inetum realdolmen

Positive digital flow

"La Cybersecurité, une vaccination pour votre environment digital"

General program introduction

30/03/2022

Program overview

1 Security market watch “Understanding the trends, challenges & threats”

Goal: Understanding the challenges and risks you face by clarifying and becoming aware of the impact and likelihood of threats

By: Inetum-Realdolmen – Thomas Tardieux

2 Security vision ”How to navigate your security transformation”

Goal: Gaining practical insights in how you can approach your digital security transformation journey to improve your security posture and support the hospital business objectives

By: Inetum-Realdolmen – Thomas Tardieux

3 Achieving adequate cybersecurity in Healthcare with Microsoft technology

Goal: Gaining insights in achieving adequate cybersecurity in healthcare

By: Microsoft – Jonathan Jacqmin & Nadia Aime

inetum realdolmen

Positive digital flow

Security Vision

How to navigate your security transformation

Content

1 Security transformation and the shift

2 How to start your security transformation journey

3 Key Takeaways

1

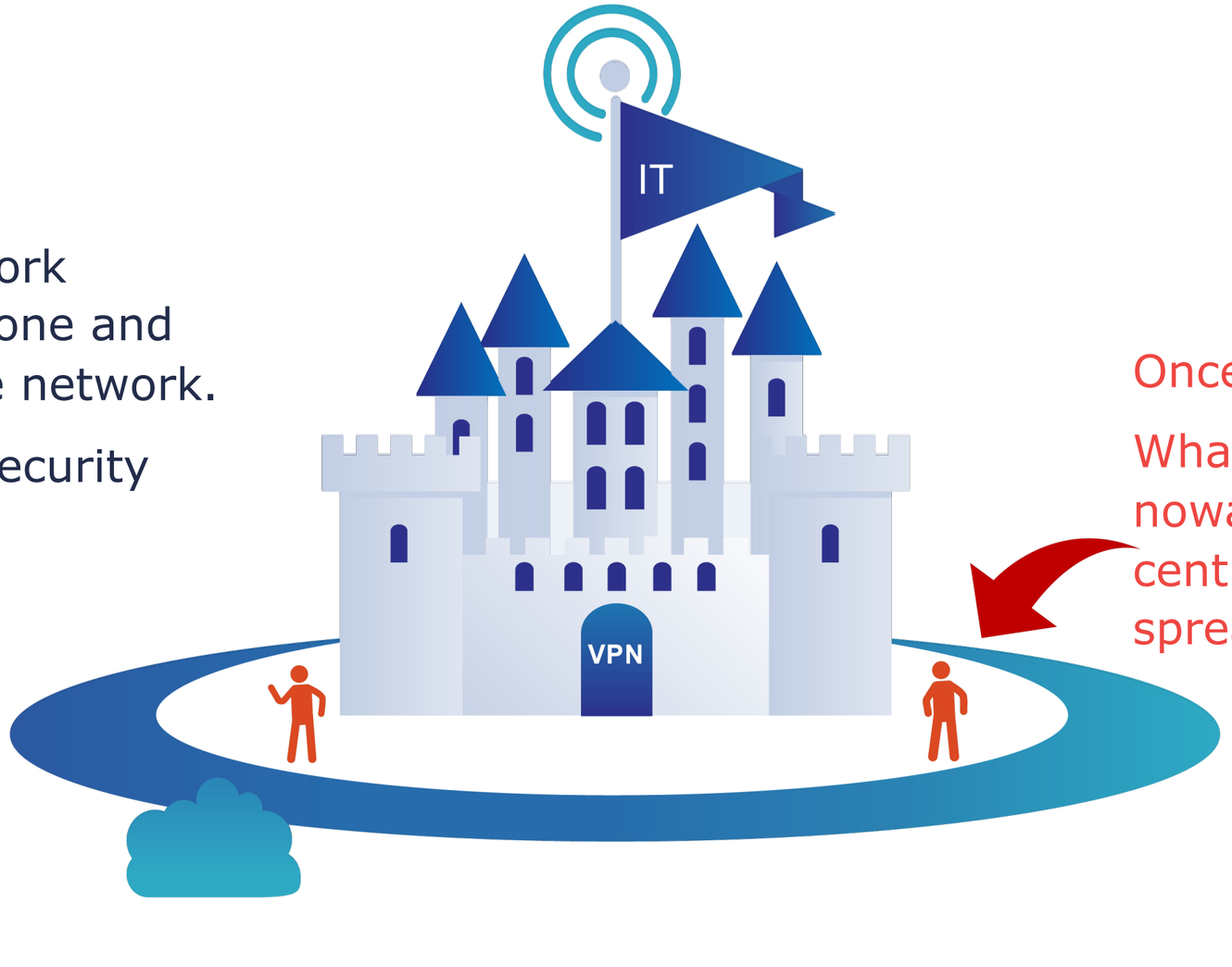
Security transformation “the shift”

from a traditional security to modern security approach

Traditional security in the “Old Days”

Traditional IT network security trusts anyone and anything inside the network.

Castle-and-moat Security model



Once an attacker is in, they're IN.

What makes things worse, nowadays your data is no longer centralized in the castle, but spread across the Cloud.

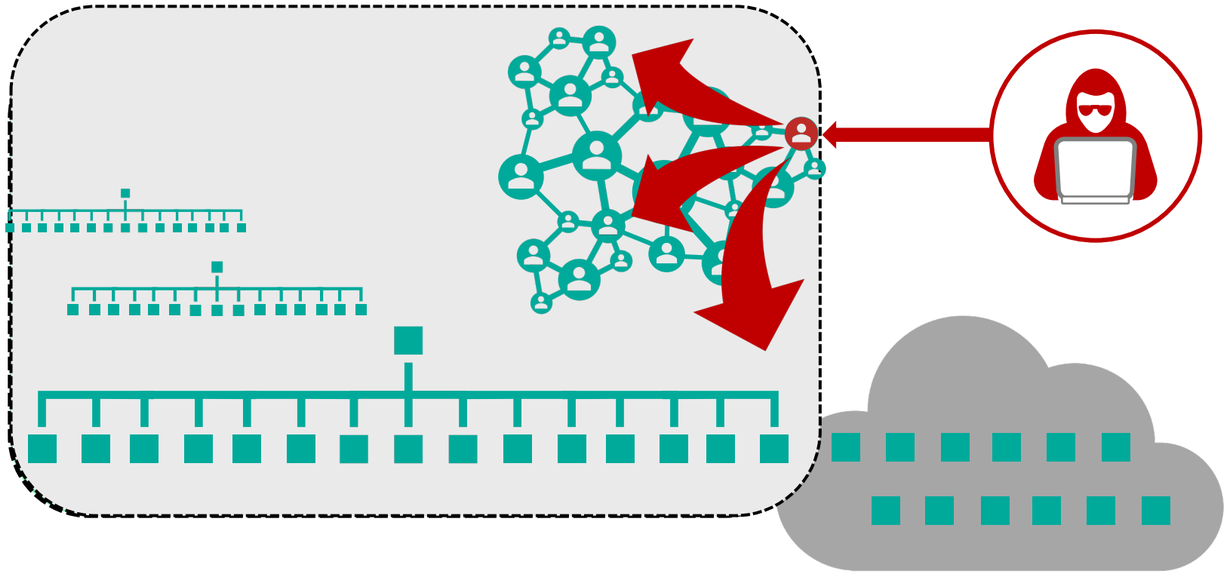
Why shift to a new modern approach?

The world has changed

~~Users are employees~~		Employees, partners, customers, bots
~~Corporate managed devices~~		Bring your own device and IoT
~~On-premises applications~~		Explosion of cloud applications
~~Monolithic applications~~		Composite apps and API’s
~~Corp network and firewall~~		Expanding perimeters
~~Local packet tracking and logs~~		Explosion of signals
~~On premise solutions~~		Containerized solutions, microservices

Attackers shifted already

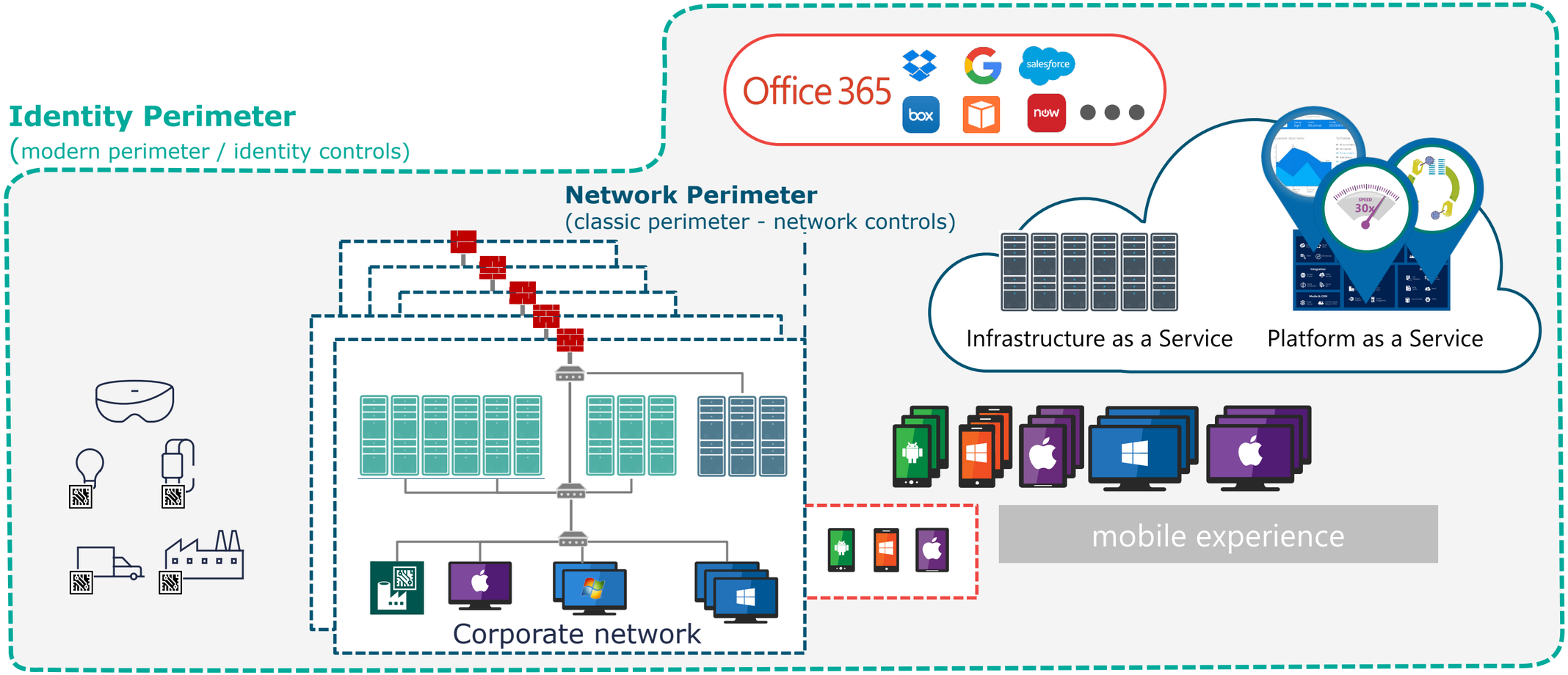
Evolution of the the modern workplace and the attacker's response



1. **IT Security is Complex**
   - Many Devices, Users, & Connections
2. **"Trusted network" security strategy**
   - Initial attacks were network based
   - *Seemingly* simple and economical
   - Accepted lower security within network
3. **Assets increasingly leave network**
   - BYOD, WFH, Mobile, and SaaS
4. **Attackers shift to identity attacks**
   - Phishing and credential theft
   - Security teams often overwhelmed

Access Control: Keep **Assets** away from **Attackers**

So we need a new security perimeter



New reality needs new security mindset

Security mindset shift

- Security is **essential** to evolve as an organization in the **digital transformation** era and become digitally, secure and resilient
- Security is essential to **protect the trust** that is needed in customer, partner and employee relationships in order to do business
- Security is a **business enabler** and **protecting business assets and goals** of the organization by reducing risks to acceptable levels and allowing business to make use of new technologies to stay relevant. So, all **about staying safe while doing what is needed to stay relevant.**
- Security is not only protecting profitability and reputation but also good for **sustainability (ESG score)** and **shareholder value**

New reality needs new security approach

Security approach shift

- Security approach needs to evolve from a solely maturity-based approach to a **business risk driven security approach**
- Embedding **zero trust approach** on top of your traditional approach

NEVER TRUST, ALWAYS VERIFY

ZERO TRUST

New reality needs new security principles

Zero trust principles

Verify Explicitly

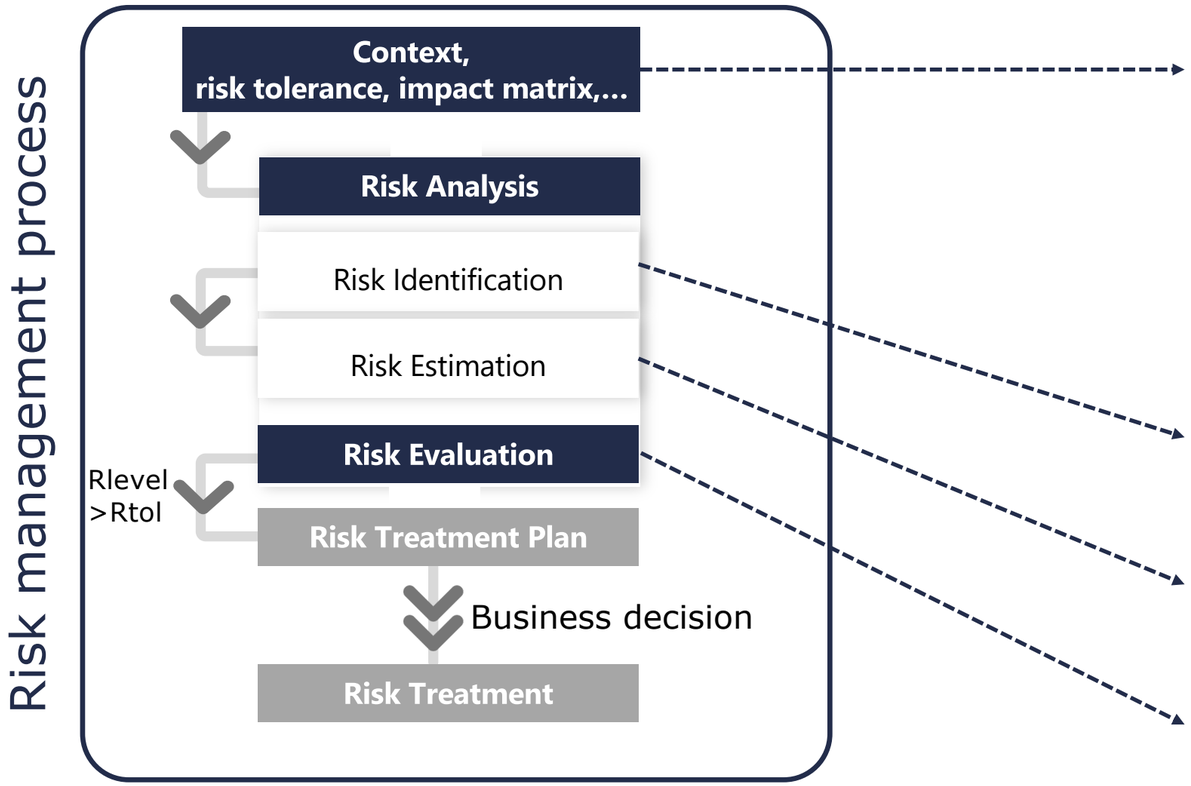
Least Privilege

Assume Breach

Zero trust is an integrated approach to securing access with adaptive controls and continuous verification across your entire digital estate

Risk, the essence of your security approach

Business risk driven security to find the **right balance** and set the **right priorities** that support the realization of the business outcomes most effectively by **protecting the trust to do business**



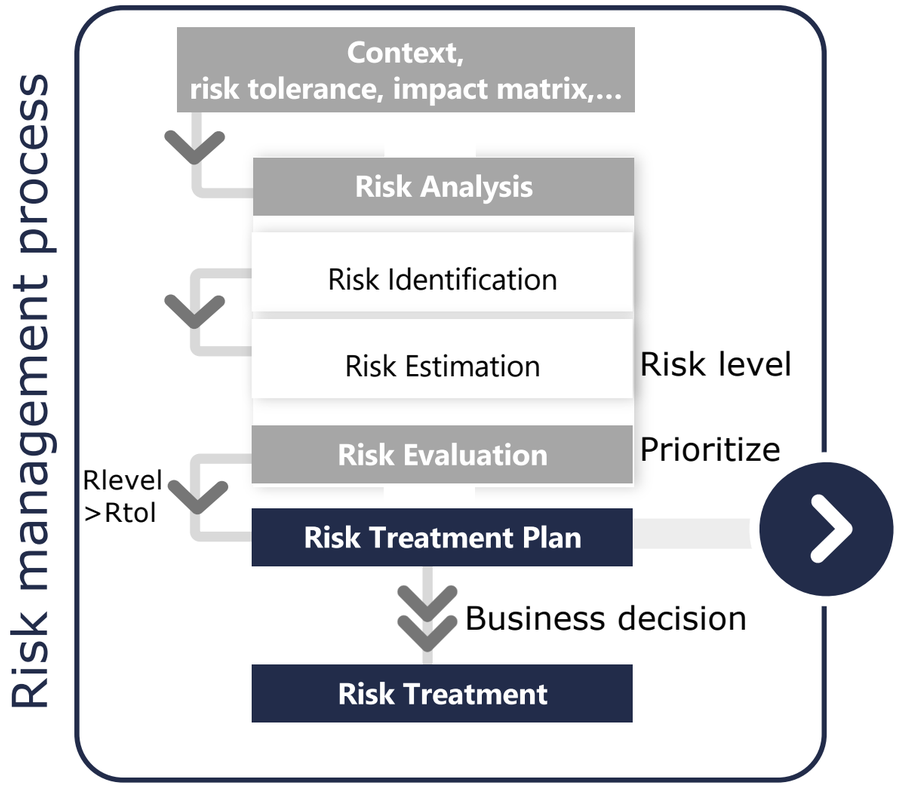
Know
- your risk appetite
- your risk tolerance levels
- your business impact matrix
- the criticality of your assets
- who is responsible for risk management process
- who is responsible to take decisions

- **Identify risks** based on scenarios or dynamic input from your environment and risk events

- **Determine** the risk level

- **Evaluate and decide** if you are going to treat the risk or not

Risk, the essence of your security approach



Some important security measure to consider

Risk mitigation measures

1. Endpoint protection:
2. Network protection: segregation and micro segmentation
3. Identity protection: MFA
4. Access control: least privileged acces
5. Monitoring and detection controls
6. Infrastructure: Vulnerability management and patching

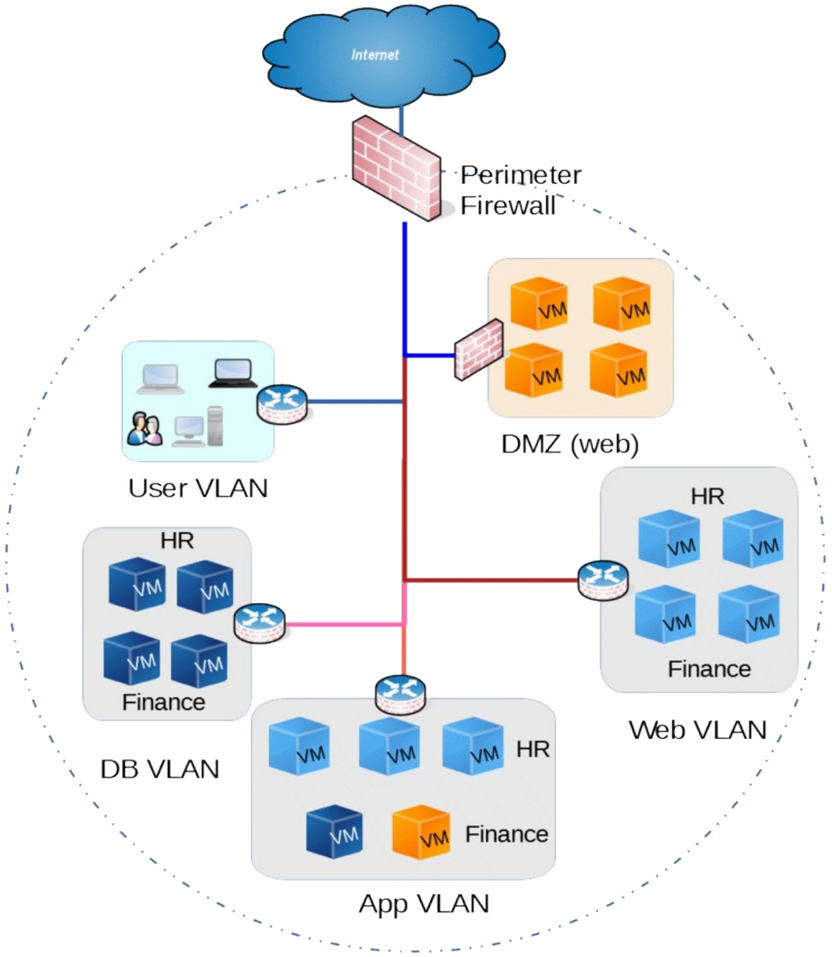
…

1. Endpoint Protection & Security

- The endpoint is untrusted
- Proper endpoint management in place to ensure device has proper security controls.
- Only approved devices are used
- Private key material is properly secured

2. Network security: segmentation

- Use micro segmentation to to maintain security
- Break security perimeters up into smaller regions on separate parts of the network based on data classification with separate access
- Users can't access different zones without extra authentication



3. Identity protection: MFA

- Cornerstone of Zero Trust
- Ensures users are properly validated before being granted access
- Uses hardware to fight credential phishing and impersonation

4. Access Control & least privilege acces

- Minimize attack surface
- Strict controls on user and device access
- Monitor devices and users
- Provide the least privilege to do the job

Least privileged access

- Minimize exposure between sensitive parts of the environment and give users only the access they need
- Never trust, always verify
- Need to know basis
- Part of wider IAM strategy

5. Monitoring and detection controls

- 24x7 monitoring
- SIEM/SOC services
- (M-)XDR services

2

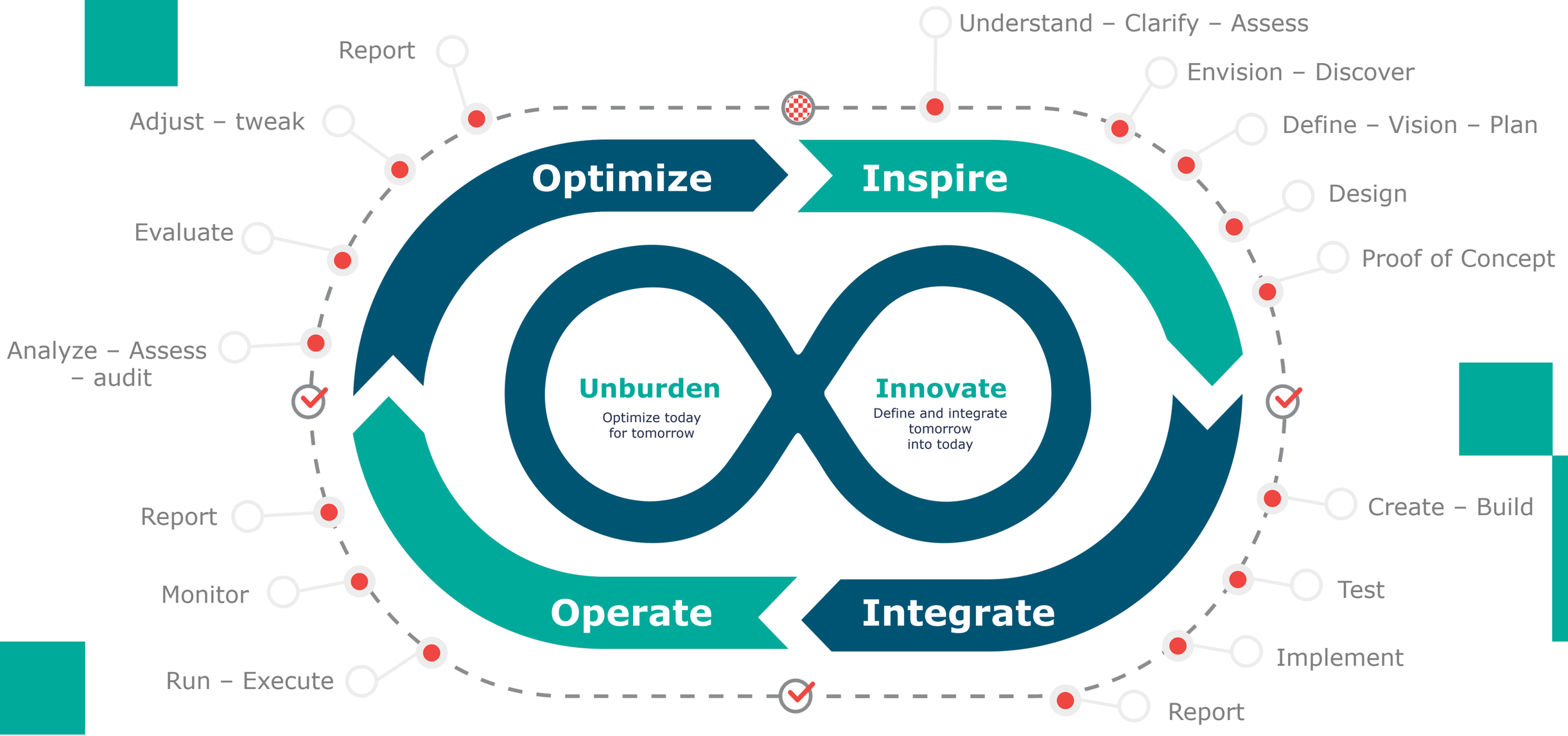
How to start your digital security transformation journey

and make the shift

Security transformation principles

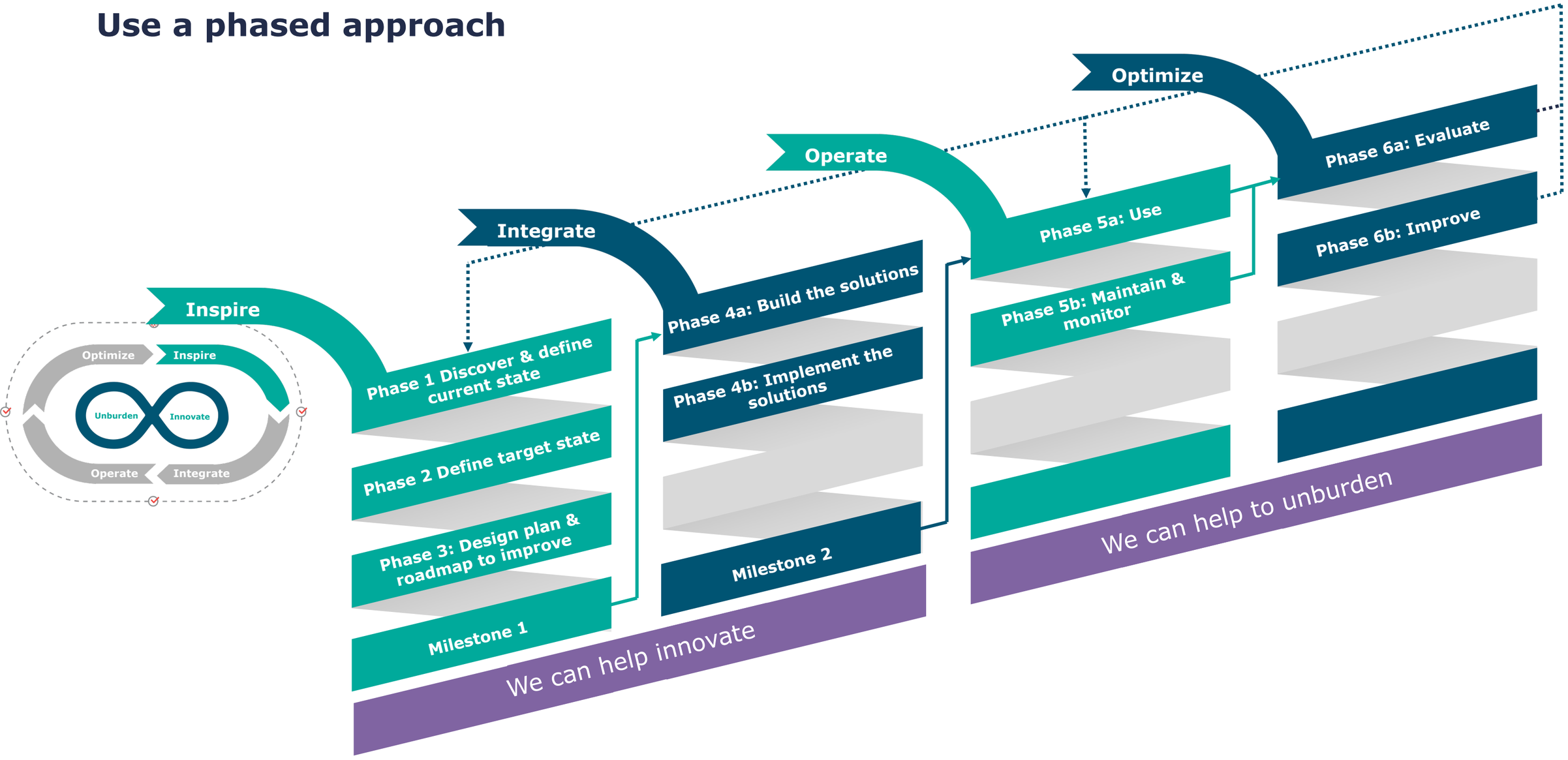
1. Start small and Keep pace
2. Use a business risk driven approach
3. Keep focus on the business value
4. Plan and position for change
5. Shift to zero trust in a controlled way
    1. Improve your security foundations to become transformation ready
    2. Shift to trust but verify
    3. Shift to full zero trust: never trust always verify

Use the 4x4 digital security transformation accelerator model to drive your transformation



Security transformation phased approach

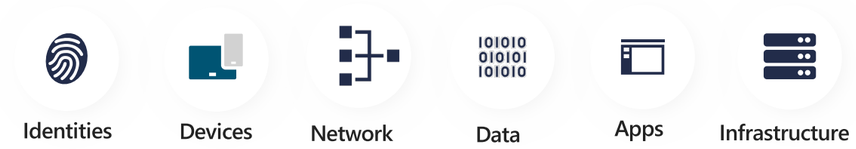
Use a phased approach



How to start with your first journey?

Journey 1: improve foundations

Select the technology domain you find important to look into



Don’t know where to start?

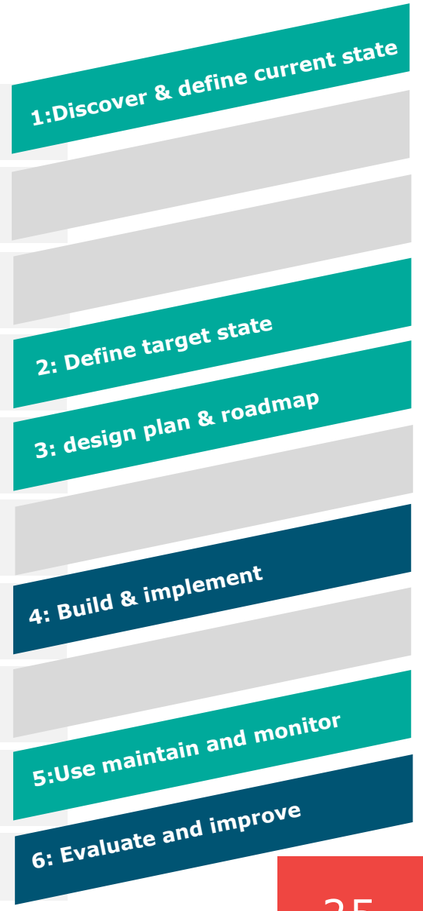
- Assessment cross domain
- workshop
  - discovery
  - envision
  - strategy
  - risk

How to start with your first journey?

Journey 1: improve foundations

Then use the phased approach and follow these steps

1. Run technical scans and penetration test on your assets (in function of specific domain or cross domain)
2. Execute Assessment (focus on architecture / zero trust / specific assets or domain)
3. Analyze results and findings of step 1 and 2
4. Define security transformation baseline to be reached
5. Analyze and evaluate risks
6. Build security improvement roadmap in function of business impact (risk) and business value (baseline)
7. Build and implement quick wins and key improvements
8. Activate improvements and release to operations
9. Operational use ; maintenance of new technology / improvements ; monitoring
10. Assess, evaluate, optimize if needed and good for productivity / risk mitigation / next transformation preparation



Always keep zero trust principles in mind

3

Key Takeaways

Key Takeaways

Security transformation
Start small
Keep pace
Start your flow

Go for zero trust in a controlled way

Use a business risk driven security approach

MORE THAN
27 000
CONSULTANTS

2019 (Pro Forma)
€ 2.3
BILLION
IN REVENUE

26 COUNTRIES

FRANCE, SPAIN, PORTUGAL, BELGIUM, MEXICO, LUXEMBOURG, POLAND, MOROCCO, ROMANIA, SWITZERLAND, BRAZIL, TUNISIA, COLOMBIA, COTE D'IVOIRE, PERU, USA, ANGOLA, CAMEROON, SINGAPORE, ENGLAND, UAE, RP OF PANAMA, CHILI, COSTA RICA, DOMINICAN REPUBLIC, ARGENTINA

6
ACTIVITIES

+ **CONSULTING**
+ **APPLICATION & INFRASTRUCTURE SERVICES**
+ **SYSTEM INTEGRATION**
(Business Solutions, ERP, CRM, PLM...)
+ **OUTSOURCING**
+ **VALUE ADDED RESELLING**
+ **SOFTWARE:**
  - 4 vertical solutions :
    Local governement, Insurance, Healthcare social, Retail
  - Transverse Solutions
    Time Management (Chronotime)
    DDM (Business Document)

MORE

+ Proximity-Intimacy-Agility
+ Industrialisation-Automation
+ Innovation-Business

5
VALUES
& PRINCIPLE
OF ACTION

SOLIDARITY
We have a united entrepreneurial spirit.

AMBITION
Our local power fosters our global success.

EXCELLENCE
Our culture of excellence is a product of our daring.

ENGAGEMENT
We grow but stay close to our clients.

INNOVATION
We are constantly co-inventing the technology based business of our customers

Thank you!
Time for questions

6 INNOVATION CENTERS

PARIS, NANTES, LYON, GHENT, LISBON, MADRID

Casablanca & Warsaw in 2021

GROUP ALLIANCES

SAP, Microsoft, Oracle, Salesforce

AWS, IBM, Sage, HRAccess

PTC, Siemens, Dassault

21 SERVICE CENTERS

APAC (*Macau*) ▪ **BRAZIL** (*São Paulo*) ▪
COLOMBIA (*Bogota*) ▪
FRANCE (*Lille, Lyon, Meudon, Nantes, Toulouse*) ▪
INDIA (*Pune*) ▪ **MOROCCO** (*Casablanca*) ▪
POLAND (*Warsaw-Poznan-Lublin*) ▪
PORTUGAL (*Lisbon-Covilha-Bragança*) ▪
ROMANIA (*Bucarest-Constanza*) ▪
SPAIN (*Alicante-Bilbao*) ▪ **TUNISIA** (*Tunis*)

10 GROUP PRACTICES

DIGITAL BANKING ▪
DIGITAL INSURANCE ▪ DIGITAL RETAIL ▪
DIGITAL UTILITIES ▪ E-HEALTHCARE ▪
INDUSTRY 4.0 ▪ SMART CITIES ▪
DIGITAL TELECOM ▪
DIGITAL TRANSPORT ▪
SMART DATA & AI ▪

7
BUSINESS SECTORS

- FINANCIAL SERVICES
- INDUSTRIES
- PUBLIC-HEALTHCARE
- TELECOM-MEDIA-TECHNOLOGIES
- ENERGY-UTILITIES-CHEMICALS
- RETAIL-CONSUMER GOODS
- TRANSPORTATION-TRAVEL-SERVICES

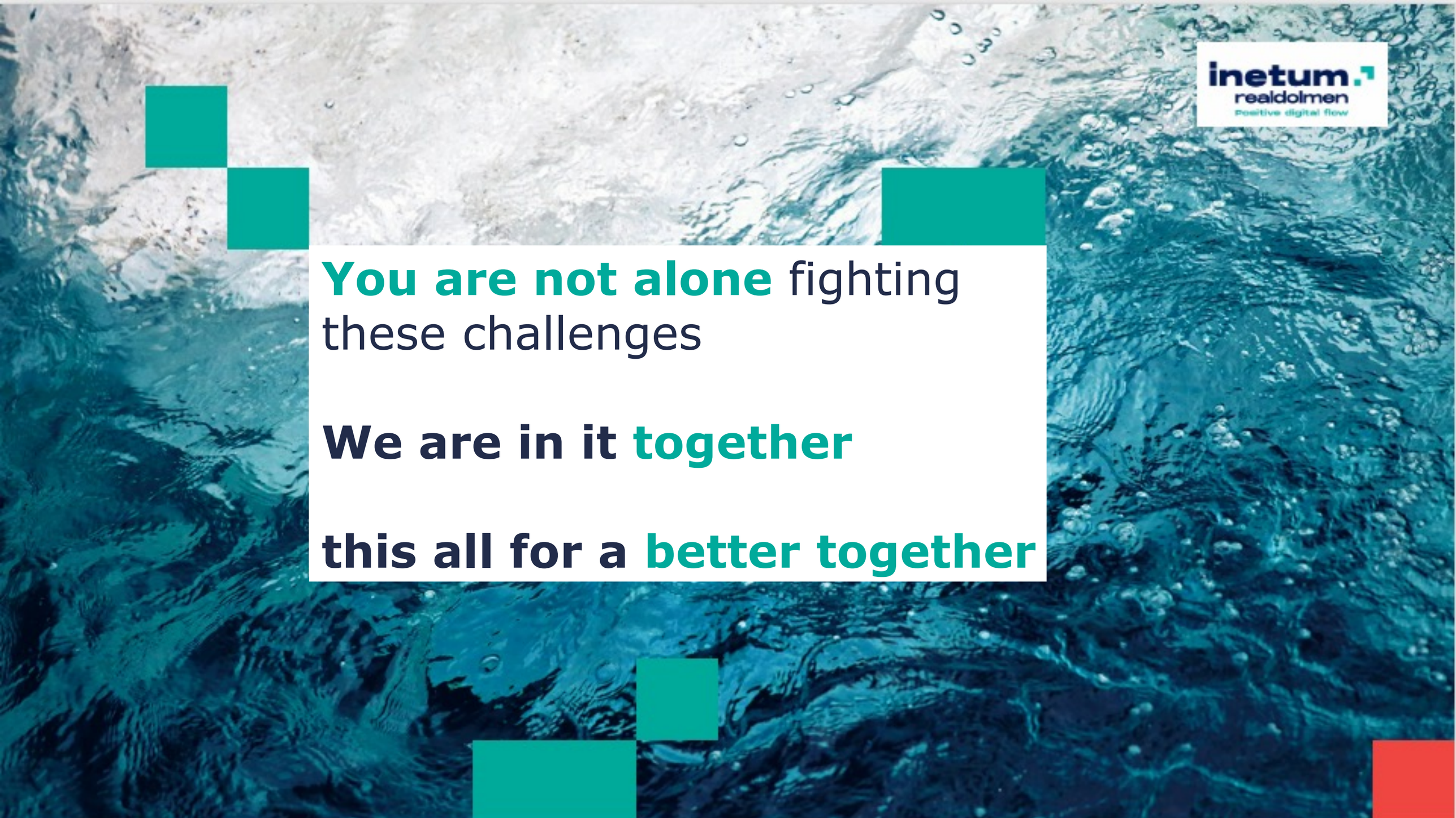
HANDBALL

SPONSOR

Inetum is Top Sponsor of Paris Saint-Germain Handball

October 2020
@2020 Inetum
V. 14/10/2020

For more information: **inetum.world**


inetum.
realdolmen
Positive digital flow
You are not alone fighting these challenges
We are in it together
this all for a better together

inetum
realdolmen
Positive digital flow

inetum.world

FRANCE | SPAIN | PORTUGAL | BELGIUM | SWITZERLAND | LUXEMBOURG | ENGLAND | POLAND | ROMANIA | MOROCCO | TUNISIA | SENEGAL | CÔTE D'IVOIRE | ANGOLA | CAMEROON | USA | BRAZIL | COLOMBIA | MEXICO | RP OF PANAMA | PERU | CHILI | COSTA RICA | DOMINICAN REPUBLIC | ARGENTINA | SINGAPORE | UAE