



Mystified Defender for Servers

Markus Lintula, 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

Home

Incidents & alerts

Hunting

Actions & submissions

Threat intelligence

Secure score

Learning hub

Trials

Partner catalog

Assets

Devices

Identities

Endpoints

Vulnerability management

Dashboard

Recommendations

Remediation

Inventories

Weaknesses

Event timeline

Baselines assessment

Partners and APIs

Evaluation & tutorials

Configuration management

Email & collaboration

Investigations

Explorer

Microsoft Defender Vulnerability Management dashboard

To see information about the Log4j vulnerability and other CVEs, visit the [Weaknesses page](#).

[Filter by device groups \(2/2\)](#)

Organization exposure score

Exposure score

This score reflects the current exposure associated with devices in your organization. The score is potentially impacted by active exceptions.

15/100

Low 0-29 | Medium 30-69 | High 70-100

Show more Show exceptions

Exposure score over time

Date (UTC) Event Originally impacted devices (%)

May 3, 2023 OpenSSL has a new vulnerability impacting 1 device 1 (6%)

Improve score Show more

Top security recommendations

Recommendation	Exposed devices	Threats	Impact	Tags
Block all Office applications from creating child pr...	13	0	-14.15 + 9.00	+2
Block Office applications from creating executable...	13	0	-14.15 + 9.00	-1
Block JavaScript or VBScript from launching downl...	13	0	-14.15 + 9.00	-1

Microsoft Secure Score for Devices

Your score for devices:...

This score reflects the collective security configuration posture of your devices across OS, Application, Network, Accounts and Security Controls. Score is potentially impacted by active exceptions.

464/850 points achieved

Application

OS

Network

Accounts

Score for devices over time

Device exposure distribution

Exposure distribution

Exposed devices are easy targets for cybersecurity attacks. Ensure that these devices can receive security updates, have critical security controls, and are properly configured.

Top remediation activities

This table lists top activities that were generated from security recommendations.

Activity	Count
Update 7-zip to version 21.7.0.0	0/0

Top vulnerable software

Software	OS platform	Weaknesses	Threats	Exposed devices
.net	Windows	2	0	5 / 7
Jre	Windows	132	0	1 / 1
Sql Server 2019	Windows	8	0	1 / 1

Terminology

- Defender
- Microsoft Defender
- Azure Defender
- Azure Security Center
- Microsoft Security Center
- Defender for Endpoint (MDE)
- Defender for Endpoint for Servers
- Defender for Cloud
- Defender for Business Servers
- Defender for Servers (Plan 1)
- Defender for Servers (Plan 2)
- Defender for Cloud for Servers

Defender for Endpoint for Servers

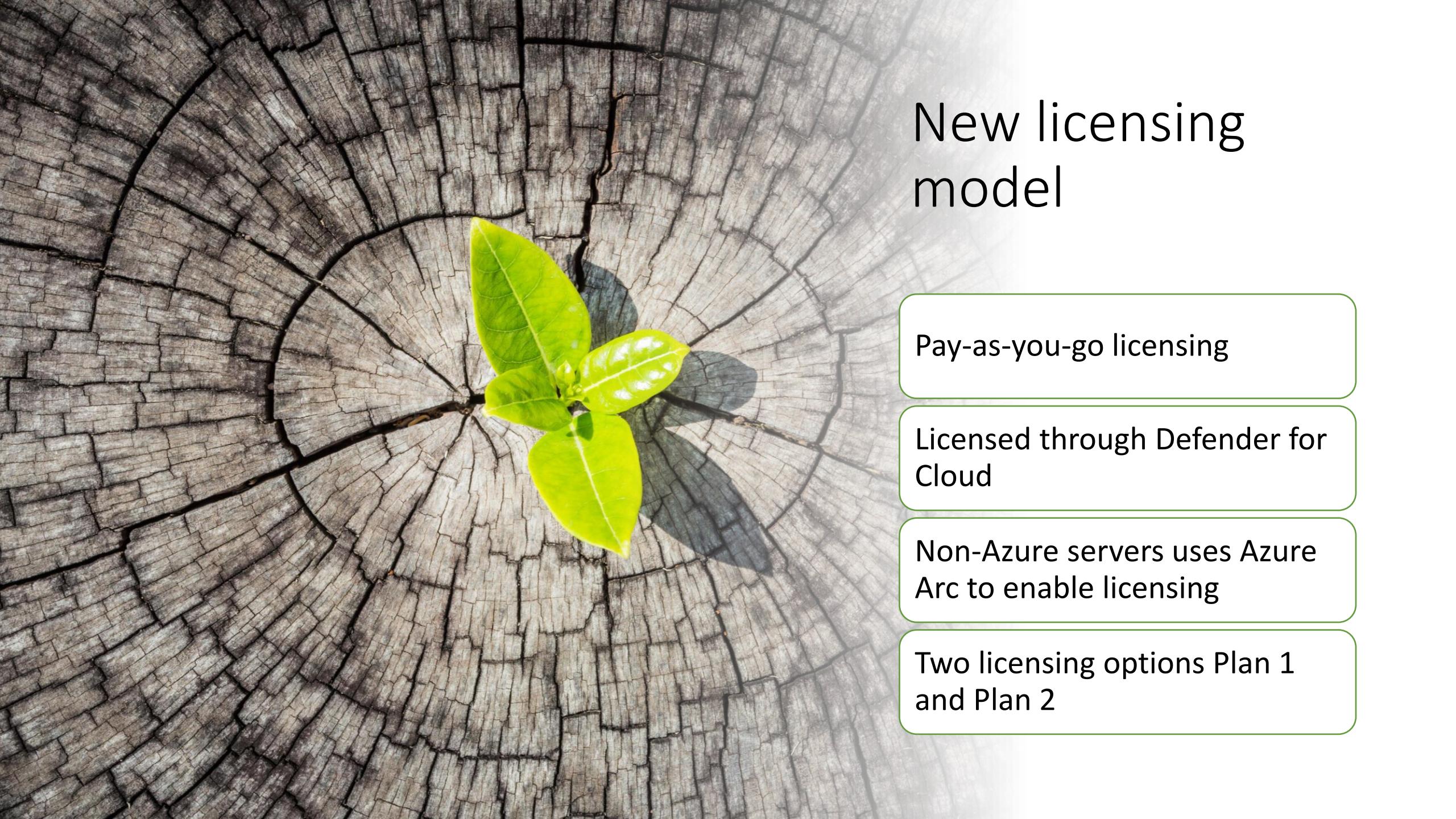
Endpoint
protection for
servers

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



Microsoft Defender for Servers Plan 1

\$5/Server/Month

Plan details

- ✓ Microsoft Defender for Endpoint
- ✓ Microsoft Defender vulnerability management
- ✓ Automatic agent onboarding, alert and data integration
- ✗ Just-in-time VM access for management ports
- ✗ Network layer threat detection
- ✗ Adaptive application controls
- ✗ File integrity monitoring
- ✗ Adaptive network hardening
- ✗ Integrated vulnerability assessment powered by Qualys
- ✗ Log Analytics 500MB free data ingestion

Defender for Servers PLAN 2

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

 Microsoft Defender for Servers Plan 2	\$15/Server/Month
 Plan details	 Recommended
<ul style="list-style-type: none">✓ Agentless vulnerability scanning✓ Microsoft Defender for Endpoint✓ Microsoft Defender vulnerability management✓ Automatic agent onboarding, alert and data integration✓ Just-in-time VM access for management ports✓ Network layer threat detection✓ Adaptive application controls✓ File integrity monitoring✓ Adaptive network hardening✓ Integrated vulnerability assessment powered by Qualys✓ Log Analytics 500MB free data ingestion	

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

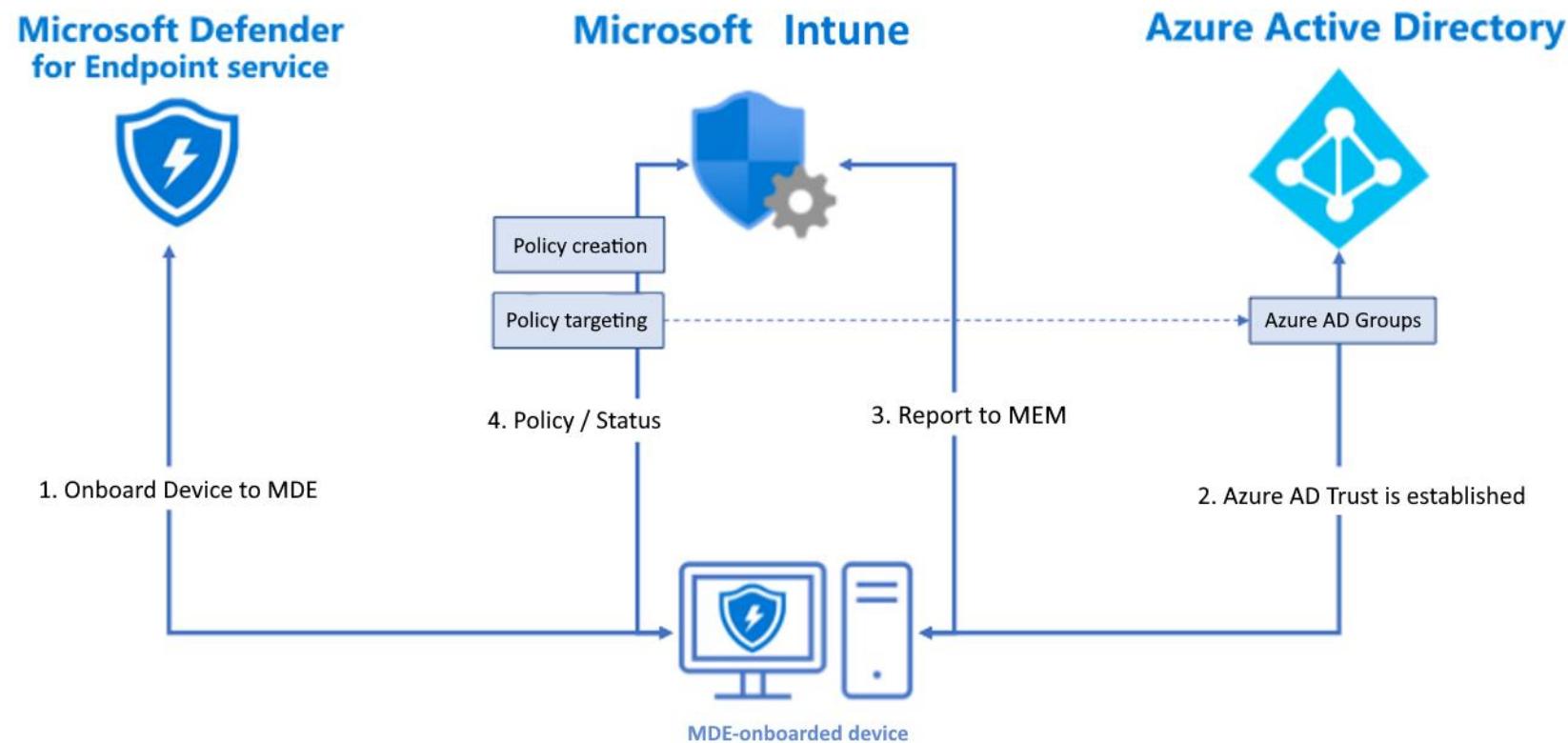
How to scale?

Azure Arc

How to pay?

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

How to manage servers then?

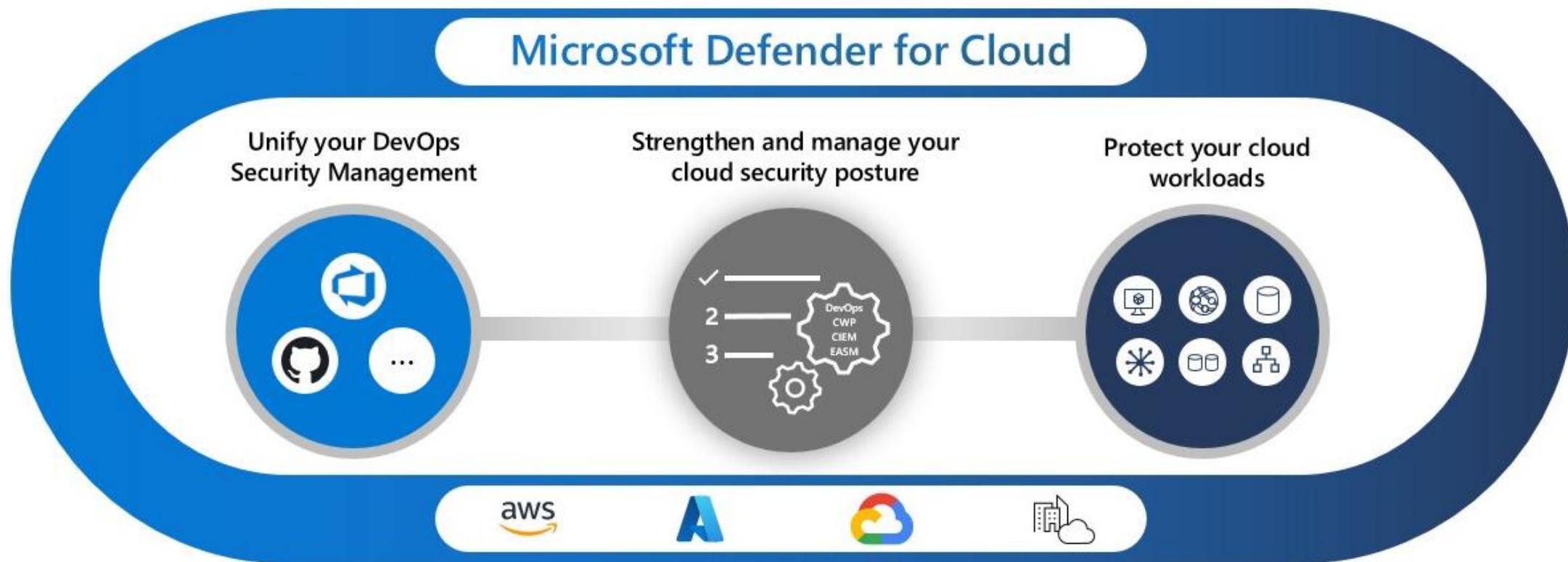


Remember when managing with Intune

- 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

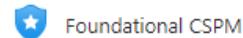


What is Defender for Cloud?



What is Defender for Cloud?

Plan



Foundational CSPM



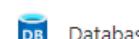
Defender CSPM



Servers



App Service



Databases



Storage



Containers



Key Vault



Resource Manager



DNS



APIs

What is Defender for Cloud?

Unify your DevOps security management

Strengthen and manage your security posture

Detect threats and protect your workloads



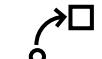
DevOps posture visibility across pipelines



Infrastructure as Code security



Code to cloud contextualization



Integrated workflows & pull request annotations



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



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

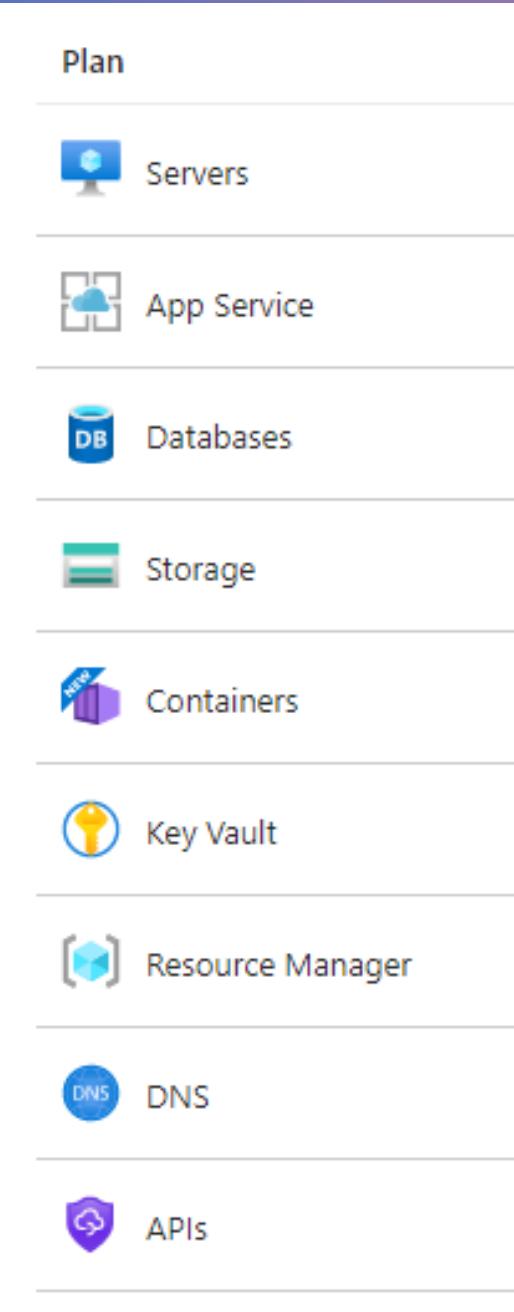
Recognize risky
misconfigurations

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

<50% do
something
immediately

50-65 do
something

Target > 65%

Attack paths

Home > Microsoft Defender for Cloud >

Internet exposed VM with critical vulnerabilities has high privileged permissions to a subscription

Refresh

Attack path instances Recommendations

Below you can find all instances of the attack path in the selected subscriptions

Showing 1-8 of 8 items

Name ↑

ADFSHIR → ContosoDc

Description

VM with vulnerability from critical severity is running and reachable from the internet, and have managed identity assigned to it with contributor permissions on a subscription. Attacker with network access to the VM can exploit the vulnerability and use the managed identity permissions to manage the resources in the subscription.

zscaler-miror-cef Virtual Machine

Info Insights Recommendations

exposed to the internet

Defender EASM findings At the last 2 days Source IP Addresses Open EASM >

The screenshot shows the Microsoft Defender for Cloud interface. The main title is "Internet exposed VM with critical vulnerabilities has high privileged permissions to a subscription". Below it, there's a heading "Attack path instances" with a "Refresh" button and a "Recommendations" tab. A sub-section title "Below you can find all instances of the attack path in the selected subscriptions" is followed by "Showing 1-8 of 8 items". A table lists three entries:

Name	Entry point	Target	Count
ADFSHIR	→	ContosoDc	43
A'joseph.ludwig	→	CAUOMS-Ubuntu20.04	12
cxedemo-db (cxedemo-sql/cxedemo-db)	→	ContosoDc	4
sara.bara	→	PurviewNinjaSQL (nijasql/PurviewNinjaSQL)	35

Each entry row contains a collapsible icon, a status icon, a name, an arrow indicating the direction of the attack path, another status icon, the target name, and a count value. Below the table is a navigation bar with "Page 1 of 1" and "Next >". On the right side, there's a detailed view for the first entry: "zscaler-miror-cef Virtual Machine" with tabs for "Info", "Insights", and "Recommendations". It also shows a section titled "exposed to the internet" with "Defender EASM findings" and a link to "Open EASM >". A large diagram below the table illustrates the attack path: "127.127.127 IP address" connects to "Can communicate with" → "ADFSHIR shiri virtual... Virtual machine" (with a count of 16) which connects to "Can login to" → "app234 Virtual machine" (with a count of 16) which connects to "Has permissions to" → "Contoso Subscription" (with a count of 16).

Security Explorer

Find

Find information
that you want
without writing a
line of KQL or other
languages

Hunt

Hunt fast

Place

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

