

---

# Microsoft Sentinel Workspace Architecture



# \$whoami

## Peter Chen

Cybersecurity Consultant

### Currently:

- Microsoft 365 Security + Azure Security
- Enterprise Security

### Previously:

- 10+ years, architecting and securing critical IT infrastructures
- Messaging, Directory Services, Enterprise Mobility Management



[@EhloWorldIO](https://twitter.com/EhloWorldIO)



<https://www.linkedin.com/in/petchen/>



[EHLOWorld.IO](https://ehloworld.io)

# Disclaimer

The views and opinions expressed in this presentation are those of the presenter and do not necessarily reflect the view and opinions of my employer.

Any material presented by the presenter in any format, without limitation, is for informational purposes only. The reader is expected to conduct their own due diligence and assessment of the vendor, product, or services as appropriate for their needs.

# Thank you



## Communauté Microsoft Azure Québec

📍 Québec, QC

👤 1,179 members · Public group ?

👤 Organized by Tidjani B. and 3 others

Share:    

# Objective

- Microsoft Defender for Endpoint (MDE)
- Microsoft Defender for Servers
  - Azure Defender for Cloud
  - Azure Arc
- Unified Management Agent
- Security Management for MDE

# Agenda

1. Overview
2. Endpoints
3. Architecture
4. Unified Solution
5. Security Management
6. Defender for Cloud
7. Integration
8. Summary





# Overview



# What is Microsoft Defender for Endpoint?

- Enterprise endpoint security platform
  - prevent, detect, investigate, and respond to advanced threats
- Attack surface reduction
- Next-generation protection
- Endpoint detection and response (EDR)
- Automated investigation and remediation
- Vulnerability Management



# Terminologies



## **Microsoft Defender Antivirus**

- Built-in Windows Antivirus



## **Microsoft Defender for Endpoint**

- Applies to both Workstations and Servers
- Managed from Microsoft Defender Security Center Portal
- Microsoft Defender Antivirus is optional



## **Microsoft Defender for Server**

- Applies to Servers and Azure Virtual Desktop (AVD)
- Managed from Microsoft Defender for Cloud
- Includes and extends features from Microsoft Defender for Endpoint

---

# Endpoints



# Defender for Endpoint OS Support

<b>iOS</b> <ul style="list-style-type: none"><li>• iOS 12.0 and above</li></ul>	<b>Android</b> <ul style="list-style-type: none"><li>• Android 6.0 and above</li></ul>
<b>MacOS</b> <ul style="list-style-type: none"><li>• 10.15 (Catalina)</li><li>• 11 (Big Sur),</li><li>• 12 (Monterey)</li></ul>	<b>Linux</b> <ul style="list-style-type: none"><li>• Red Hat Enterprise Linux 6.7 or higher (Preview)</li><li>• Red Hat Enterprise Linux 7.2 or higher</li><li>• Red Hat Enterprise Linux 8.x</li><li>• CentOS 6.7 or higher (Preview)</li><li>• CentOS 7.2 or higher</li><li>• Ubuntu 16.04 LTS or higher LTS</li><li>• Debian 9 or higher</li><li>• SUSE Linux Enterprise Server 12 or higher</li><li>• Oracle Linux 7.2 or higher</li><li>• Oracle Linux 8.x</li><li>• Amazon Linux 2</li><li>• Fedora 33 or higher</li></ul>

# Defender for Endpoint OS Support

## Windows

- Windows 365
- Windows Virtual Desktop
- Windows 11 Enterprise
- Windows 11 Education
- Windows 11 Pro
- Windows 11 Pro Education
- Windows 10 Enterprise
- Windows 10 Enterprise LTSC 2016 (or later)
- Windows 10 Enterprise IoT
- Windows 10 Education
- Windows 10 Pro
- Windows 10 Pro Education
- Windows 8.1 Enterprise
- Windows 8.1 Pro
- Windows 7 SP1 Enterprise (Requires ESU for support.)
- Windows 7 SP1 Pro (Requires ESU for support.)

## Windows server

- Windows Server 2008 R2 SP1 (Requires ESU for support)
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server, version 1803 or later
- Windows Server 2019
- Windows Server 2022

# Microsoft Defender Antivirus Support



- Windows 11
- Windows 10
- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server version 1803, or newer



- Windows 7 SP1
- Windows 8.1
- Windows Server 2008 R2 SP1
- Windows Server 2012 R2

System Center Endpoint Protection (SCEP)



# Feature Comparison

Feature	Description	Windows 7 SP1	Windows 8.1	Windows 10/11	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016	Windows Server 2019/2022	macOS	Linux	Android phones	iOS
Endpoint protection platform												
Microsoft Defender Antivirus (MDAV) / Next Generation Protection	Core antimalware engine that provides behaviour-based, heuristic, and real-time AV protection; powers "next-generation protection" features <i>in addition to</i> standard signature-based detections.			✓		✓	✓	✓				
System Centre Endpoint Protection (SCEP) / Microsoft Antimalware for Azure (MAA) / etc	"Down-level" operating systems do not have an antivirus engine built-in, however Microsoft's antimalware platform is available through other channels such as SCEP (comes with ConfigMgr), MAA (if managed with Azure), or Windows Defender (consumer-level).	✓	✓		✓	Only if not using unified agent						
Preventative antivirus	"Traditional" antivirus approach to potential threats. May have behavioural monitoring capabilities but is not the Next Generation Protection MDAV client seen in Windows.	✓	✓		✓				✓	✓		
Block at first sight	Sends hash value of executables with mark of the web to cloud to determine reputation; if unknown hash, upload file for more analysis.			1803+		✓	✓					
Cloud-delivered protection	Sends metadata to the cloud protection service to determine if a file is safe based on machine learning and Intelligent Security Graph.			✓		✓	✓	✓	✓			
Tamper protection	On Windows, blocks certain changes to MDAV via registry, PowerShell, and GPO. On mobiles, detect if out of protection for seven days and inform device compliance.			✓		✓	✓	✓			✓	✓
Potentially unwanted app protection	Blocks software that isn't necessarily malicious but otherwise undesirable, such as advertising injectors and cryptominers.			✓		✓	✓	✓	✓	✓		
Passive mode	If third-party endpoint protection is also running, antimalware engine doesn't provide preventative real-time protection (including ASR rules, etc) but can scan on-demand. Can be supplemented by EDR in block mode.			✓ Automatic		✓ Manual	✓ Manual	✓ Manual	✓ Manual	✓ Manual		
Device discovery	Endpoints passively or actively collect events and extract device information (basic mode) or actively probe observed devices (standard mode; default). This refers to OSs that can perform discovery.			1809+				✓				
Respect indicators of compromise – files and certificates	Custom block or allow controls on the endpoint based on hash value or CER/PEM files.			1703+		✓	✓	✓				
Respect indicators of compromise – IPs, URLs, domains	Custom block or allow controls based on public IP or FQDNs (or full web paths for Microsoft web browsers).			1709+		✓	✓					
Windows Defender Firewall with Advanced Security (WFAS)	Control the inbound and outbound network traffic allowed on the device based on the type of network connected, as well as other controls such as IPsec.	✓	✓	✓	✓	✓	✓	✓				
Host firewall reporting	Dedicated reporting available in the Microsoft 365 Defender portal about inbound + outbound connections and app connections.			✓				✓				

# Licensing

- Defender for Endpoint Plan 1
- Defender for Endpoint Plan 2
- Defender for Endpoint for Servers
- Microsoft Defender for Servers Plan 1
- Microsoft Defender for Servers Plan 2
- Defender Vulnerability Management add-on



---

# Architecture



# Environment Architecture

Defender for Endpoint architecture is defined on

- The “endpoints” we are protecting and onboarding
- The appropriate “management solution” supporting these endpoints

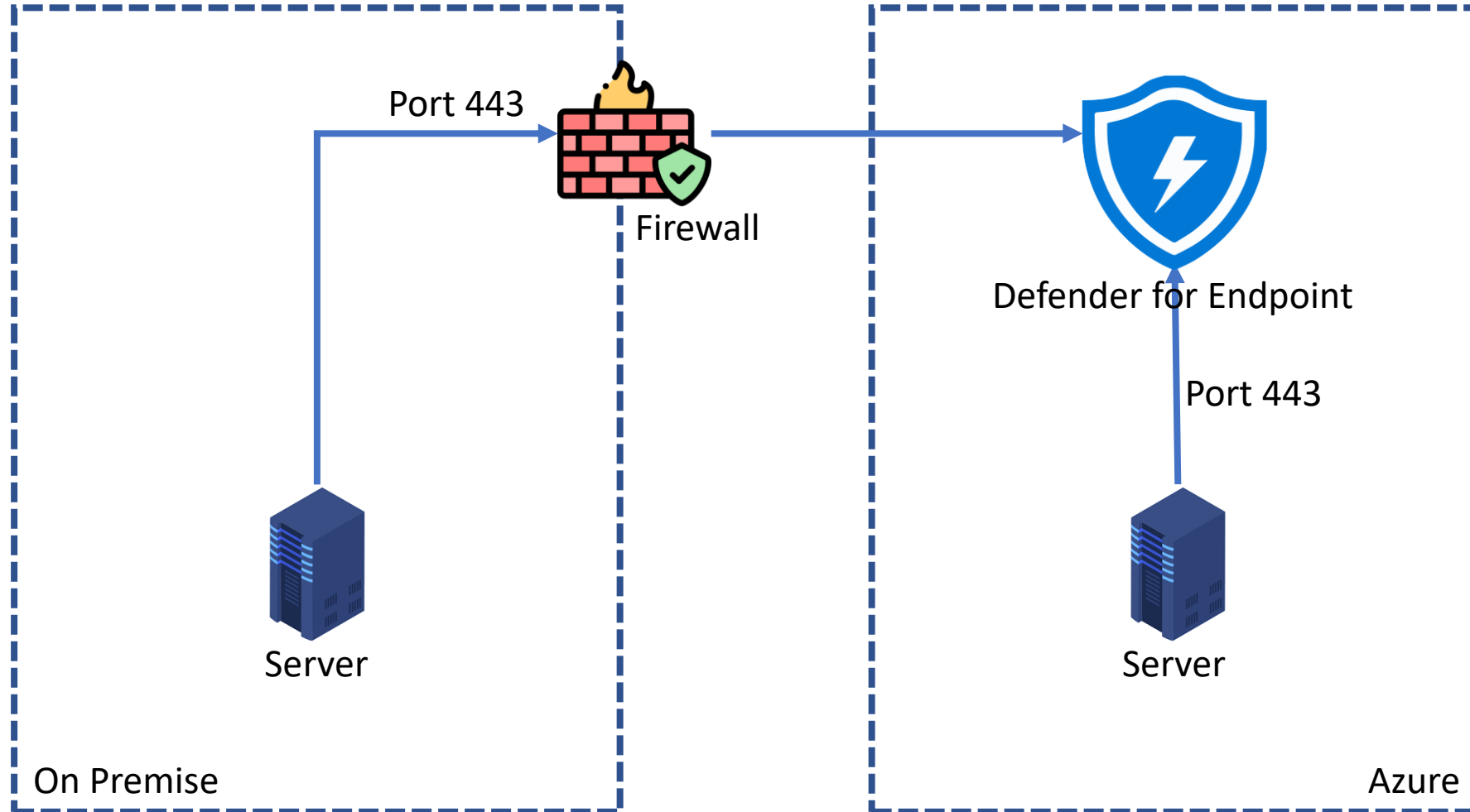
# MDE Agent

Built-in agent for

- Windows 10 and 11
- Windows Server 2019 and 2022
- Agent must be deployed and onboarded to MDE
- Agent must have Internet connectivity
  - [Microsoft Defender for Endpoint URL list](#)



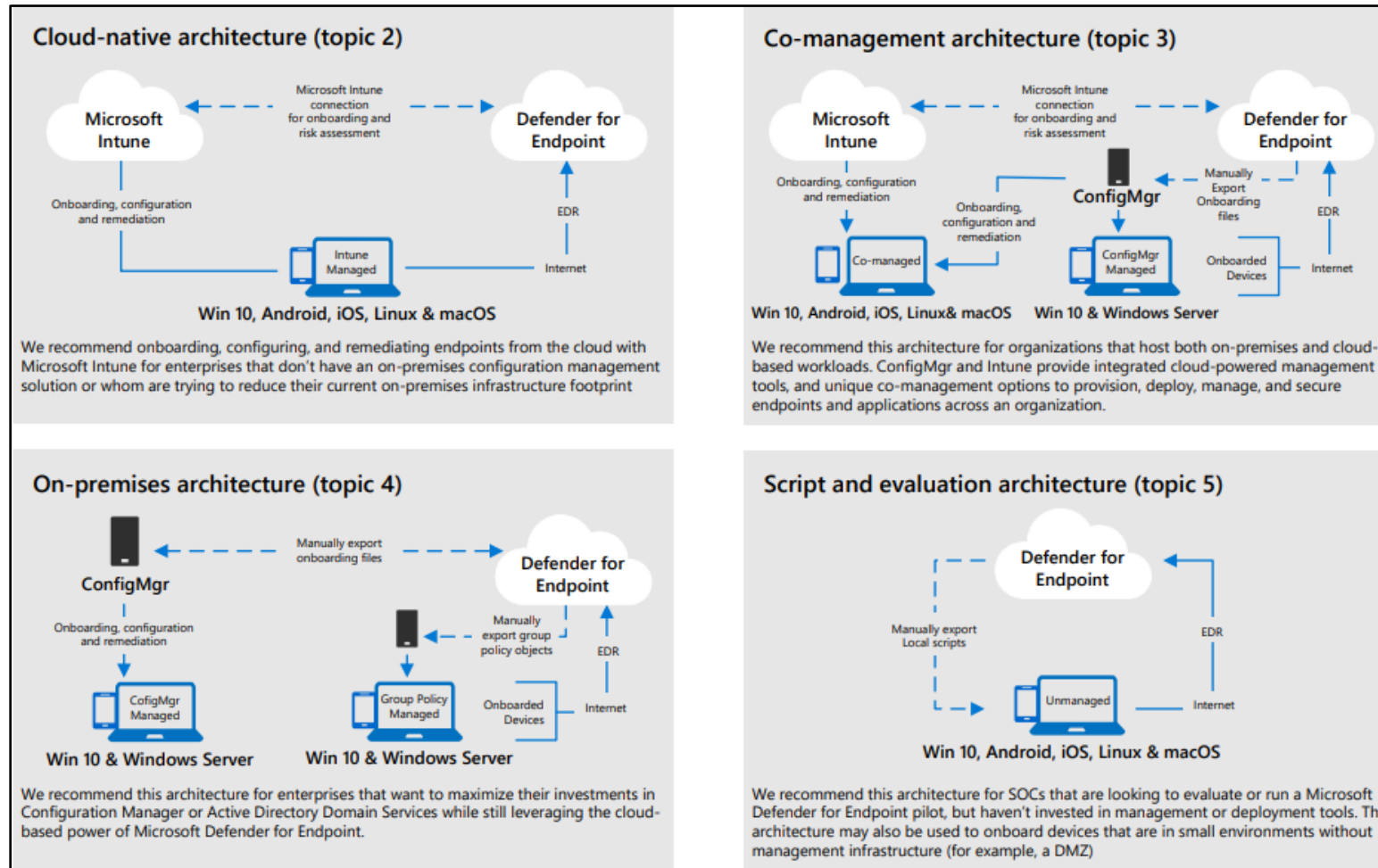
# Sample Agent Architecture



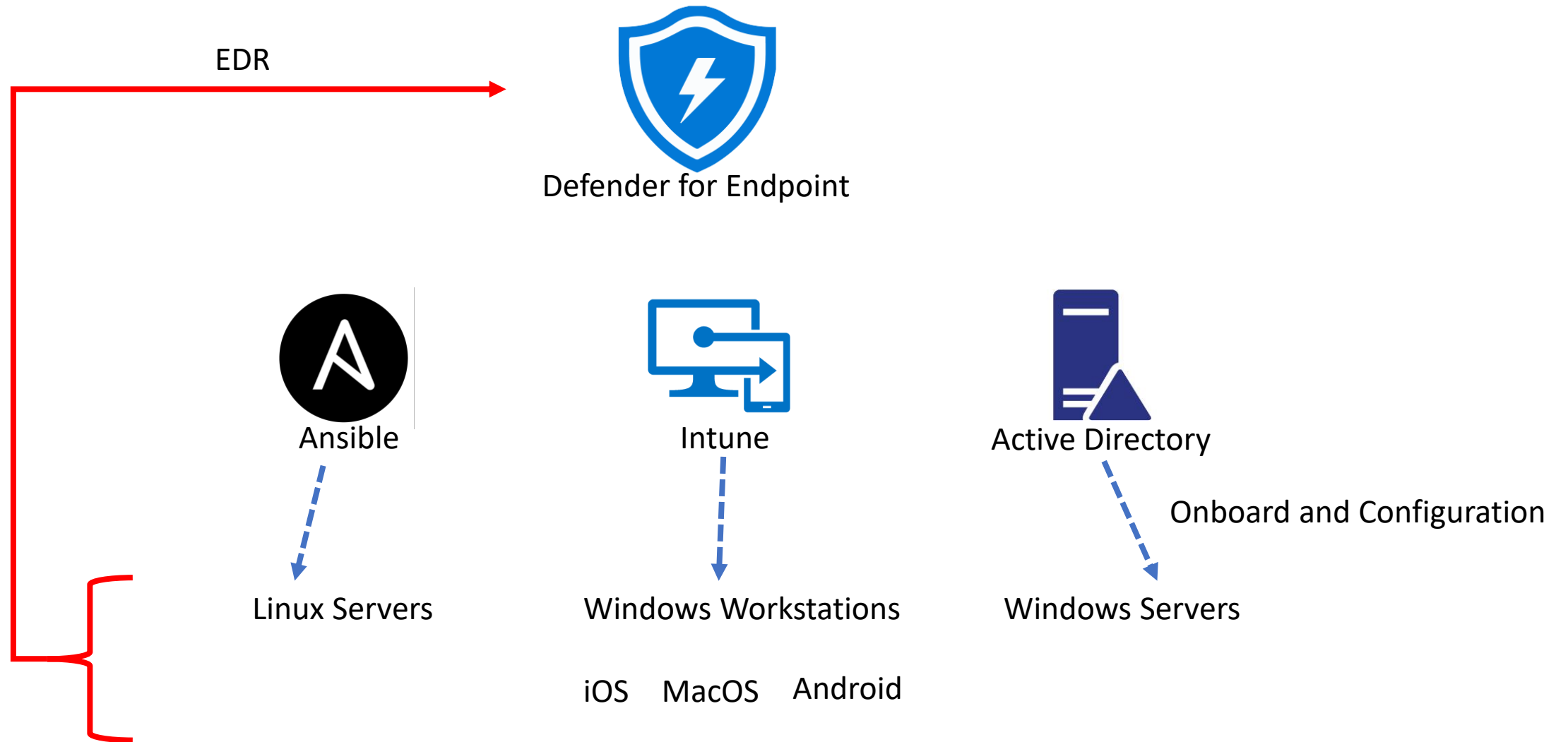
# Endpoint Management Solution

Endpoint	Tools
Windows	Local script (up to 10 devices) Group Policy Microsoft Endpoint Manager/ Mobile Device Manager Microsoft Endpoint Configuration Manager VDI scripts Integration with Microsoft Defender for Cloud
MacOS	Local script Microsoft Endpoint Manager JAMF Pro Mobile Device Management
Linux	Local script Puppet Ansible
iOS	Microsoft Endpoint Manager
Android	Microsoft Endpoint Manager

# Microsoft Architecture



# Sample Architecture



---

# Unified Solution





# Use-Case

- No feature parity for Windows Server 2012 R2 and 2016
- Windows Server 2012 R2 required SCEP
- Windows Server 2012 R2 and 2016
  - Tamper Protection
  - Attack Surface Reduction rules
  - Passive Mode
  - EDR Block
  - Live Response
  - Automated Investigation & Response (AIR)

# Supported Capabilities

Operating System	Windows 10 & 11	Windows Server 2012 R2 <sup>[1]</sup>	Windows Server 2016 <sup>[1]</sup>	Windows Server 2019 & 2022	Windows Server 2025+
Prevention					
Attack Surface Reduction rules	Y	Y	Y	Y	Y
Device Control	Y	N	N	N	N
Firewall	Y	Y	Y	Y	Y
Network Protection	Y	Y	Y	Y	Y
Next-generation protection	Y	Y	Y	Y	Y
Tamper Protection	Y	Y	Y	Y	Y
Web Protection	Y	Y	Y	Y	Y
Detection					
Advanced Hunting	Y	Y	Y	Y	Y
Custom file indicators	Y	Y	Y	Y	Y
Custom network indicators	Y	Y	Y	Y	Y
EDR Block & Passive Mode	Y	Y	Y	Y	Y
Sense detection sensor	Y	Y	Y	Y	Y
Endpoint & network device discovery	Y	N	N	N	N

---

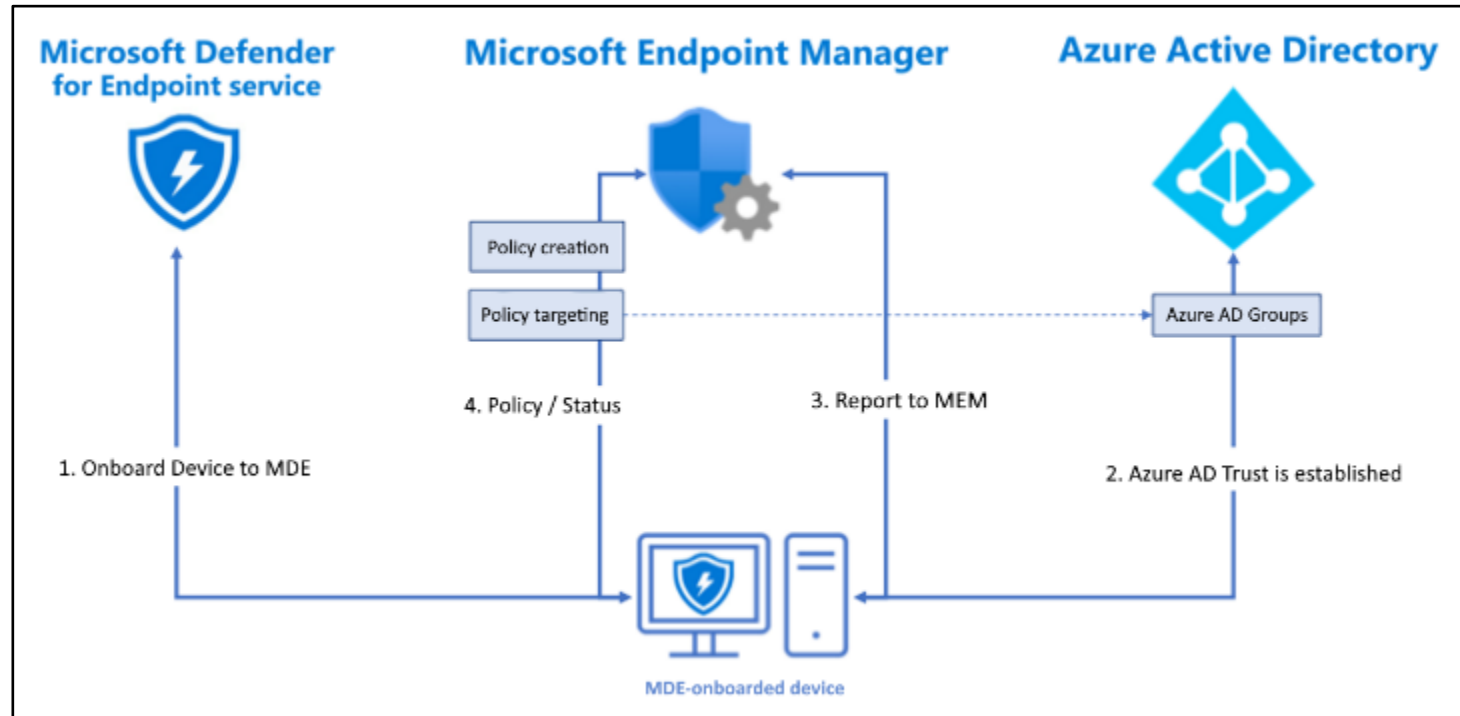
# Security Management



# Use-Cases

- Windows 10 that cannot be managed
- Windows Servers cannot be managed by Microsoft Endpoint Manager
- Windows Server configuration comes from GPO or SCCM
- Organizations with a cloud first mindset

# MDE Management Architecture





# Supported Workload

Microsoft Endpoint Manager	Workload	Policy	MDE Security configuration	Microsoft Endpoint Manager
Endpoint security	Antivirus	Antivirus	✓	✓
	Antivirus	Antivirus Exclusions	✓	✓
	Antivirus	Windows Security Experience		✓
	Disk Encryption	All		✓
	Firewall	Firewall	✓	✓
	Firewall	Firewall Rules	✓	✓
	Endpoint detection and response	Endpoint detection and response	✓	✓
	Attack surface reduction	All		✓
	Account Protection	All		✓
	Device Compliance	All		✓
	Conditional Access	All		✓
	Security baselines	All		✓

# Configure Security Management

1

## Security setting management

Allow security setting in Microsoft Endpoint Manager (MEM) to be enforced by Microsoft Defender for Endpoint (MDE). This configuration setting will apply to devices that are not yet enrolled to Microsoft Endpoint Manager.

You'll need to turn on the integration in Microsoft Defender for Endpoint connector settings under Microsoft Endpoint Manager. For more information, see [Onboard Windows devices in Microsoft Endpoint Manager through Microsoft Defender for Endpoint](#).

## Use MDE to enforce security configuration settings from MEM

☒ On

Choose which OS platforms to apply the settings on

☐ Windows Client devices

☐ Windows Server devices

## Pilot Mode

☐

If you would like to test this feature on a single or a couple of devices, you will need to tag devices with the "MDE-Management" tag. For more details on tagging, see [Create and manage device tags](#).

### Manage Security settings using Configuration Manager

☐ Off

Microsoft Defender for Endpoint will manage security settings on devices even if Config

For more information on co-existence with Configuration Manager, [see here](#).

3

## AV policies

[+ Create Policy](#) [↺ Refresh](#) [↓ Export](#)

 Search by column value

Policy name	Policy type	Assigned	Platform	Target
Microsoft Defender Antivirus	Microsoft Defender Antivirus	No	Windows 10 and later	mdm:microsoftSense

2

## Endpoint Security Profile Settings

Allow Microsoft Defender for Endpoint to enforce Endpoint Security Configurations ⓘ

# Exception: Microsoft Defender for Cloud

## ⓘ Note

**Exception:** If you have access to Microsoft Defender for Endpoint as part of a Microsoft Defender for Cloud only license (formerly Azure Security Center), the Security Management for Microsoft Defender for Endpoint functionality isn't available.

---

# Defender for Cloud



# What is Defender for Servers?

- Enhanced security features for Windows and Linux servers
- Integrated with Defender for Cloud
- Protect machines in hybrid and multi-cloud environments

# Defender for Servers Vs. Defender for Endpoint

## Defender for Servers

- Integrated license for Microsoft Defender for Endpoint
- Vulnerability Assessment using Qualys
- Adaptive application controls
- File integrity monitoring
- Just-in time VM access
- Adaptive network hardening

## Defender for Endpoint

- Standalone pricing for Servers
- Not include license for Defender for Servers

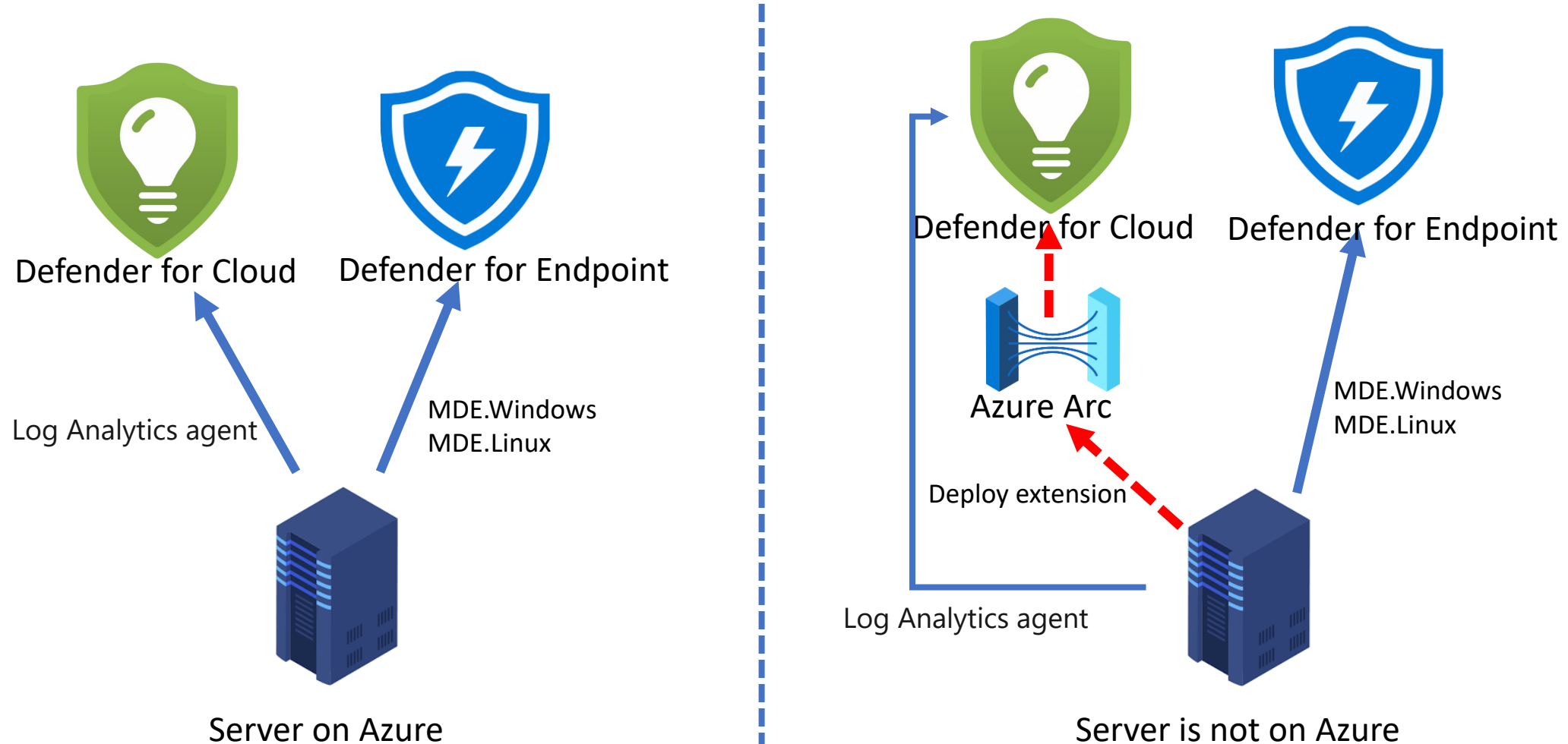


VS





# Architecture Comparison



# Multi-cloud & hybrid protection in Defender for Cloud



## Security posture & compliance

- Secure score
- Asset management
- Policy



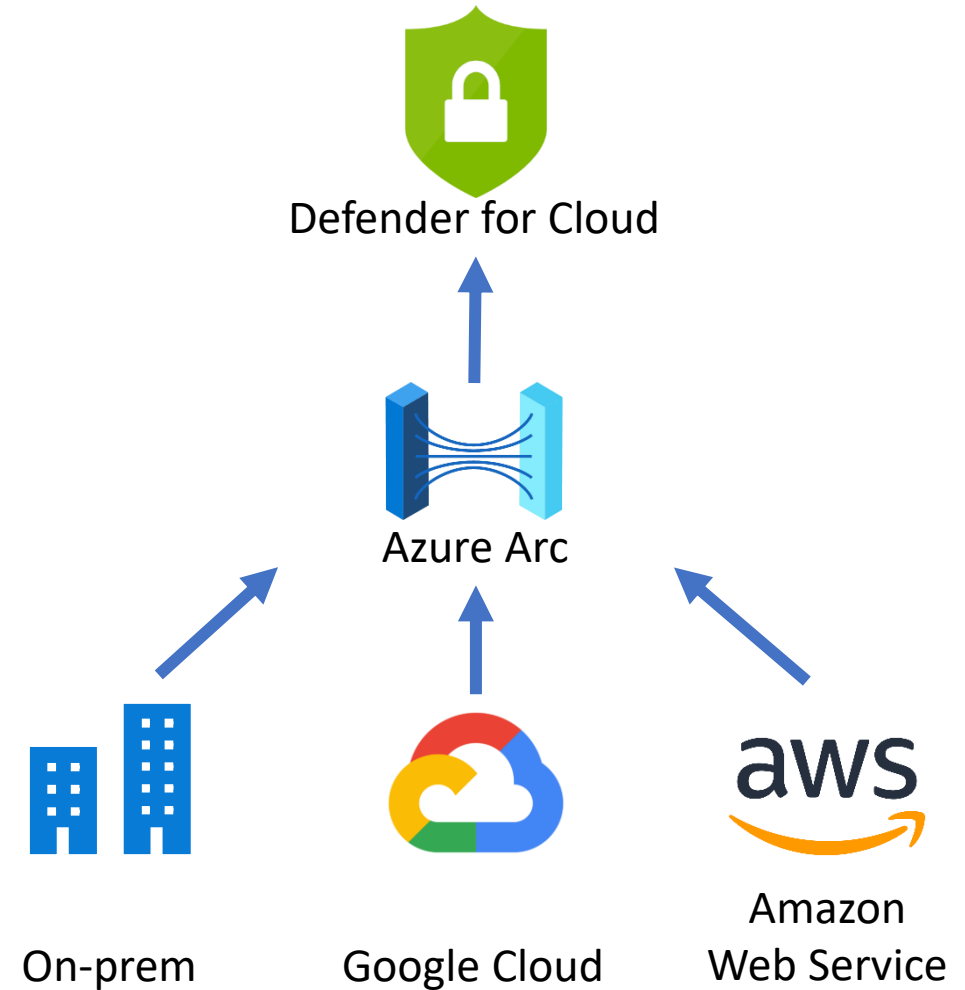
## Azure Defender

- Threat detection
- Vulnerability assessment
- Application control



## Automation & management

- Automation
- SIEM integration
- Export



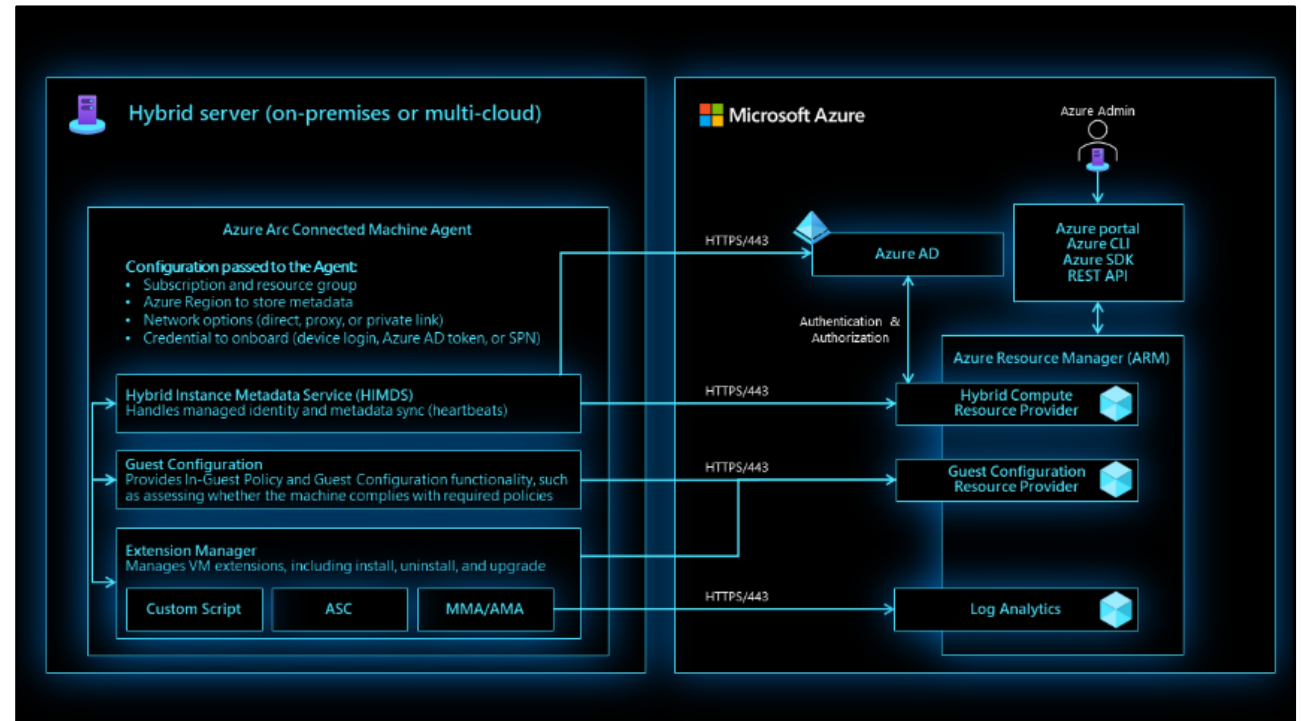
# Azure ARC Agent

## Azure ARC Components

- Hybrid Instance Metadata Service (HIMDS)
- Guest Configuration Agent
- Extension Manager Agent

## Azure ARC deploy extensions for MDE

- MDE.Windows
- MDE.Linux



# Unified Solutions

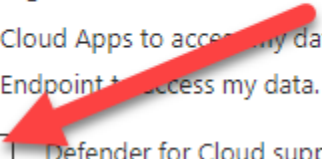
- Supports Microsoft Defender for Endpoint unified solution for Windows servers 2012R2 and Windows servers 2016
- Log Analysis Agent still required for non-MDE features

### Enable integrations

To enable Defender for Cloud to integrate with other Microsoft security services, allow those services to access your data.

- ☒ Allow Microsoft Defender for Cloud Apps to access my data. [Learn more >](#)
- ☒ Allow Microsoft Defender for Endpoint to access my data. [Learn more >](#)

Enable unified solution Defender for Cloud supports Microsoft Defender for Endpoint unified solution for Windows servers 2012R2 and Windows servers 2016. [Learn more >](#)



---

# Integration Architecture

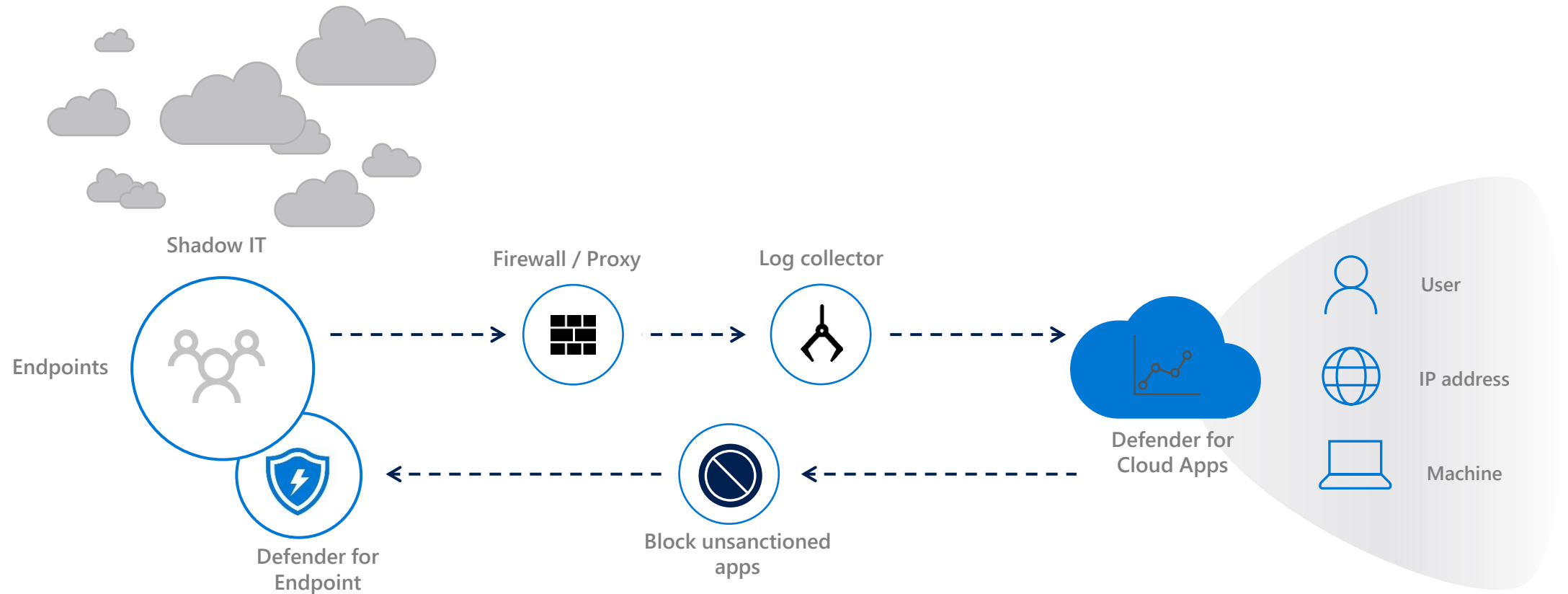


# Integration Architecture

- Microsoft Defender for Cloud
- Microsoft Sentinel
- Microsoft Endpoint Manager (Intune)
- Microsoft Defender for Cloud Apps
- Microsoft Defender for Identity
- Microsoft Defender for Office



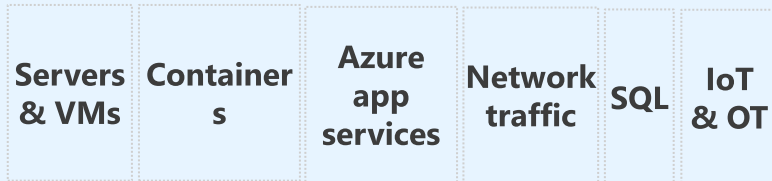
# Defender for Cloud Apps



# Extended Detection and Response (XDR)

## *Extended Detection and Response (XDR)*

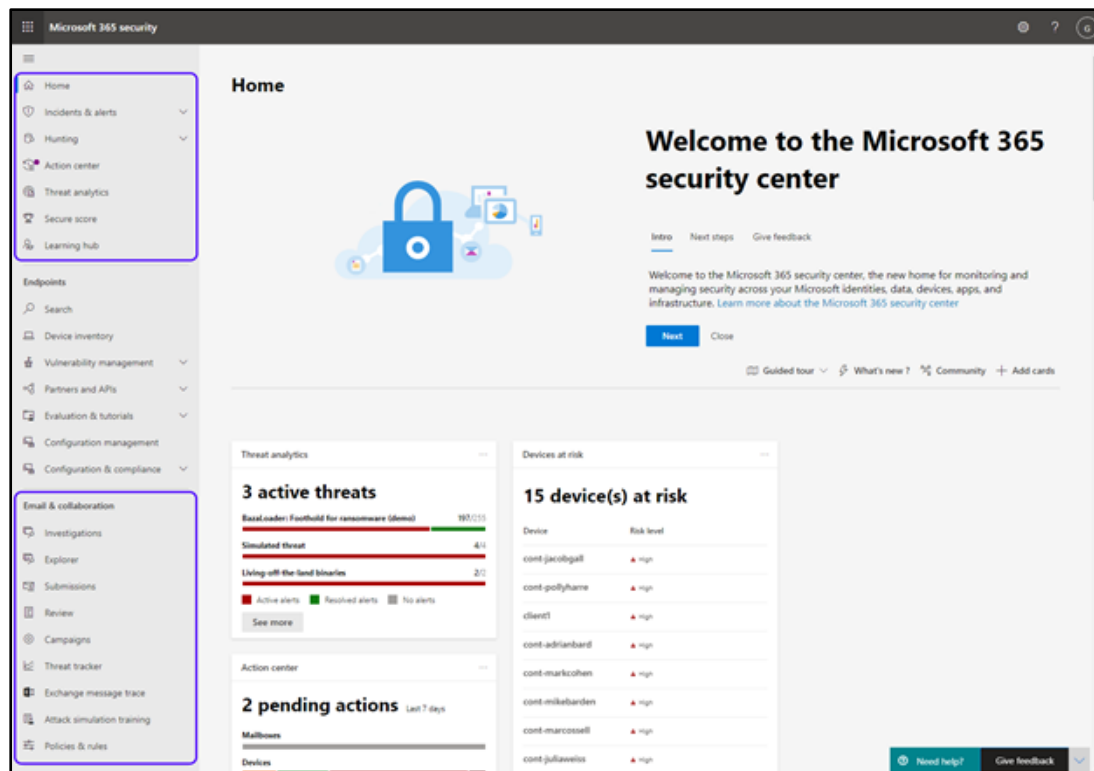
### Azure Defender



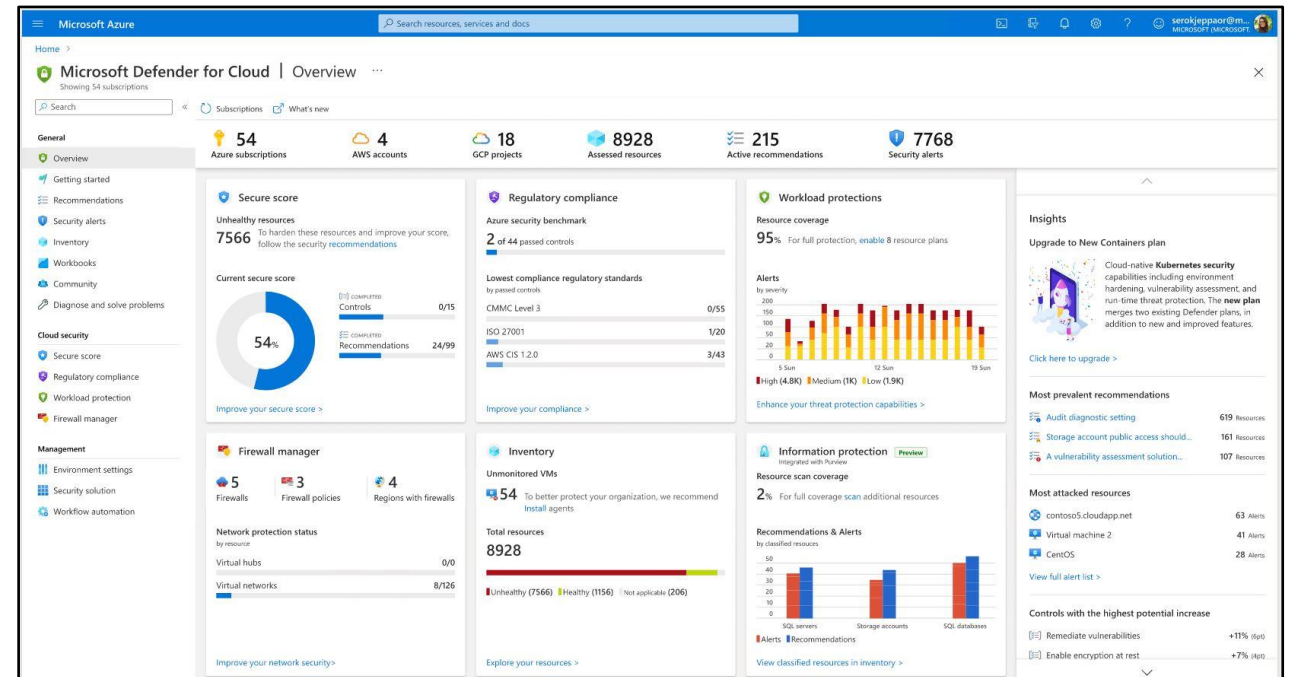
### Microsoft 365 Defender



# XDR Portal

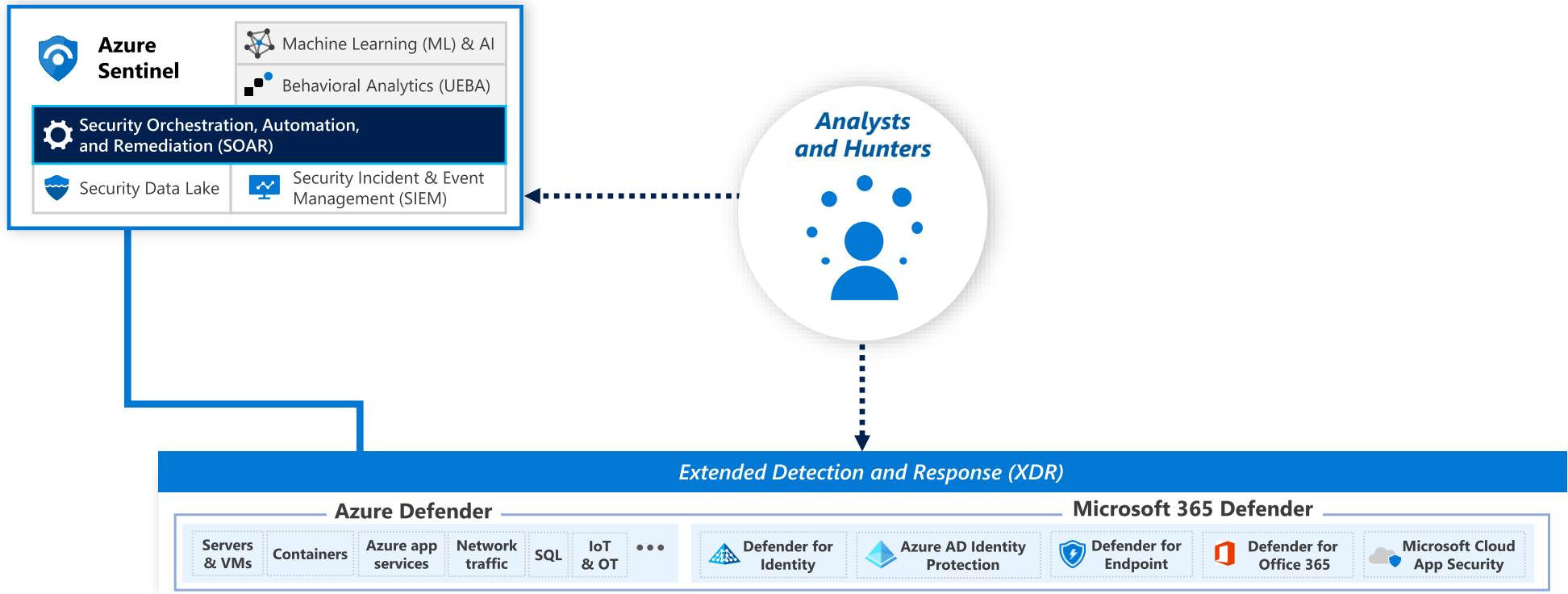


Microsoft 365 Defender Portal

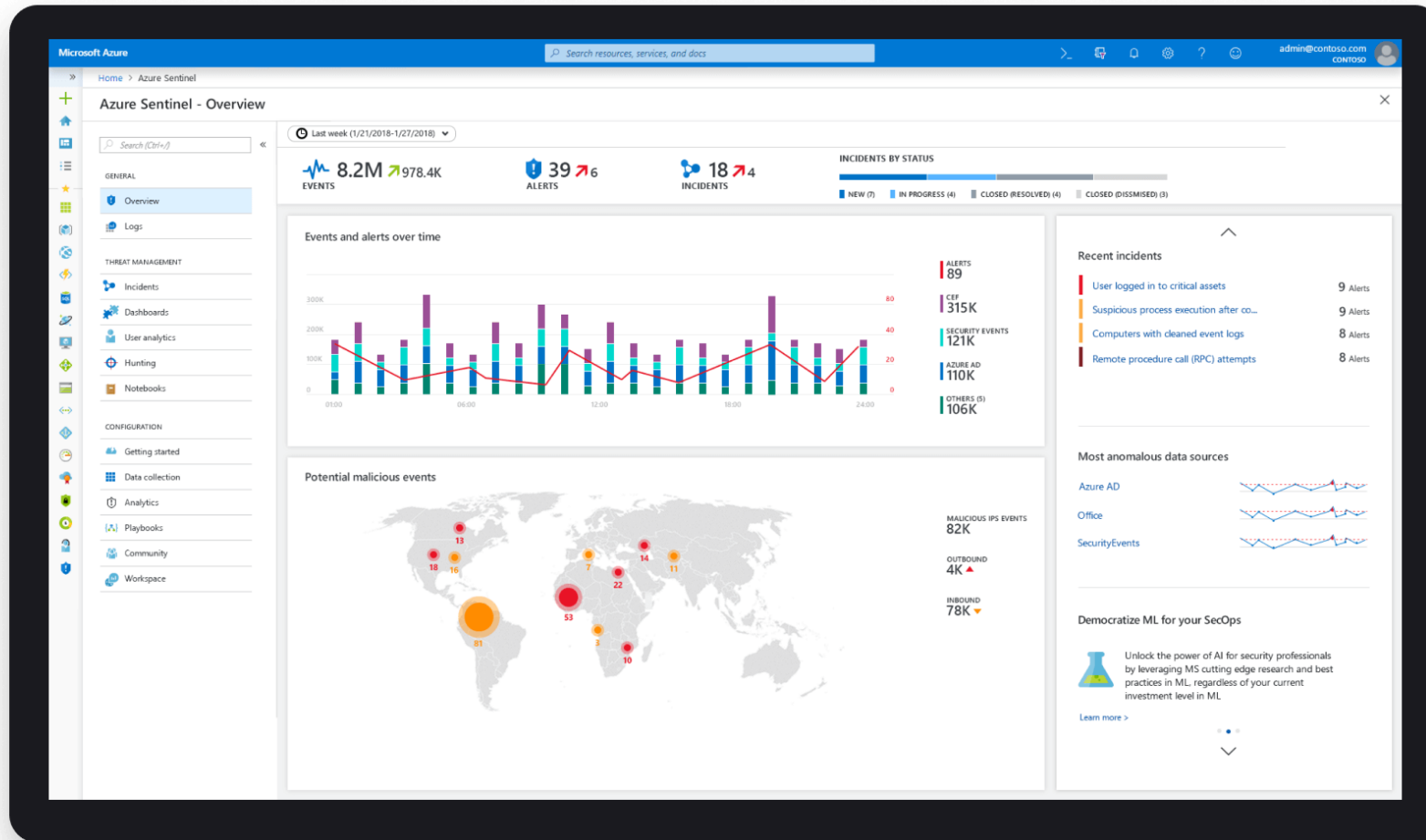


Defender for Cloud Portal

# XDR + SEIM



# Sentinel Portal



Microsoft Sentinel Portal

# Summary

- Windows 7 & Server 2008 require SCEP + MDE (or 3<sup>rd</sup> party AV)
- Deployment and configuration (at scale) requires an endpoint management solution
- Unified Solution Agent for Windows Server 2012 R2 & 2016
- Security Management for Windows endpoints not managed by MEM
- Enhanced security for Windows and Linux server through Defender for Cloud
- Multi-cloud and On-prem support through Azure ARC Agent for Defender for Cloud
- Integration with other Microsoft security solutions for XDR+SIEM+SOAR



# Thank You !!!



[@EhloWorldIO](https://twitter.com/EhloWorldIO)



<https://www.linkedin.com/in/petchen/>



[EHLOWorld.IO](https://www.EhloWorld.IO)