ISC 2018 ISC互联网安全大会 | 360互联网安全中心

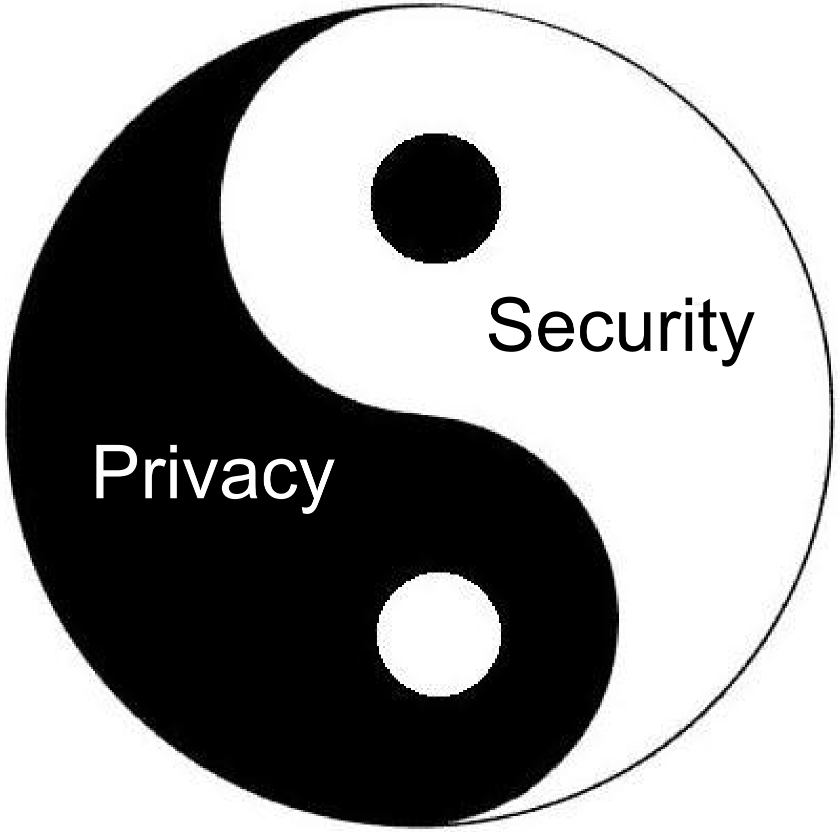
GLOBAL CHALLENGES

Building Enterprise-Grade Cloud Security & Privacy

Jim Reavis CEO, CSA

ISC 互联网安全大会 中国 · 北京
Internet Security Conference 2018 Beijing · China

No Privacy without Security



GENERAL DATA PROTECTION REGULATION (GDPR) FINES 20M EUROS OR 4% WORLDWIDE REVENUE

RANSOMWARE DAMAGE COSTS PREDICTED TO HIT $11.5B BY 2019 (SOURCE CYBERSECURITY VENTURES)

CLOUD IS THE FOCAL POINT FOR THE FUTURE OF IT AND THE MECHANISM FOR DELIVERING SECURITY AND PRIVACY

Overheard Everywhere

MY REPORT COMES TO THE CONCLUSION THAT CLOUD TECHNOLOGY IS OF NO USE TO THIS COMPANY. I'LL UPLOAD IT TO DROP BOX SO YOU CAN TAKE A LOOK AT IT.
© D.Fletcher for CloudTweaks.com

BE **AWARE** OF YOUR CLOUD USAGE

BUILD **STRATEGIES** FOR SECURING CLOUD

BE **OPPORTUNISTIC** TO IDENTIFY CLOUD SOLUTIONS TO ADVANCE THE STRATEGY (“**CLOUD FIRST**”)

BE **AGILE** AND **TRANSFORM** SECURITY AND PRIVACY

EVERYONE IS **MULTI-CLOUD**

About CSA

cloud security alliance®

Building the Global Trusted Cloud Ecosystem

GLOBAL NON-PROFIT NGO

BUILD SECURITY AND PRIVACY BEST PRACTICES FOR CLOUD, IOT AND NEXT GENERATION IT

RESEARCH AND EDUCATIONAL PROGRAMS

CLOUD PROVIDER CERTIFICATION – CSA STAR

USER CERTIFICATION – CCSK

CHINA CSA: WWW.C-CSA.CN

Basic vs Mature

BASIC CLOUD ADOPTER

"LIFT AND SHIFT" LEGACY APPS INTO CLOUD

LOW VISIBILITY INTO CLOUD ADOPTION BY DEPARTMENTS

MANUAL APPROACH TO UPGRADES AND SECURITY PATCHING

IDENTITY MANAGEMENT DETERMINED BY INDIVIDUAL APPLICATION

CLOUD CAN USE SIMILAR ARCHITECTURES AND STRATEGIES AS LEGACY IT

MATURE CLOUD ADOPTER

BUILD CLOUD NATIVE APPS USING DEVOPS

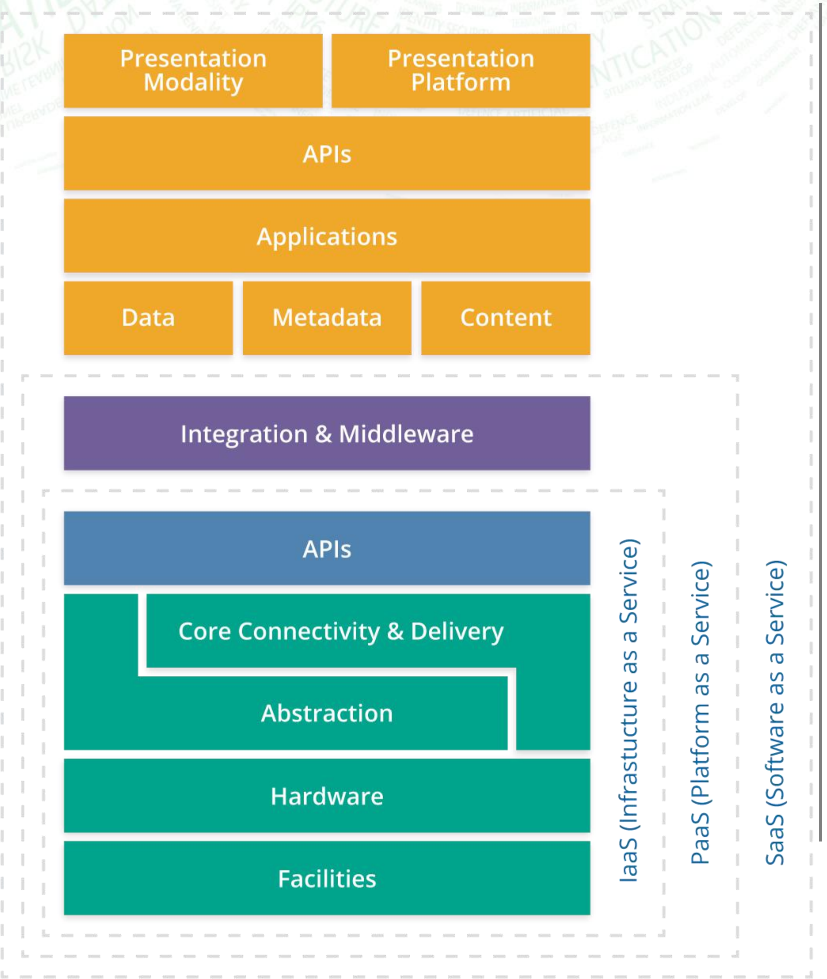
LEVERAGE CLOUD ACCESS SECURITY BROKER (CASB) OR SIMILAR

USE CLOUD ORCHESTRATION TOOLS TO AUTOMATE WORKLOAD OPERATIONS

IDENTITY "DIALTONE" OF IDENTITY FEDERATION AND MULTI-FACTOR AUTHENTICATION

CLOUD = SOFTWARE-DEFINED COMPANY

CSA Cloud Model



LAYERED S-P-I MODEL

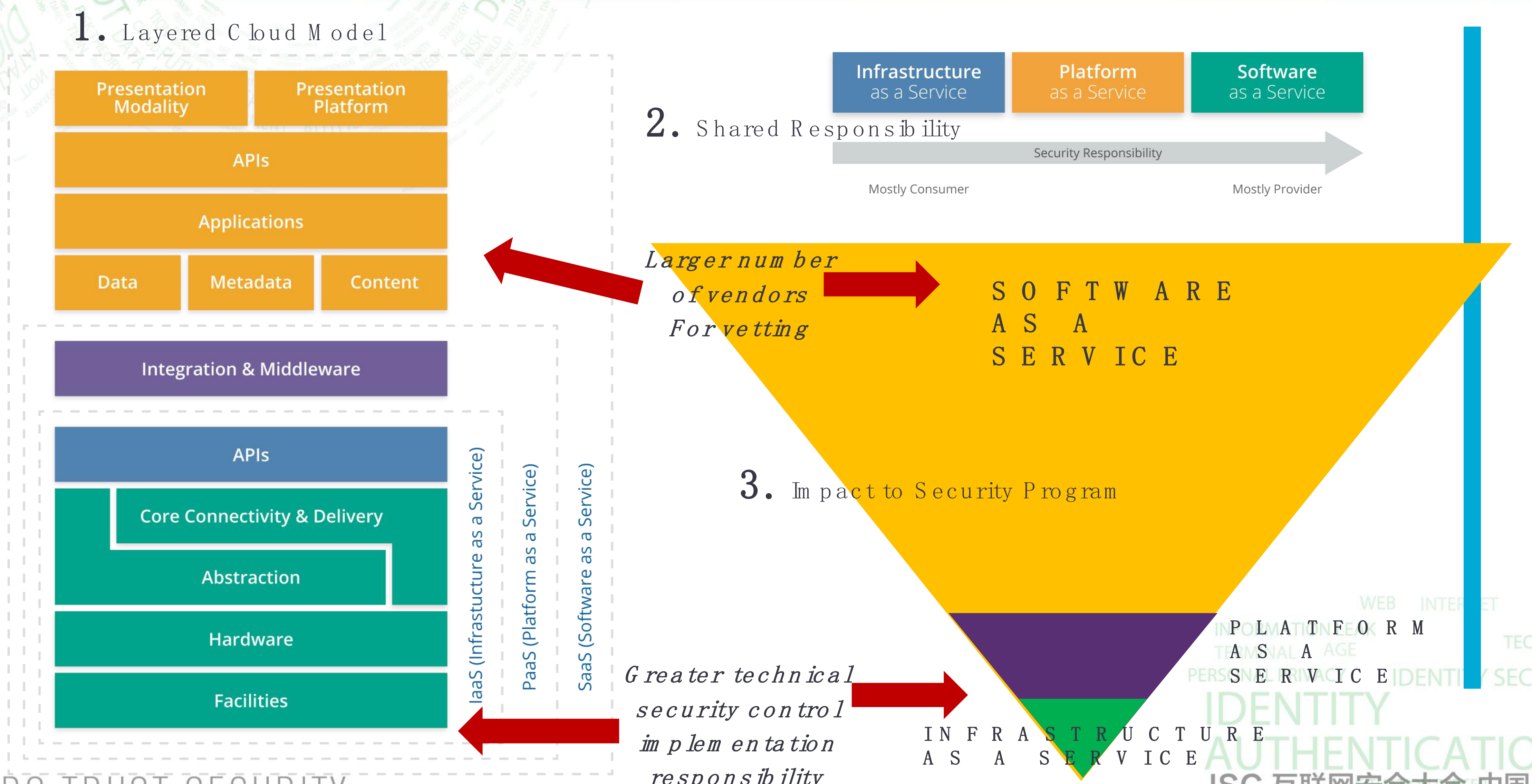
VIRTUAL ARCHITECTURE

DYNAMIC (CODE CHANGES DAILY!)

ABSTRACT (CONTAINERS AND MICROSERVICES)

CLOUD APPS ARE “MASHUPS”

1-2-3 Cloud Security



1. Layered Cloud Model

2. Shared Responsibility

Larger number of vendors For vetting

3. Impact to Security Program

Greater technical security control implementation responsibility

ZERO TRUST SECURITY

Enterprise-Grade Cloud Security

- ***Continuous Encryption***: reduce the “plaintext” window of exposure
- ***Identify Mgt*** beyond the human to all entities
- ***Software Defined Perimeter***
- ***DevSecOps*** automates the Cloud-Native Security
- ***AI/Machine*** learning to scale up

Secure Perimeter

- Micro-perimeter -- isolating applications and data with a hardened configuration immune to attack
- Strong abstraction layer from hardware and VM environment
- Restricted visibility into computing environment
- Discrete and limited perimeter which can be subjected to effective monitoring

Continuous Encryption

- Encryption of data at rest
- Encryption of data in transit
- Secure key management-- – leveraging PKI for transaction functions

Ready Incident Response

- Hybrid automation and manual response

Continuous Monitoring

- Reachable attachment points for monitoring capabilities through comprehensive APIs
- Robust monitoring data availability
- Easy integration of third party monitoring capabilities

Resilient Operations

- Capable of withstanding attack
- Minimal degradation of performance as a result of environmental failures
- Continuous function in the presence of a ongoing attack

Highly Granular Access Control

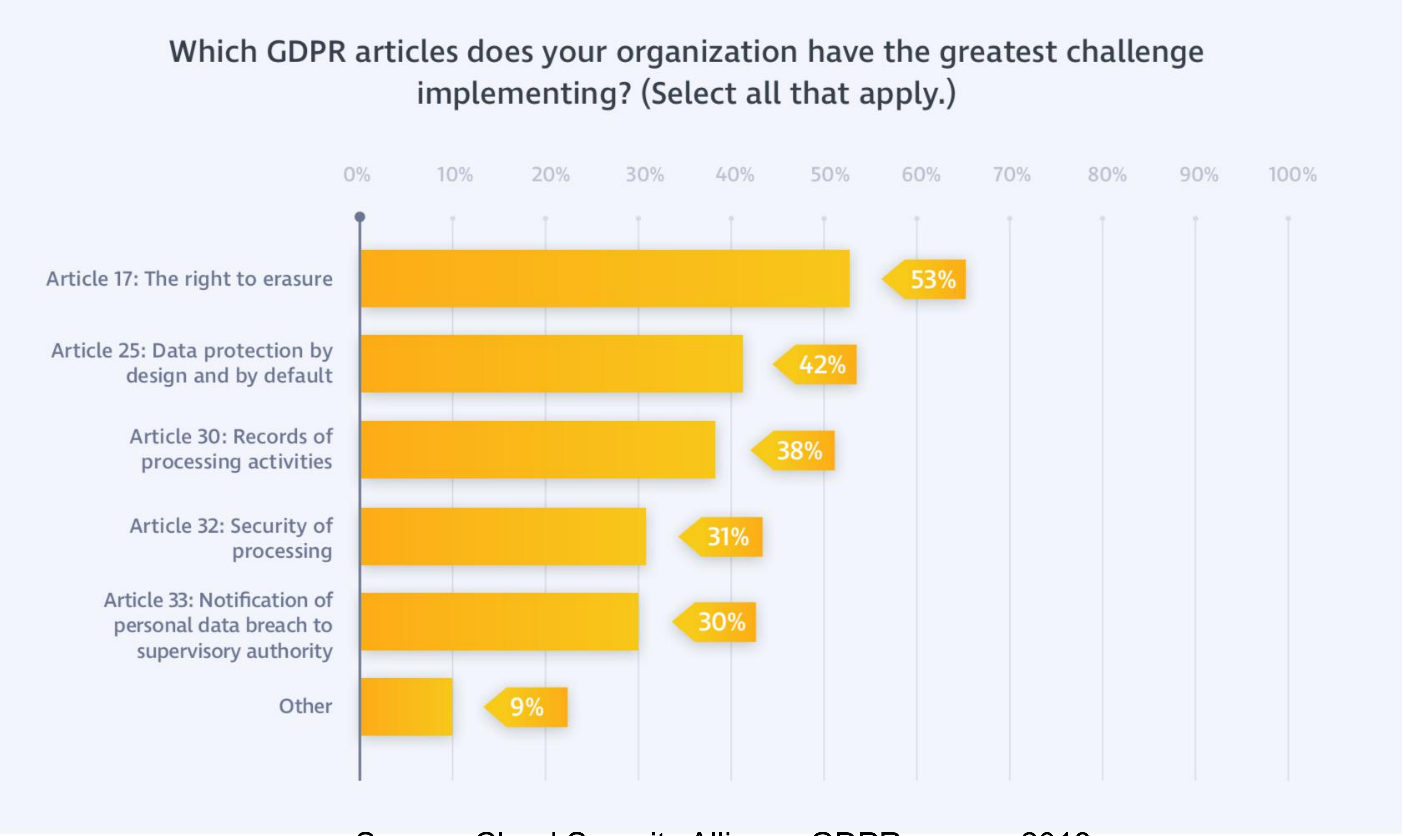
- Capable highly granular resource allocation
- Strong cryptographic identity management
- Ubiquitous – users, administrators, applications, data

Identity Infrastructure

Governance, Risk Management, Compliance

- Visibility of configurations
- Auditable evidence
- Readily identify gaps or other weaknesses
- Broad regulatory and compliance certifications

Privacy = GDPR



Source: Cloud Security Alliance GDPR survey, 2018

FOCAL POINT FOR PRIVACY

EVERYONE DOES BUSINESS IN EUROPE

GDPR GUIDANCE USED FOR PRIVACY PROGRAMS

GDPR MODEL FOR OTHER PRIVACY LAWS

REQUIRES SPEED AND AGILITY IN YOUR PRIVACY PROGRAM

GDPR Game Changers

DATA CONTROLLER ACCOUNTABILITY

RISK-BASED DATA PROTECTION

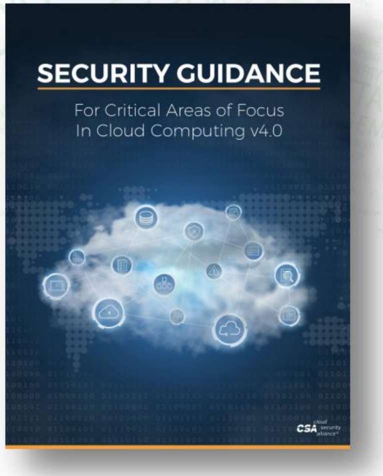
CONSUMER RIGHT TO REMEDIES

TRANSPARENCY IN COMPLIANCE ACTIVITIES

ALIGN PRIVACY WITH SECURITY PROGRAM – DATA PROTECTION OFFICER (DPO)

USE A **CODE OF CONDUCT** TO PROVE COMPLIANCE

CSA Tools for Enterprise-Grade Cloud Security and Privacy



SECURITY GUIDANCE

For Critical Areas of Focus In Cloud Computing v4.0

CLOUD SECURITY ALLIANCE
CODE OF CONDUCT
FOR GDPR COMPLIANCE

PRIVACY LEVEL AGREEMENT WORKING GROUP, NOVEMBER 2017

CCM™
Cloud Controls Matrix

CSA STAR™
Security, Trust & Assurance
Registry

V4 GUIDANCE TO BUILD A MODERN SECURITY PROGRAM

CLOUD CONTROLS MATRIX FOR YOUR CONTROLS FRAMEWORK

GDPR CODE OF CONDUCT FOR YOUR PRIVACY PROGRAM ROADMAP

CSA STAR FOR PROVIDER CERTIFICATION AND TRANSPARENCY

ALL TOOLS ARE FREE AND TRANSLATED TO CHINESE AT WWW.C-CSA.CN

Final thoughts

Building the Global Trusted Cloud Ecosystem

CLOUD IS MORE SECURE THAN ON-PREMISE WHEN DONE RIGHT

BUILD A VIRTUAL, SOFTWARE-DEFINED, DEV(SEC)OPS, AUTOMATED PROGRAM FOR SECURITY AND AGILITY

SUPPORT RAPID RESPONSE PRIVACY

THINK TOWARDS THE FUTURE

CSA IS HAPPY TO BE YOUR PARTNER IN YOUR CLOUD JOURNEY

ISC 2018

ISC互联网安全大会

360互联网安全中心

THANKS

ISC 互联网安全大会 中国 · 北京

Internet Security Conference 2018 Beijing · China