Deploy an endpoint detection and response (EDR) solution with Microsoft

Architect Microsoft Defender ATP for your organization, onboard machines, and integrate it with your Security Operations Center (SOC)

This topic is 1 of 6 in a series 1 2 3 4 5 6

For more architecture resources like this, see aka.ms/cloudarch.

Onboard machines to the Microsoft Defender ATP service

Microsoft Defender Advanced Threat Protection (ATP) is a platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats. Use this guide to select the appropriate Microsoft Defender ATP architecture based on your organizational needs and then assist your Security Operations Center (SOC) in onboarding machines and securing endpoints. This guide will provide high-level information on prerequisites, design, and configuration options. To get more detailed information about a particular topic (e.g., proxy settings or supported platforms) please review our public guidance.

Microsoft Endpoint Manager

Microsoft Endpoint Manager is a unified endpoint management and security platform, including the features and functionality delivered by Configuration Manager and Microsoft Intune

Microsoft Intune

Microsoft Intune is a cloud-based service that focuses on mobile device management (MDM) and mobile application management (MAM). When you use it with Microsoft 365, you can enable your workforce to be productive on all their devices, while keeping your organization's information protected.

Configuration Manager

Configuration Manager (ConfigMgr) is a comprehensive management solution for servers, desktops, and laptops. It can be leveraged to deploy applications, software updates, and operating systems in a secure and scalable manner.

Integrating Microsoft Defender ATP into your SOC

Deciding how to onboard, remediate and manage endpoints to the Microsoft Defender ATP service comes down to two important decisions: which architecture best maps to your organizations strategy and which deployment methods can be used based on the enterprises' current configuration management and deployment tools.

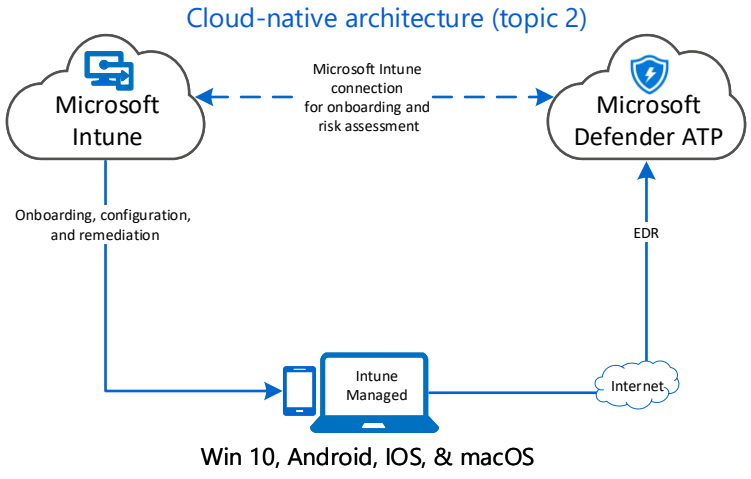
WHICH ARCHITECTURE?

- ☐ Cloud-native
- ☐ Co-management
- ☐ On-premises
- ☐ Script and evaluation

WHAT DEPLOYMENT METHOD?

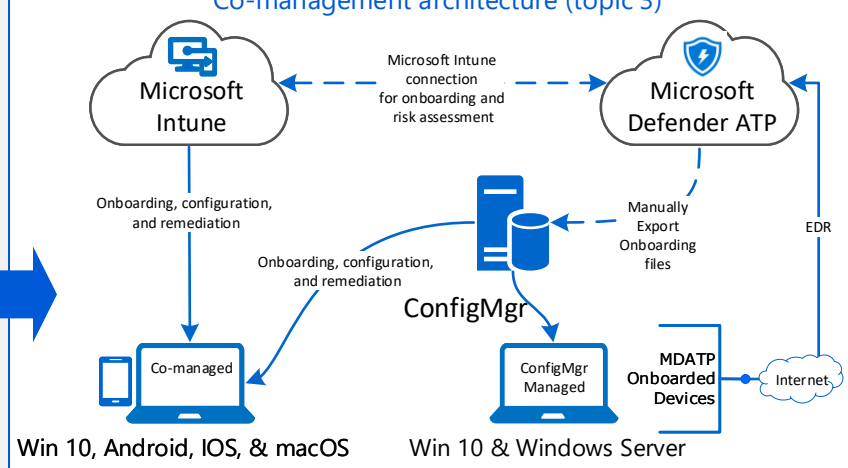
- ☐ Microsoft Intune
- ☐ Configuration Manager
- ☐ Group Policy
- ☐ Local script

Cloud-native architecture (topic 2)



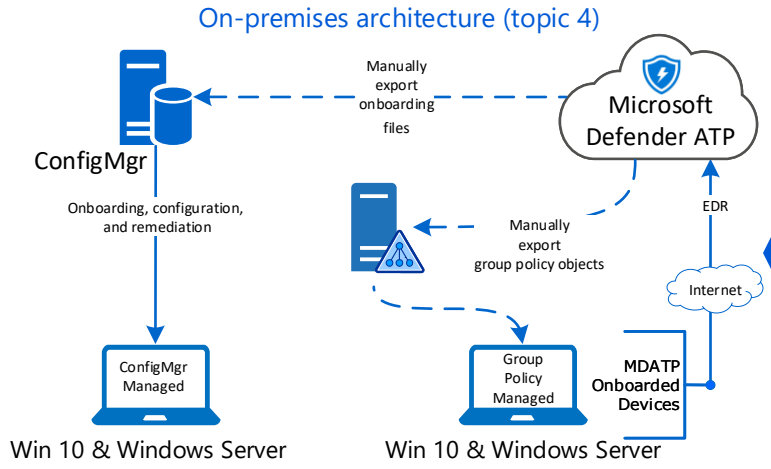
We recommend onboarding, configuring, and remediating Microsoft Defender ATP endpoints from the cloud with Microsoft Intune for enterprises that don't have an on-premises configuration management solution or whom are trying to reduce their current on-premises infrastructure footprint

Co-management architecture (topic 3)



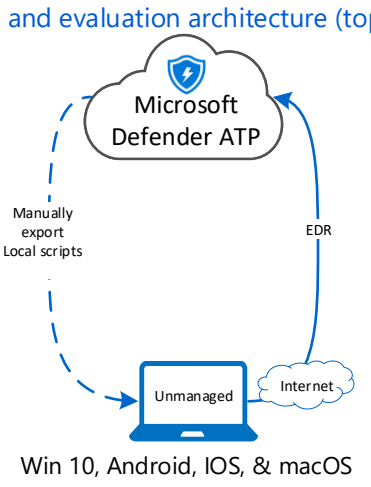
We recommend this architecture for organizations host both on-premises and cloud-based workloads. ConfigMgr and Intune provide integrated cloud-powered management tools, and unique co-management options to provision, deploy, manage, and secure endpoints and applications across an organization.

On-premises architecture (topic 4)



We recommend this architecture for enterprises that what to maximize their investments in Configuration Manager or Active Directory Domain Services while still leveraging the cloud-based power of Microsoft Defender ATP.

Script and evaluation architecture (topic 5)



We recommend this architecture for SOCs that are looking to evaluate or run a Microsoft Defender ATP pilot, but haven't invested in management or deployment tools. This architecture may also be used to onboard machines that are in small environments without management infrastructure (e.g., a DMZ)

Next steps to gain immediate value post-onboarding (topic 6)

Service Adoption Order: Microsoft defender ATP comes with several modules and services that can be enabled. This section will detail which services you should prioritize and the order that you should adopt them based on their value and ease of implementation.

Microsoft

Deploy an endpoint detection and response (EDR) solution with Microsoft

Architect Microsoft Defender ATP for your organization, onboard machines, and integrate it with your Security Operations Center (SOC)

This topic is 2 of 6 in a series 1 **2** 3 4 5 6

For more architecture resources like this, see aka.ms/cloudarch.

Onboard Microsoft Defender ATP using Microsoft Intune

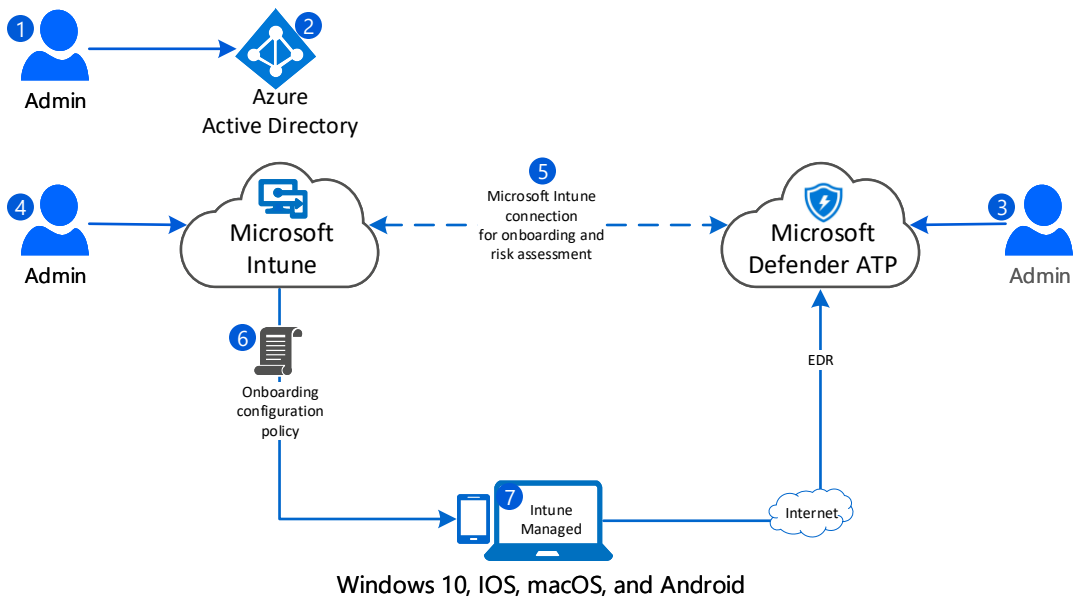
Microsoft Intune provides support for many different platforms and can be connected to the Microsoft Defender ATP service to ease onboarding. Microsoft Intune can also collect data about machines to help assess risk level then enforce compliance policies. When used with conditional access policies, users can be blocked from accessing corporate resources if they are non-compliant. Devices can be onboarded using other MDM solutions, but Microsoft officially supports only Intune, OMA-URIs, and JAMF-based deployments.

WHICH ARCHITECTURE? ☐ Cloud-native

WHAT DEPLOYMENT METHOD? ☐ Microsoft Intune

Onboard machines to Microsoft Defender ATP using Microsoft Intune

1. Sign in to the Azure Portal and configure automatic enrollment for Intune by configuring the **MDM User Scope** in Azure Active Directory
2. Assign Intune licenses to users in Azure Active Directory and ensure their devices are enrolled
3. Sign in to the Microsoft Defender Security Center and complete the initial setup wizard
4. Sign in to the Microsoft Endpoint Manager admin center and navigate to **Open the Microsoft Defender Security Center** to connect to the Microsoft Defender ATP service
5. In the Microsoft Defender Security Center, turn on the **Microsoft Intune connection** setting
6. In the Microsoft Endpoint Manager admin center, create a device configuration policy using the **Microsoft Defender ATP (Windows 10 Desktop)** profile type (please note that non-Windows devices require an installation package that must be downloaded from the Microsoft Defender Security Center)
7. To verify that the machines are properly onboarded and reporting, run a detection test on the newly onboarded devices (commands can be found in the Microsoft Defender Security Center settings under **Onboarding**)



Prepare

1. Assess your infrastructure: including network proxy configurations, internet connectivity to endpoints, deployment and management tools, and hosting environments.

2. Choose compatible platforms: including Windows 10, macOSX, and Android. Ensure that they are both supported by Microsoft Defender ATP and that your enterprise's deployment and management tools can perform onboarding and remediation tasks.

3. Assess application compatibility: including supported browsers, diagnostic data settings, Microsoft Defender ATP agents for non-Windows devices, and the coexistence of existing endpoint security solutions.

4. Choose the right architecture: use the cloud-only, Microsoft Intune approach if you don't have existing management and deployment tools capable of supporting Microsoft Defender ATP or if your are trying to reduce your total cost of ownership and datacenter footprint.

Setup

1. Identify pilot users and platforms: identify the users and platforms that you want to participate in the pilot and prepare their devices by ensuring they have internet connectivity (see public guidance for proxy URLs), diagnostic data settings enabled (Windows devices), and licensed operating systems

2. Procure and assign Microsoft Intune and Defender ATP licensing: ensure that the appropriate Microsoft Defender ATP and Intune licensing has been procured (see public guidance or contact a licensing specialist) and assign it to user's participating in the pilot through Azure Active Directory

3. Setup Microsoft Defender Security Center: complete the initial setup wizard in the Microsoft Defender Security Center which includes role-based access control (RBAC), data retention policies, organizational size, geographical storage locations, and the option to use preview features

4. Connect Intune and Microsoft Defender Security Center: ensure that Microsoft Intune connection is turned on in the Microsoft Defender Security Center and download onboarding packages for any non-Windows devices

Onboard

1. Onboard pilot devices: create a device configuration policy in Microsoft Intune using the **Microsoft Defender ATP (Windows 10 Desktop)** profile type

Optional: create compliance policies in Microsoft Intune to determine an acceptable risk level to allow and then create conditional access policies to block access to corporate resources if a device is determined to be non-compliant

2. Verify onboarding was successful: on the first devices onboarded, run a detection test to ensure that the device is communicating with the Microsoft Defender ATP service (see instructions in Microsoft Defender Security Center)

3. Conduct an enterprise rollout: onboard the rest of your enterprise's devices and see topic 6 to start adopting the full suite of Microsoft Defender ATP services

February 2020

Microsoft

Deploy an endpoint detection and response (EDR) solution with Microsoft

Architect Microsoft Defender ATP for your organization, onboard machines, and integrate it with your Security Operations Center (SOC)

This topic is 3 of 6 in a series 1 2 **3** 4 5 6

For more architecture resources like this, see aka.ms/cloudarch.

Onboard to Microsoft Defender ATP using Microsoft Intune and Configuration Manager

ConfigMgr and Intune provide integrated cloud-powered management tools, and unique co-management options to provision, deploy, manage, and secure endpoints and applications across an organization. This is perfect for organizations that manage both on-premises and cloud-native workloads.

WHICH ARCHITECTURE?

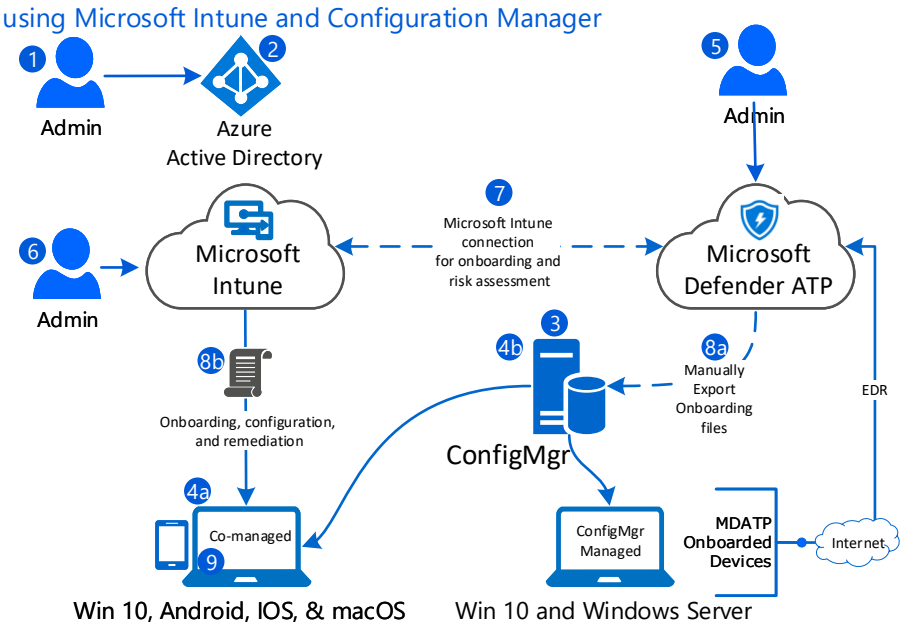
- ☐ Co-management

WHAT DEPLOYMENT METHOD?

- ☐ Microsoft Intune
- ☐ Configuration Manager

Onboard machines to Microsoft Defender ATP using Microsoft Intune and Configuration Manager

1. Sign in to the Azure Portal configure automatic enrollment for Intune by configuring the **MDM User Scope** in Azure Active Directory
2. Assign Intune licenses to users in Azure Active Directory and ensure their devices are enrolled
3. Choose which workloads you want to be managed by Microsoft Intune and switch them in the Configuration Manager co-management node
4a. Install the Configuration Manager agent on new devices that are auto-enrolled into Azure AD (see public guidance on setting up co-management and ensure that Azure AD Connect is configured for hybrid Azure AD)
4b. Configure Windows 10 devices that are already Configuration Manager clients to be hybrid Azure AD-joined, and enroll them in Intune
5. Sign in to the Microsoft Defender Security Center and complete the initial setup wizard
6. Sign in to the Microsoft Endpoint Manager admin center and navigate to **Open the Microsoft Defender Security Center** to connect to the Microsoft Defender ATP service
7. In the Microsoft Defender Security Center, turn on the **Microsoft Intune connection** setting
8a. In the Microsoft Defender Security Center, go to **Onboarding** under settings, download a System Center Configuration Manager package, and import it into your Configuration Manager environment
8b. In the Microsoft Endpoint Manager admin center, create a device configuration policy using the **Microsoft Defender ATP (Windows 10 Desktop)** profile type (please note that non-Windows devices require an installation package that must be downloaded from the Microsoft Defender Security Center)
9. To verify that the machines are properly onboarded and reporting, run a detection test on the newly onboarded devices (commands can be found in the Microsoft Defender Security Center settings under **Onboarding**)



Prepare

1. Assess your infrastructure: including network proxy configurations, internet connectivity to endpoints, deployment and management tools, and hosting environments.

2. Choose compatible platforms: including Windows 10, Windows Server, macOSX, and Android. Ensure that they are both supported by Microsoft Defender ATP and that your enterprise's deployment and management tools can perform onboarding and remediation tasks.

3. Assess application compatibility: including supported browsers, diagnostic data settings, Microsoft Defender ATP agents for non-Windows devices, and the coexistence of existing endpoint security solutions.

4. Choose the right architecture: use the co-management architecture if you manage both on-premises and cloud-native workloads and want more platform and management flexibility.

Setup

1. Identify pilot users and platforms: identify the users and platforms that you want to participate in the pilot and prepare their devices by ensuring they have internet connectivity (see public guidance for proxy URLs), diagnostic data settings enabled (Windows devices), and licensed operating systems

2. Procure and assign Microsoft Intune and Defender ATP licensing: ensure that the appropriate Microsoft Defender ATP and Intune licensing has been procured (see public guidance or contact a licensing specialist) and assign it to user's participating in the pilot through Azure Active Directory

3. Choose Microsoft Intune managed workloads: configure selected services to use Microsoft Intune in the Configuration Manager co-management node

4a. Set up new, internet-based devices: install the Configuration Manager agent on new devices that are auto-enrolled into Azure AD

4b. Set up existing Configuration Manager devices: configure Windows 10 devices that are already Configuration Manager clients to be hybrid Azure AD-joined, and enroll them in Intune (see public guidance on setting up co-management and ensure that Azure AD Connect is configured for hybrid Azure AD)

5. Setup Microsoft Defender Security Center: complete the initial setup wizard in the Microsoft Defender Security Center which includes role-based access control (RBAC), data retention policies, organizational size, geographical storage locations, and the option to use preview features

6. Connect Intune and Microsoft Defender Security Center: ensure that Microsoft Intune connection is turned on in the Microsoft Defender Security Center and download onboarding packages for any non-Windows devices

Onboard

1. Onboard Configuration Manager pilot devices: download a Configuration Manager installation package from the Microsoft Defender Security Center and import it into your configuration manager environment

2. Onboard Intune pilot devices: create a device configuration policy in Microsoft Intune using the **Microsoft Defender ATP (Windows 10 Desktop)** profile type

Optional: create compliance policies in Microsoft Intune to determine an acceptable risk level to allow and then create conditional access policies to block access to corporate resources if a device is determined to be non-compliant

3. Verify onboarding was successful: on the first devices onboarded, run a detection test to ensure that the device is communicating with the Microsoft Defender ATP service (see instructions in Microsoft Defender Security Center)

5. Run Microsoft Defender ATP's evaluation tutorial: sign in to Microsoft Defender ATP security Center and use the Evaluation and Simulation tab to evaluate the product and familiarize security administrators and operators

6. Conduct an enterprise rollout: onboard the rest of your enterprise's devices and see topic 6 to start adopting the full suite of Microsoft Defender ATP services

Microsoft

Deploy an endpoint detection and response (EDR) solution with Microsoft

Architect Microsoft Defender ATP for your organization, onboard machines, and integrate it with your Security Operations Center (SOC)

This topic is 4 of 6 in a series 1 2 3 **4** 5 6

For more architecture resources like this, see aka.ms/cloudarch.

Onboard to Microsoft Defender ATP using Configuration Manager or Group Policy Objects

Many enterprises leverage Configuration Manager or group policy objects as their primary device management solution. Additionally, an organization may use a non-Microsoft product for configuration management. This architecture enables organizations to maximize their current investments while still taking advantage of the cloud-based power of Microsoft Defender ATP.

WHICH ARCHITECTURE?

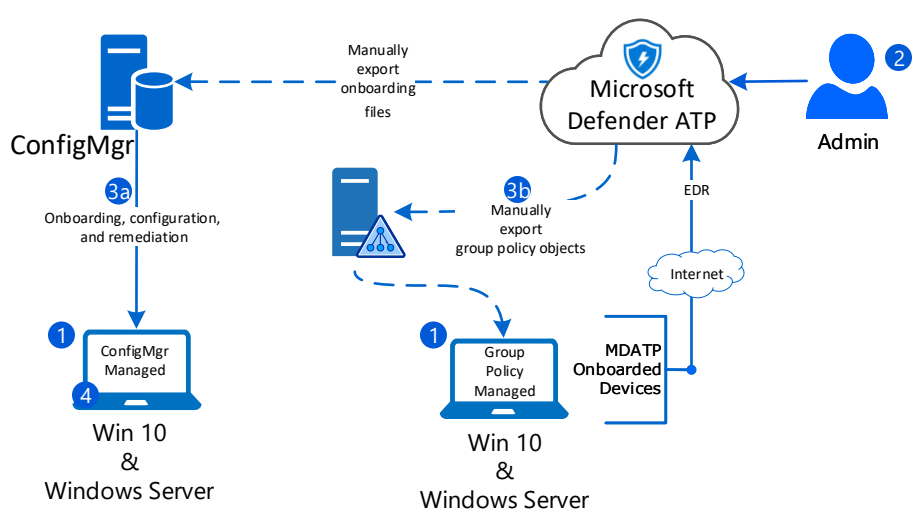
- ☐ On-premises

WHAT DEPLOYMENT METHOD?

- ☐ Configuration Manager
- ☐ Group Policy Objects

Onboard machines to Microsoft Defender ATP using Configuration Manager or Group Policy Objects

1. Ensure that the devices to be onboarded are either communicating to the Configuration Manager service or pulling policy from a domain controller
2. Sign in to the Microsoft Defender Security Center and complete the initial setup wizard
3a. To onboard using Configuration Manager, go in to the Microsoft Defender Security Center's **Onboarding** tab under settings, download a System Center Configuration Manager package, and deploy it to a predefined collection
3b. To onboard using group policy, go in to the Microsoft Defender Security Center's **Onboarding** tab under settings, download a Group Policy package, create a scheduled in the Group Policy Management Console, and instruct it to run a task to run the onboarding script as a program
4. To verify that the machines are properly onboarded and reporting, run a detection test on the newly onboarded devices (commands can be found in the Microsoft Defender Security Center settings under **Onboarding**)



Prepare

1. Assess your infrastructure: including network proxy configurations, internet connectivity to endpoints, deployment and management tools, and hosting environments.

2. Choose compatible platforms: including Windows 10 and Windows Server. Ensure that they are both supported by Microsoft Defender ATP and that your enterprise's deployment and management tools can perform onboarding and remediation tasks.

3. Assess application compatibility: including supported browsers, diagnostic data settings, Microsoft Defender ATP agents for non-Windows devices, and the coexistence of existing endpoint security solutions.

4. Choose the right architecture: use the on-premises architecture to maximize investments in Configuration Manager or Active Directory Domain Services while still leveraging the cloud-based power of Microsoft Defender ATP.

Setup

1. Identify pilot users and platforms: identify the users and platforms that you want to participate in the pilot and prepare their devices by ensuring they have internet connectivity (see public guidance for proxy URLs), diagnostic data settings enabled (Windows devices), and licensed operating systems

2. Procure and assign Defender ATP licensing: ensure that the appropriate Microsoft Defender ATP licensing has been procured (see public guidance or contact a licensing specialist)

3a. Set up Configuration Manager devices: ensure that devices are communicating the Configuration Manager service via an agent and if necessary, create device collections to control which devices get onboarded to the Microsoft Defender ATP service first

3b. Set up group policy managed devices: ensure that the devices are domain-joined to an Active Directory Domain Services domain and receiving policy from a domain controller

4. Setup Microsoft Defender Security Center: complete the initial setup wizard in the Microsoft Defender Security Center which includes role-based access control (RBAC), data retention policies, organizational size, geographical storage locations, and the option to use preview features

Onboard

1. Onboard Configuration Manager pilot devices: download a Configuration Manager installation package from the Microsoft Defender Security Center and import it into your configuration manager environment

2. Onboard group policy pilot devices: download the group policy installation package from the Microsoft Defender Security Center, create a group policy object with a scheduled task, and run the onboarding command file as a program to filter, pilot devices

3. Verify onboarding was successful: on the first devices onboarded, run a detection test to ensure that the device is communicating with the Microsoft Defender ATP service (see instructions in Microsoft Defender Security Center)

4. Run a detection test on each type of platform: on the first devices onboarded, run a detection test to ensure that the device is communicating with the Microsoft Defender ATP service (see instructions in Microsoft Defender Security Center)

5. Run Microsoft Defender ATP's evaluation tutorial: sign in to Microsoft Defender ATP security Center and use the Evaluation and Simulation tab to evaluate the product and familiarize security administrators and operators

6. Conduct an enterprise rollout: onboard the rest of your enterprise's devices and see topic 6 to start adopting the full suite of Microsoft Defender ATP services

February 2020

Microsoft

Deploy an endpoint detection and response (EDR) solution with Microsoft

Architect Microsoft Defender ATP for your organization, onboard machines, and integrate it with your Security Operations Center (SOC)

This topic is 5 of 6 in a series 1 2 3 4 **5** 6

For more architecture resources like this, see aka.ms/cloudarch.

Onboard to Microsoft Defender ATP using local scripts

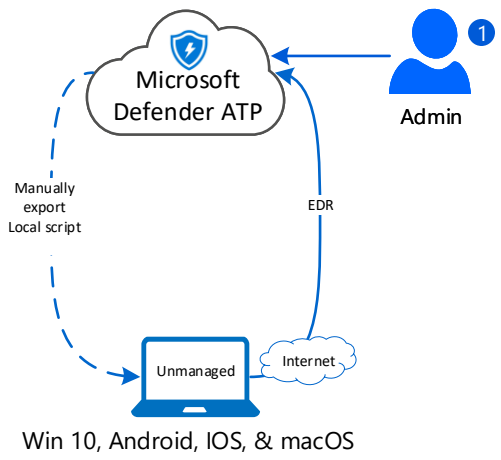
Local scripts are a great way to conduct a quick Microsoft Defender ATP evaluation or to onboard machines that are in small, specialized environments without management infrastructure (e.g., DMZ). Each script can be used on a limited number of machines (up to 10) and is ran locally on the device.

WHICH ARCHITECTURE? □ Script and evaluation

WHAT DEPLOYMENT METHOD? □ Local script

Onboard machines to Microsoft Defender ATP using Configuration Manager or Group Policy Objects

1. Sign in to the Microsoft Defender Security Center and complete the initial setup wizard
2. Go in to the Microsoft Defender Security Center's **Onboarding** tab under settings, select the appropriate operating system, and download a Local script
3. Copy the script to the devices you want to onboard and run it locally
4. To verify that the machines are properly onboarded and reporting, run a detection test on the newly onboarded devices (commands can be found in the Microsoft Defender Security Center settings under **Onboarding**)



Prepare

1. Assess your infrastructure: including network proxy configurations, internet connectivity to endpoints, deployment and management tools, and hosting environments.

2. Choose compatible platforms: including Windows 10, Windows Server, macOSX, and Android. Ensure that they are both supported by Microsoft Defender ATP and that your enterprise's deployment and management tools can perform onboarding and remediation tasks.

3. Assess application compatibility: including supported browsers, diagnostic data settings, Microsoft Defender ATP agents for non-Windows devices, and the coexistence of existing endpoint security solutions.

4. Choose the right architecture: use the evaluation and local onboarding architecture to conduct a minimally invasive evaluation of Microsoft Defender ATP or to deploy to small, specialized environments without a robust management solution (e.g., a DMZ)

Setup

1. Identify pilot users and platforms: identify the users and platforms that you want to participate in the pilot and prepare their devices by ensuring they have internet connectivity (see public guidance for proxy URLs), diagnostic data settings enabled (Windows devices), and licensed operating systems

2. Procure and assign Defender ATP licensing: ensure that the appropriate Microsoft Defender ATP licensing has been procured (see public guidance or contact a licensing specialist)

4. Setup Microsoft Defender Security Center: complete the initial setup wizard in the Microsoft Defender Security Center which includes role-based access control (RBAC), data retention policies, organizational size, geographical storage locations, and the option to use preview features

Onboard

1. Onboard pilot devices: download a local script installation package from the Microsoft Defender Security Center and run it locally on the devices you want to onboard

2. Verify onboarding was successful: on the first devices onboarded, run a detection test to ensure that the device is communicating with the Microsoft Defender ATP service (see instructions in Microsoft Defender Security Center)

3. Run a detection test on each type of platform: on the first devices onboarded, run a detection test to ensure that the device is communicating with the Microsoft Defender ATP service (see instructions in Microsoft Defender Security Center)

4. Run Microsoft Defender ATP's evaluation tutorial: sign in to Microsoft Defender ATP security Center and use the Evaluation and Simulation tab to evaluate the product and familiarize security administrators and operators

5. Conduct an enterprise rollout: onboard the rest of your enterprise's devices using a scalable deployment method (local scripts are restricted to 10 devices each) and see topic 6 to start adopting the full suite of Microsoft Defender ATP services

Microsoft

Deploy an endpoint detection and response (EDR) solution with Microsoft

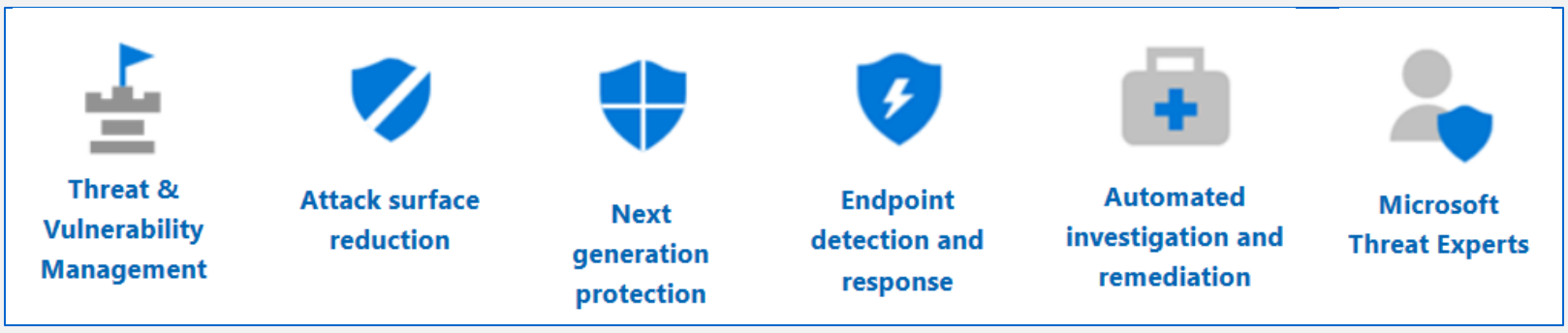
Architect Microsoft Defender ATP for your organization, onboard machines, and integrate it with your Security Operations Center (SOC)

For more architecture resources like this, see aka.ms/cloudarch.

Microsoft Defender ATP adoption order

Most organizations have existing endpoint security products deployed in their environment prior to onboarding devices to Microsoft Defender ATP. It is common that Microsoft Defender ATP will need to exist along-side these existing endpoint security products either indefinitely or during a cutover period (see public guidance on placing Windows Defender AV in passive mode).

Fortunately, Microsoft Defender ATP and the endpoint security suite is modular and can be adopted in a systematic approach. The content below provides Microsoft's recommended adoption order and will help your organization gain immediate value.



Service Adoption Order

Component	Description	Adoption Rank Order
Endpoint Detection & Response (EDR)	Endpoint detection and response capabilities are put in place to detect, investigate, and respond to advanced threats that may have made it past the first two security pillars. Advanced hunting provides a query-based threat-hunting tool that lets you proactively find breaches and create custom detections.	1
Threat & Vulnerability Management (TVM)	This built-in capability uses a game-changing risk-based approach to the discovery, prioritization, and remediation of endpoint vulnerabilities and misconfigurations. Threat & Vulnerability Management also includes Configuration Score. Configuration score gives you visibility and control over the security posture of your organization based on security best practices. High configuration score means your endpoints are more resilient from cybersecurity threat attacks.	2
Next Generation Protection (NGP)	Microsoft Defender Antivirus is a built-in antimalware solution that provides next generation protection for desktops, portable computers, and servers.	3
Attack Surface Reduction (ASR)	The attack surface reduction set of capabilities provide the first line of defense in the stack. By ensuring configuration settings are properly set and exploit mitigation techniques are applied, these set of capabilities resist attacks and exploitation. This set of capabilities also includes network protection and web protection, which regulate access to malicious IP addresses, domains, and URLs.	4
Auto Investigation & Remediation (AIR)	Microsoft Defender ATP uses Automated investigations to significantly reduce the volume of alerts that need to be investigated individually. The Automated investigation feature leverages various inspection algorithms, and processes used by analysts (such as playbooks) to examine alerts and take immediate remediation action to resolve breaches. This significantly reduces alert volume, allowing security operations experts to focus on more sophisticated threats and other high value initiatives.	Not applicable
Microsoft Threat Experts (MTE)	Microsoft Defender ATP's new managed threat hunting service provides proactive hunting, prioritization, and additional context and insights that further empower Security operation centers (SOCs) to identify and respond to threats quickly and accurately.	Not applicable