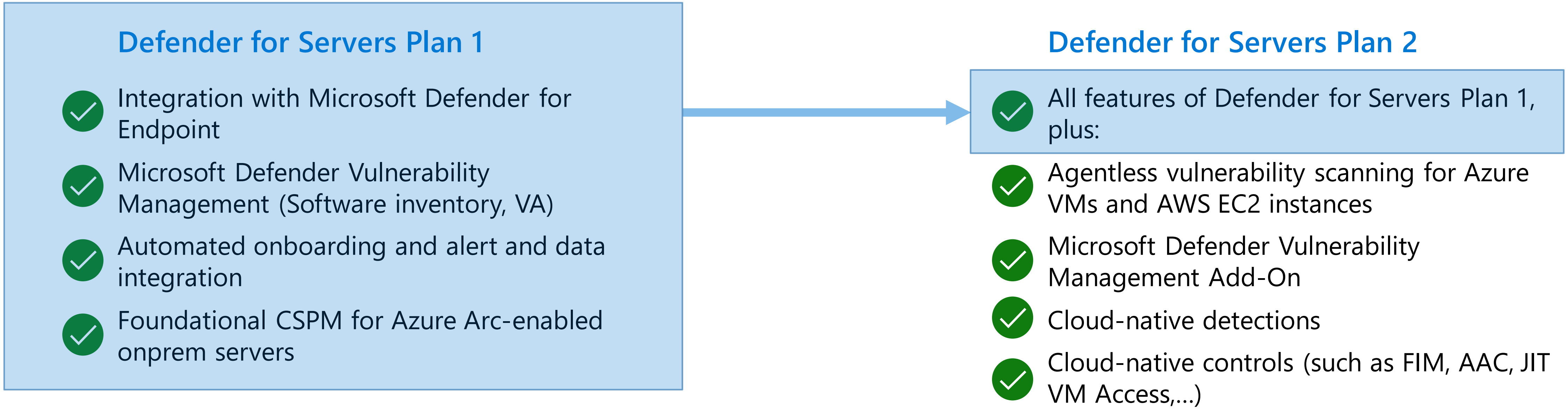
Server security in the cloud is different

- 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



Defender for Servers Plan 1

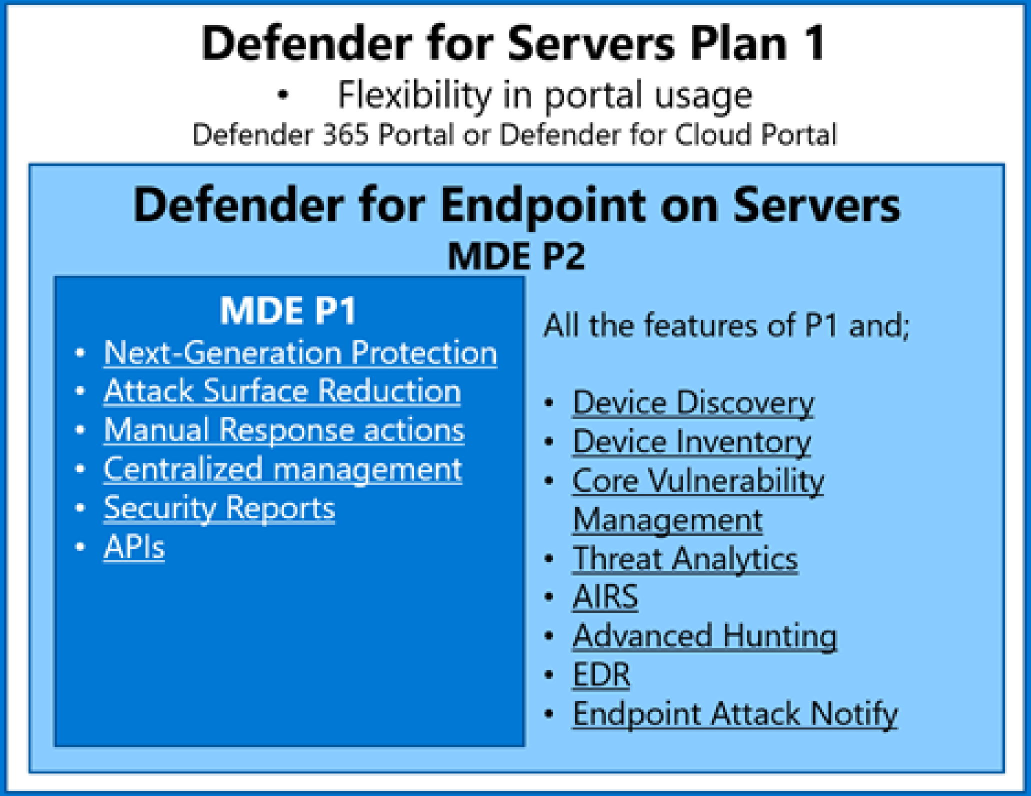
- ✓ Integration with Microsoft Defender for Endpoint
- ✓ Microsoft Defender Vulnerability Management (Software inventory, VA)
- ✓ Automated onboarding and alert and data integration
- ✓ Foundational CSPM for Azure Arc-enabled onprem servers

Defender for Servers Plan 2

- ✓ All features of Defender for Servers Plan 1, plus:
- ✓ Agentless vulnerability scanning for Azure VMs and AWS EC2 instances
- ✓ Microsoft Defender Vulnerability Management Add-On
- ✓ Cloud-native detections
- ✓ Cloud-native controls (such as FIM, AAC, JIT VM Access,…)

Features of Defender for Servers plans

Defender for Server Plan 2



Defender for Servers Plan 1

- Flexibility in portal usage

Defender 365 Portal or Defender for Cloud Portal

Defender for Endpoint on Servers

MDE P2

MDE P1

- Next-Generation Protection
- Attack Surface Reduction
- Manual Response actions
- Centralized management
- Security Reports
- APIs

All the features of P1 and;

- Device Discovery
- Device Inventory
- Core Vulnerability Management
- Threat Analytics
- AIRS
- Advanced Hunting
- EDR
- Endpoint Attack Notify

All the features of Plan 1 and;

- Network Layer Thread Detection*
- Security Policy and Regulatory Compliance
- 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**

MDVM

Add-On to MDE P2

- Security baseline assessment
- Block vulnerable apps
- Browser extensions
- Digital certificate analysis
- Network share analysis
- Hardware and firmware assessment
- Authenticated scan for Windows

*Currently Azure Only
**Azure and AWS

Feature comparison

Feature	Defender for Endpoint for Servers ($5)	Defender for Servers P1 ($5)	Defender for Servers P2 ($15)
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)		■	■
Defender Vulnerability Management add-on capabilities: Security Baselines, Firmware & Hardware, 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