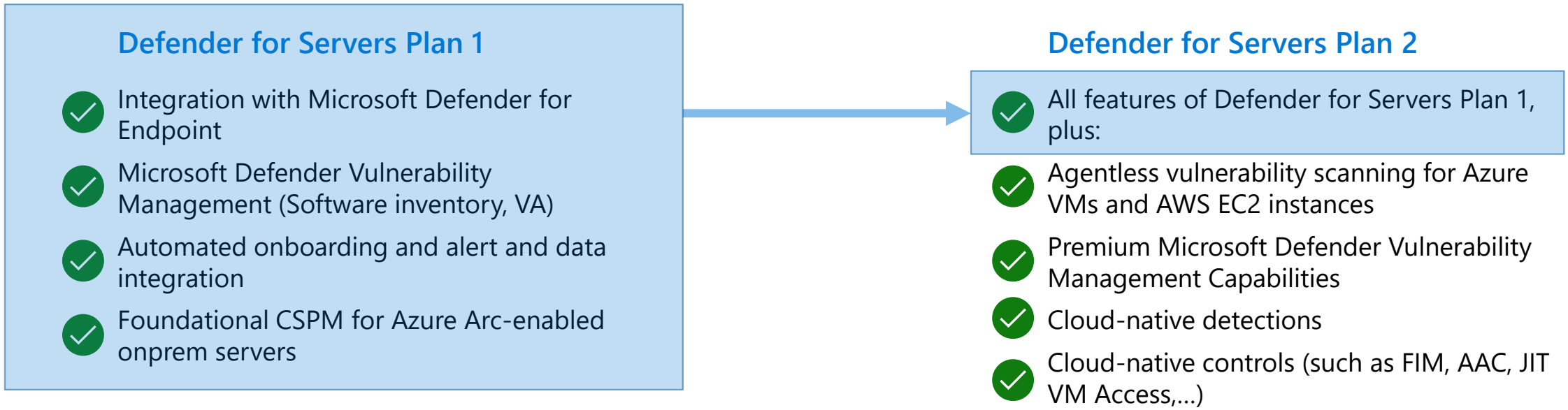
Server security in the cloud is different

- Running VMs in the cloud requires an additional layer of security to protect the control plane surrounding your servers
- Threat detections need to extend to connected, cloud-native components including network, storage, and the control plane to fully assess and protect the security state of your servers
- To be effective, modern workload protection solutions need to provide traditional VM security and provide optimised detections and mechanisms for cloud-based resources

Features of Defender for Servers plans

Protecting Servers using Defender for Cloud



Features of Defender for Servers plans

Annual M365 license AND Azure consumption based options

M365

Azure

[Select a Defender for Servers plan in Microsoft Defender for Cloud | Microsoft Learn]

Defender for Servers Plan 2

All the features of Defender for Servers Plan 1 and;

* Network Layer Threat Detection*
* Security Policy and Regulatory Compliance
* Premium Vulnerability Management functions
* Adaptive App Control
* 500MB no-cost select data ingest
* Just-in-Time virtual machine access**
* Adaptive network hardening *
* File integrity monitoring
* Docker host hardening
* Network map*
* Agentless vulnerability scanning**

Defender for Servers Plan 1

Defender for Endpoint P2

All the features of P1 and;

* Device discovery
* Device inventory
* Core Vuln Mgmt.
* Threat Analytics
* AIRs
* Advanced Hunting
* EDR
* Endpoint Attack Notify

Defender for Endpoint P1

**endpoints only

* Next-generation protection
* Attack surface reduction
* Manual response Actions
* Centralized management
* Security reports
* APIs

* Currently Azure Only

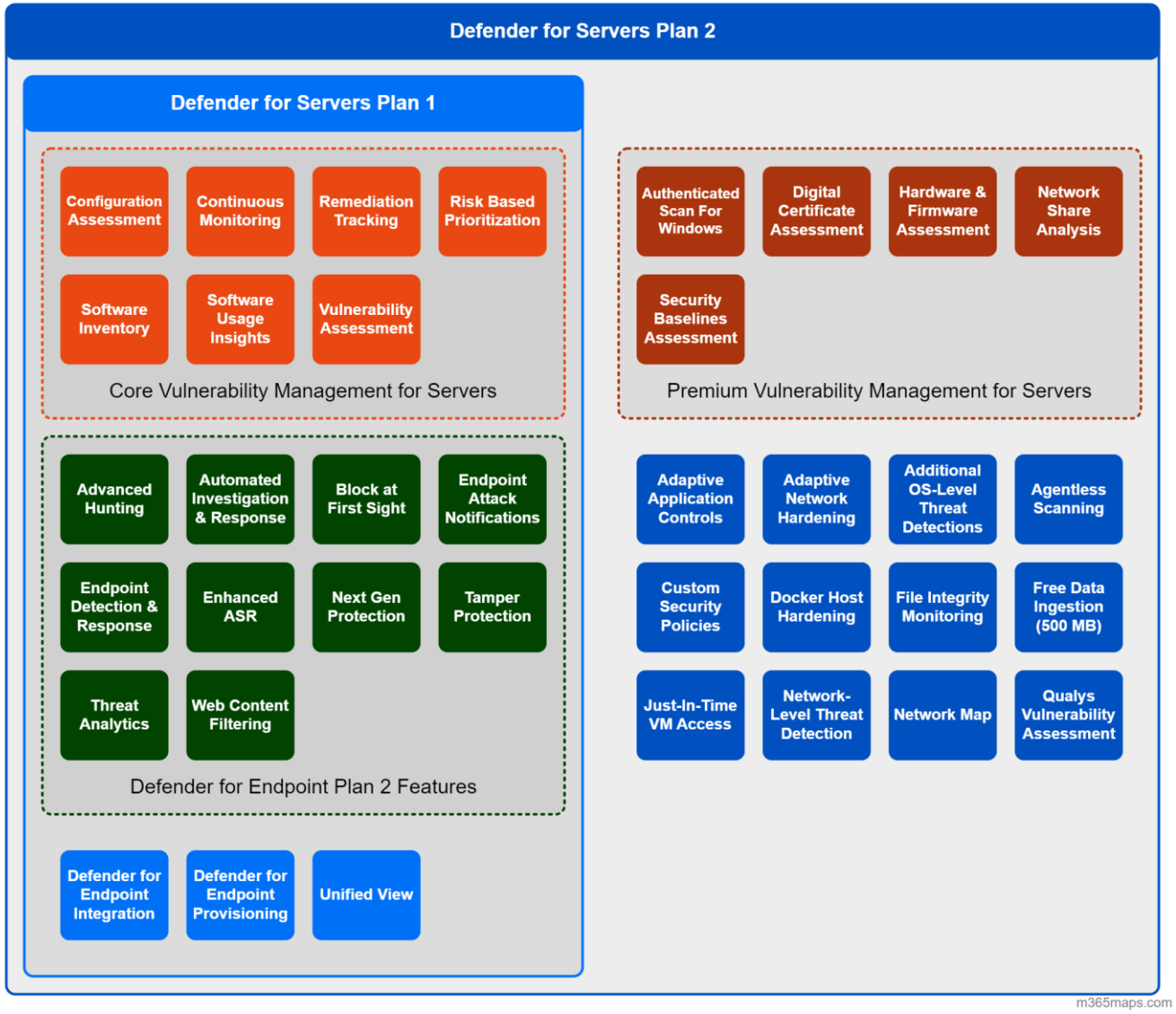
**Azure and AWS

Feature comparison

Feature	Defender for Endpoint for Servers	Defender for Servers P1	Defender for Servers P2
Hardening recommendations	■	■	■
Asset discovery	■	■	■
Vulnerability assessment using Microsoft Defender Vulnerability Management	■	■	■
Attack surface reduction	■	■	■
Next generation antivirus protection	■	■	■
Endpoint detection & response	■	■	■
Automated self-healing	■	■	■
Hourly billing optimized for dynamic cloud resources	■	■	■
Automatic agent onboarding for resources in Azure, AWS, GCP	■	■	■
Management optimized for cloud environments		■	■
Support for AWS and GCP-native compute (EC2 + Google Compute Engine)		■	■
Unified experience for all workload types (Servers, containers, databases, and more)		■	■
All Defender Vulnerability Management Premium capabilities: Security Baselines, Firmware & Hardware assessment, Digital Certificates, Network share analysis, Blocking Vulnerable Applications			■
Log-analytics (500MB free)			■
Regulatory compliance assessment			■
Vulnerability assessments and security benchmarks			■
Network layer threat detection *			■
Adaptive application controls			■
File integrity monitoring			■
Just-in-time VM access for management ports			■
Adaptive network hardening *			■

* Currently Azure-only

Another view – from m365maps.com



[Microsoft Defender for Servers | M365 Maps]