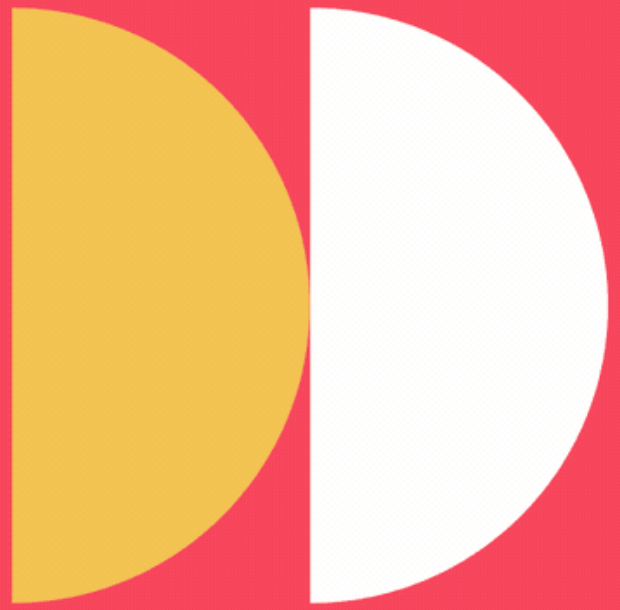
devoteam

# Digital Workplace

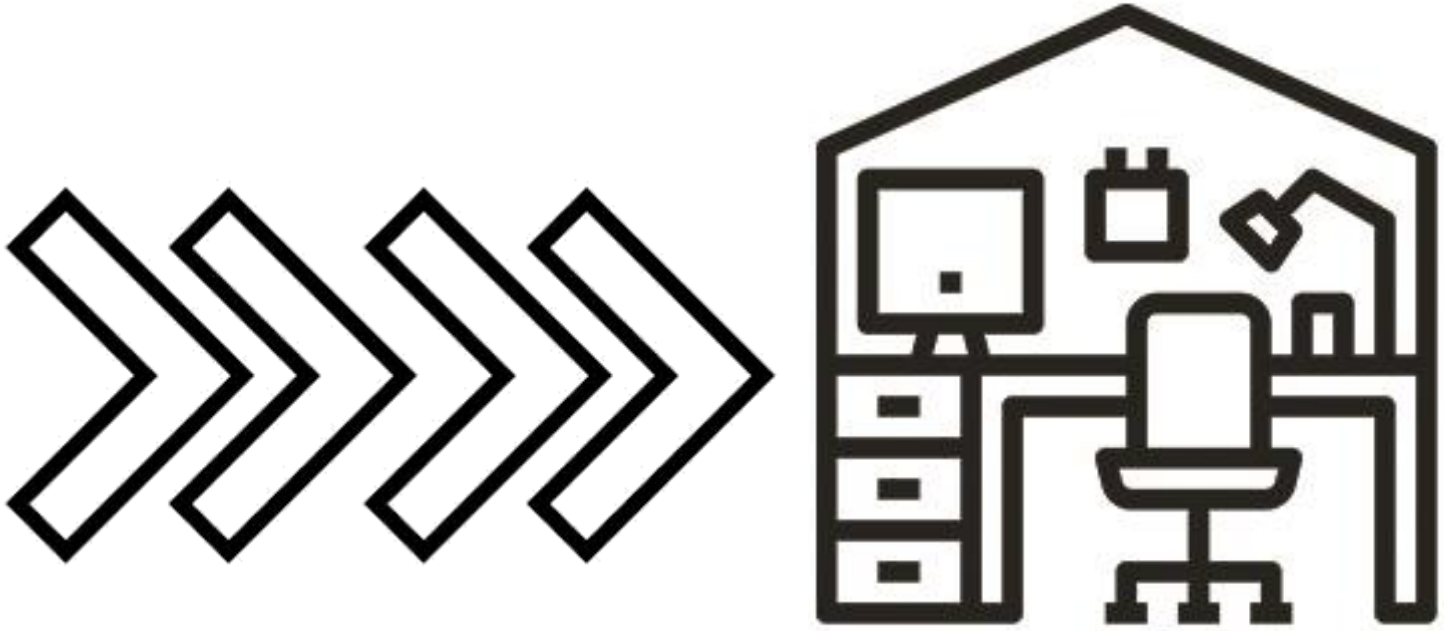
## Security Assessment

**Joey Bergen & Potmans Olivier**

**April 20th, 2020.**



**Innovative technology consulting for business.**



***Covid has accelerated the Shift to the remote work...***

# How to become **productive** in a Remote Working?

## Secure Connection

Which create a link between the laptop and the Digital Workplace and guarantee the isolation from the untrusted network

## Self Motivation & Discipline

Put in place daily plan to prevent the procrastination and find a good balance between the work and the private

## Mobile Device

Laptop owned by the company for example for the mobility with a good Internet connection

## Digital Workplace

Including the Apps, the Office and the communications tools (chat – videocall – phone) and a controlled access to the data assets.

## Objectives Oriented

Switch from Time management to objectives management weekly defined according to a S.M.A.R.T approach

# Three possible situations

## Quick and Dirty

Not well prepared for this crisis, your employees are forced to find quick and dirty solutions to work


This is the worst situation because beside the shadow IT which is not controlled by the company. Example: Use public collaborative video conf call (ex: Zoom), use your private address, office and drive to store company data.

## VPN & Citrix

Objective is not changing how the processes work but improve it. Make existing process more efficient, faster and cheap is valuable for the Business.

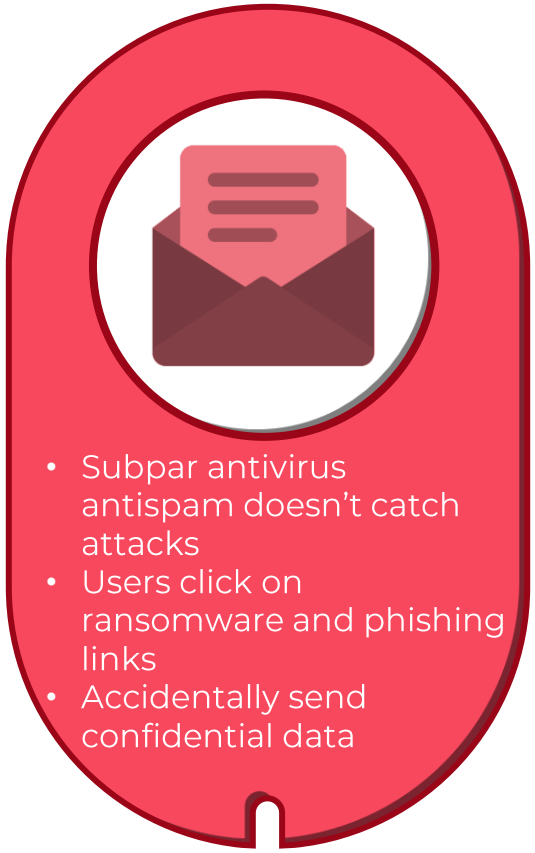

Seeing the company was forced to move all the workforce on the VPN, it's clear that the infra is undersized. Is the endpoint also secure?

## Office 365 & RemoteAPP

The company migrated Office & Collaborative tools on Office 365 and use Remote Desktop on Azure.

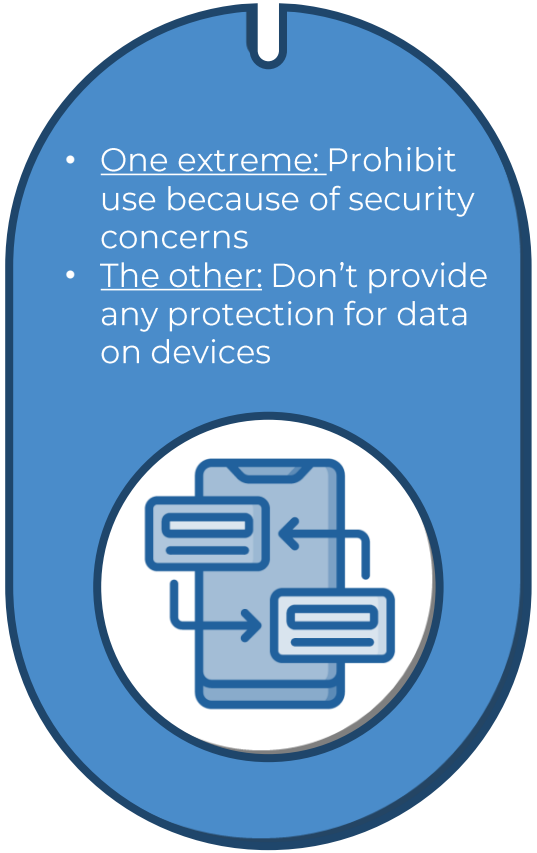
This is best approach to manage that crisis. The partner cloud absorbs the load and your employees can work but are you sure to be totally safe and GDPR compliant?

# What are the main « Remote Work » **Security Risks** ?



- Subpar antivirus antispam doesn't catch attacks
- Users click on ransomware and phishing links
- Accidentally send confidential data

## EMAIL



- One extreme: Prohibit use because of security concerns
- The other: Don't provide any protection for data on devices

## MOBILITY

- Users have same passwords across all accounts, increasing risk if compromised (no MFA)
- Attackers have sophisticated methods to easily steal credentials

## CREDENTIALS

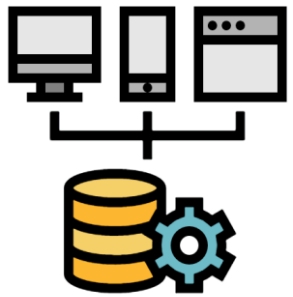
- Standards don't change based on company size
- Requirements for GDPR and other regulations are rigorous and complex

## REGULATION

# Digital Workplace **Security** Offers

## **People** focus

Propose a Cyber Awareness program to ingrain in the culture of the company employees the importance of protecting sensitive information, the management of the information in a secure way and the risks of mishandling the information.



## **Platform** focus

Propose an audit of Office 365 implementation to measure the Maturity Level of your Digital Workplace Security including a full assessment of the 3P (People – Process - Platform and an evaluation of the respect of GDPR regulation.

# What's our **Methodology** ?

Business Stakeholders

Security Maturity Target

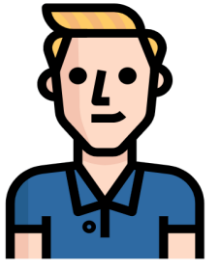
Gap Analysis

Roadmap Planning

Security Maturity

Collaboration

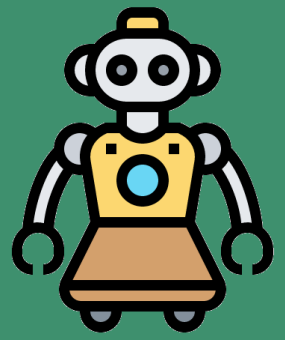
IT Stakeholders



Security Maturity Assessment

Security Maturity Enhancement

# What are the **Tools** used during this assessment ?



## Agents

The agents will scan the critical assets (AD – Azure AD - Office365 – SharePoint endpoints) and delete themselves once the job is done

The effort required from the internal IT department is kept to the minimum.

## Questionnaires

A set of questions to ask to the different stakeholders (IT & Business) to capture the requirements and assure the 3P are considered in the assessment.

# What's the **timeline** of an Assessment ?

- Organisation of the Kickoff with the different stakeholders to present the assessment, the definition of the interview planning and the technical requirements.
- Install & configure the Agents to audit the infrastructure

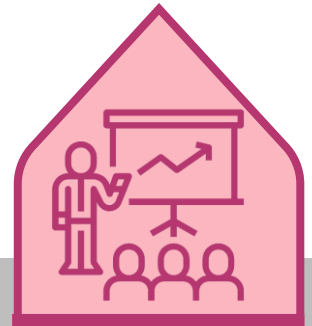
**Day 1: Kickoff**

**Day 2: Capture**

Consolidation of the Data captured by the different agents and interview with the different stakeholders (Business & IT)

- Analysis of the data captured during the interview and the agents.
- Redation of the report which determine the maturity level
- Roadmap Definition

**Day 3: Report**



**Day 4: Press**

- Definition de la presentation Powerpoint
- Presentation to the Business/IT Stakeholders

# Conclusion

## Devoteam proposes an Security Audit of your Digital Workplace

**BASED ON AN ASSESSMENT** 1

combining automatic Data Capture by Infrastructure Agent and interviews with the stakeholders (Business & IT)

**WITH AS DELIVERABLE A REPORT** 2

Based on the analysis of the data captured during the assessment and presented to the different stakeholders

**AND A ROADMAP** 3

to initiate a project based on the recommandations to improve the maturity level of the Digital Workplace

**GIVING YOU THE INSURANCE** 4

that your Digital Workplace has the expected security level of maturity and is compliant with the GDPR Regulation.

# Questions?


thank you.
#TechforPeople.
devoteam

#TechforPeople.