Technology Exploration Workshop on CLOUD COMPUTING : SECURITY (?)

Julien Airaud – CNES

julien.airaud@cnes.fr

WHAT IS SECURITY ?

Data

Process

Confidentiality

Integrity

Availability

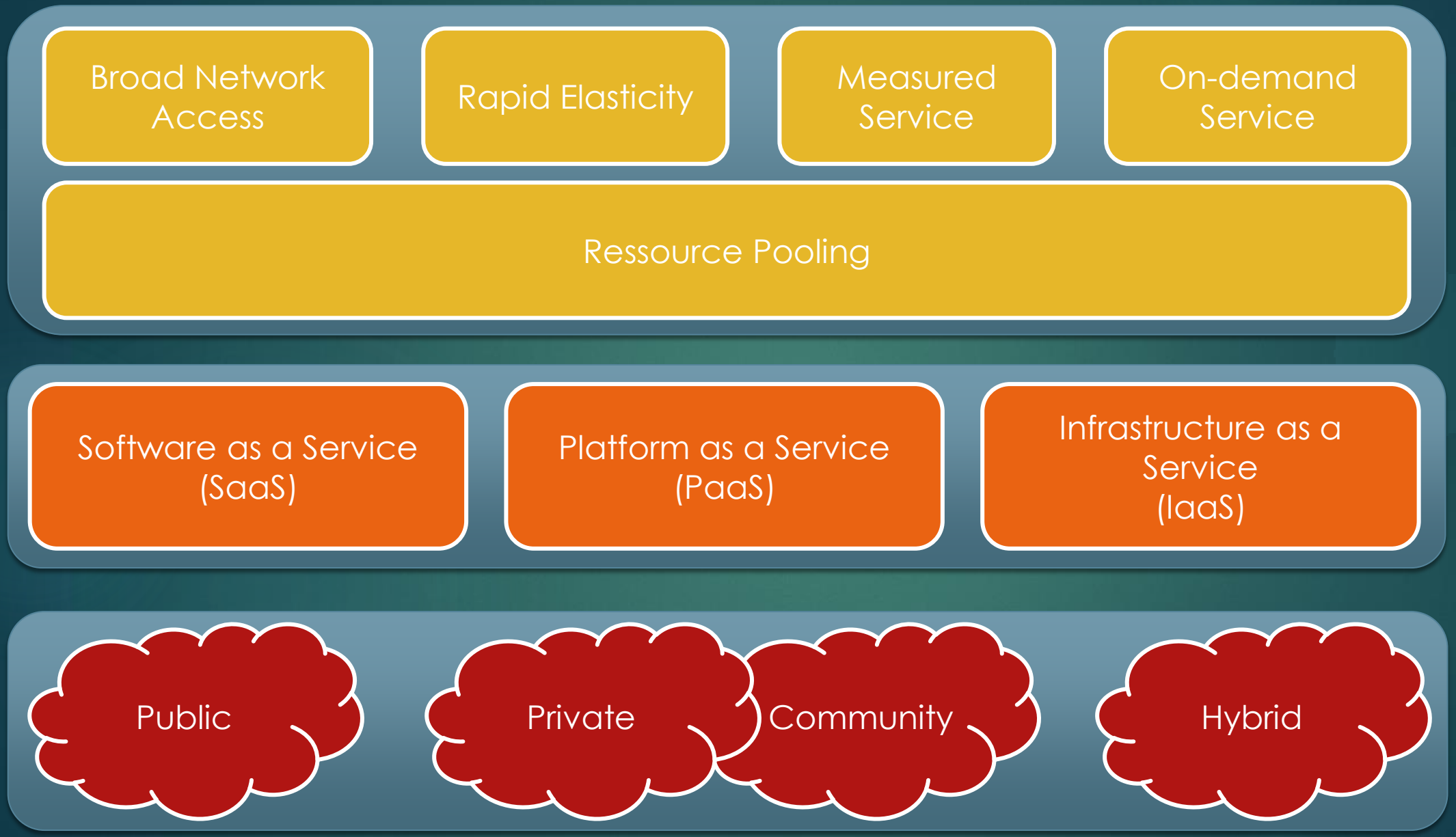
NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Special Publication 800-145

The NIST Definition of Cloud Computing

Recommendations of the National Institute of Standards and Technology

Peter Mell
Timothy Grance



NIST Visual Model of Cloud Computing Definition

Is « the cloud » secure ?

Well…it depends

Cloud

- Operational model
- There are lots of different types of cloud (and they are not created equal)

Use cases

- Data processing, off-loading, analytics, etc.
- All uses cases are differents

How does cloud computing affect our security practices ?

Security driver (short version)

Providers are usually good at security (compared to what SME or equal size organizations can afford).

Cloud characteristics : Scale

- Locations
- Elasticity means better availability

Azure regions

Azure is generally available in 30 regions around the world, and has announced plans for 4 additional regions. Geographic expansion is a priority for Azure because it enables our customers to achieve higher performance and it support their requirements and preferences regarding data location.

Explore products per region ►

Azure Status

Last updated 21 seconds ago

RSS

Refresh every 2 minutes

✓ Good ⚠ Warning ! Error i Information

Americas | Europe | Asia

PRODUCTS	GLOBAL	EAST US	EAST US 2	CENTRAL US	NORTH CENTRAL US	SOUTH CENTRAL US	WEST CENTRAL US	WEST US	WEST US 2	CANADA EAST	CANADA CENTRAL	BRAZIL SOUTH
IMPACTED SERVICES												
Visual Studio Team Services					⚠	⚠						✓
COMPUTE												
Virtual Machines		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Cloud Services		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Batch		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
RemoteApp		✓	✓	✓	✓	✓		✓				✓
Service Fabric		✓			✓	✓		✓		✓	✓	
Virtual Machine Scale Sets		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Azure Container Service		✓	✓	✓	✓	✓		✓				✓
Functions			✓	✓	✓	✓		✓	✓			✓

Cloud characteristics

- Scale
  - Locations
  - Elasticity means better availability
- Deployment
  - Robust templates for virtualization
  - Automation + orchestration = security miracles
- Audit and Incident Management

CLOUD INCIDENTS

Incidents topology

Accidents
Errors
Malicious

+

Internal
External

+

Skill

« ACCIDENTS »

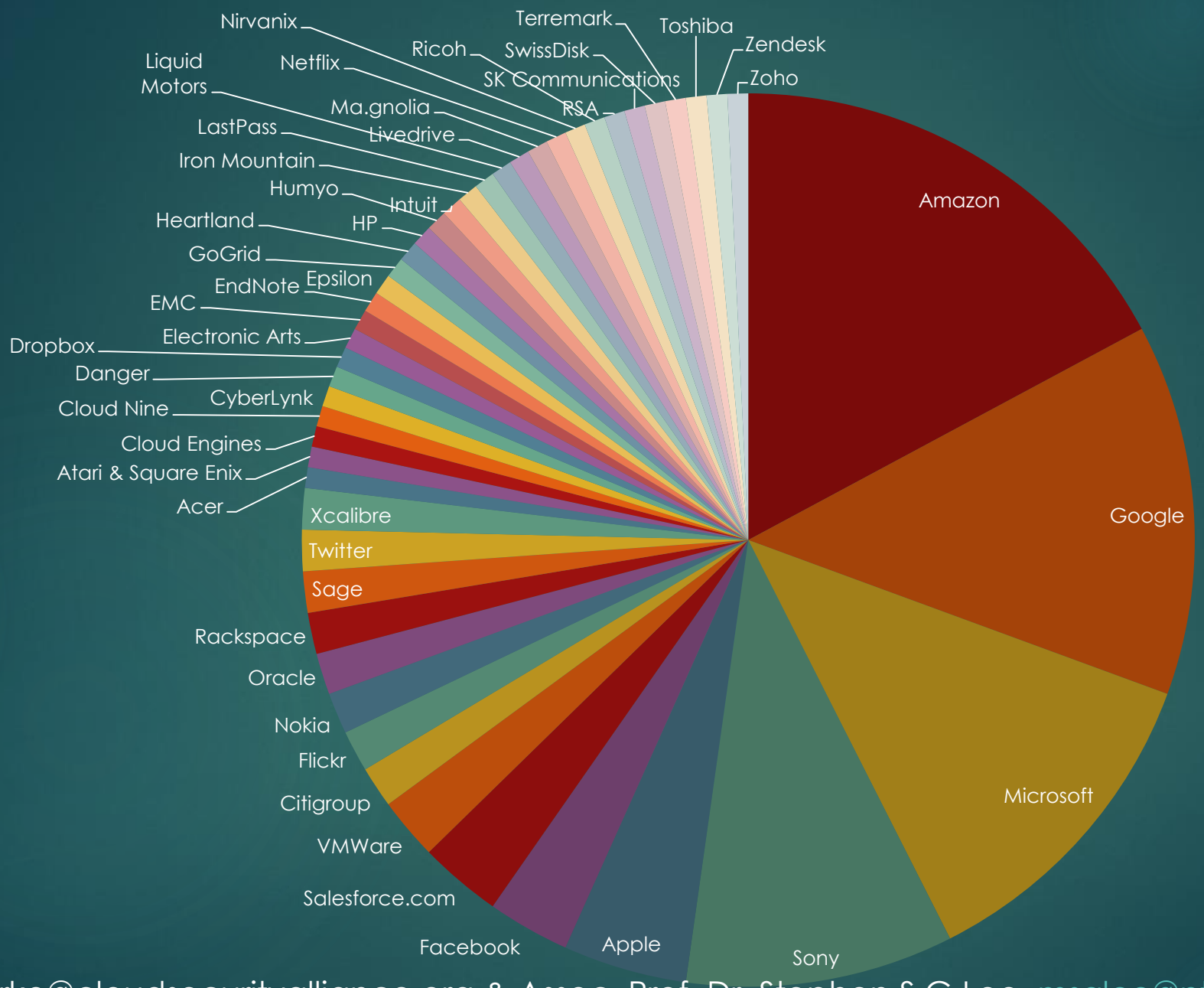
- 9/9/2014 : Amazon rebooted 10% of EC2 instances to patch a Xen vulnerability.
- 18-19/11/2014 : Microsoft Azure was down for 40 hours
- 01/2015 : Verizon planed a 48 hours maintenance shutdown of all systems.

EXPLOITING THE CLOUD

- 01/2014 Bitcoin rush : AWS xl instances + GPU service (cudaminer).
  - Caused by careless users putting credentials on GitHub,
  - Detected by Amazon thanks to Github's repositories monitoring
  - Amazon reversed the charges

- Defcon 2015 : Cloud Computing : A weapon of Mass Destruction ? (Netspi)
  - Cloud Usage for DDoS, Botnets C & C,
  - Easy due to automation, plentiful bandwidth

Breakdown of Cloud Provider - Incidents



Dr. Ryan Ko – rko@cloudsecurityalliance.org & Assoc. Prof. Dr. Stephen S G Lee msglee@ntu.edu.sg in

Cloud Computing Vulnerability Incidents: A Statistical Overview

CLOUD FOR SPACE ?

CCSDS

Consultative Committee for Space Data Systems

cnes

- Use case :
  Standards interoperability testing between spa ce agencies
- First test : Space Data Link Security testing within ESA's provider :
  CloudSigma
- Three cases :
  - One cloud, one shared VM
  - One cloud, one VM per agency
  - Multiple clouds linked though VPN over public space

CCSDS

- NASA
  - Only FEDRAMP services can be used:
    - AWS FedRAMP zones,
    - VMware vCloud Government Service
  - Only US datacentres
- ESA
  - Interoute / Cloud Sigma / OBS
  - Specific requirements on security & privacy
- UK Space Agency
  - No cloud, no policy
- DLR
  - T-System but difficult to open

PLANING FOR THE CLOUD

Guidance

cnes

enisa European Network and Information Security Agency

NIST

cloud CSA security alliance®

Bundesamt für Sicherheit in der Informationstechnik

FedRAMP

GOV.UK

ORGANISATIONAL SECURITY CONCERNS

Organisational Security Concerns

- Governance = contract

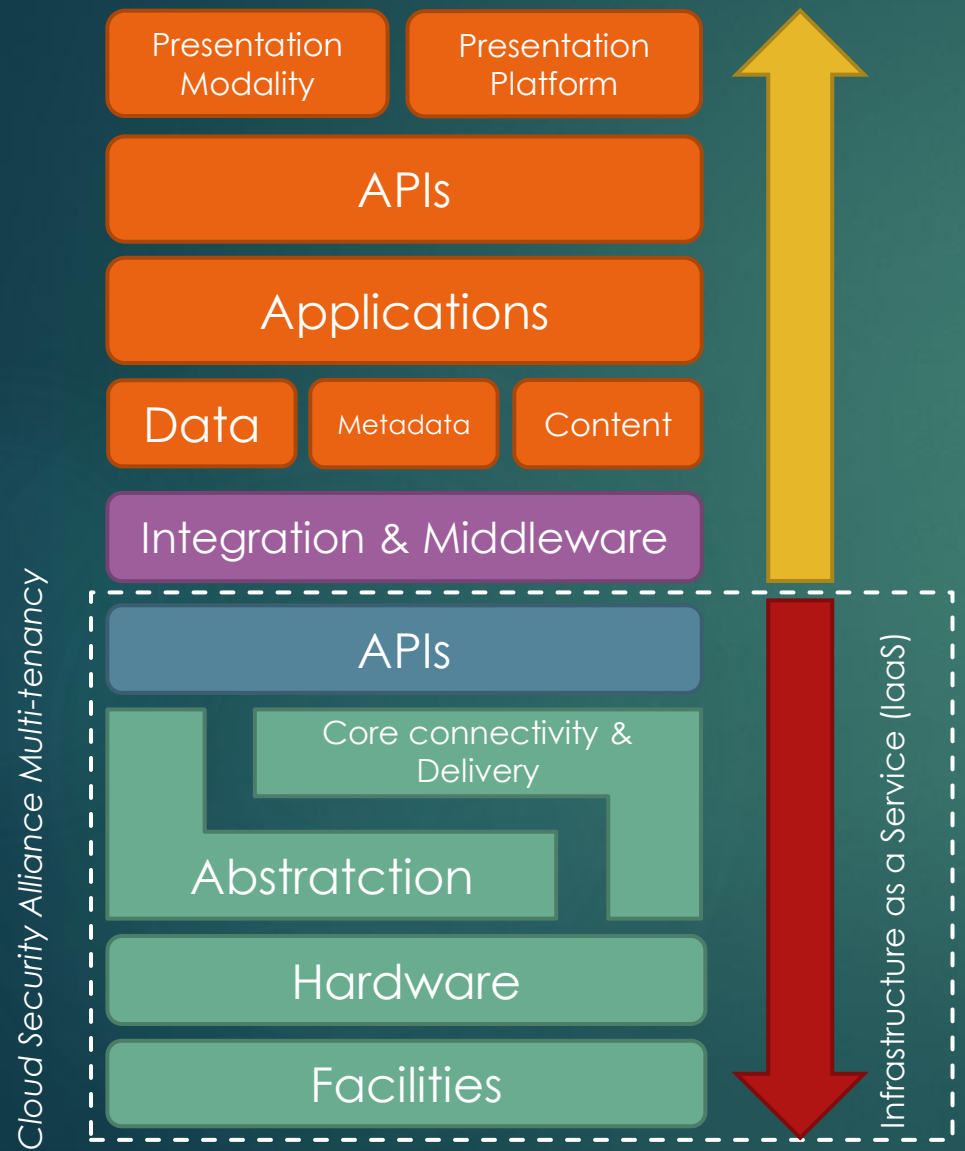
ORG risks – Contract ?

THE SERVICE OFFERINGS ARE PROVIDED “AS IS.” WE AND OUR AFFILIATES AND LICENSORS MAKE NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE REGARDING THE SERVICE OFFERINGS OR THE THIRD PARTY CONTENT, INCLUDING ANY WARRANTY THAT THE SERVICE OFFERINGS OR THIRD PARTY CONTENT WILL BE UNINTERRUPTED, ERROR FREE OR FREE OF HARMFUL COMPONENTS, OR THAT ANY CONTENT, INCLUDING YOUR CONTENT OR THE THIRD PARTY CONTENT, WILL BE SECURE OR NOT OTHERWISE LOST OR DAMAGED. EXCEPT TO THE EXTENT PROHIBITED BY LAW, WE AND OUR AFFILIATES AND LICENSORS DISCLAIM ALL WARRANTIES, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR QUIET ENJOYMENT, AND ANY WARRANTIES ARISING OUT OF ANY COURSE OF DEALING OR USAGE OF TRADE.

Organisational Security Concerns

- Governance
- Security responsibility

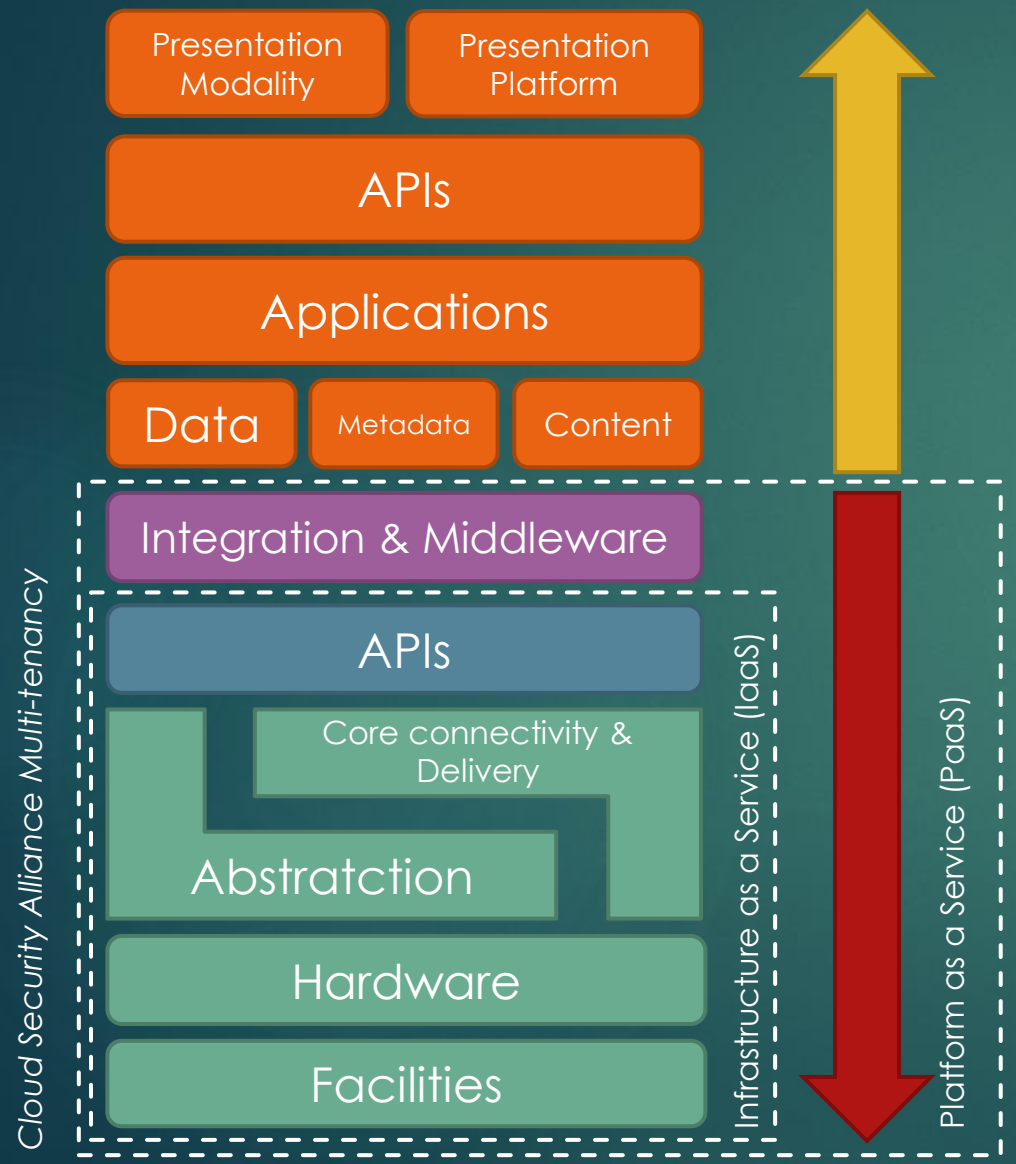
Shared responsibility – IaaS



User is responsible for confidentiality and integrity (security starts at the guest/VM)

Provider secures the infrastructure to cover availability and multi-tenancy.

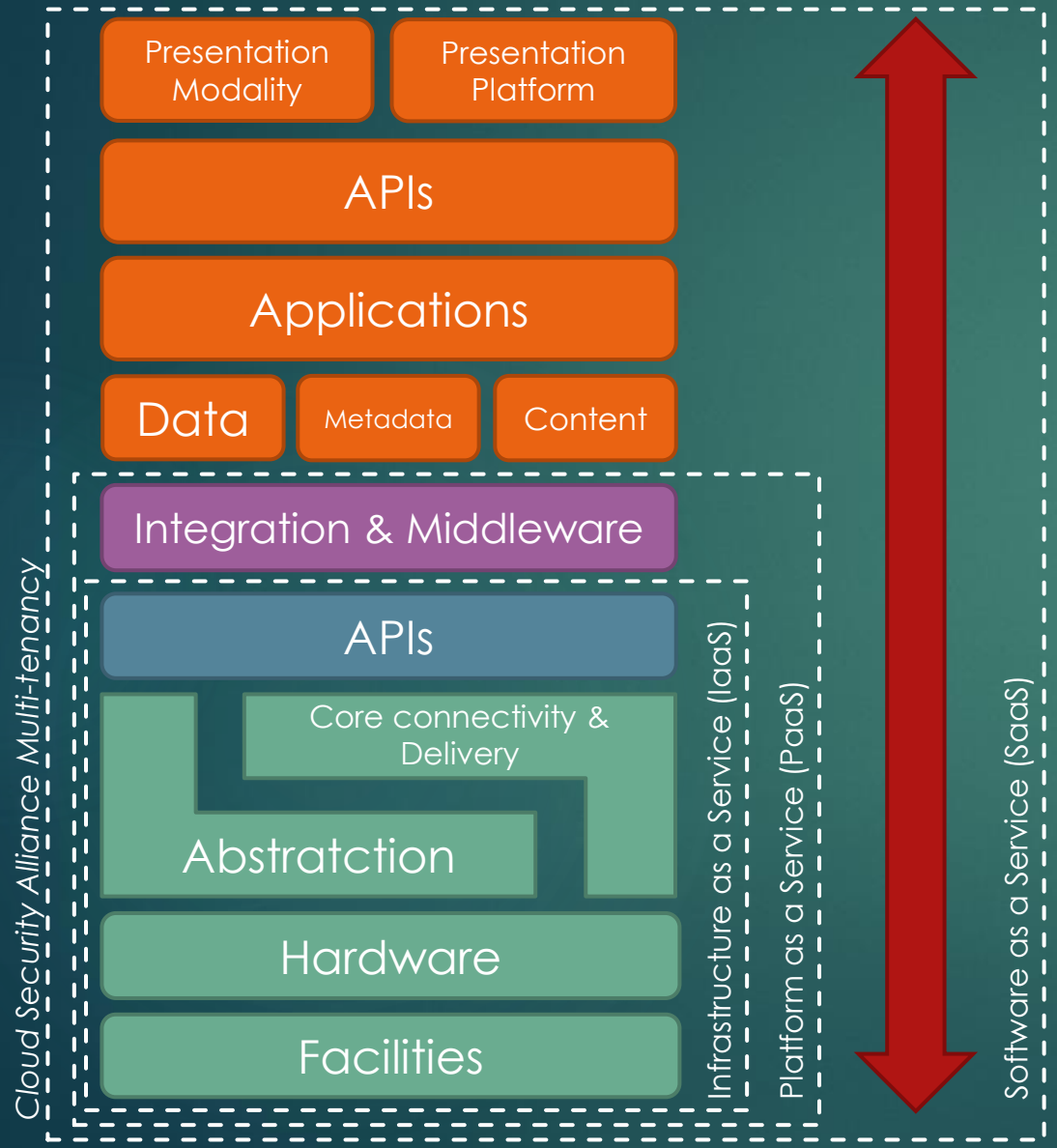
Shared responsibility – PaaS



User creates the application. Writing secure applications and ensuring your data is safe is your responsibility

Provider secures compute, network, storage layers & programmatic interface

Shared responsibility – SaaS



Contract / Access

Provider secures everything

Organisational Security Concerns

- Governance
- Security responsibility
- Compliance to legal and sectorial regulations

COMPLIANCE

- Security of information and computer systems

- Privacy of personal data
  - EU Data Protection Regulation
- Zone selection

Solutions

- Contracts
- Supplier Assessments
- Compliance, audits of control
- Risk management

Cloud Computing risks

Everything old is new again

- Information system security
  - Management
  - Data security
  - Infrastructure
- Cloud layers
- DDoS : Distributed Denial of Service
- EDos : Economical Denial of Service

Management Plane

- Although abstracted, the management plane is there, web or API based.
- Centralisation of everything owned

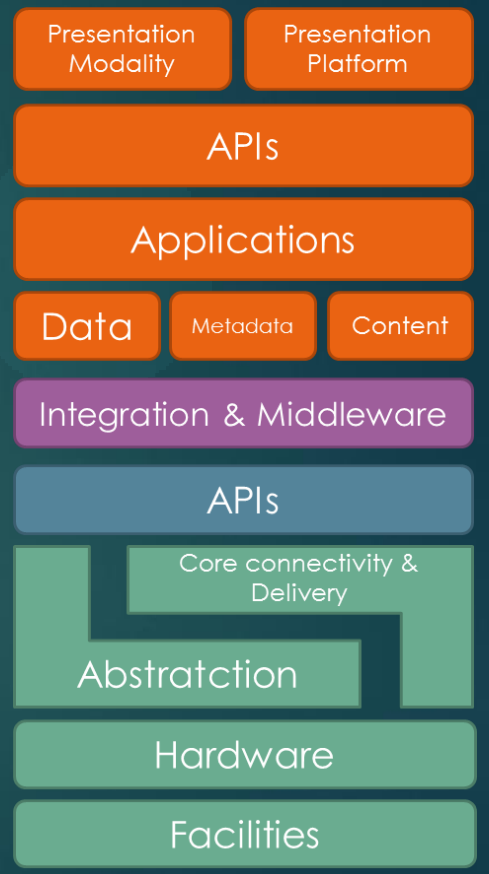
- Malicious insider from the back-office, with high privileges
- Management interface is only as secure as your secret credentials
- Compromise of the service engine

Data

- Data can be intercepted in transit to or from the cloud, or when moving inside
- Data at rest
- Data erasing
  - No guarantee (tapes, hard disk, etc.)
  - No real tool can be used

Computations

- Infrastructure is based on virtualization, abstraction layers, automation technologies and secret sauce.
- Vulnerabilities apply to compute, network and storage (and secret sauce)
- A compromised node in a processing infrastructure can lead to :
  - data leakage,
  - incorrect output,
  - Infrastructure attacks (man in the middle, DoS)



SECURITY NEEDS

DATA PROCESSING USE CASE

- Availability and Integrity are the primary needs.
  - The common requirement we have is no interruption shall exceed 5 min.
- Confidentiality comes after and is often limited to the Intellectual Property (algorithm or a subset of the data) – classified missions excluded.

So…

- Data processing solutions or architectures are built with performance in mind.
- Security is left to the surrounding infrastructure

« By default Hadoop runs in non-secure mode in which no actual authentication is required. »
https://hadoop.apache.org/docs/current/hadoop-project-dist/hadoop-common/SecureMode.html

Security features of Hadoop consist of authentication, service level authorization, authentication for Web consoles and data confidentiality.

And…

- Data processing infrastructure is connected to untrusted resources (multi-tenancy in community/public deployment).
- One component can compromise the entire « cluster », the provider can't be trusted.
- The Virtual Machine or computing node is the new boundary of the system.
- **So security must be integrated in the design pattern of the system.**
- Bonus : you have got new tools on your side (automation, APIs…)

SECURING THE CLOUD

Infrastructure Security

- Infrastructure needs to be trusted :
  - Use node authentication and configuration control
  - Private networks are required for non public facing resources
  - Automate deployment of security
- The code needs to be developed with multi-tenancy in mind (see OWASP for guidelines)
- Kill the resources you don't need

Data Security

- Information architectures
  - IaaS, PaaS and SaaS provides different solutions to store information
- Data Dispersion
- Information Management and lifecycle
- Confidentiality

Data Security

- Encryption for data at rest and in transit
  - Use client, servers or app encryption capabilities
  - VPN to the cloud, TLS for transports
  - Keep the control of encryption keys (prefer to use your own PKI)
- Data erasing
  - Provider's responsibility (certifications like SAS-70 cover this)

Access controls

- Use Identity & Access Management
- Maintain least privilege
- Create suitable roles for users and multiple access keys, security groups
- Identity federation & SSO from internal sources.
- Trace actions

Security monitoring

- The usual + cost monitoring
- Be prepared and ready for the coming incidents

Thanks.

CNES ?

- As a CNI operator, we are constrained by regulations.
- ANSSI will publish a cloud reference, applicable to FR public entities.
- Close to FEDRAMP and based on ISO 27002 security controls tailored to cloud.
- Two qualification levels
  - Secure Cloud : regular data → Suitable for mots Data processing cases.
  - Secure Cloud Plus : RESTRICTED SYSTEMS

Cloud Access Security Brokers