

Microsoft Security Porfolio

Get the best out of Microsoft Defender for Endpoint



Agenda



Introduction

- Business →Trust →Security
- Devoteam Security Portfolio

IAM = Security Foundation

- IAM Fabric Definition
- Microsoft IAM = Azure AD

Microsoft Defender for endpoint

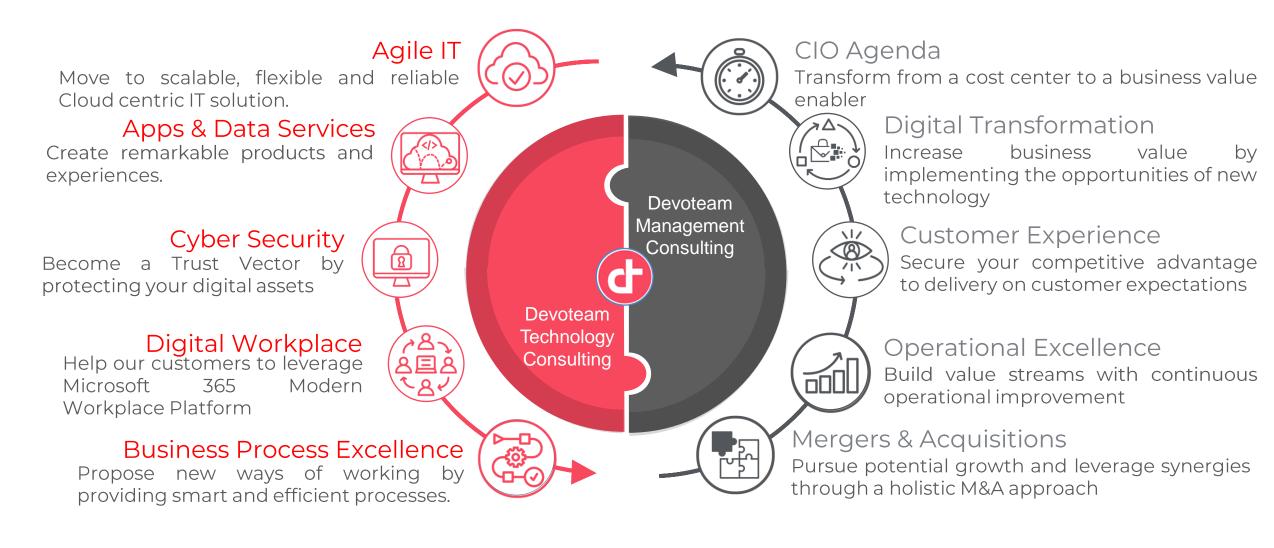
- Endpoint security Maturity Level
- The 6 domains of Endpoint security

Security Posture Improvement

- Agile Methodology based on continuous improvement
- How to start the initiative?

5 Questions?

End-2-end Portfolio to shape your digital company...



"We magnify your value by boosting Business & IT collaboration"



Trust: The Business Catalyser

Make your investigation

Ask your family, your friends about a good address good shopping combining business friendly, good expertise and good experience for the service,

Safety Feeling

When you enter in the shopping, you feel secure thanks to the guard post at the entrance, the cameras., articles physically protected, and the sale welcomes you

Receive good advices

The sale asks your expectations and proposes the best in class product promoting their features and answering your questions.

Close the deal

You are convinced by the sale and you decide to buy the product.

Buy the product

You go to the cash to pay your product with a credit card. For big paiement, the identity card is sometimes asked.

Make your investigation

Look the products on different testing sites, read the comments, send emails to your friends to have their ideas.

....Safety Feeling

When you connect to the platform, the registration requires multiple factors of authentication, my personal data is protected (GDPR),

Receive good advices

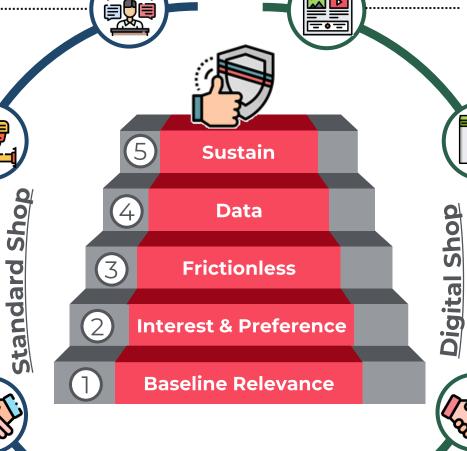
On the platform, you read the comments of the other users. You also use the social networks to have the feedback.

.......... Close the deal

On the platform, thanks to a frictionless approach (a few clicks) driven by an automated business flow, you close the deal for a specific product...

...... Buy the product

On platform, you can access a secure access gateway which enables you to use your . , you need an identity proof (example: scan identity card





How to create the Trust?

What are your 3 major expectations to create the Trust, Business Catalyser?



Consumers, customers, business partners, and employees all expect great user experiences.

Their loyalty and commitment are shaped by friction less experience of interactions when using new digital services.

Failure to manage digital identities well, threatens the quality of the delivered services.



Accountability



The majority of the consumers is not aware of the amount of information they shared about themselves online. Their knowledge of their rights regarding the use and the protection of their personal data is really limited

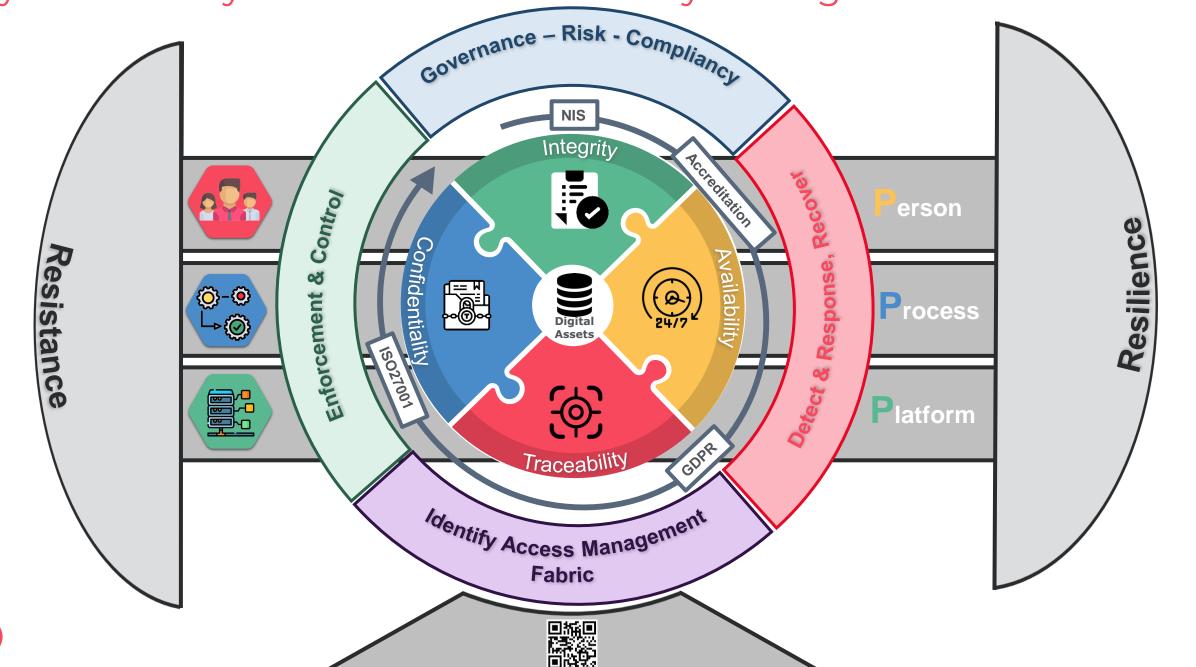


Consent

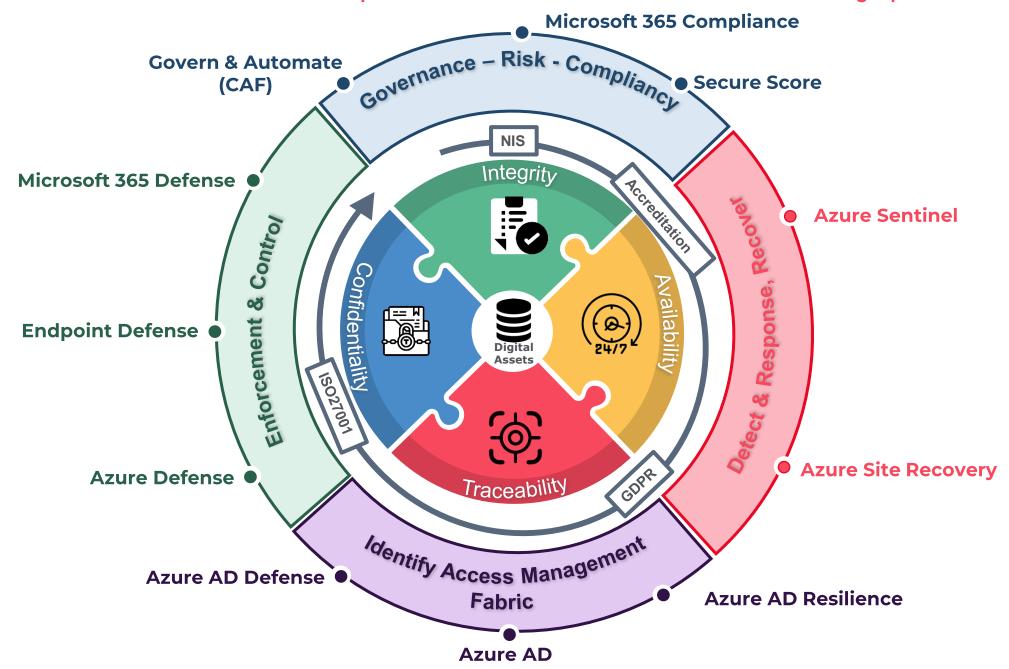
Consumers want that the sharing of their personal information is possible if and only if they give the consent. This consent can be easily given and removed thanks to a frictionless application. They also want a complete transparency and tracability about the consents they have.



Cyber Security Portfolio calibrated for your Digital Transformation



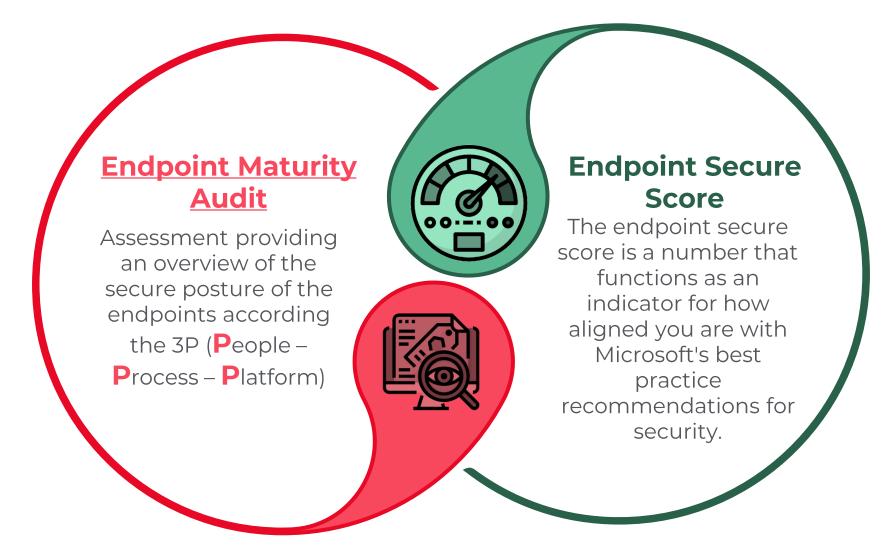
The Microsoft Roadmap for a best-in-class security posture





What's your Endpoint security maturity level?

Two approaches





What's your endpoint level of maturity?

Driven by an assessment covering six dimensions Threat & Vulnerability

Management

- Do you know which vulnerable softwares are running?
- Do you quickly understand the real risk associated with vulnerabilities?
- Do you take your unique business context to evaluate the risk?
- Do you remediate the vulnerabilities timely?
- Can you justify to internal audit why exceptions have been granted?

Security Posture Management

- Do you bootstrap your devices in a consistent way?
- Is a newly delivered device secure by default?
- Do you rely on enterprise network connectivity?
- Do you have a complete inventory available?
- Did you adopt modern management?
- Did you define acceptable use policies?
- Did you define device policies?
 - Do you prepare the onfiguration drift?
 - Do you capture process execution trees?
 - Do you capture command-line parameters?
 - Do you capture changes to critical configuration items?
 - Do you enrich the endpoint telemetry with other sources?

Protection

- Does your protection agent leverage machine learning?
- · Can you quickly adapt to new indications of compromise?
- Do you protect credentials properly?
- · Do you use the endpoint risk score to control access to assets?

Attack Surface Reduction

- Do you have control on malicious network destinations access?
- Do you block productivity applications from behaving out of the normal?
- Do you allow applications to run from removable storage?



- Do you auto-remediate with high confidence level?
- Can you connect to endpoints for deeper investigation?
- Can you quickly isolate a compromised endpoint?
- Can you find the initial vector of compromise?
- Can you make an accurate assessment on how critical a security incident is?



What's your endpoint level of maturity?

Driven by an assessment covering six dimensions

Threat & Vulnerability Management



Security Recommendations



Software inventory



Exposure Score

Threat Analytics

Protection



Credentials Guard



Bit Locker



Defender AV





Device Inventory



Device Health and Compliance



Device configuration management

Detection



Defender ATP



Advanced Hunting







Live Response



Automated Investigation and Response



Action Center





ASR Rules



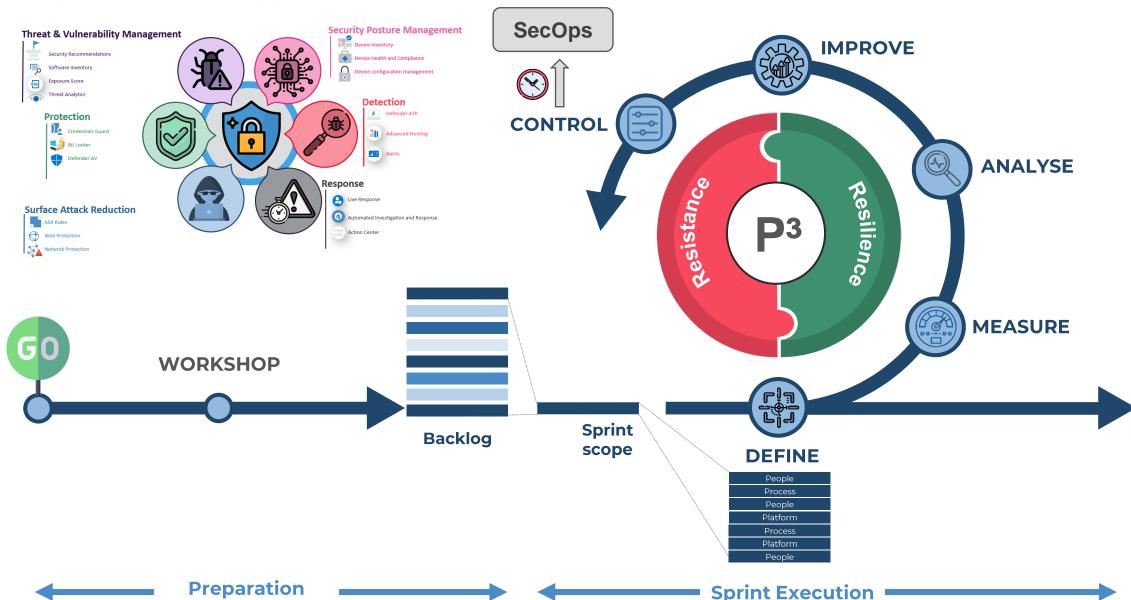
Web Protection



Network Protection

How to improve your Security Posture?

An Agile Methodology focused on Continuous Improvement

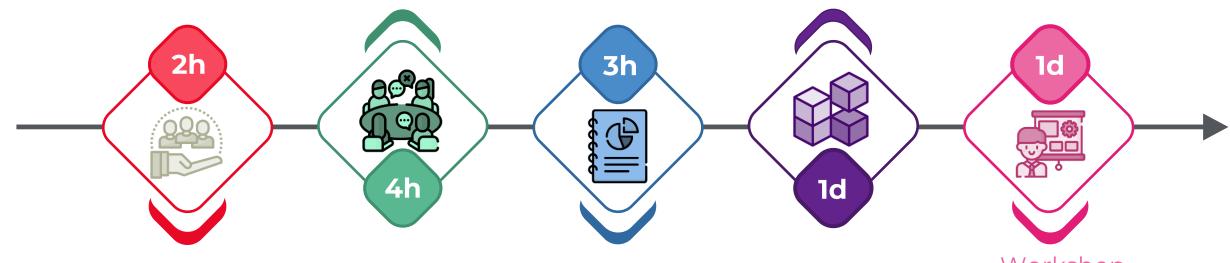


How to improve your Security Posture? The Workshop

Engagement Setup

- · Kick-Off Meeting
- Secure Score Overview & Security Posture

Design & Planning



Pre-Engagement

- Pre-Engagement Call
- Endpoint Security Workshop Questionnaire

Reporting

 Application Discovery Reporting & Discussion

Workshop

- Customer Value Conversation
- Discovery Session
- Demos
- Key Results, recommandations & next steps



How to improve your Security Posture?

Iteration loop for the Threat and Vulnerability management activity



People

We need to follow the approach ADKAR to correctly execute a change:

- Create and execute a communication plan
- Create and execute education plan for key stakeholders
- Create different communication content to create user awareness (newsletter email poster)



Process

Integrate the TVM in the different IT processes:

- Integrate the TVM on-boarding in the staging process
- Integrate TVM remediation activities in IT support processes
- Create TVM exception governance process



Platform

Azure TVM is automatically enabled when on-boarding device in MDE:

- Implement RBAC model
- Setup integration with ITSM platform
- Setup alerting for critical findings



Measure

The proposed measure points are:

- Evolution of the Secure Score for Devices
- Evolution of the Exposure score
- % of endpoints on-boarded
- · Mean time to remediate



TVM

Backlog