



Cloud Journey

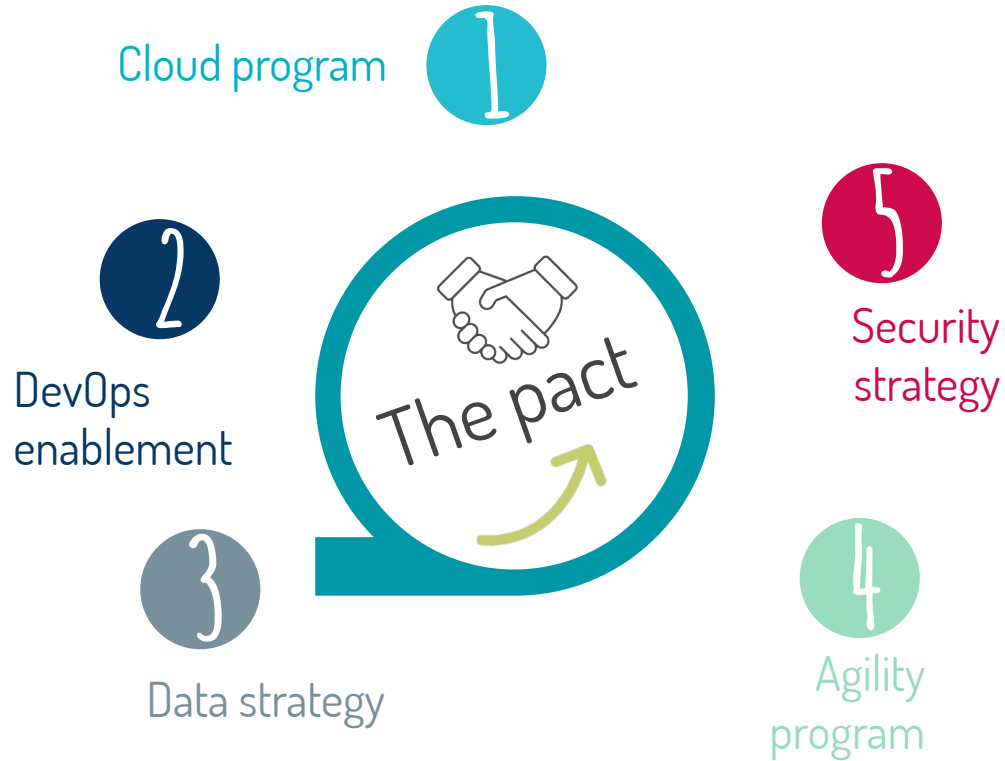
Net Centric 2020

How to quickly re-invent your offer in an uncertain environment?

Challenges for business








The facilitators of the pact



Cloud strategy

Challenges for Information System

Objectives for the IS: the contribution of the cloud

<p>Increase the agility of the business</p> 	  	<p>Time To Market Quick access to cloud services</p> <p>Adjust to customers, competition and the market Ability to develop what customers will adopt: Agility, Devops, cloud and Data / Analytics Measure the user adoption rate of new IS functionalities in order to reorient them</p>
<p>Release innovation</p> 	  	<p>Immediacy SaaS applications and PaaS and IaaS platforms for rapid experimentation</p> <p>Marginal cost savings Capacity and cost elasticity Virtually endless compute and storage capacities</p> <p>Open ecosystem Innovation at a steady pace</p>
<p>Compliance and security</p> 	 	<p>New regulations Compliance of cloud provider offers Cloud Provider Security Services</p>      

DevOps enablement

→ Devops achieves its objectives when the team culture, application and infrastructure architectures, processes, methods and tools have been adapted

Teams

Mixed and multidisciplinary composed of developers and operational staff
Focused on the culture of cooperation
Organized by functional area (features team) and small in size
(pizza team in You Build it you Run it)

Process et Methodologies

Continuous integration
Continuous deployment
New standards and methods of application development
focused on tests
Change review (IaC)



Architectures

Topologies and models adapted to the types of applications developed (Microservices)
Component standardization
Culture of measurement oriented towards business, application and at all levels

Tools

Code management
Infrastructure provisioning
Management of application and infrastructure configurations (IaC)
Monitoring (APM)

Data strategy quel soutien à la transformation ?

Challenges for Information System

Objectives for the IS: the contribution of the data

Have a global view of all data, varied, internal or external



Break the silots

Extraction and storage technologies that provide visibility global data, whatever the fields: contracts, customers, services, reimbursements, CRM, websites

Agility, variety of data sources and structures

NoSQL, structured or unstructured data: text, image, videos

Internal or external data

Internal or external sources: social networks, open data, partners

Enrich with new data over time

Use analytical and machine learning tools



Take advantage of technological offers in analytics and machine learning

Know the adoption by customers of services

Marketing segmentation based on objective criteria

Predict attrition

Increase the performance of marketing campaigns

Offer customers personalized offers

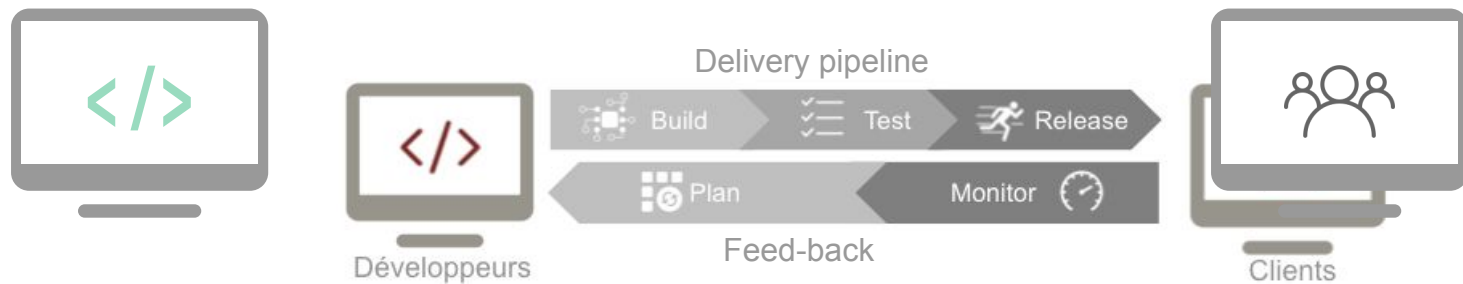
Compliance and security



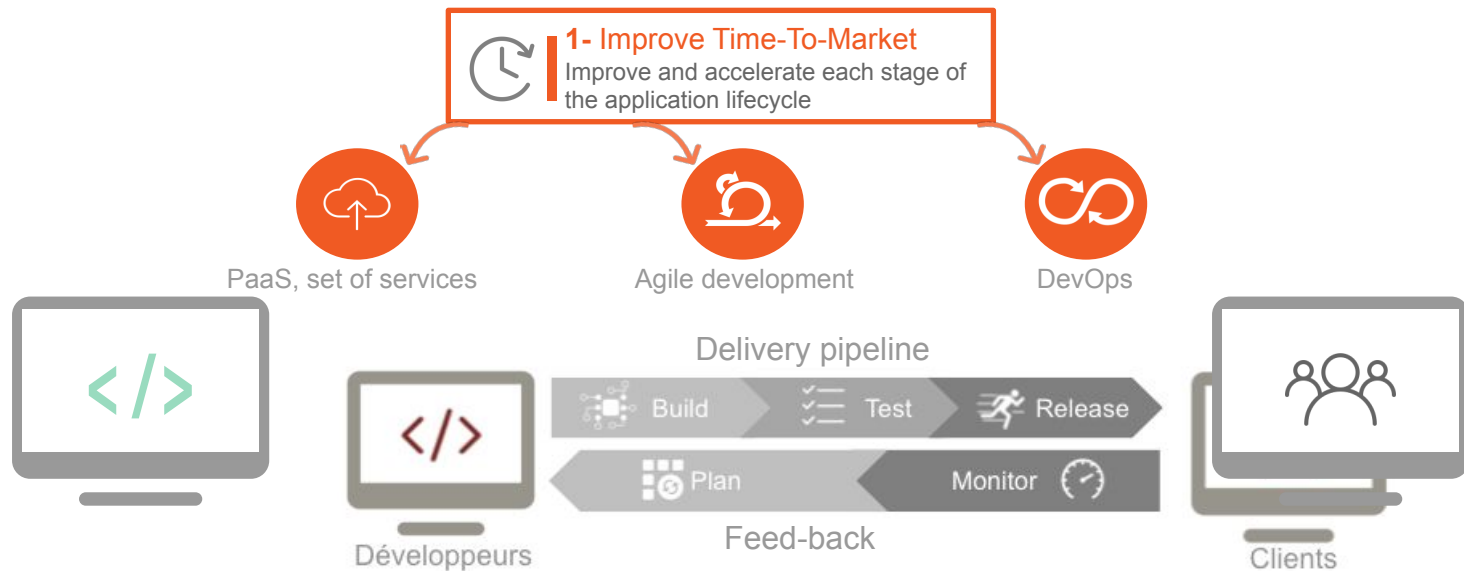
Regulatory compliance & Security

Hybrid solutions for housing regulatory data from suppliers with regulatory compliance

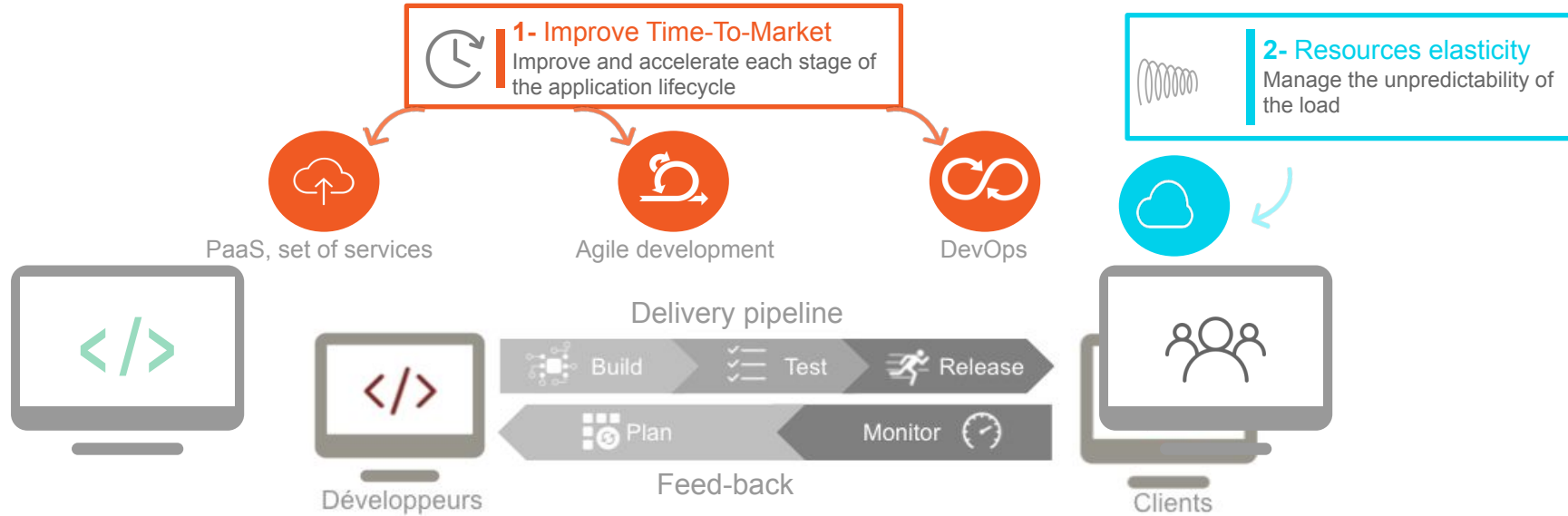
Agility program the value of agility



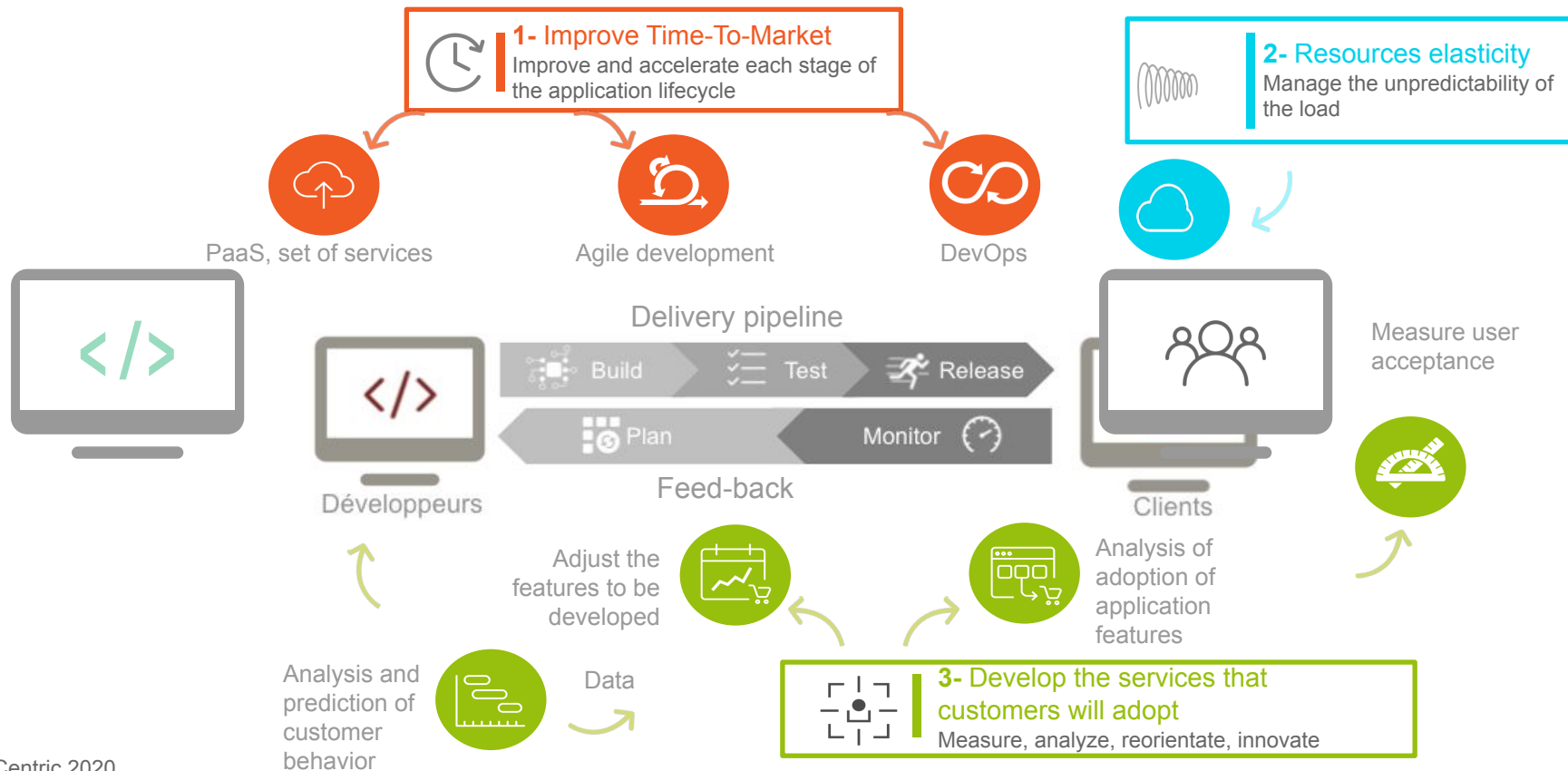
Agility program the value of agility



Agility program the value of agility



Agility program the value of agility



InfrasS security: new uses, new risks

1 Make infrastructure practices more flexible

An overly complex infrastructure leads to a decrease in profitability. It penalizes the growth of the company and slows it down in its innovation projects.

Each company must now have an inherent infrastructure management policy using new technologies to unleash innovation.

3 Facilitate new uses

Digital technology has developed through a series of technological innovations that continue to accelerate. Mobility, the cloud, data, connected objects and social networks are now the foundations of digital.

We must take advantage of these opportunities to promote and embrace the emergence of new services.

2 Monitor, secure, anticipate & deal with threats

Regardless of its size, a business needs to realize that it will face cybercrime. Whether it is, for example, malicious acts aimed at destroying data or economic and industrial espionage.

We must put in place all the measures (proactive and reactive) to anticipate and deal with the different types of threats.

4 Promote mobility

It is no longer necessary to have a data center to develop your business, a new way of consuming IT resources is born. Resources become services that we use according to our needs.

Our success depends greatly on our ability to provide exceptional quality of experience to end users (employees, customers, prospects and partners).



Fortified Castel VS Airport

Actual model

Fortified castle



Mindset

- The danger is seen from afar and comes from outside.
- A wall reduces penetration and only one access point is possible
- The only access point is static and heavy to handle: drawbridge
- Security relies on the surveillance of the guards on the walls
- There are patrols of soldiers inside for possible disturbances
- The treasure is kept in chests
- The peasants go to the fields which are not protected

Build

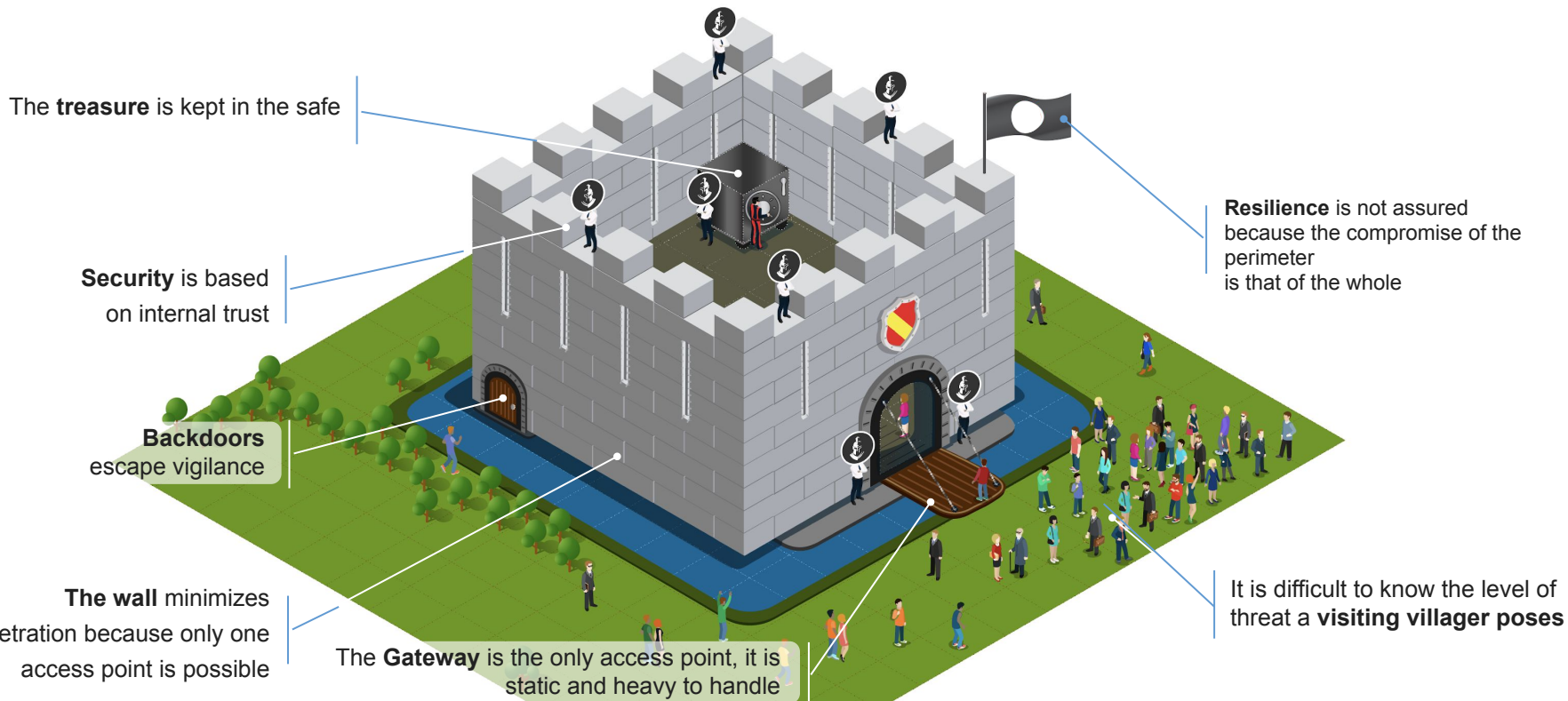
- Perimeter defense: PKI on workstations, authentication on a single forest and firewall between the outside and the inside
- The firewall is static and its management complicated
- Safety relies on safety and security committees
- IDS probes identify the most obvious attacks
- Workstations have an antivirus but can be corrupted

Conclusion

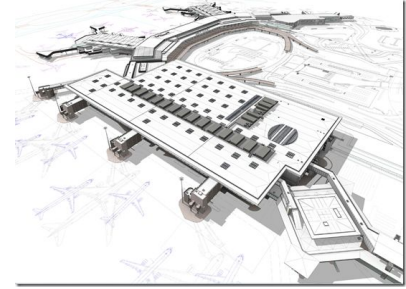
- A compromised user station can nevertheless authenticate itself correctly and access everything, potentially contaminating everything
- 802.1x protects the LAN well but is cumbersome to deploy and requires IPsec to differentiate the level of security
- The security implemented is perceived as a constraint (budget, mobility)

Le modèle « château fort »

Une protection périmétrique qui ne nous protège plus assez



Airport model : security by design



Mindset

- The risk is everywhere and sometimes very close. We must react quickly
- The movement of people and goods is necessary for business
- The access points are multiple and adapted to each mode
- Security applies to a large volume and must be efficient
- Safety relies on personnel assisted by tools
- Safety is combined
- In the event of a proven risk, the appropriate procedure is implemented quickly and efficiently

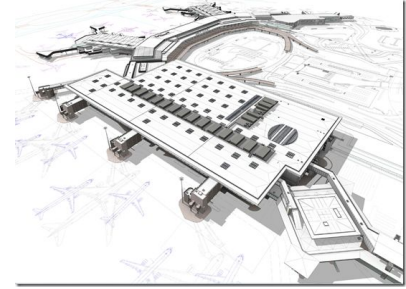
Build

- Use of micro-segmentation
- Defense by design
- Security by contract: partner, branch, subsidiary, application
- Each user has a precise list of accessible IT resources according to their equipment
- Automation, AI programming, machine learning processes the volume
- Risk analysis is more fluid
- Collaborate with cells that share the same security interest
- Event driven architecture: the areas are modified to limit the risk and allow intervention

Conclusion

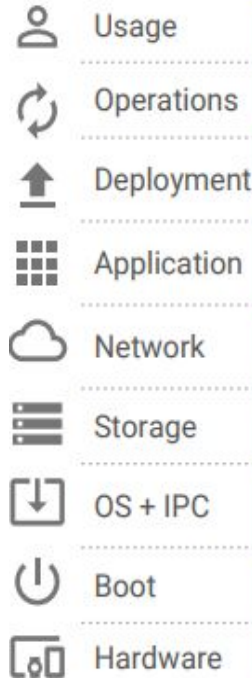
- The danger is contained in the application bubble.
- Everything is monitored in a differentiated way and according to the context
- Ready for the Internet of Things, possible leverage on Big Data
- Security is consistent regardless of volume and desired performance
- Experts write rules and protocols
- Defense takes into account the user journey
- Assets can be moved and protected dynamically

Airport model : security by design



Mindset

- The infrastructure is made up of areas that can potentially be compromised
- The breach must be detected quickly and contained
- Each zone is informed in real time of the confidence level of the other zones
- Users can move freely in the areas provided they meet the security conditions for each area
- Security monitoring is ongoing and may result in immediate revocation of access



Framework

- Zero trust: authenticate, authorize and audit continuously without assuming identity
- ABAC: continuously identify risks based on equipment attributes and behavior
- Micro-segmentation: fine-tuning of flows in the IS regardless of network addressing
- Security by contract: the level of security depends on the contract
- Security by design: new applications, IoT, Big Data ...
- AI, machine learning: security is regulated with the volume to be processed
- Defense in depth: frontline surveillance and multiple coordinated and orderly lines of defense
- Event driven architecture: the architecture changes in reaction to events, eg. security breach
- Automation of actions for responsiveness and workload



Control Tower



Zone 1

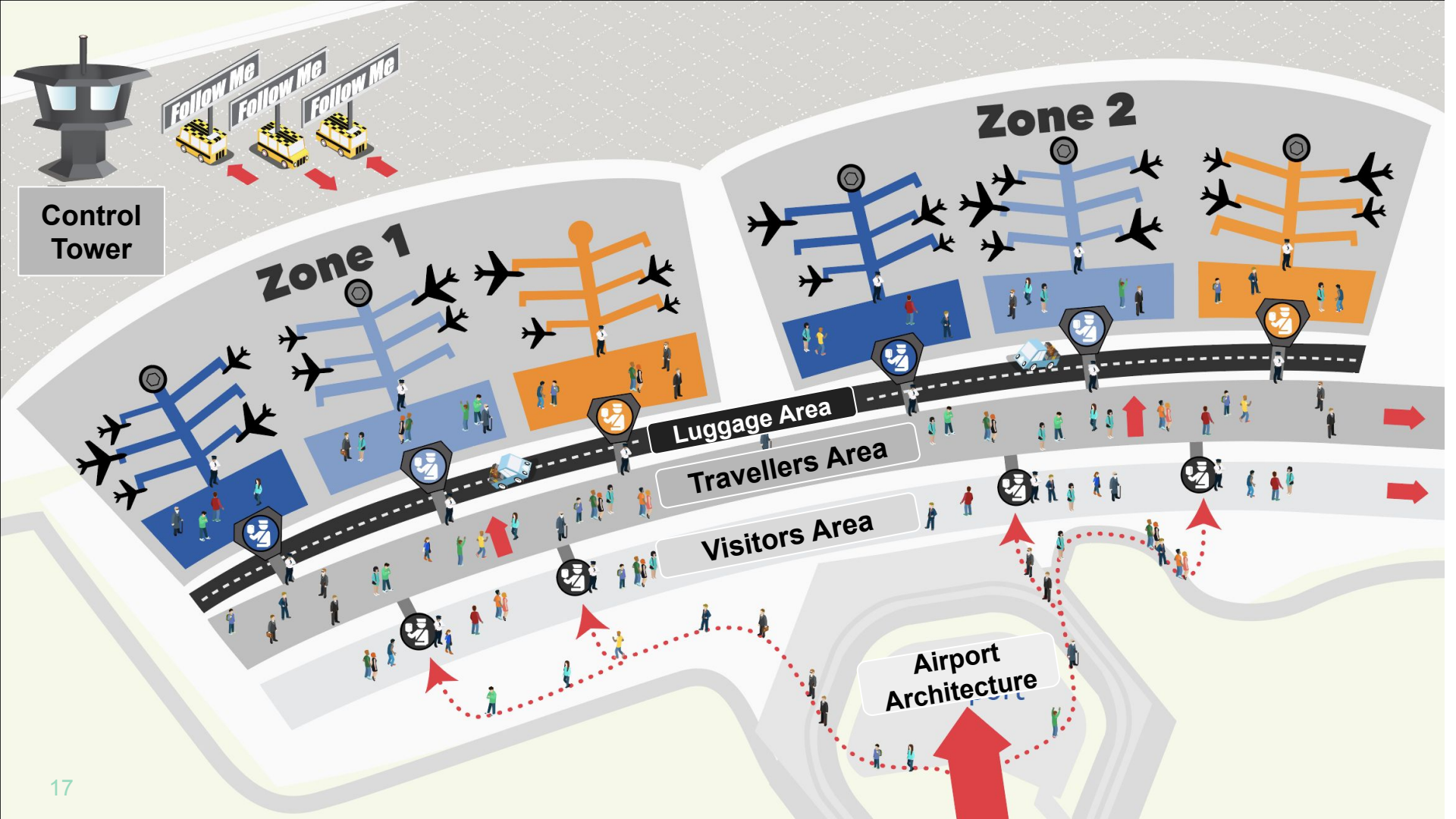
Zone 2

Luggage Area

Travellers Area

Visitors Area

Airport Architecture





Fouad Guenane
Infrastructure Management expert
fouad.guenane@gmail.com



Questions