Microsoft

Mystified Defender for Servers

Markus Lintuala, Elisa Oyj

Markus Lintuala

CLOUD HERO

markus@lintuala.fi | +358 40 585 5531

elisa

- Public speaker
- Can’t say no for anything new
- Gastronomic, craft beer and wine geek
- Loves travelling and aviation
- Waze map editor

@MarkusLintuala

@mmaraa

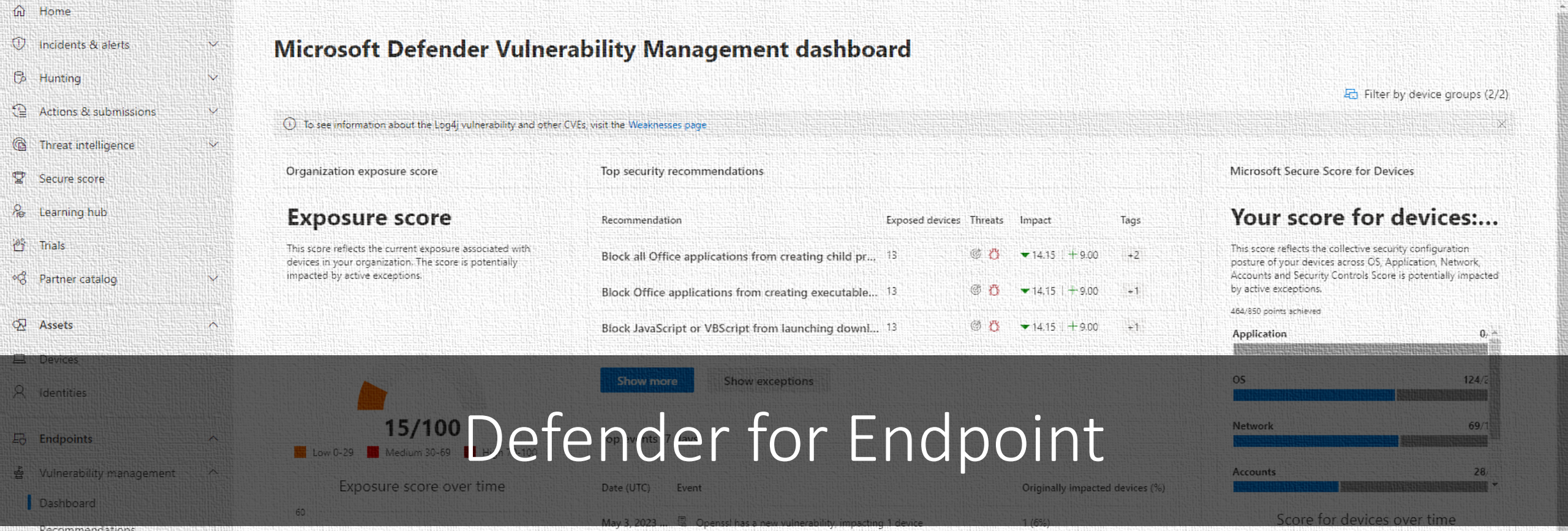
Agenda

Defender for Endpoint for Servers

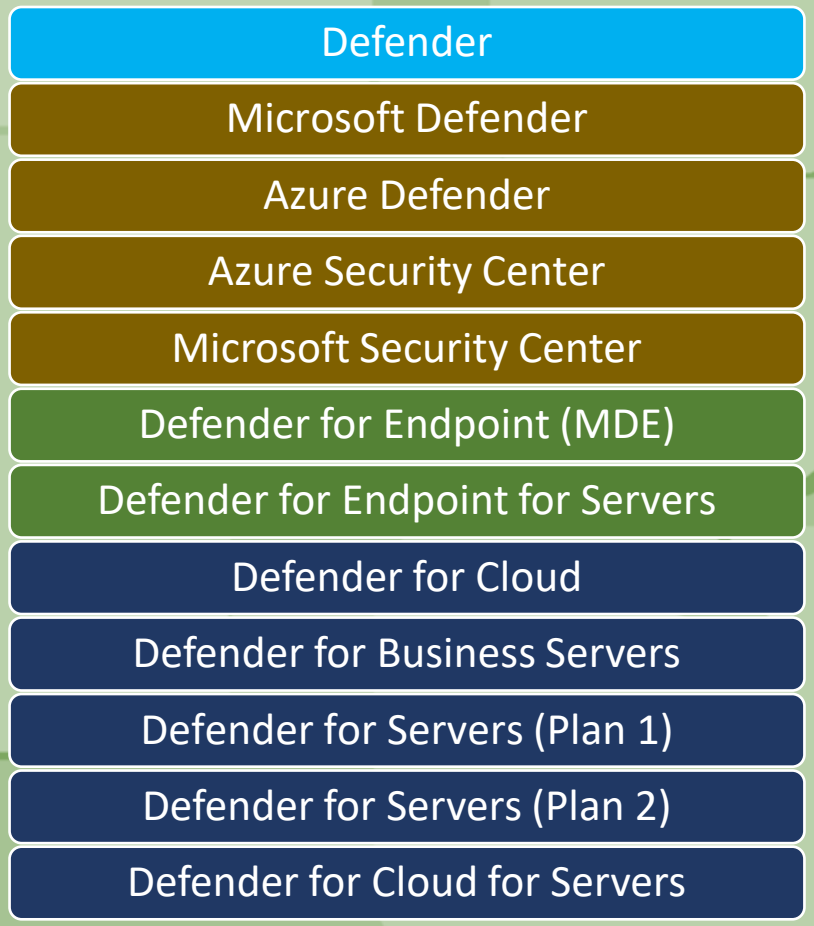
Defender for Servers

Defender for Cloud other features

Defender for Endpoint



Terminology



Defender for Endpoint for Servers

Endpoint protection for servers

Retired licensing model

Old licensing model

Through CSP or EA

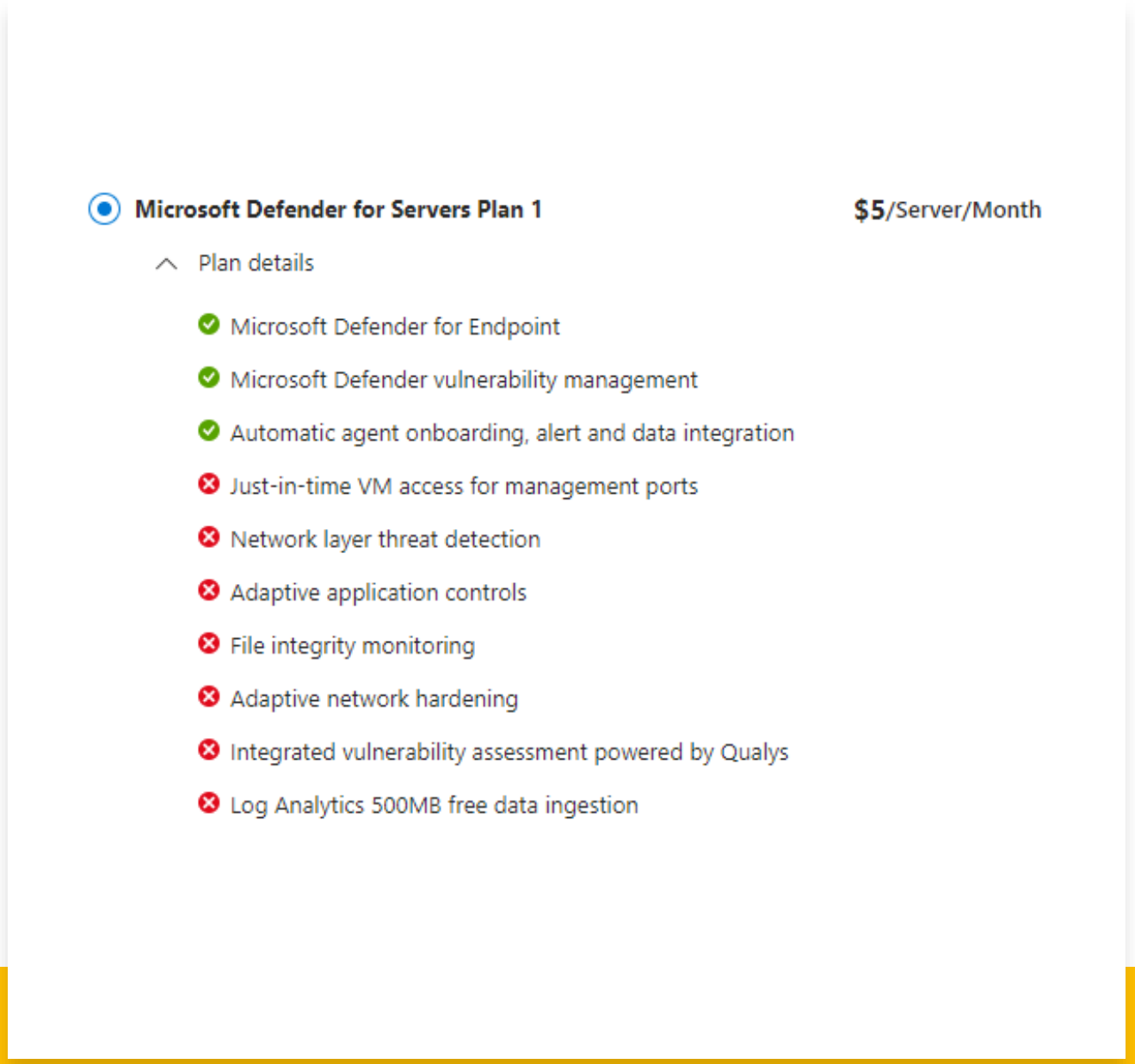
Monthly or yearly licensing

New licensing model

- Pay-as-you-go licensing
- Licensed through Defender for Cloud
- Non-Azure servers uses Azure Arc to enable licensing
- Two licensing options Plan 1 and Plan 2

Defender for Servers PLAN 1

- Provides free capabilities of Defender for Servers
- Microsoft vulnerability management engine
- Easy onboarding



Defender for Servers PLAN 2

- All features included in PLAN 1
- All Defender for Servers features
- Microsoft Defender vulnerability management add-on

Vulnerability add-on

- Continuously assess security baseline instead of continuous scanning of compliance
- Block running vulnerable applications
- Browser extension assessment
- Certificate monitoring and assessment
- Network share assessment
- Hardware and firmware assessment
- Authenticated scan for Windows (remote scan)

Compare Defender for Servers plans

PLAN 1

- Can be compared with features to retired licensing model
- Pricing same than the old one

PLAN 2

- Second point of view to vulnerabilities with **Qualys**
- Agentless vulnerability scanning for **AWS** and **GCP** environments
- More **cloud centric security** thinking
- Security policy and regulatory **compliance** reports
- **File integrity** monitoring
- **Fileless attack** detection
- **Adaptive application** control
- Basic **Cloud Security Posture Management**
- Network hardening
- Vulnerability add-on

What is Azure Arc for Servers

Non-Azure server management through Azure

Requires only HTTPS outbound

Enables huge amount of management capabilities

Public cloud benefits when using hybrid

Next level authentication for access management

Highly scalable automation platform

Modern security solutions for servers

Which plan to choose?

- For MDE, only Plan 1 is ok
- Plan 2 recommended if you want single pane of glass view or extend infrastructure securing capabilities

Matrices of Defender for Servers features in foundational CSPM, Azure Arc, multicloud, and endpoint protection solutions | Microsoft Learn

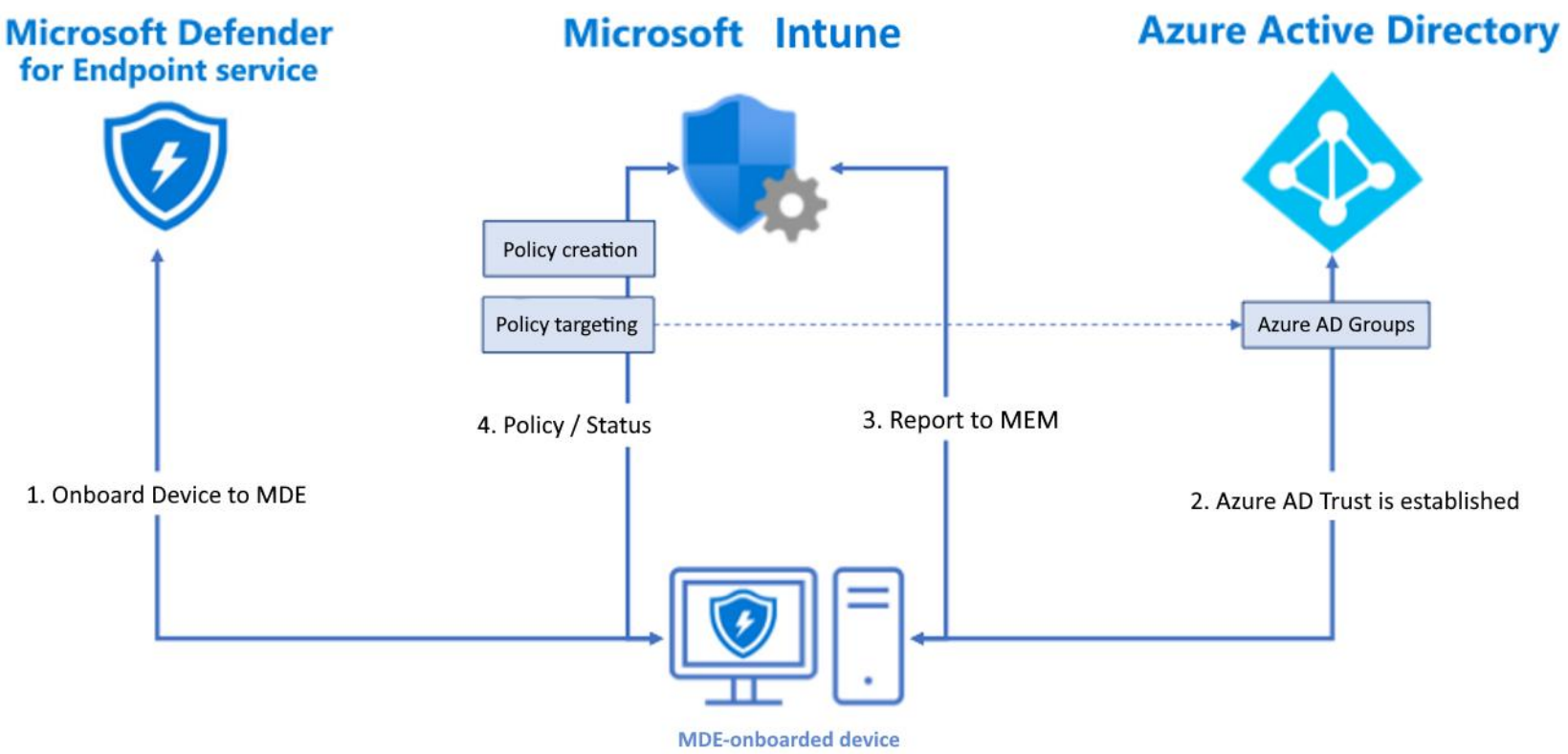
How to scale?

Azure Arc

How to pay?

Subscription based payment, pay-as-you-go – no extra fees

How to manage servers then?

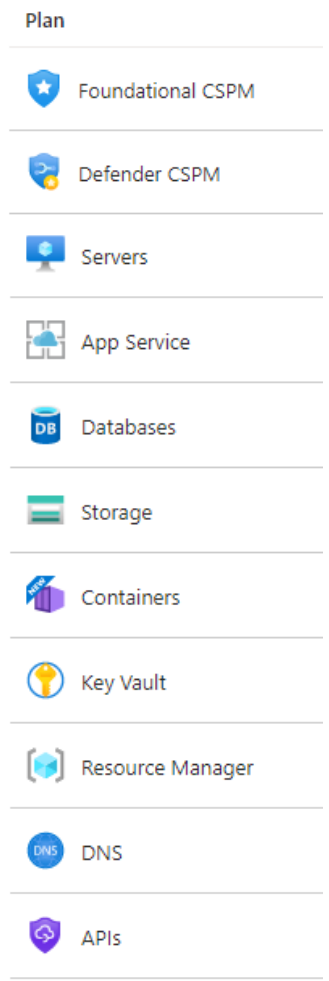


Remember when managing with Intune

- Core servers are not supported
- AAD Trust relationship is mandatory
- Configuration needed in Intune and in MDE
- Avoid making conflict policies
- Make the most important configurations still with GPO

What is Defender for Cloud?

What is Defender for Cloud?



What is Defender for Cloud?

Unify your DevOps security management

- DevOps posture visibility across pipelines
- Infrastructure as Code security
- Code to cloud contextualization
- Integrated workflows & pull request annotations

Strengthen and manage your security posture

- Full visibility with agentless and agent-based scanning
- Integrated insights across DevOps, EASM, CIEM, and workloads
- Attack path-based prioritization
- At-scale governance & automated remediation
- Security compliance management

Detect threats and protect your workloads

- Full-stack threat protection
- Vulnerability assessment & management

Automate with the tools of your choice

Amazon Web Services | Microsoft Azure | Google Cloud Platform | On-premises

Cloud Security Posture Management

Cloud security compliance management

Vulnerabilities and attack paths

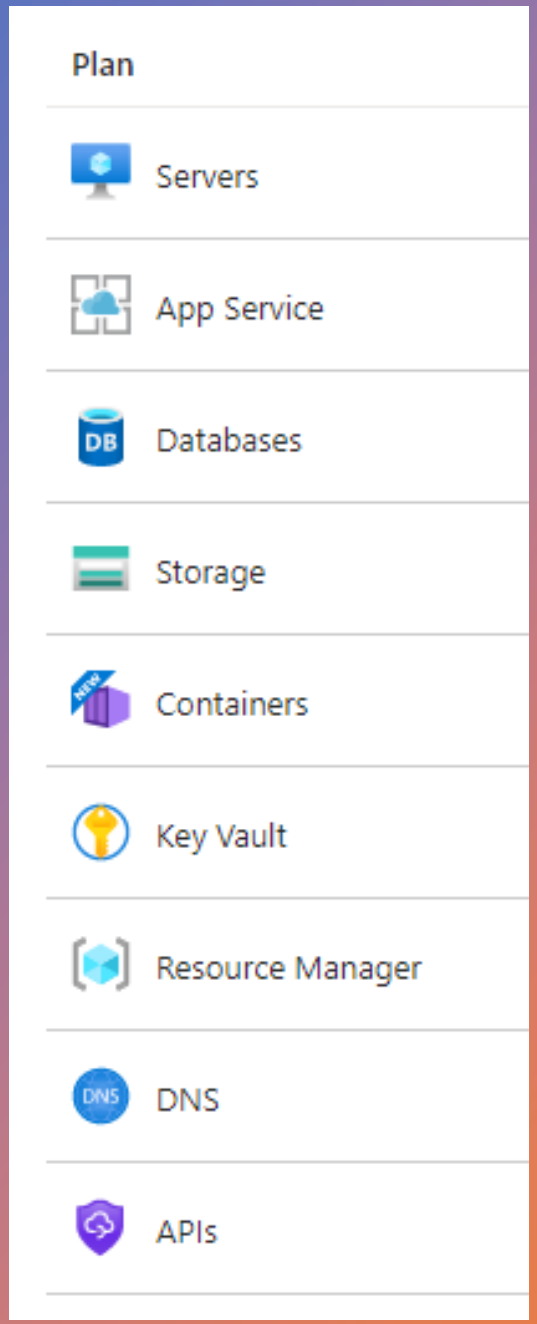
Recognize risky misconfigurations

Defender for CSPM

- Paid plan to get more features out from cloud security posture
- Automate your posture management
- Check how you meet regulatory compliance

Pricing: Based on subscription size, counting Compute and Data resources Defender CSPM is free until August 1st. When enabling Defender CSPM, automatic discounts will be applied in case other Defender plans are enabled learn more

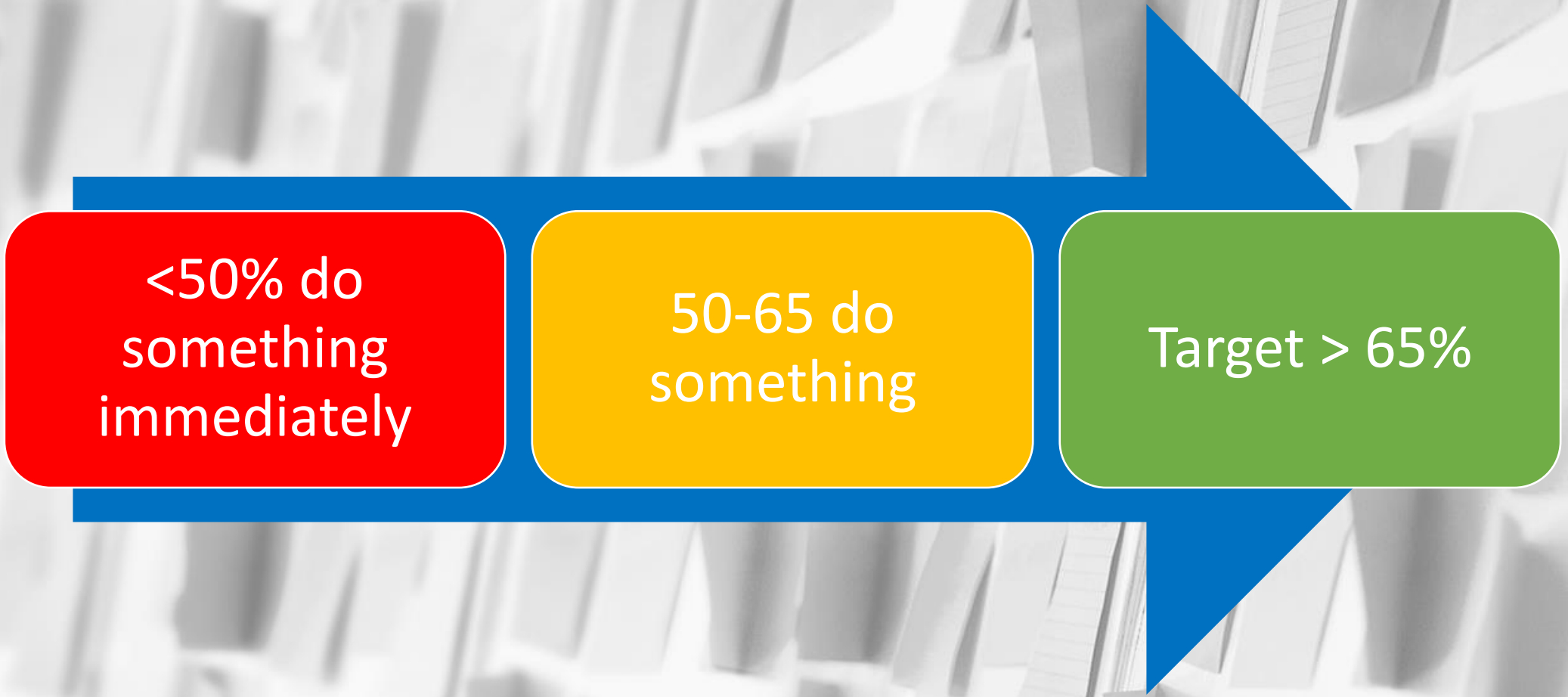
- Identity and role assignments discovery
- Network exposure detection
- Attack path analysis
- Cloud security explorer for risk hunting
- Agentless vulnerability scanning
- Governance rules to drive timely remediation and accountability
- Regulatory compliance and industry best practices
- Data-aware security posture
- Agentless discovery for Kubernetes
- Agentless vulnerability assessments for container images, including registry scanning



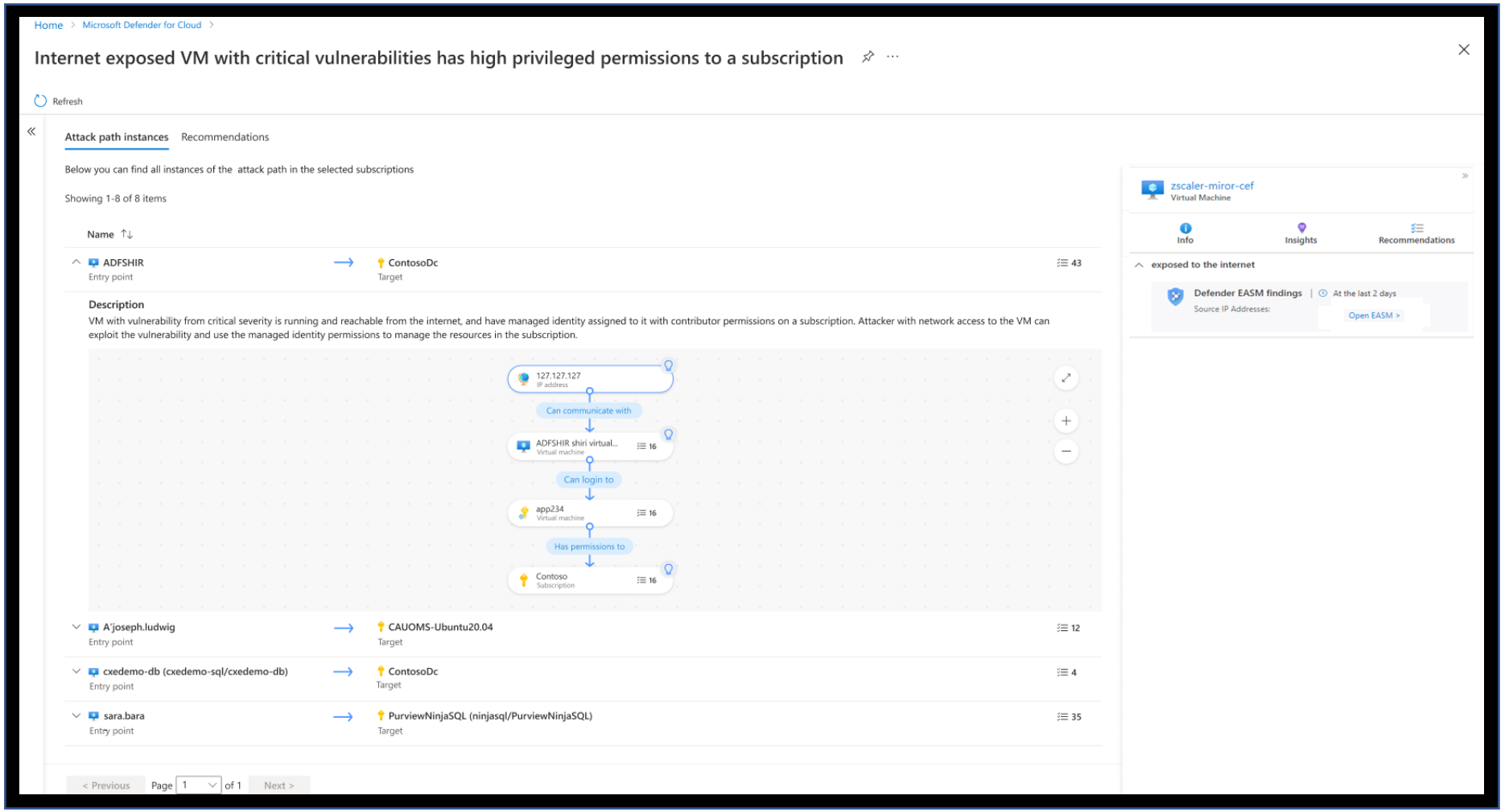
Defender for Cloud services

- Monitor PaaS solutions
- Find misconfigurations
- Detect attacks
- Understand your exposure
- Protect PaaS and SaaS solutions

Secure score



Attack paths



Security Explorer

Find	Hunt	Place
Find information that you want without writing a line of KQL or other languages	Hunt fast	Place to start, if critical vulnerabilities are published

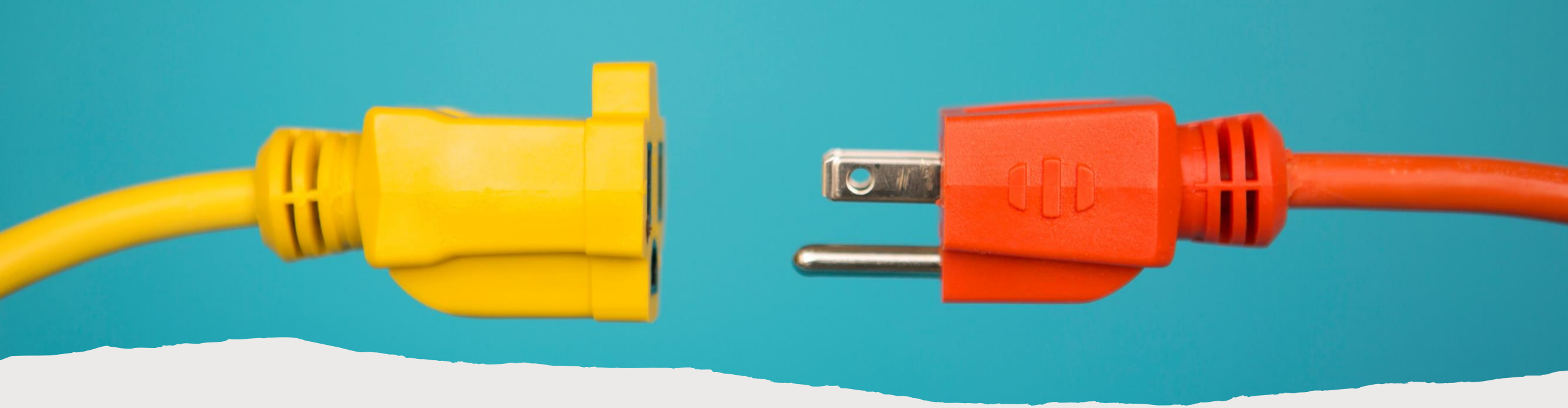
Extend to multicloud

PART OF TOOLS AVAILABLE FOR AWS ACCOUNTS AND GCP PROJECTS

GET SINGLE VIEW THROUGH ALL YOUR CLOUDS

Defender for APIs

- Detect unauthenticated API endpoints
- Detect OWASP top 10 critical threats in real time
- Classify sensitive data content to support risk prioritization



Integrations to other platforms

- Microsoft EASM
- Microsoft Sentinel
- Workflow automations
- REST API for more

Key takeaways

- Go to hybrid
- Use automatic enrolment to MDE
- Enable Defender for Cloud plans and start using it

Q & A

Thank you