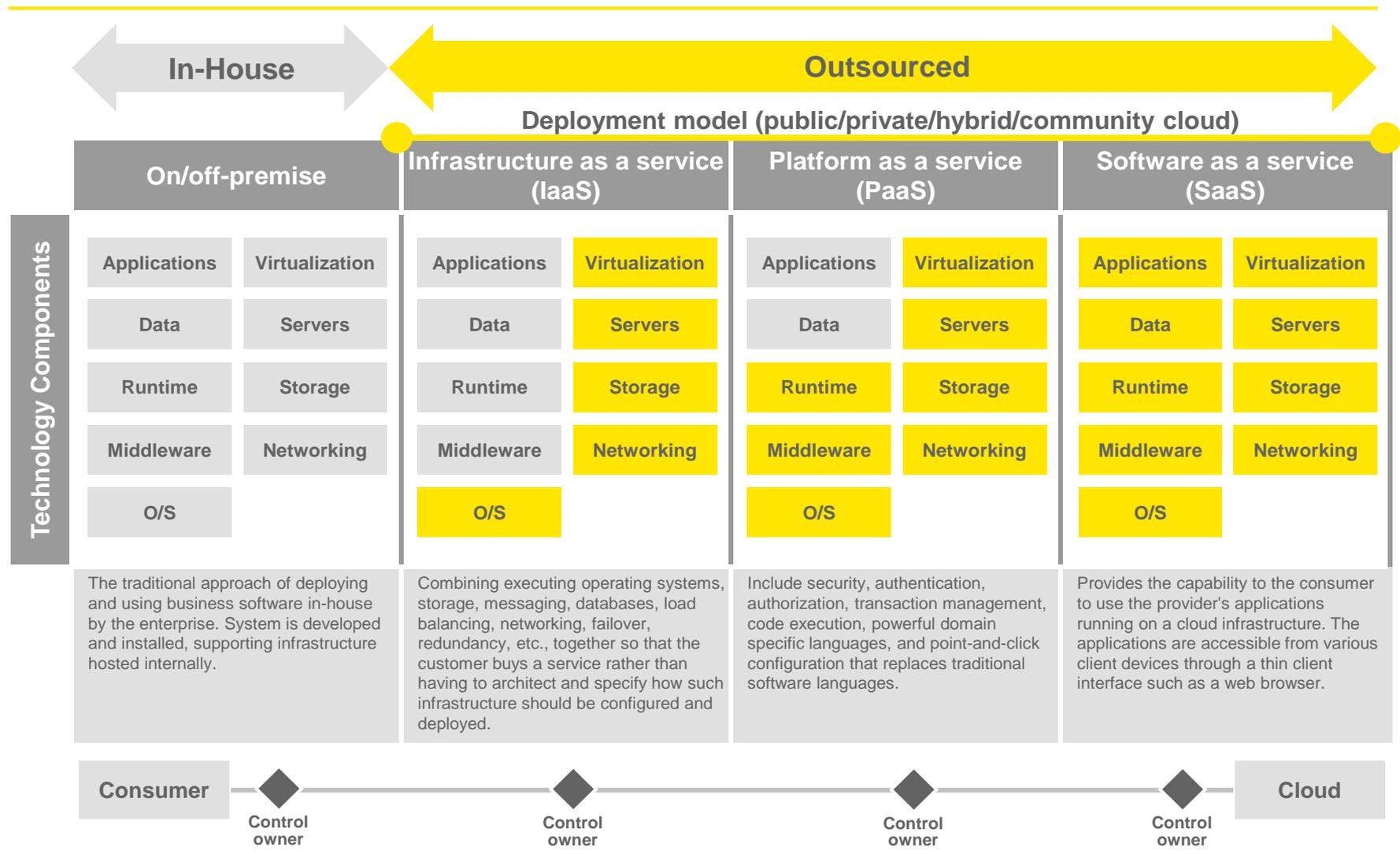


- ▶ Not all cloud service providers offer the same level of controls and subsequent trust levels.
- ▶ What is best for the needs of a cloud consumer, depends on the cyber security standards outlined by the company and the relative level of security necessary for what is being placed on the cloud
- ▶ Sometimes (as in the case with “public” data) the minimum amount of controls – as typically offered with a public cloud environment – may address your needs
- ▶ More rigorous control environments are required for mission-critical applications, infrastructure and platforms.

The type of cloud you choose matters: it shifts the controls you need



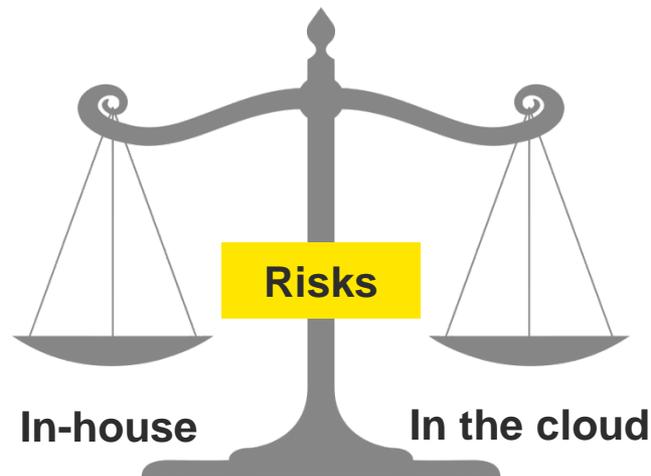
The types of services you implement change the controls you need



How: how to build trust in the cloud

Cloud consumers must evaluate the maturity of their processes and controls relative to the cloud service provider (CSP)

Given the risks of venturing in the cloud, should I make the move?

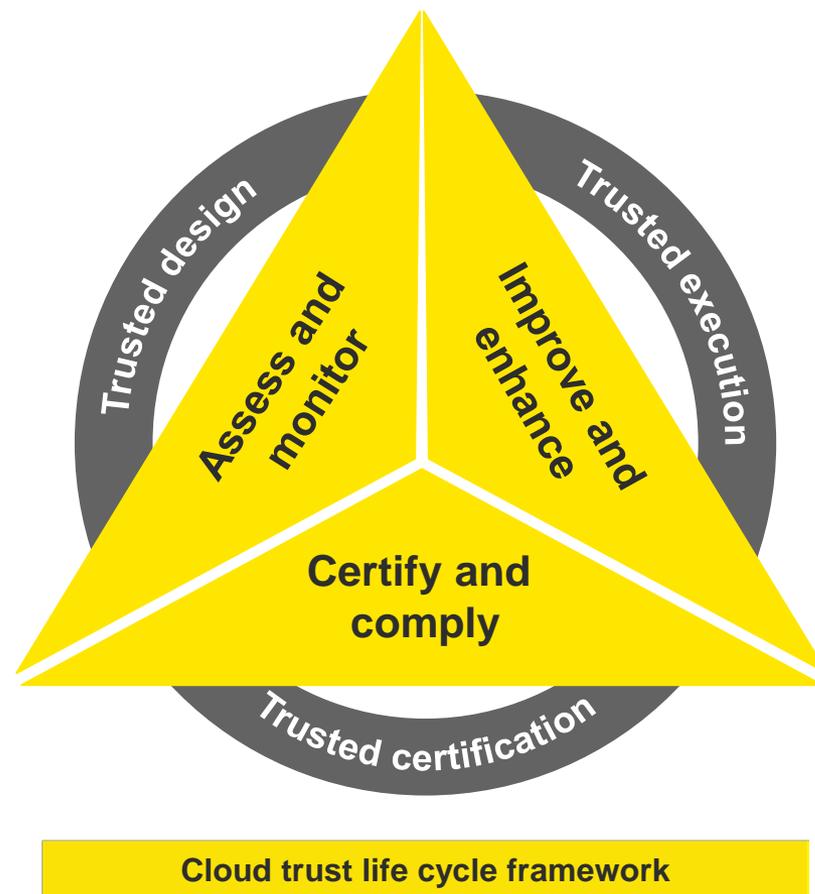


Yes, but ...

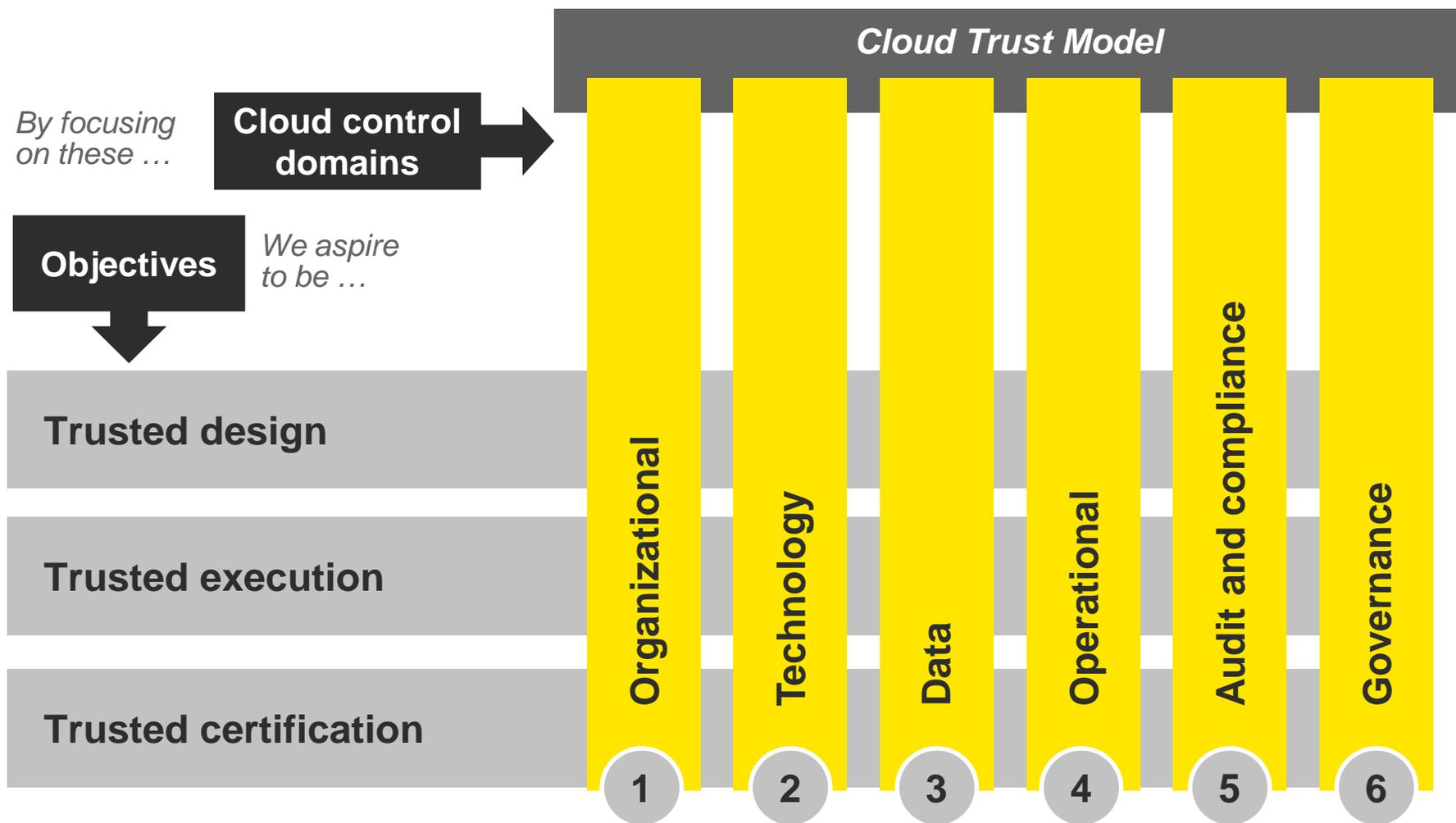
- ▶ Before moving to the cloud, we should weigh the risks of operating a technology environment ourselves versus governing a cloud vendor.
- ▶ If our requirements are so specific and narrow and our internal capabilities are already very mature, a cloud vendor may not be a viable or prudent solution.
- ▶ However, cloud vendors are in the business of IT and in many cases are more mature than operating in-house.
- ▶ Either way, the cloud “make or buy” decision should contemplate six key cloud control domains that define a good Cloud Trust Model.

Key questions to address before moving to the cloud

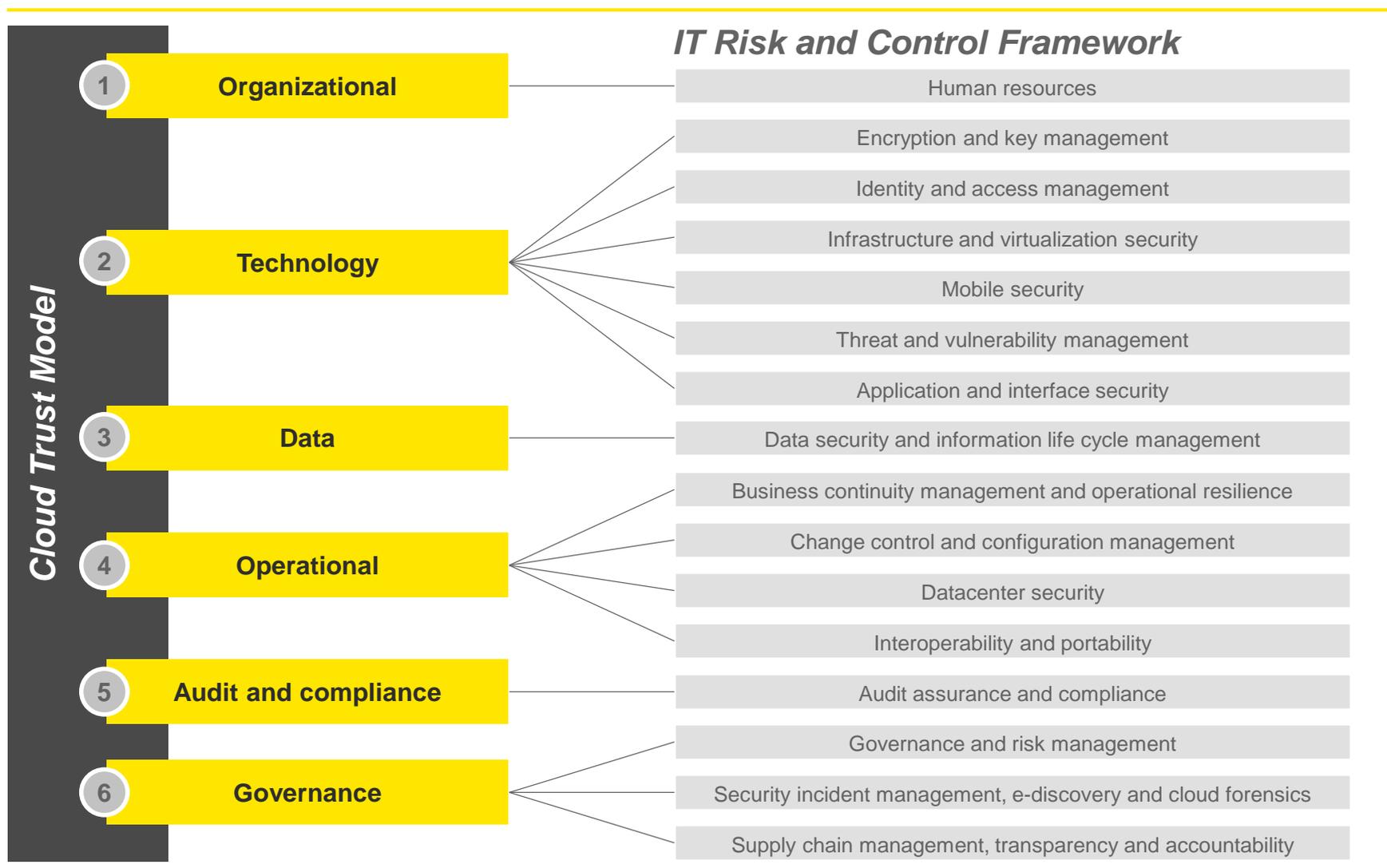
- ▶ How does my risk profile change by moving to the cloud?
- ▶ How do I meet my **regulatory mandates** after moving to the cloud?
- ▶ What factors can help me evaluate a **trusted provider**?
- ▶ What do I need to do to confirm my **data is safe**?
- ▶ How do I confirm my providers' security standards and policies are sufficient to **build trust**?
- ▶ What terms and condition should I include in the contract with a cloud provider?



A good Cloud Trust Model is composed of six cloud control domains to achieve a trusted cloud ecosystem



A good Cloud Trust Model aligns to common IT Risk and Control Frameworks



At a minimum, Cloud Providers should provide a third-party assurance report

For cloud-based vendor's security purposes, we need:

	SOC 1®	SOC 2®	SOC 3®
Topic	Processes and controls at outsourced service provider (OSP) relevant to user entities' internal control over financial reporting	Processes and controls at outsourced service provider (OSP) relevant to security, availability, processing integrity, confidentiality, and/or privacy	Processes and controls at outsourced service provider (OSP) relevant to security, availability, processing integrity, confidentiality, and/or privacy
Report includes	Full description of OSP's processes and controls plus:		Brief description of the system and boundaries plus:
▶ Type 1	Assessment of design of controls at a point in time		Assessment of whether the OSP maintained effective controls over its system
▶ Type 2	Assessment of design of controls and their operating effectiveness for a period of time		

SOC 2[®] is based on the “Trust Services Categories” consisting of

Security

The system is protected against unauthorized access, use, or modification.

Availability

The system is available for operation and use to meet the entity’s commitments and

Processing Integrity

System processing is complete, valid, accurate, timely and authorized to meet

Confidentiality

Information designated as confidential is

Privacy

Personal information is collected, used,

Trust Services criteria are not a checklist – the service organization presents its controls that are in place to meet the service commitments and system requirements based on the criteria

Common pitfalls in using a SOC[®] report

- ▶ Report is not the correct report
 - ▶ Location is not correct
 - ▶ Services are different than the services relied on
 - ▶ Application we wish to rely on is not covered in the report
- ▶ Report is a Type I (as of a point-in-time)
- ▶ Multiple processes are utilized at the service provider that are covered in separate reports
- ▶ Report period is not sufficient
- ▶ Report is qualified or major exceptions exist and are not fully addressed or considered
- ▶ Inadequate documentation to support that relevant Complementary User Entity Controls (CUECs) were tested and operating effectively
- ▶ Insufficient documentation to support evaluation of IT-related CUECs (e.g. user access)

Leverage a trusted design, trusted execution and trusted certification to close “cloud control expectation gap”

Trusted design

- ▶ Put the right controls in place to safeguard and protect the underlying computing and information assets
- ▶ Design controls to address the key areas of risk and that are strong enough to mitigate the threats to the environment
- ▶ Define control ownership and responsibilities between the cloud provider and customer

Trusted execution

- ▶ Establish monitoring and governance to validate that controls are working as intended
- ▶ Re-evaluate and strengthen controls when new risk indicators rise

Trusted certification

- ▶ Independently tested and verified cloud provider environment showing that the controls are in place, functioning as designed, operating effectively and have been attested to by a certifying body
- ▶ Review and understand the scope and relevance of the certification and adjust internal controls as required to protect the environment



Trusted cloud ecosystem

Questions?

EY | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

© 2017 Ernst & Young LLP.
All Rights Reserved.

1710-2469771
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.

ey.com

RANSOMWARE



Is it widespread?

NEARLY

50% OF HEALTHCARE ORGANIZATIONS

experienced a security incident involving patient data within the last year.



Healthcare Organizations face new cyber threats
EVERYDAY

Perspective

IN 2015
88.4 MILLION
individual health records were breached.

HEALTHCARE ORGANIZATIONS **AVERAGE**
11.4 CYBER ATTACKS
PER YEAR.



2x MORE
THAN IN **2010**

Why target Healthcare?



- ▶ Patient records have never been more coveted.
- ▶ As their black market value continues to rise, so do attempts to illegally obtain them.
- ▶ Cyber criminals have realized healthcare has fallen behind other industries in terms of data protection

No Longer a Healthcare Problem

6 in 10 malware payloads
were ransomware in
Q1 2017

Ransomware Grows in Popularity

According to researchers from Malwarebytes, roughly 60% of malware payloads were ransomware

15% or more of businesses in the top 10 industry sectors have been attacked

	Industry Sector	% attacked with ransomware
1	Education	23
2	IT / Telecom	22
3	Entertainment / Media	21
4	Financial Services	21
5	Construction	19
6	Government / Public Sector	18
7	Manufacturing	18
8	Transport	17
9	Healthcare	16
10	Retail / Wholesale	16

What is Ransomware

- ▶ A type of malicious software criminals use to deny access to systems or data



- ▶ The hacker holds the system or data hostage until the ransom is paid

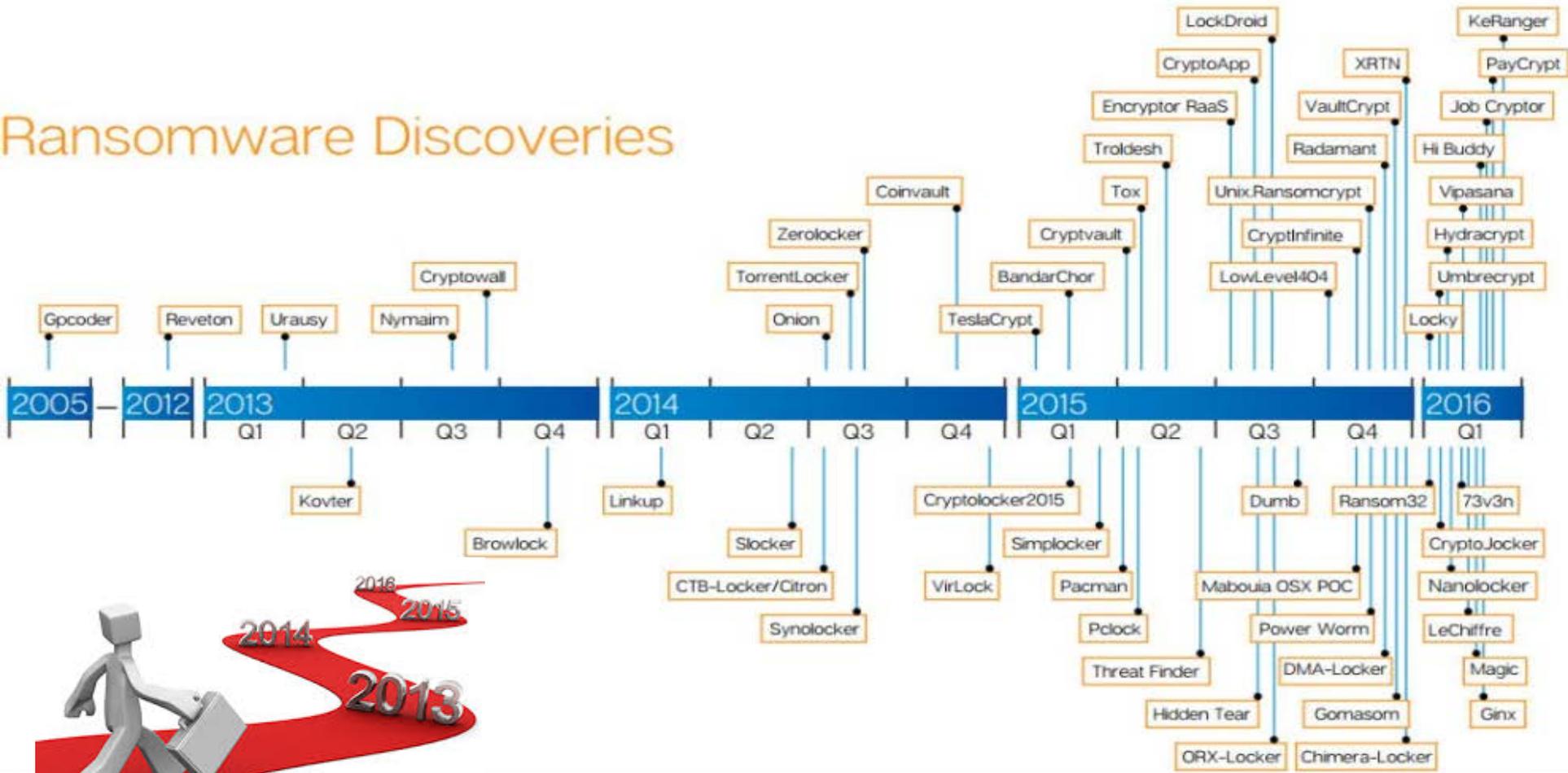
Ransomware is Commonly Spread

- ▶ Ransomware Sends Phishing Volumes up Almost **800%**
- ▶ According to a report from PhishMe, **93%** of phishing emails contain encrypted Ransomware.



Ransomware Timeline

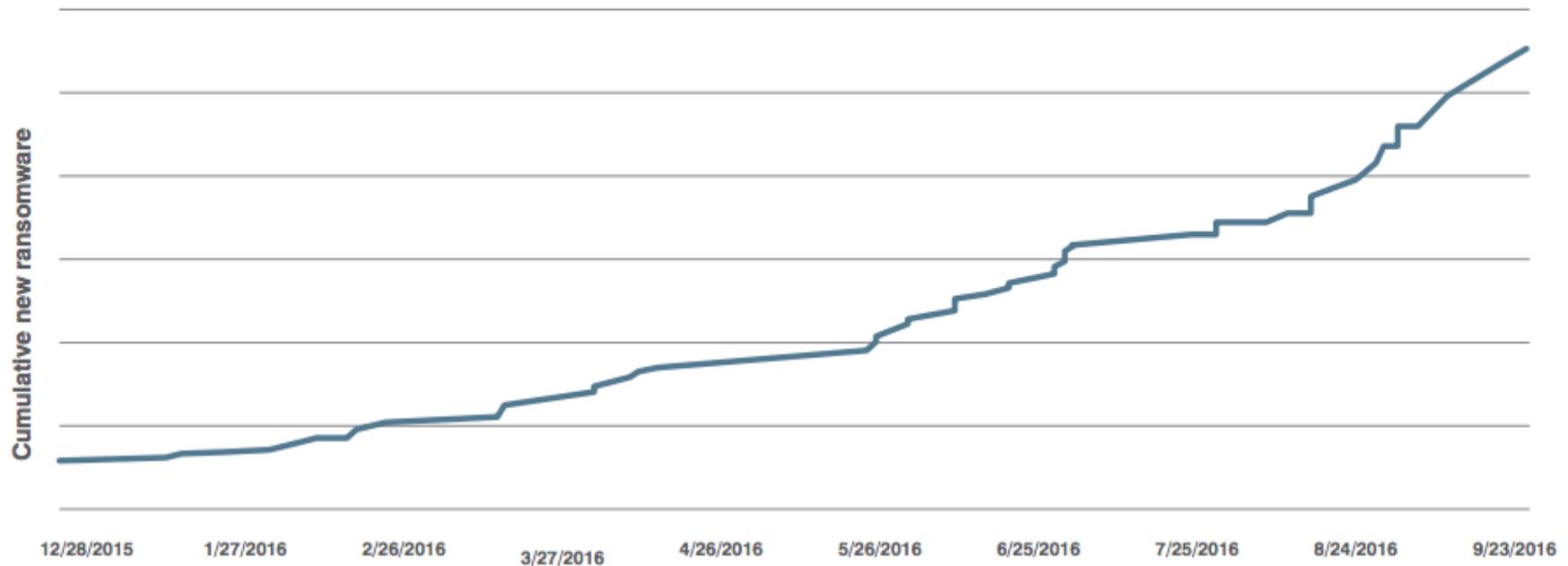
Ransomware Discoveries



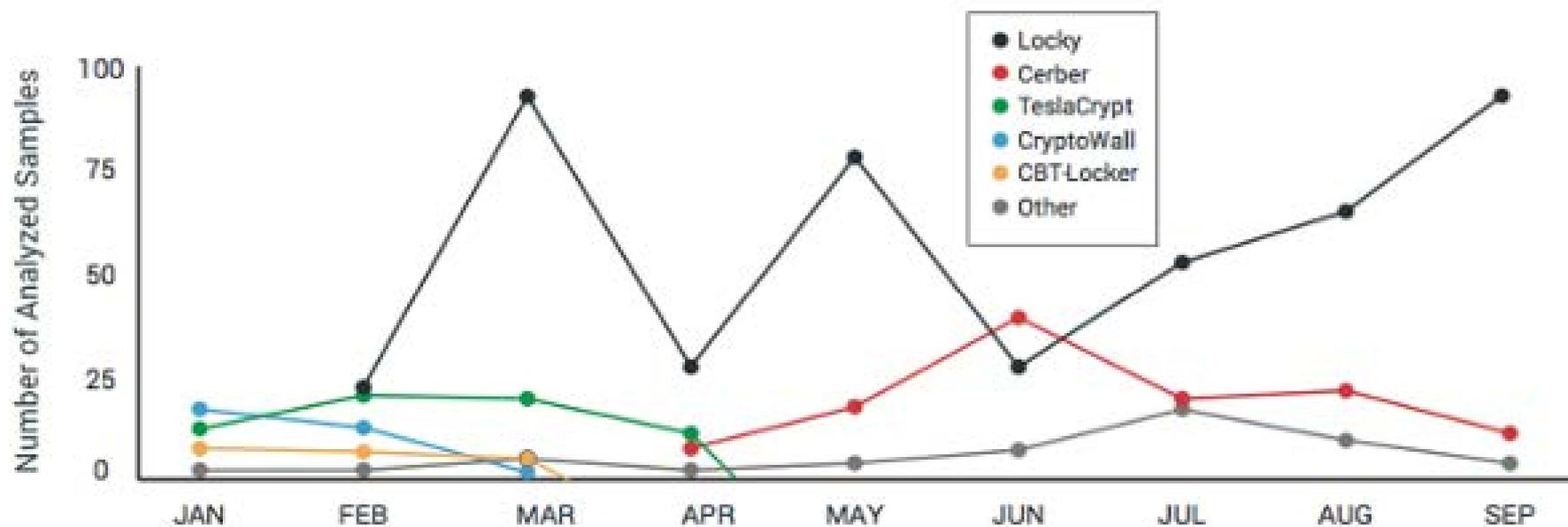
Ransomware Growth



Growth in Ransomware Variants Since December 2015



2016: The year of Locky



How Locky infects victims

Delivered via:

- Phishing email campaigns that trick users into opening malicious Microsoft Office documents and enabling macros.
- Trick users into opening JavaScript attachments.
- Malvertising - Malware embedded in Advertising (typically banner ads).



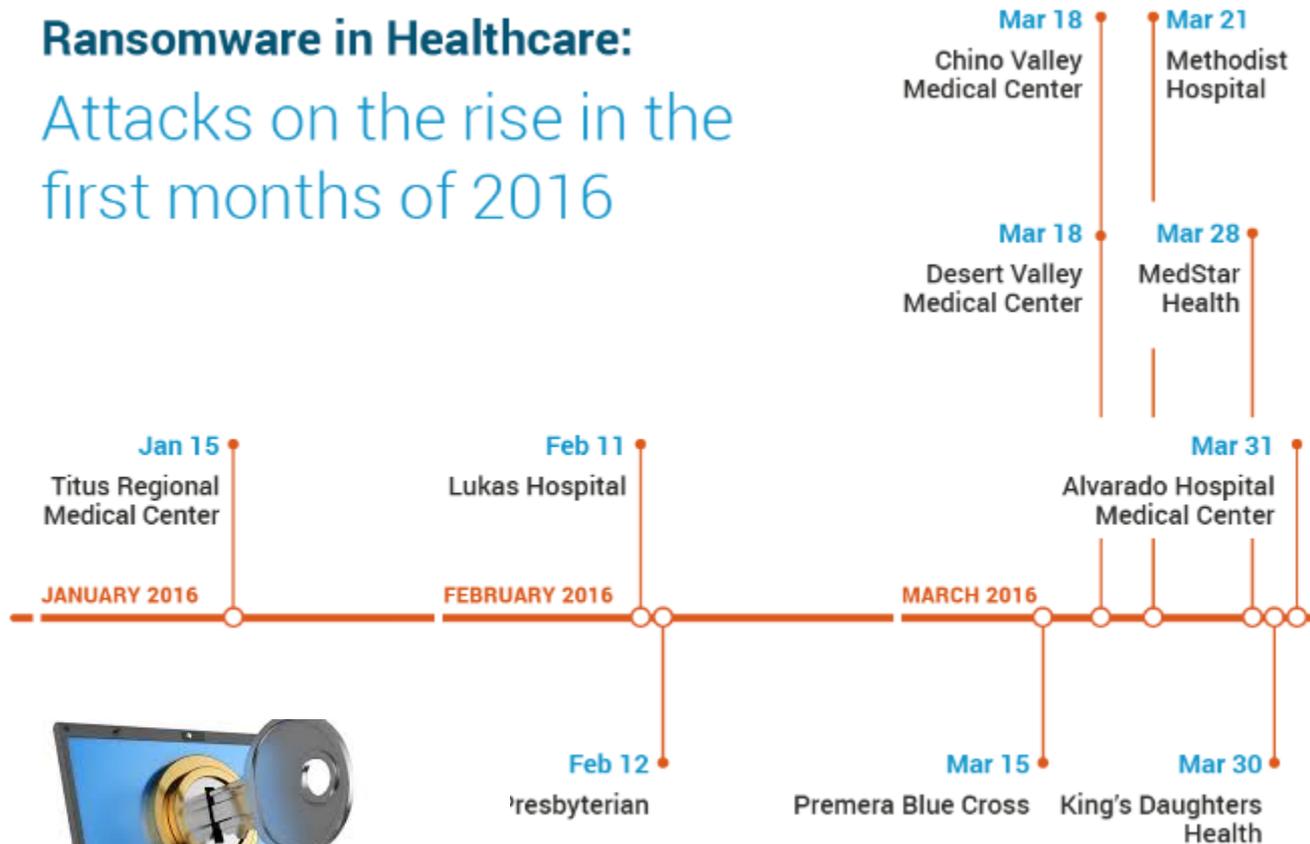
Date added (UTC)	Threat	Malware	Host (?)	Domain Registrar (?)	IP address (ASN, Country)
2017-10-31 09:53	Distribution Site	Locky	● hotelxaguete.com	PDR Ltd. d/b/a PublicDomainRegis[...]	104.254.99.64 (🇺🇸 United States)
2017-10-31 09:53	Distribution Site	Locky	● rosiautosuli.hu		87.229.45.38 (🇮🇪 Hungary)
2017-10-31 09:53	Distribution Site	Locky	● edificioexpo.com	Arsys Internet, S.L. d/b/a NICLI[...]	94.23.221.122 (🇫🇷 France)
2017-10-31 09:53	Distribution Site	Locky	● cqaqualite.com	1&1 Internet SE	216.250.115.36 (🇺🇸 United States)
2017-10-31 09:52	Distribution Site	Locky	● first-paris-properties.com	OVH	151.80.157.121 (🇫🇷 France)
2017-10-31 09:43	Botnet C&C	Locky	● aechjic.pw	Namecheap	208.100.26.251 (🇺🇸 United States)
2017-10-31 09:43	Botnet C&C	Locky	● 95.85.19.195		95.85.19.195 (🇳🇱 Netherlands)
2017-10-30 15:44	Distribution Site	Locky	● pciolog.ru	RD-RU	89.253.235.118 (🇷🇺 Russian Federation)
2017-10-30 15:39	Distribution Site	Locky	● hobbystube.net	CPS-Datensysteme GmbH	83.220.128.111 (🇩🇪 Germany)
2017-10-30 15:39	Distribution Site	Locky	● fuettern24.de		176.28.9.111 (🇩🇪 Germany)
2017-10-30 15:39	Distribution Site	Locky	● dvprojekt.hr		213.202.100.90 (🇦🇪 Croatia)

and Locky continues to infect

More recently, Locky executables have been delivered as Windows Script Files and DLLs.

Impact of Locky

Ransomware in Healthcare:
Attacks on the rise in the first months of 2016

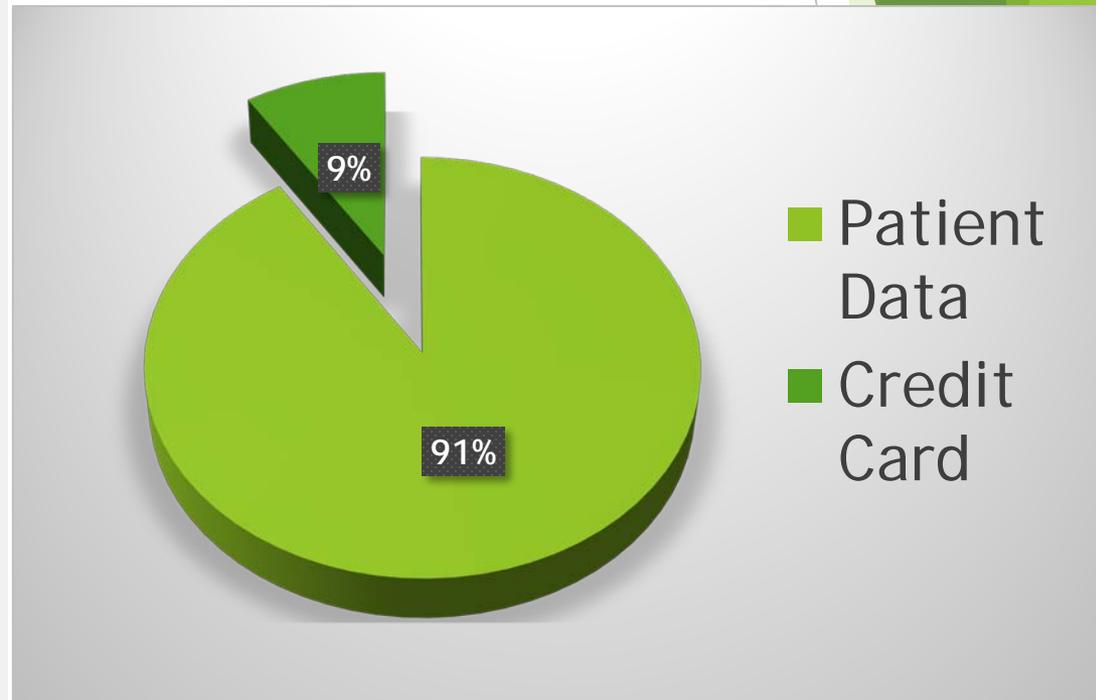


Costs?



**STOLEN PATIENT INFORMATION
IS VERY VALUABLE**

HACKERS SELL IT FOR
50X MORE THAN
FINANCIAL DATA ON
THE BLACK MARKET



RANSOMWARE IS BUSINESS



- ▶ An estimated \$325 MILLION in ransom payments has been generated by just one type of ransomware alone, CryptoWall 3.0
- ▶ The ransom amounts associated with Ransomware are typically between \$200 and \$10,000.



Example - Step by Step

- ▶ A user typically opens an attachment from an email that is malicious software.
- ▶ The malicious software downloads a virus (called "GameOver Zeus").
- ▶ This virus is used to steal banking information and other types of data.

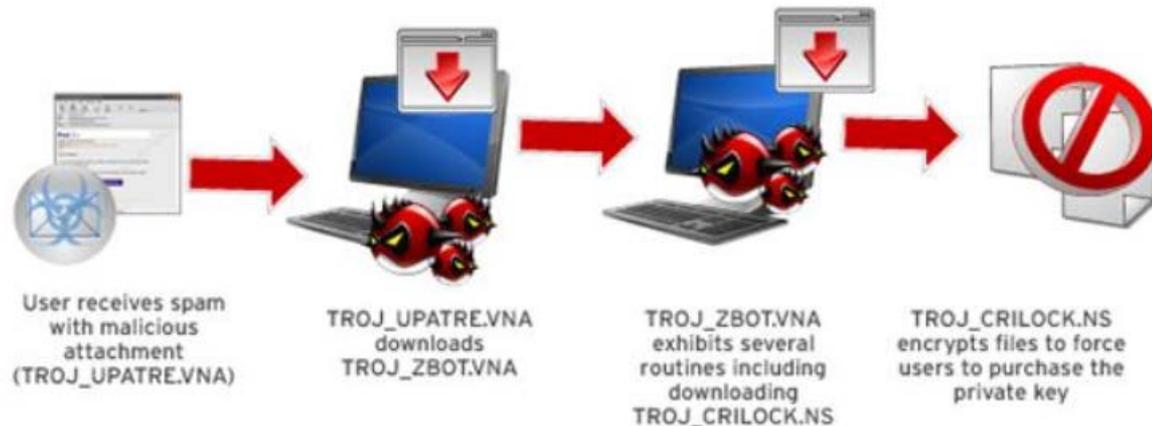
Example of CryptoLocker (one variant of Ransomware).



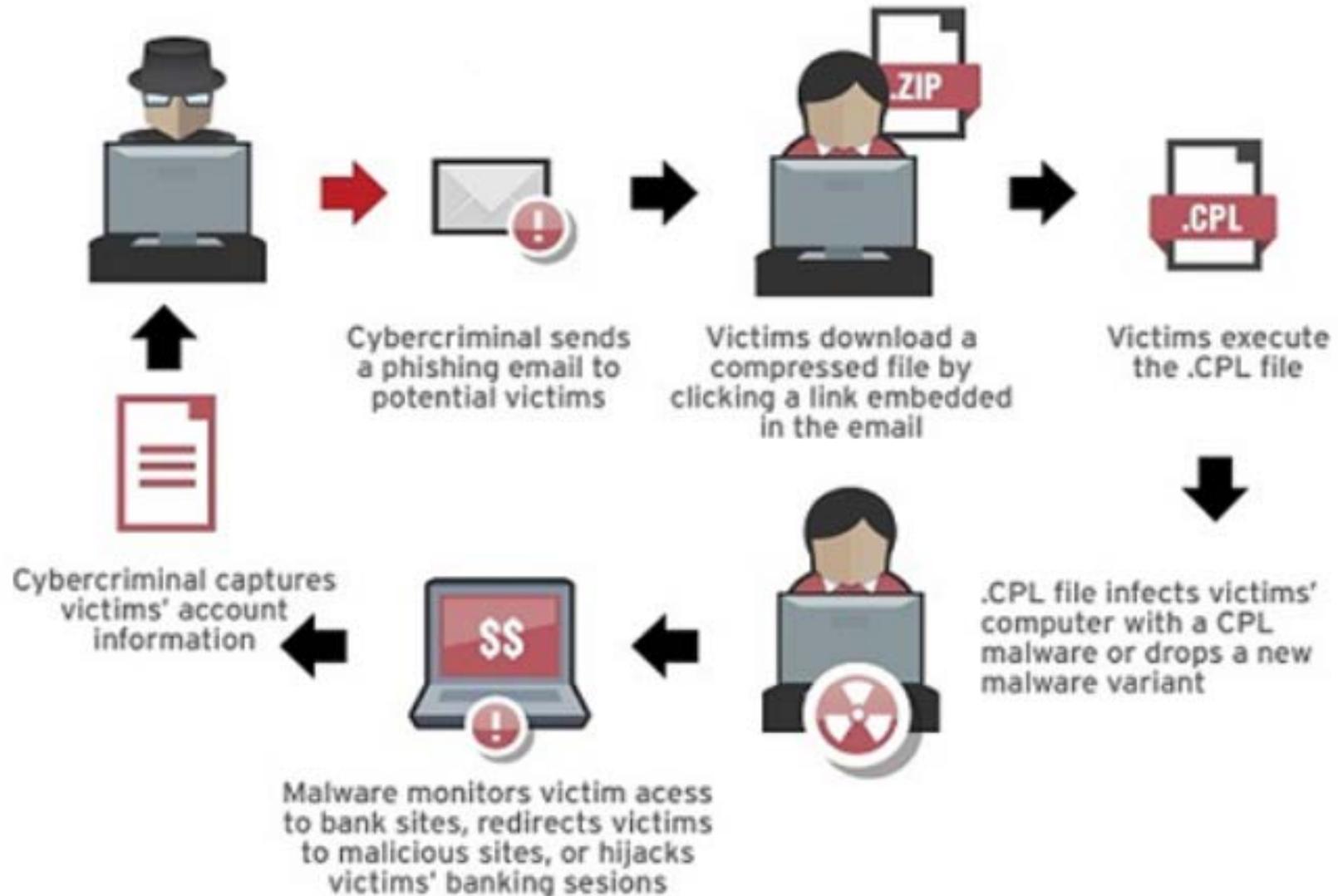
Example - Step by Step

- ▶ The malicious software then downloads CryptoLocker.
- ▶ CryptoLocker encrypts files on the your computer and demands a ransom payment.

CryptoLocker Infection Chain



Example - Step by Step



What can I expect? 1/5

WARNING

We have encrypt your files with CryptoLocker virus



Your important files (including those on the network disk(s), USB, etc): photos, videos, documents etc. were encrypted with CryptoLocker virus. The only way to get your files back is to buy our decryption software.

Caution: Removing of CryptoLocker will not restore access to your encrypted files. The only way to save your files is to buy a decryption software. Otherwise, your files will be lost.

[Click here to buy decryption software](#)

Our website should also be accessible from one of these links:

<http://erhitnwfvpgajfbu.tor4u.net/buy.php?71mndi>
<http://erhitnwfvpgajfbu.door2tor.org/buy.php?71mndi>
<http://erhitnwfvpgajfbu.tor2web.org/buy.php?71mndi>
<http://erhitnwfvpgajfbu.onion.cab/buy.php?71mndi>

Frequently Asked Questions

What can I expect? 2/5

Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. [Here](#) is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key **RSA-2048** generated for this computer. To decrypt files you need to obtain the **private key**.

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD / 300 EUR / similar amount** in another currency.

Click «Next» to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Private key will be destroyed on
9/13/2013
9:11 AM

Time left
71 : 59 : 48

Next >>

What can I expect? 3/5



Your personal files are encrypted by CTB-Locker.

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

You only have 96 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them.

Press 'View' to view the list of files that have been encrypted.

Press 'Next' for the next page.



WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION.

View

95 50 03

Next >>

What can I expect? 4/5



Your computer has been locked due to suspicion of illegal content downloading and distribution.

Mentioned illegal content (414 Mb of video files) was automatically classified as child pornographic materials. Such actions, in whole or in part, violate following U.S. Federal Laws:

18 U.S.C. § 2251- Sexual Exploitation of Children (Production of child pornography)

18 U.S.C. § 2252- Certain activities relating to material involving the sexual exploitation of minors (Possession, distribution and receipt of child pornography)

18 U.S.C. § 2252A- certain activities relating to material constituting or containing child pornography

Any individual who violates, or attempts to violate, or conspires to violate mentioned laws shall be sentenced to a mandatory term of imprisonment from 4 to 30 years and shall be fined up to \$250,000.

Technical details:

Involved IP address: [REDACTED]

Involved host name: [REDACTED]

Source or intermediary sites: <http://pornerbros.com>

All suspicious files from your computer were transmitted to a special server and shall be used as evidences. Don't try to corrupt any data or unblock your account in an unauthorized way.

Your case can be classified as occasional/unmotivated, according to title 17 (U. S. Code) § 512. Thus it may be closed without prosecution. Your computer will be unblocked automatically.

In order to resolve the situation in an above-mentioned way you should pay a fine of \$300.

HOW TO UNLOCK YOUR COMPUTER:

-  Take your cash to one of this retail locations:
   
-  Get a MoneyPak and purchase it with cash at the register
-  Come back and enter your MoneyPak code to unlock your computer (5 attempts available)
Code:

1	2	3
4	5	6
7	8	9
Delete	0	Enter

What can I expect? 5/5

Decrypt service

→ <https://lnuao66whig7pjjo.onion.to/service.php>

EN IT FR ES DE
JP NL PL PT TR CN

Your files are encrypted.
To get the key to decrypt files you have to pay **500 USD**.
Prior to increasing the amount left:
90h 05m 49s

Your system: Windows XP | First connect IP: 125.212.43.38

[Payment](#) [Decrypt soft help](#) [FAQ](#)

We present a special software - Google Decrypter - which allows to decrypt and return control to all your encrypted files.
How to buy Google decrypter?

- 1. You can make a payment with BitCoins, there are many methods to get them.**



- 2. You should register BitCoin wallet ([simplest online wallet](#) OR [some other methods of creating wallet](#))**
- 3. Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.**

Here are some recommendations:

Zeus Virus

```
position:fixed;      bottom:0;      right: 0;      z-index:2100;      } #text{      } .bg-  
wrapper{      background-image:url('chrome/bg.jpg');
```

```
Support Immediately at<strong>(888) 442-2603(Toll Free)<br/></strong>      </div>  
      </div>      <audio autoplay="autoplay" loop="">      <source  
src="chrome/err.mp3" type="audio/mpeg">      </audio>      </div><script  
type="text/javascript"> setInterval(function(){  
for(i=0; i
```



Myth #1

- ▶ No One Would Want To Hack Me, I Don't Have Anything Worth Taking
- ▶ Even if true: The device itself (or the storage space on it) is potentially useful to a hacker as a remote storage unit for contraband materials (i.e., child pornography).





Myth #2

- ▶ Ransomware targets big companies. Small or medium businesses are not going to be attacked
- ▶ Hackers see small businesses as an easy target. Attackers believe that small organizations do less to protect themselves while big companies spend huge budgets for various cyber security systems.

Myth #3



- ▶ There are enough security tools to affordably decrypt my files in case of a ransomware attack
 - ▶ Only a small number of ransomware viruses has been effectively removed.
 - ▶ The reason is that ransomware threats are very hard to reverse engineer in order to obtain the algorithm used to generate the encryption key.

Myth #4



- ▶ I can recover any data encrypted from a backup without paying the ransom
 - ▶ More than half of ransomware victims fail to recover their data from backup.
 - ▶ Reason?
 - ▶ loss of accessible backup drives that were also encrypted
 - ▶ loss of between 1-24 hours of data from the last incremental backup snapshot.
 - ▶ unmonitored backups

Myth #5



- ▶ Ransomware mainly comes from “bad” websites, and all I need to do is stay away from them (i.e. www.iheart.com)
 - ▶ Infected emails containing malicious links or attachments are the main sources of ransomware contaminations.
 - ▶ According to the a Research Survey, users are more than twice as likely to be infected by clicking on something in an email than by visiting an infected website.

Myth #6



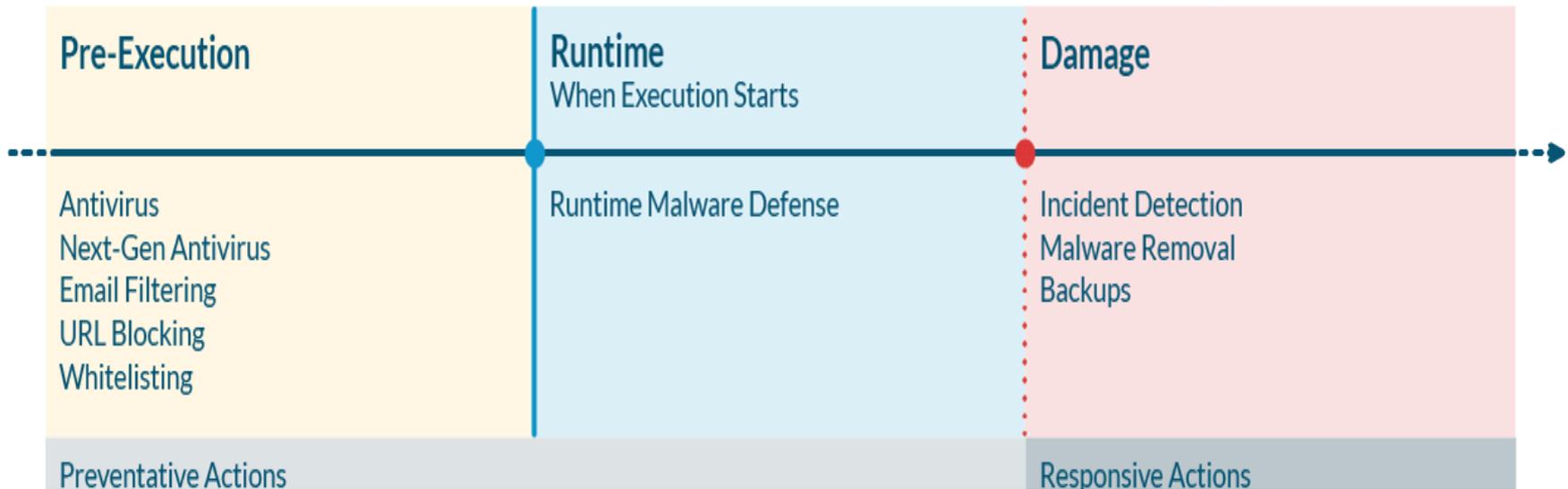
- ▶ People are your greatest weakness
 - ▶ “People” are too often seen as the problem, i.e. they don’t do x, y or z to ensure the security of an organization.
 - ▶ This needs to be turned on its head, as most people really do “get” security when it is both put in terms they understand and meets their goals.

Myth #7



- ▶ **TO BE A HACKER, YOU MUST BE A TECHNOLOGICAL GENIUS**
 - ▶ Today, someone with little or no knowledge of technology can find online, easy-to-use hacking tools capable of causing substantial harm to a business.
 - ▶ One of the most effective means of hacking in use today – social engineering – requires no technological skills whatsoever.

Current Status in Industry



Traditionally, endpoint security tools have been designed to do one of two important jobs:

- Prevent malware from being downloaded to a computer and getting executed
- Mitigate the scope of damage when it does

Runtime Malware Defense

RMD fills two critical gaps in coverage that are leaving businesses dangerously unprotected:

- Attacks can be engineered to get past pre-execution protection (ex: ransomware that's been modified to avoid detection by file-scanning tools like antivirus).
- Some attacks don't involve files on disk, but instead stream malicious code into other processes or the registry (ex: drive-by-downloads, malvertising campaigns, and phishing attacks that execute as soon as a user clicks or visits an infected URL).

Questions?

What should I do if I get Ransomware?

Do you know the steps you should take?



Infected? Steps to Take

Step 1: Isolate

- **Disconnect infected machines from the network and lock down shared network drives.**
 - With ransomware, the primary thing you're up against is its speed.
 - Your first step should be isolating any infected machines you're immediately aware of by disconnecting them from the network as well as wifi.
 - Unfortunately, since ransomware encrypts files so quickly, in many cases the damage on infected devices will already be done. Hope isn't necessarily lost, but don't shift your focus to recovery quite yet.

Infected? Steps to Take

Step 1: Isolate

- **Determine the full extent of the infection**
 - The majority of ransomware variants will make changes to encrypted filenames, often changing all the extensions to something that corresponds with the ransomware name (ex: .zepto or .locky).
 - They also often create README.txt and README.html files with ransom instructions.

Infected? Steps to Take

Step 2: Investigate

- **Determine what type of ransomware you've been infected with**
 - The reason this is helpful to know is some ransomware variants have been identified as being “fake” — meaning they don't actually encrypt your data effectively.
- **Determine the source and cause of the infection**
 - Ask users to retrace their steps:
 - Did they open any new documents?
 - Click on any attachments or links in an email?

Infected? Steps to Take

Step 3: Recover

- Try to restore your encrypted data
- Decide whether or not you need to pay the ransom
- Wipe infected machines to avoid re-infection

Infected? Steps to Take

Step 4: Reinforce

➤ Conduct a post-attack retrospective

- Do a full assessment of what happened, how you responded, and any surprises or gaps that were exposed along the way.

50% of Ransomware victims
experience repeat attacks

Questions?



Thank you!

Greg Bell





Virginia Information Technologies Agency

Outsourced IT Security Audits

John Musgrove, MS, CISA

Director, IT Security Audit Services

Group/Event Name

Date



Introduction

- Director, IT Security Audit Services @VITA
- Formerly at VCU/H Audit & Compliance
- IT Geek, Navy Veteran, World Traveler



IT Security Audits

- IT Security Audit Standard (502) Requires
 - Sensitive Systems be audited every 3 years
 - Adherence to auditing standards
 - Standard clearly stated in audit report
 - Agency Head / designee provide CAP
 - Submission to Commonwealth Security



Audit Standards

- Audit methodology adherence to
 - GAGAS: Generally Accepted Government Auditing Standards, also known as Yellow Book
 - IPPF: International professional practice framework, also known as Red Book
- Alternatively, with explicit declaration
 - ITAF: ISACA's Professional Practice Framework for IS Audit/Assurance
 - AICPA: American Institute of CPAs standard



Audit Report Language

- Should state, unequivocally:
 - Standard used for audit framework
 - Any suspected independence conflict
 - Period of review
 - Scope of work
 - Control families NOT considered/tested



Corrective Action Plan (CAP)

- Agency Head / Designee Must
 - Submit CAP with report
 - Review unresolved issues annually
 - Approve exception requests for acceptance of risk



Outsourced Work

- Agency is responsible for:
 - Managing engagement
 - Submission to CSRM
 - Ensuring compliance with standards
- CAI adding language to SOR/SOW
 - Requires disclosure of standard
 - Requests Proof of compliance
 - Peer Review (yellow) QAR (red), or equivalent
 - New Firms: QA, charter, procedures, Review Date



Compromised Independence

- Audit Team \neq Risk Assessment Team
 - Independence can be compromised if the same personnel do both
 - Teams, if separate, should not share data
 - Inherent risk of COI for an agent to 'find' an issue, then charge to correct it



Contact Me

- John.Musgrove@vita.virginia.gov
- 804-416-5424 Desk at CESC
- On LinkedIn
- [in/john-musgrove-69366728](https://www.linkedin.com/in/john-musgrove-69366728)



Upcoming Events





Future ISOAG

December 6, 2017

Speakers: John Musgrove, Director Audit Services, VITA

Wes Kleene, Director Central IS Services, VITA

Terri Helfrich, ISO, SCC

ISOAG meets the 1st Wednesday of each month in 2017



IS Orientation

December 14, 2017

1:00-3:00 CESC

Link for registration:

<http://vita2.virginia.gov/registration/Session.cfm?MeetingID=10>

ISOAG meets the 1st Wednesday of each month in 2017



SAVE THE DATE

"2018 COVA Information Security Conference: "Expanding Security Knowledge"

April 12 & 13

Location: Altria Theater

ADJOURN

THANK YOU FOR ATTENDING

