Endpoint Detection and Response (EDR)

or

eXtended Detection and Response (XDR)

MICROSOFT DEFENDER FOR ENDPOINT

Why EDR?

What is the event ID for new process creation?

It is 4688. But, by default process creation and termination do not generate logs

Should we onboard end-user machine logs?

The value we get out of end-user machine logs is not worth the budget it requires to onboard them . Also several logs are collected from centralized servers like AD, AV server, Web Gateway, DNS etc.

How do we get to know when a local user is created on a computer.?

SOC won’t know. Because, even though the log will be generated, it won’t reach SIEM

If we get to know data exfiltration has happened? Can we learn how much data has gone out?

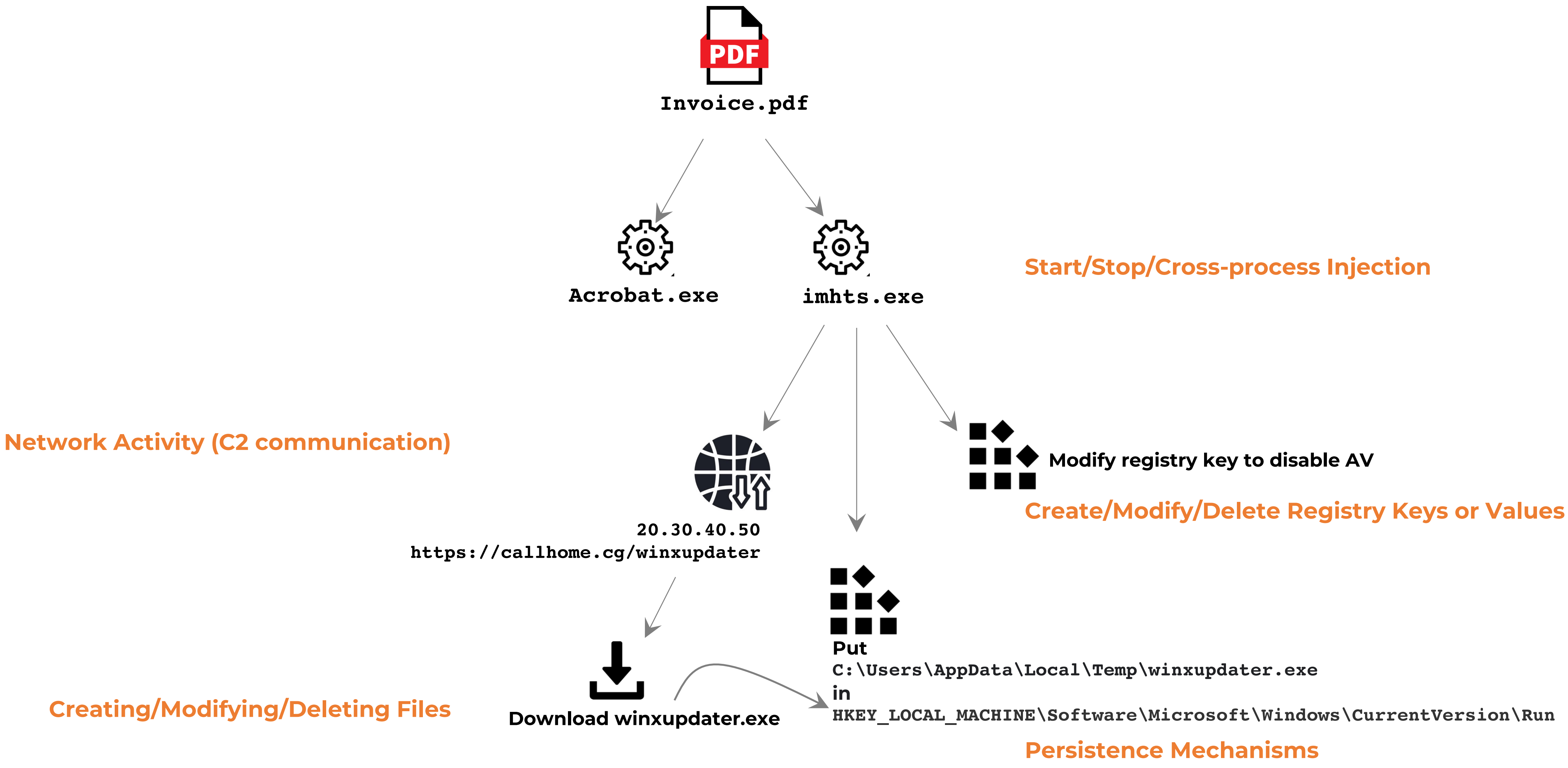
Very difficult.

LACK OF VISIBILITY or BLINDSPOT on host activities.

Levels of Scan – for Malware

1. Antivirus	Signature based	Known Malware
2. Threat Intelligence	IOC based	New or Zero-day Malware
3. Sandbox	Behavior based	New or Targeted Malware

Malware Behaviors



Invoice.pdf

Acrobat.exe

imhts.exe

Start/Stop/Cross-process Injection

Network Activity (C2 communication)

20.30.40.50
https://callhome.cg/winxupdater

Modify registry key to disable AV

Create/Modify/Delete Registry Keys or Values

Put
C:\Users\AppData\Local\Temp\winxupdater.exe
in
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

Creating/Modifying/Deleting Files

Download winxupdater.exe

Persistence Mechanisms

EDR

- **EDR** → Endpoint Detection & Response

- Detection of new/unknown malware in real-time

- Based on the *behaviors* exhibited by the file

Creating/Modifying/Deleting Files

Start/Stop/Cross-process Injection

Create/Modify/Delete Registry Keys or Values

Network Activity (C2 communication)

Persistence Mechanisms

- **Detection** happens using the *AI/ML models*

- Through EDR we can also **Respond** to (remediate) malware

→ Stop the execution of a file

→ Isolate machine

→ Get file (without remote session)

How it relates to SOC?

- XDR is monitored by the SOC team (besides SIEM).
- XDR gives greater visibility into host activities.
- Helps in investigating suspicious/malicious activities on the host. (without the need for other teams & tools OR need for end-user participation)
- Helps the SOC team in taking remediation actions quickly. (the R part of XDR)
- XDR can be an effective threat-hunting tool.

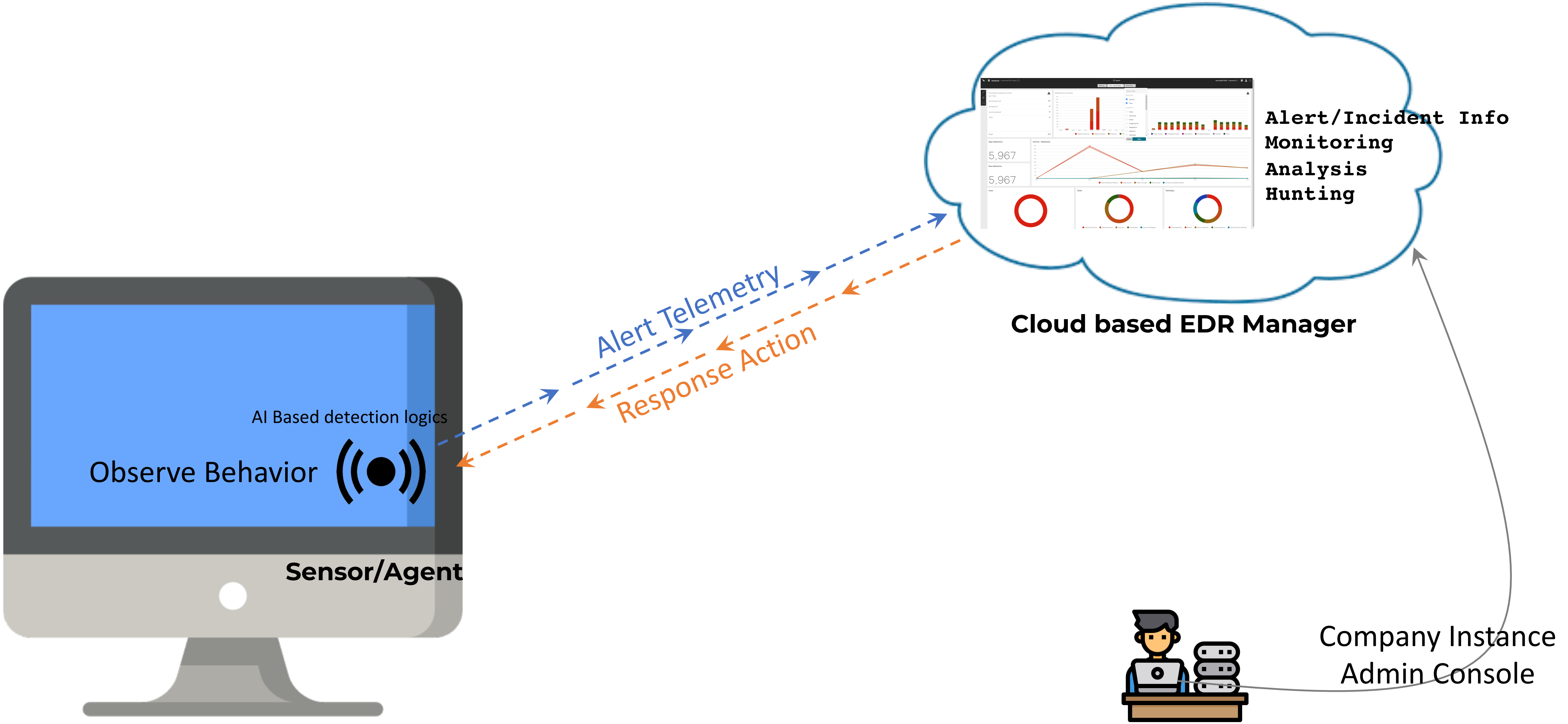
EDR vs XDR

EDR works at Endpoint layer only

Most vendors fall in between the 2 capabilities

XDR works at Endpoint, Network, Identity Management, Email and Cloud layers

General EDR/XDR Architecture



AI Based detection logics

Observe Behavior

Sensor/Agent

Alert Telemetry

Response Action

Alert/Incident Info
Monitoring
Analysis
Hunting

Cloud based EDR Manager

Company Instance
Admin Console

Microsoft Defender for Endpoint

Microsoft Defender for Endpoint

MICROSOFT
DEFENDER FOR ENDPOINT

Next-gen AV protection

Typical AV features | Signature based detection | Heuristic based detection

Firewall

Host firewall

Application control

Whitelisting of application - Only trusted apps can run or make modification to critical files

Attack surface reduction

Hardening | Block certain application behaviors

Threat & vulnerability

Asset visibility | Intelligent Assessments | Built-in Remediation | Breach likelihood prediction

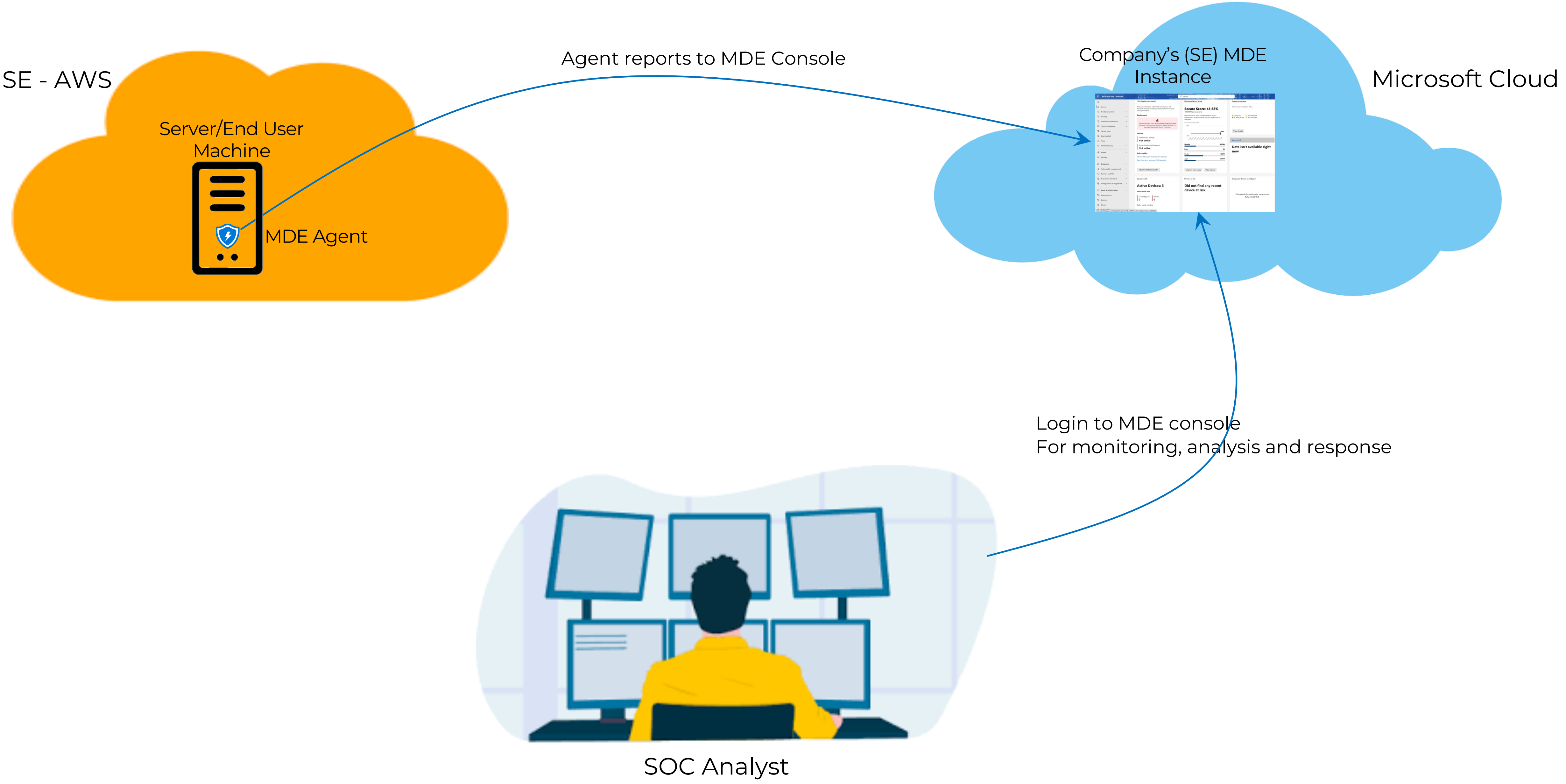
EDR behavioral sensors

Observe & record what is happening in the machine | Passed on to MDE Tenant in Cloud

EDR response controller

Isolation | Quarantining | Investigation package | Restrict app execution | Run a scan | Live Response Session

SOC Experts Lab Architecture



SE - AWS

Server/End User Machine

MDE Agent

Agent reports to MDE Console

Company's (SE) MDE Instance

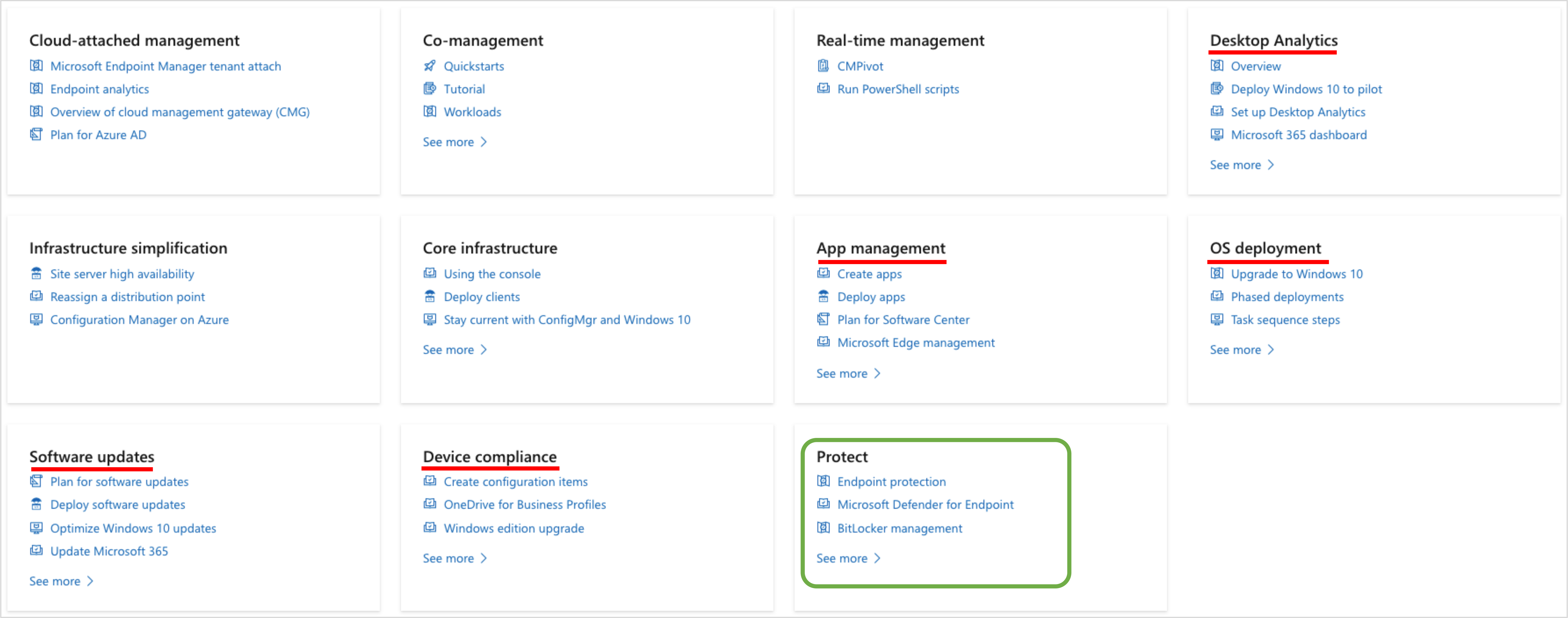
Microsoft Cloud

Login to MDE console
For monitoring, analysis and response

SOC Analyst

MDE – Configuration Management

MDE configuration is done through **Microsoft Endpoint Manager**



Cloud-attached management
- Microsoft Endpoint Manager tenant attach
- Endpoint analytics
- Overview of cloud management gateway (CMG)
- Plan for Azure AD

Co-management
- Quickstarts
- Tutorial
- Workloads

See more >

Real-time management
- CMPivot
- Run PowerShell scripts

Desktop Analytics
- Overview
- Deploy Windows 10 to pilot
- Set up Desktop Analytics
- Microsoft 365 dashboard

See more >

Infrastructure simplification
- Site server high availability
- Reassign a distribution point
- Configuration Manager on Azure

Core infrastructure
- Using the console
- Deploy clients
- Stay current with ConfigMgr and Windows 10

See more >

App management
- Create apps
- Deploy apps
- Plan for Software Center
- Microsoft Edge management

See more >

OS deployment
- Upgrade to Windows 10
- Phased deployments
- Task sequence steps

See more >

Software updates
- Plan for software updates
- Deploy software updates
- Optimize Windows 10 updates
- Update Microsoft 365

See more >

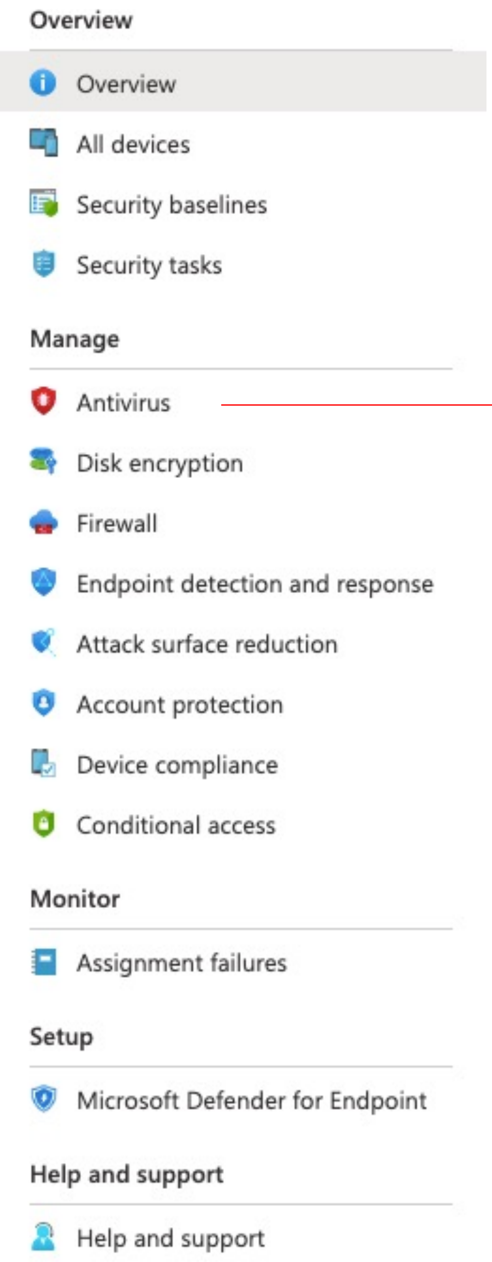
Device compliance
- Create configuration items
- OneDrive for Business Profiles
- Windows edition upgrade

See more >

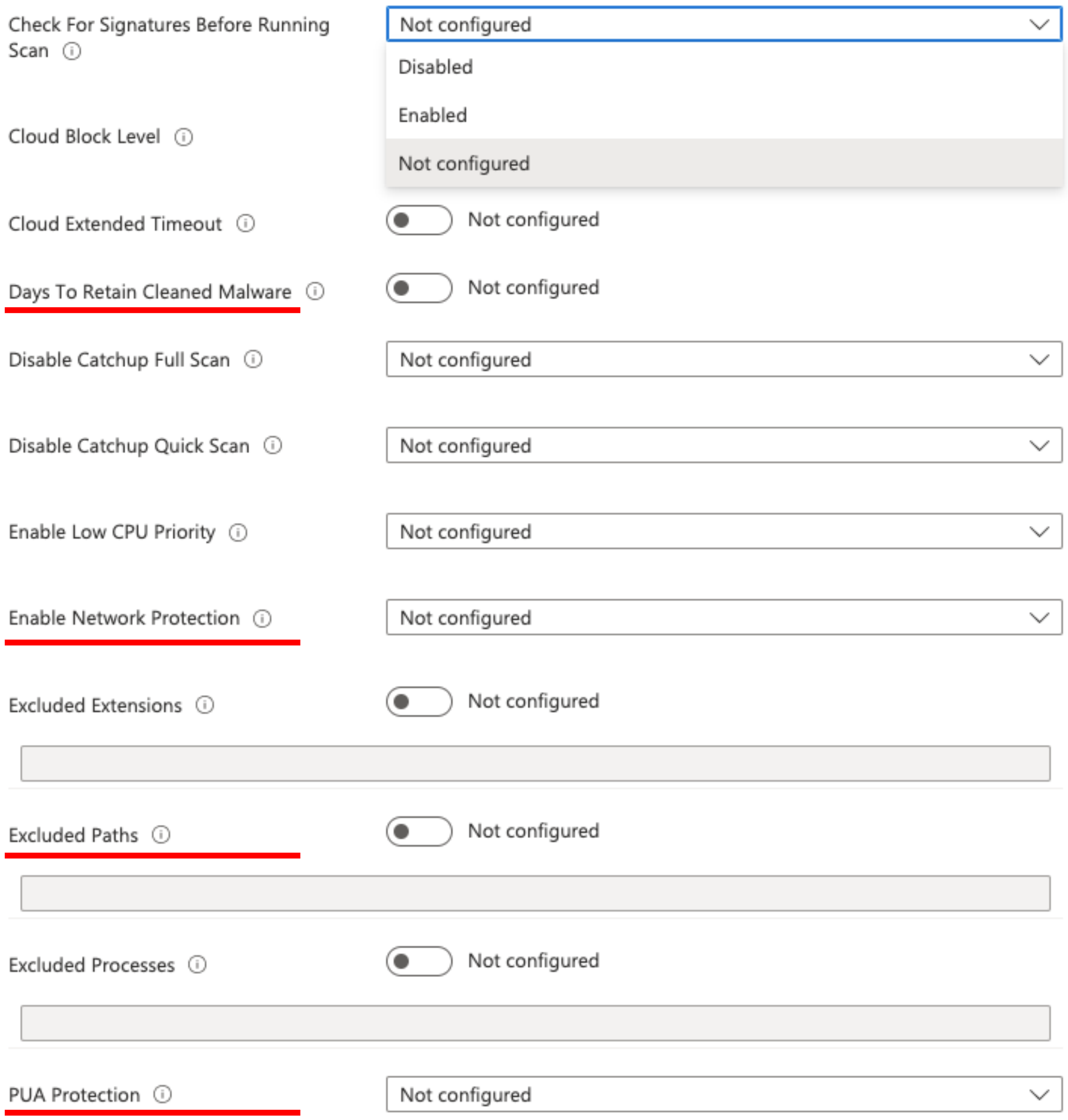
Protect
- Endpoint protection
- Microsoft Defender for Endpoint
- BitLocker management

See more >

MDE – Configuration from Endpoint Manager

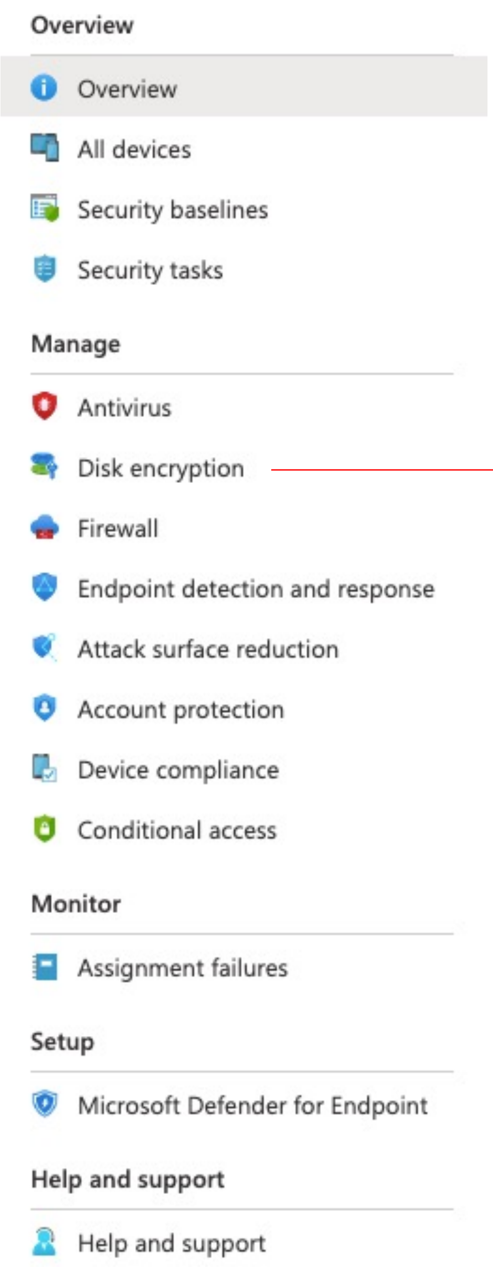


The typical AV settings



Check For Signatures Before Running Scan ⓘ	Not configured Disabled Enabled Not configured
Cloud Block Level ⓘ	
Cloud Extended Timeout ⓘ	Not configured
Days To Retain Cleaned Malware ⓘ	Not configured
Disable Catchup Full Scan ⓘ	Not configured
Disable Catchup Quick Scan ⓘ	Not configured
Enable Low CPU Priority ⓘ	Not configured
Enable Network Protection ⓘ	Not configured
Excluded Extensions ⓘ	Not configured
Excluded Paths ⓘ	Not configured
Excluded Processes ⓘ	Not configured
PUA Protection ⓘ	Not configured

MDE – Configuration from Endpoint Manager



Overview

- Overview
- All devices
- Security baselines
- Security tasks

Manage

- Antivirus
- Disk encryption
- Firewall
- Endpoint detection and response
- Attack surface reduction
- Account protection
- Device compliance
- Conditional access

Monitor

- Assignment failures

Setup

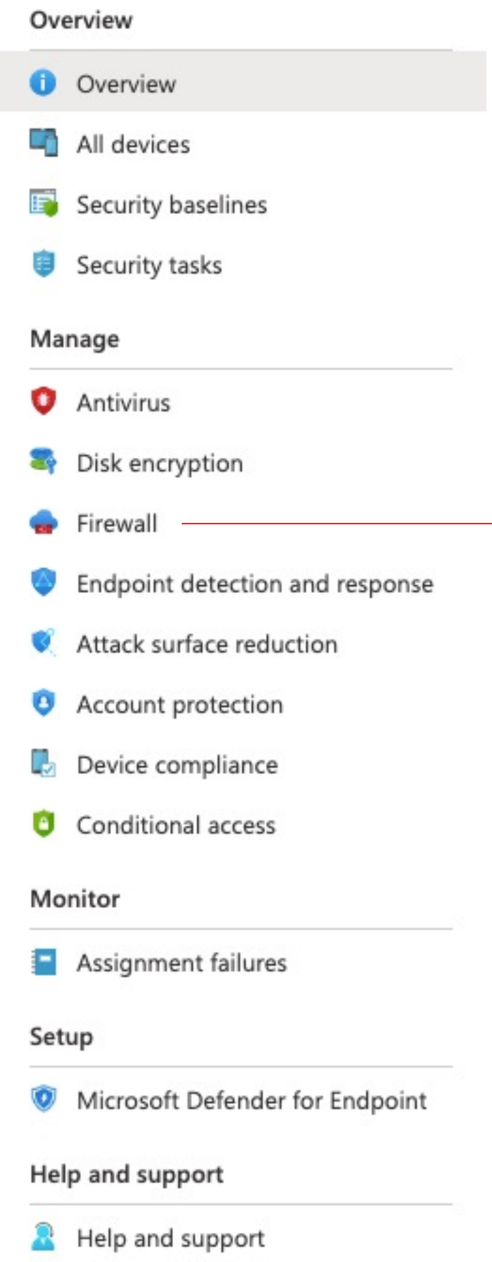
- Microsoft Defender for Endpoint

Help and support

- Help and support

Not related to EDR. **BitLocker** Configuration

MDE – Configuration from Endpoint Manager



Overview

- Overview
- All devices
- Security baselines
- Security tasks

Manage

- Antivirus
- Disk encryption
- Firewall
- Endpoint detection and response
- Attack surface reduction
- Account protection
- Device compliance
- Conditional access

Monitor

- Assignment failures

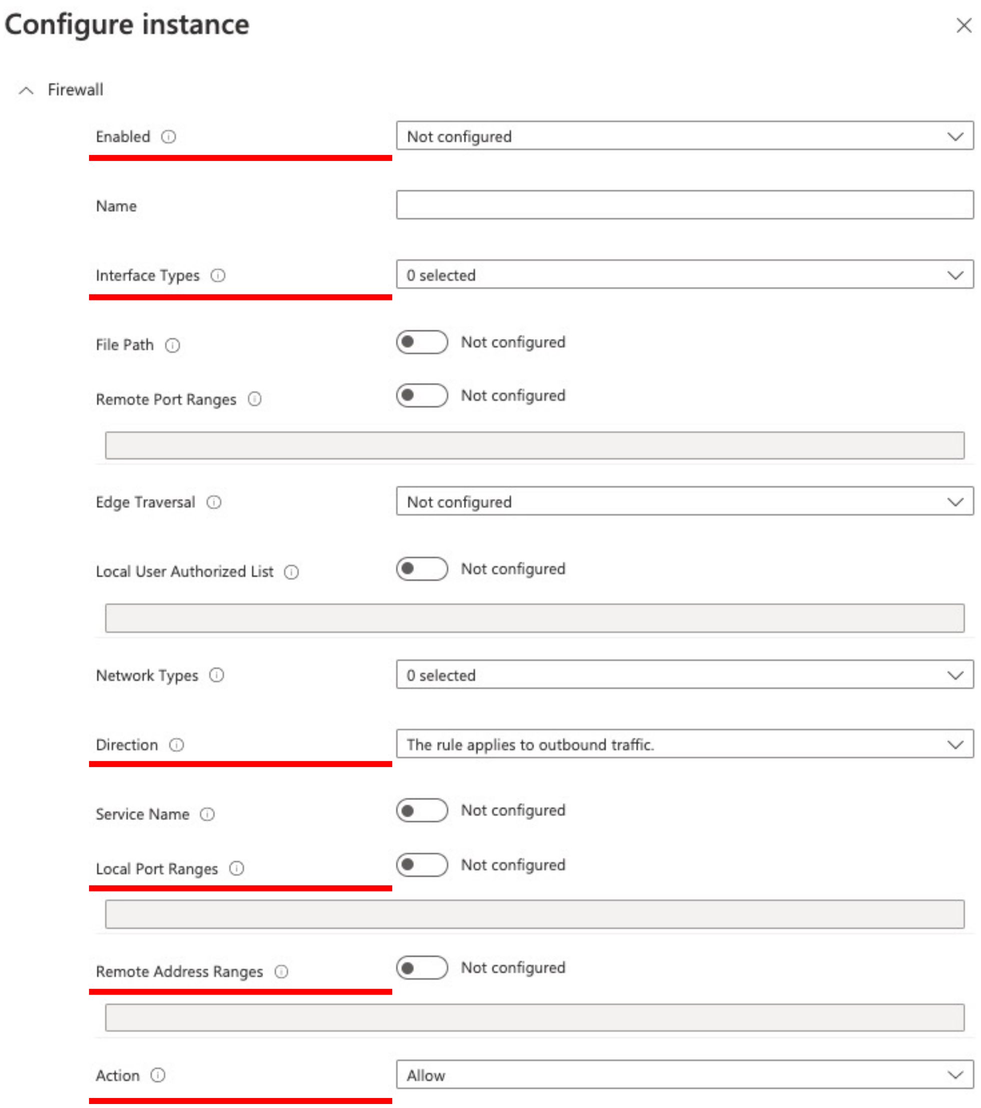
Setup

- Microsoft Defender for Endpoint

Help and support

- Help and support

Control settings of Host Firewall



Configure instance

Firewall

Enabled: Not configured

Name:

Interface Types: 0 selected

File Path: Not configured

Remote Port Ranges: Not configured

Edge Traversal: Not configured

Local User Authorized List: Not configured

Network Types: 0 selected

Direction: The rule applies to outbound traffic.

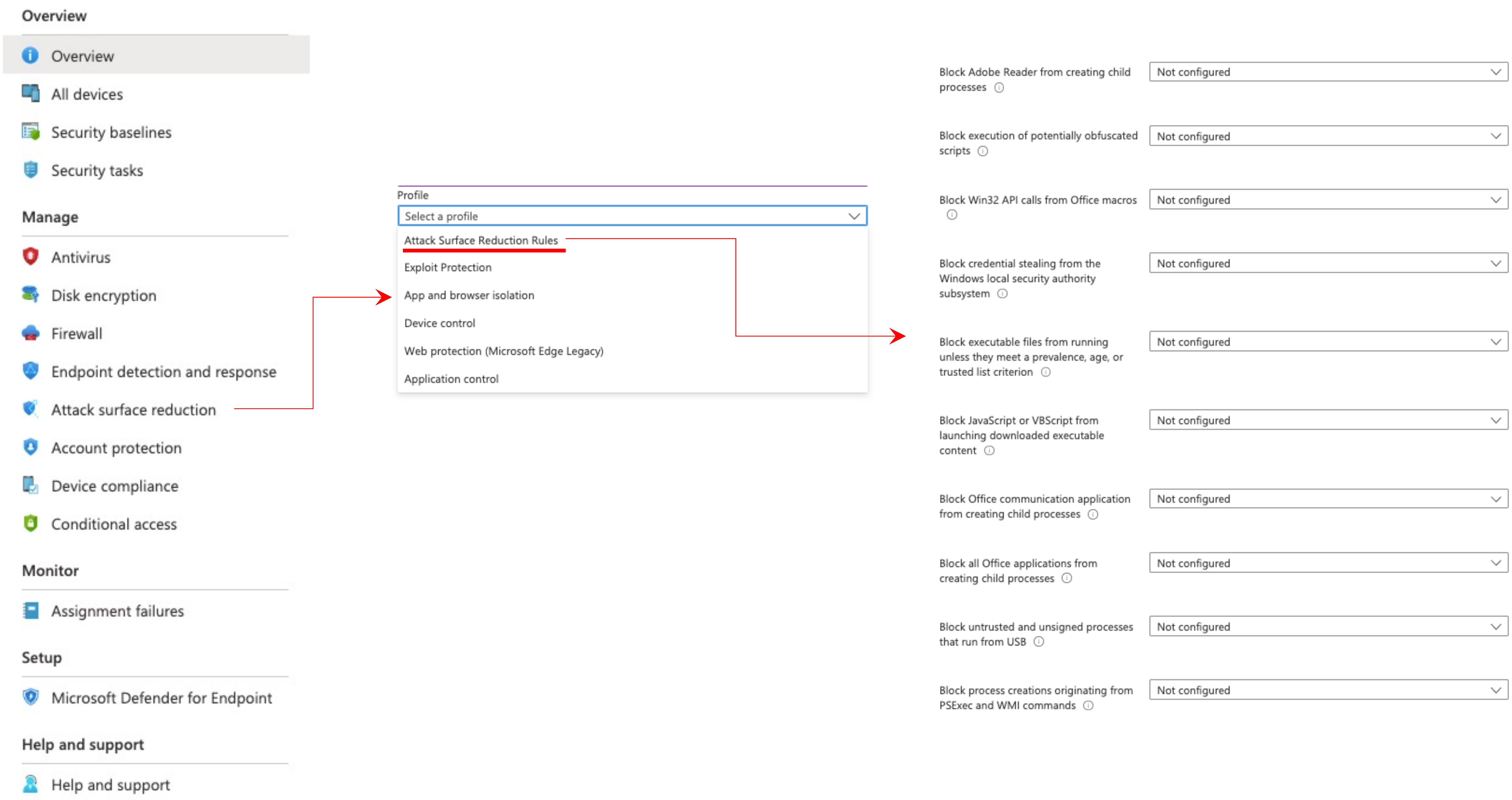
Service Name: Not configured

Local Port Ranges: Not configured

Remote Address Ranges: Not configured

Action: Allow

MDE – Configuration from Endpoint Manager



Block Adobe Reader from creating child processes: Not configured

Block execution of potentially obfuscated scripts: Not configured

Block Win32 API calls from Office macros: Not configured

Block credential stealing from the Windows local security authority subsystem: Not configured

Block executable files from running unless they meet a prevalence, age, or trusted list criterion: Not configured

Block JavaScript or VBScript from launching downloaded executable content: Not configured

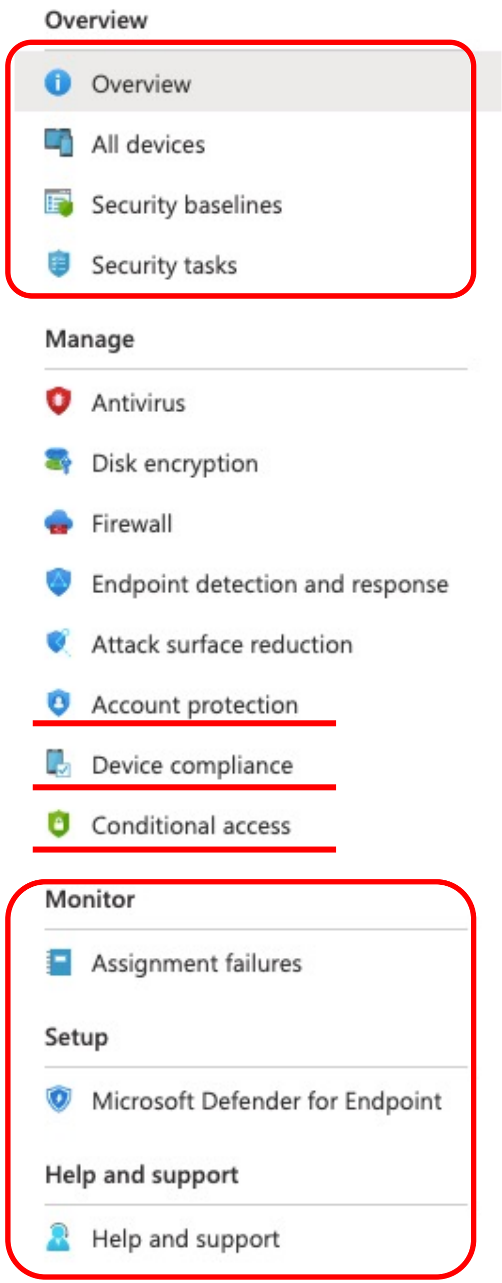
Block Office communication application from creating child processes: Not configured

Block all Office applications from creating child processes: Not configured

Block untrusted and unsigned processes that run from USB: Not configured

Block process creations originating from PSExec and WMI commands: Not configured

MDE – Configuration from Endpoint Manager



Overview

- Overview
- All devices
- Security baselines
- Security tasks

Manage

- Antivirus
- Disk encryption
- Firewall
- Endpoint detection and response
- Attack surface reduction
- Account protection
- Device compliance
- Conditional access

Monitor

- Assignment failures

Setup

- Microsoft Defender for Endpoint

Help and support

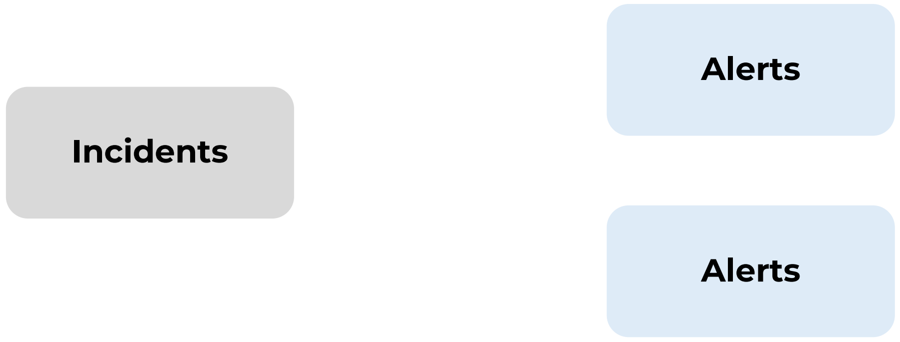
- Help and support

MDE

for Monitoring and Analysis

Incidents

What you see



Incidents

Alerts

Alerts

What you can do

Manage Incident

- Assign to
- Status → Active, In Progress, Resolved
- Classification
- Comment

Alerts

Alerts

What you see

Alert Story

Holds all relevant information about the triggered alert, like:

- Alert Name
- File name
- Hash value
- Size
- VT detection ratio
- Threat Name
- Remediation Status

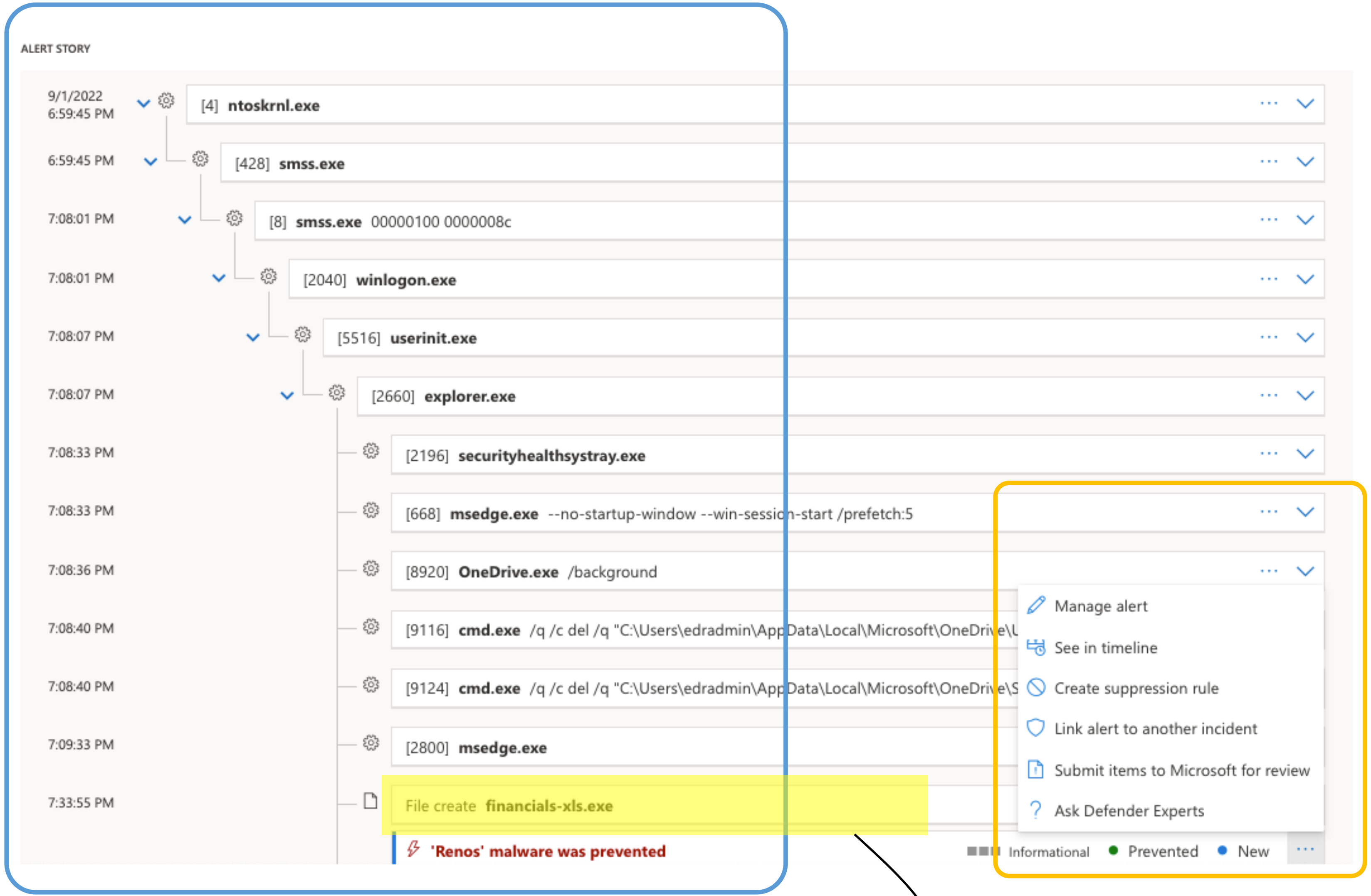
What you can do

Manage Alert

- **Status → New, In Progress, Resolved**
- **Assign to**
- **Classification**
- **Comment**

- **See in Timeline**
- **Create Suppression Rule**
- **Link alert to another Incident**
- **Open File Page**
- **Add Indicator**
- **Download File**
- **Submit for Deep Analysis (Sandbox)**
- **Stop and Quarantine File**

Alert Story and Alert Actions



ALERT STORY

9/1/2022 6:59:45 PM [4] **ntoskrnl.exe**

6:59:45 PM [428] **smss.exe**

7:08:01 PM [8] **smss.exe** 00000100 0000008c

7:08:01 PM [2040] **winlogon.exe**

7:08:07 PM [5516] **userinit.exe**

7:08:07 PM [2660] **explorer.exe**

7:08:33 PM [2196] **securityhealthsystray.exe**

7:08:33 PM [668] **msedge.exe** --no-startup-window --win-session-start /prefetch:5

7:08:36 PM [8920] **OneDrive.exe** /background

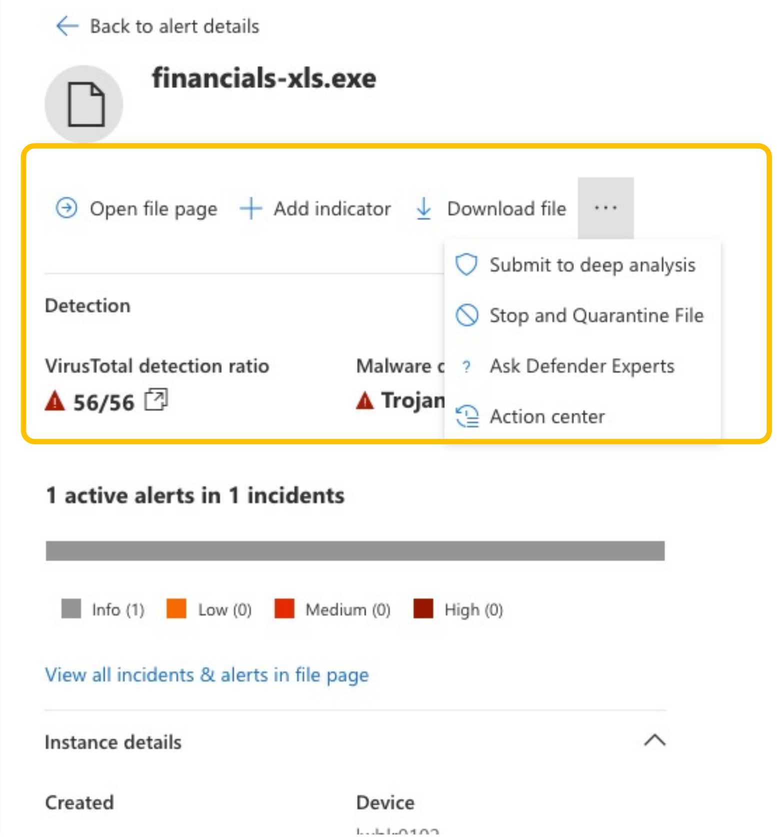
7:08:40 PM [9116] **cmd.exe** /q /c del /q "C:\Users\edradmin\AppData\Local\Microsoft\OneDrive\L

7:08:40 PM [9124] **cmd.exe** /q /c del /q "C:\Users\edradmin\AppData\Local\Microsoft\OneDrive\S

7:09:33 PM [2800] **msedge.exe**

7:33:55 PM File create **financials-xls.exe**

'Renos' malware was prevented Informational ● Prevented ● New



← Back to alert details

financials-xls.exe

Detection

VirusTotal detection ratio: 56/56

Malware c... Trojan

1 active alerts in 1 incidents

Info (1) Low (0) Medium (0) High (0)

View all incidents & alerts in file page

Instance details

Created

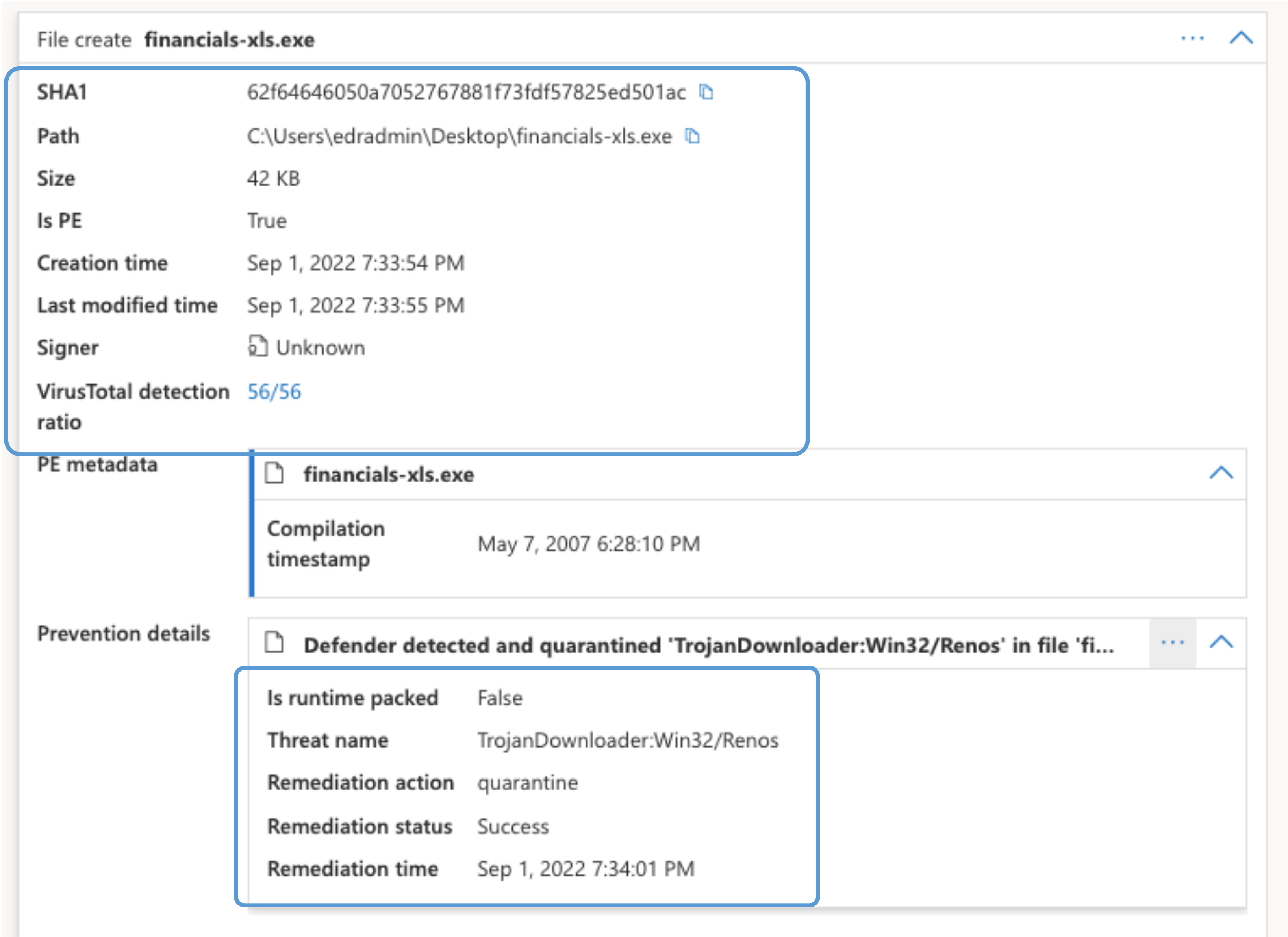
Device

Next Page

What you see

What you can do

Alert Story and Alert Actions



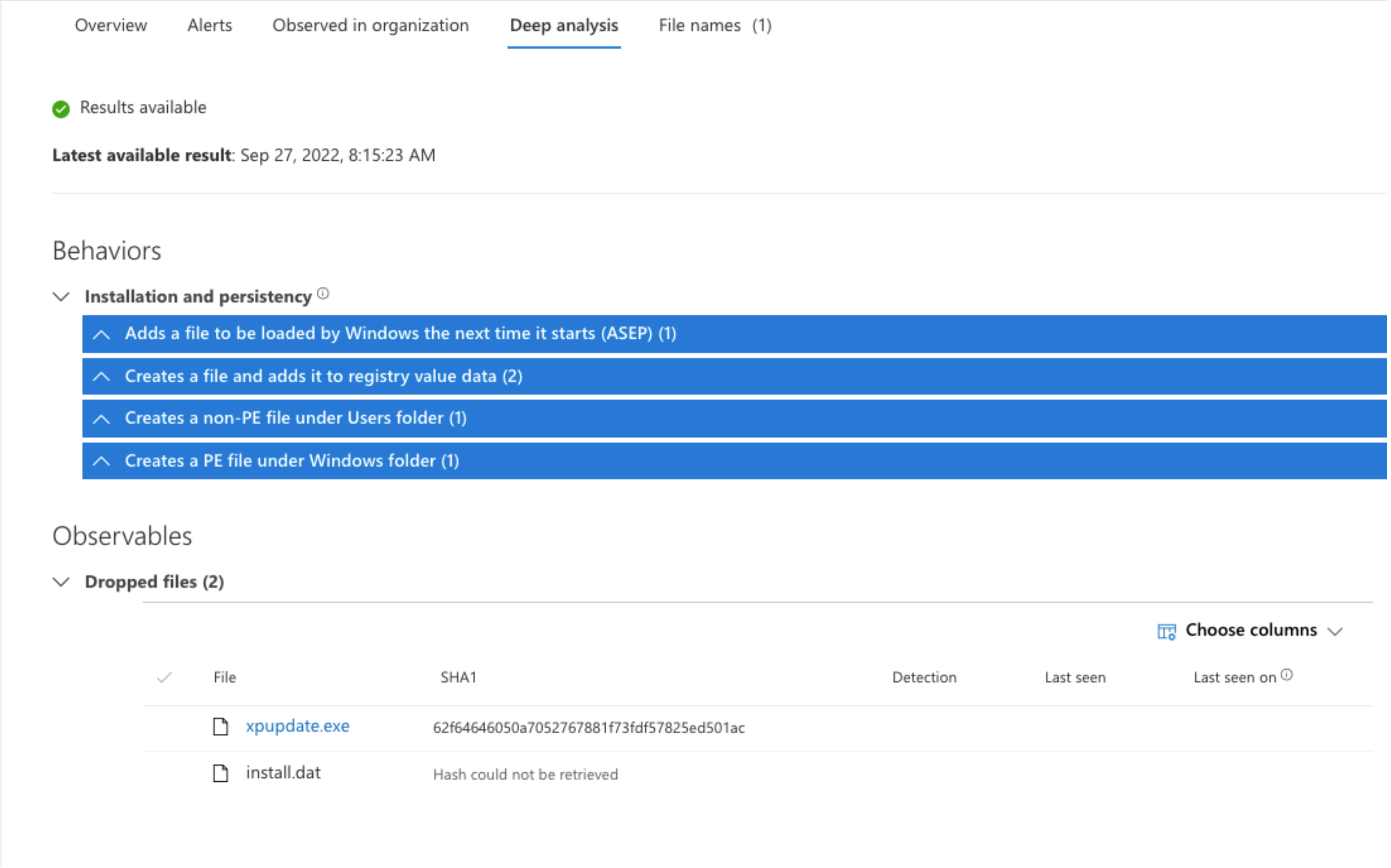
File create **financials-xls.exe**

SHA1	62f64646050a7052767881f73fdf57825ed501ac
Path	C:\Users\edradmin\Desktop\financials-xls.exe
Size	42 KB
Is PE	True
Creation time	Sep 1, 2022 7:33:54 PM
Last modified time	Sep 1, 2022 7:33:55 PM
Signer	Unknown
VirusTotal detection ratio	56/56
PE metadata	**financials-xls.exe** Compilation timestamp: May 7, 2007 6:28:10 PM
Prevention details	**Defender detected and quarantined 'TrojanDownloader:Win32/Renos' in file 'fi...**

Is runtime packed	False
Threat name	TrojanDownloader:Win32/Renos
Remediation action	quarantine
Remediation status	Success
Remediation time	Sep 1, 2022 7:34:01 PM

Submit for Deep Analysis

The selected file will be analyzed in Microsoft's Sandbox. Once analyzed it gives details about the behaviors and observables.



✓ Results available

Latest available result: Sep 27, 2022, 8:15:23 AM

Behaviors

Installation and persistency

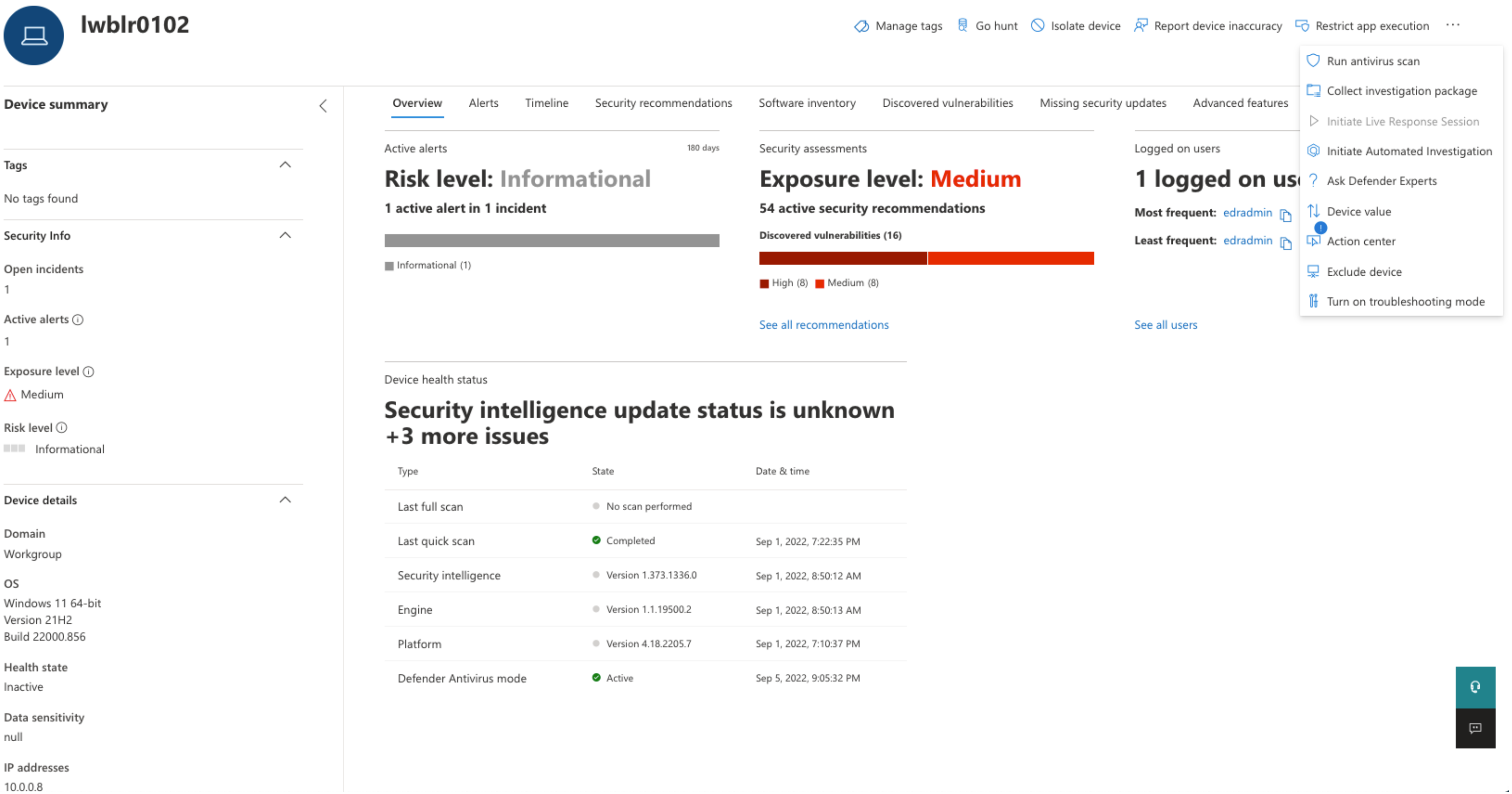
- Adds a file to be loaded by Windows the next time it starts (ASEP) (1)
- Creates a file and adds it to registry value data (2)
- Creates a non-PE file under Users folder (1)
- Creates a PE file under Windows folder (1)

Observables

Dropped files (2)

File	SHA1	Detection	Last seen	Last seen on
xpupdate.exe	62f64646050a7052767881f73fdf57825ed501ac			
install.dat	Hash could not be retrieved			

Device Page



lwblr0102

Device summary

Tags

No tags found

Security Info

Open incidents
1

Active alerts ⓘ
1

Exposure level ⓘ
⚠ Medium

Risk level ⓘ
Informational

Device details

Domain
Workgroup

OS
Windows 11 64-bit
Version 21H2
Build 22000.856

Health state
Inactive

Data sensitivity
null

IP addresses
10.0.0.8

Active alerts 180 days

Risk level: Informational

1 active alert in 1 incident

■ Informational (1)

Security assessments

Exposure level: Medium

54 active security recommendations

Discovered vulnerabilities (16)

■ High (8) ■ Medium (8)

See all recommendations

Logged on users

1 logged on us

Most frequent: edradmin

Least frequent: edradmin

See all users

Device health status

Security intelligence update status is unknown +3 more issues

Type	State	Date & time
Last full scan	● No scan performed	
Last quick scan	✓ Completed	Sep 1, 2022, 7:22:35 PM
Security intelligence	● Version 1.373.1336.0	Sep 1, 2022, 8:50:12 AM
Engine	● Version 1.1.19500.2	Sep 1, 2022, 8:50:13 AM
Platform	● Version 4.18.2205.7	Sep 1, 2022, 7:10:37 PM
Defender Antivirus mode	✓ Active	Sep 5, 2022, 9:05:32 PM

Device Page

What you see

- **Device Summary**

OS | IP | Open Incidents | Exposure Level | Risk Level Logged on User | Security Intelligence updates

- **Discovered Vulnerabilities**
- **Software Inventory**
- **Security Recommendations**

What you can do

- **Go Hunt**
- **Isolate Device**
- **Restrict App Execution**
- **Run Antivirus scan**
- **Collect Investigation Package**
- **Initiate Live Response Session**
- **Initiate Automated Investigation**

Take response actions on a device

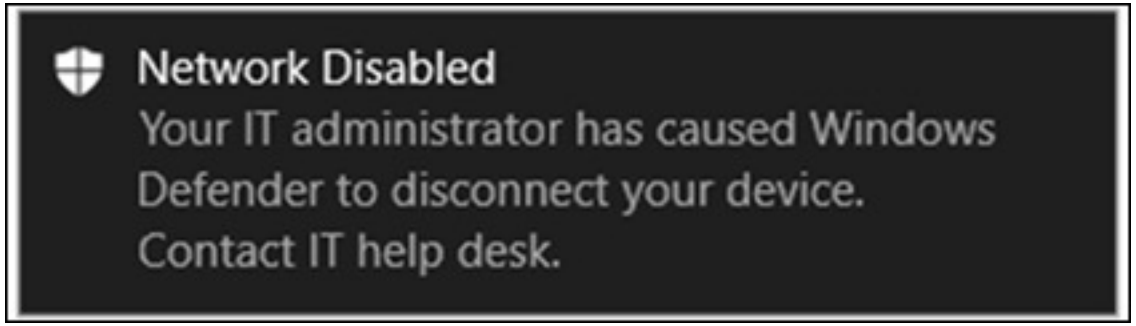
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/respond-machine-alerts?view=o365-worldwide

Isolate Device

This device isolation feature disconnects the compromised device from the network while retaining connectivity to the Defender for Endpoint service, which continues to monitor the device.

On Windows 10, version 1709 or later, you'll have more control over the network isolation level.
You can also choose to enable Outlook, Microsoft Teams, and Skype for Business connectivity (a.k.a 'Selective Isolation').

End user will see this notification



Network Disabled
Your IT administrator has caused Windows Defender to disconnect your device. Contact IT help desk.

Investigation Package

Folder	Description
Autoruns	Contains a set of files that each represent the content of the registry of a known auto start entry point (ASEP) to help identify attacker's persistency on the device.
Installed programs	This .CSV file contains the list of installed programs that can help identify what is currently installed on the device.
Network connections	ActiveNetConnections.txt Arp.txt DnsCache.txt IpConfig.txt FirewallExecutionLog.txt pfirewall.log
Prefetch files	Windows Prefetch files are designed to speed up the application startup process. It can be used to track all the files recently used in the system and find traces for applications that might have been deleted but can still be found in the prefetch file list.
Processes	Contains a .CSV file listing the running processes and provides the ability to identify current processes running on the device. This can be useful when identifying a suspicious process and its state.
Scheduled tasks	Contains a .CSV file listing the scheduled tasks, which can be used to identify routines performed automatically on a chosen device to look for suspicious code that was set to run automatically.
Security event log	Contains the security event log, which contains records of login or logout activity, or other security-related events specified by the system's audit policy.

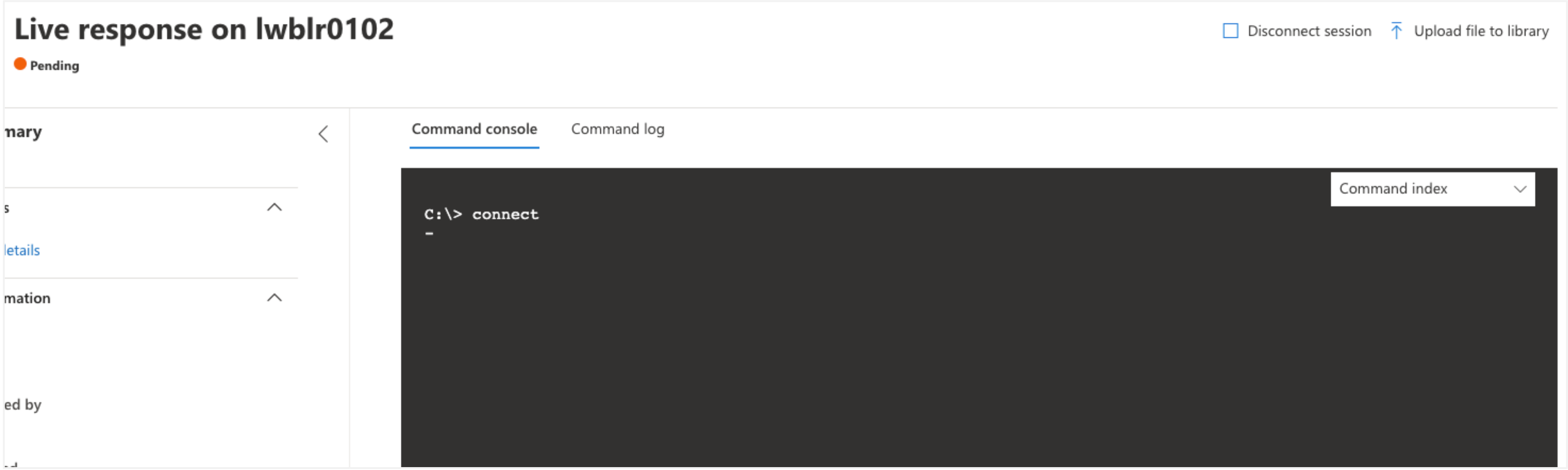
Folder	Description
Services	Contains a .CSV file that lists services and their states.
Windows Server Message Block (SMB) sessions	Lists shared access to files, printers, and serial ports and miscellaneous communications between nodes on a network. This can help identify data exfiltration or lateral movement.
System Information	Contains a SystemInformation.txt file that lists system information such as OS version and network cards.
Temp Directories	Contains a set of text files that lists the files located in %Temp% for every user in the system. This can help to track suspicious files that an attacker may have dropped on the system.
Users and Groups	Provides a list of files that each represent a group and its members.
WdSupportLogs	Provides the MpCmdRunLog.txt and MPSupportFiles.cab
CollectionSummaryReport.xls	This file is a summary of the investigation package collection, it contains the list of data points, the command used to extract the data, the execution status, and the error code if there is failure.

- Initiate from **Device Page**
- Download from **Action Center**

Live Response

Live response is a capability that gives you instantaneous access to a device by using a remote shell connection. This gives you the power to do in-depth investigative work and take immediate response actions to promptly contain identified threats in real time.

Live response is designed to enhance investigations by enabling you to collect forensic data, run scripts, send suspicious entities for analysis, remediate threats, and proactively hunt for emerging threats.



Live response on lwblr0102

● Pending

```
C:\> connect
-
```

Commands supported by live response: https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/live-response?view=o365-worldwide

Auto Investigation

- Automation works on AI based playbooks.

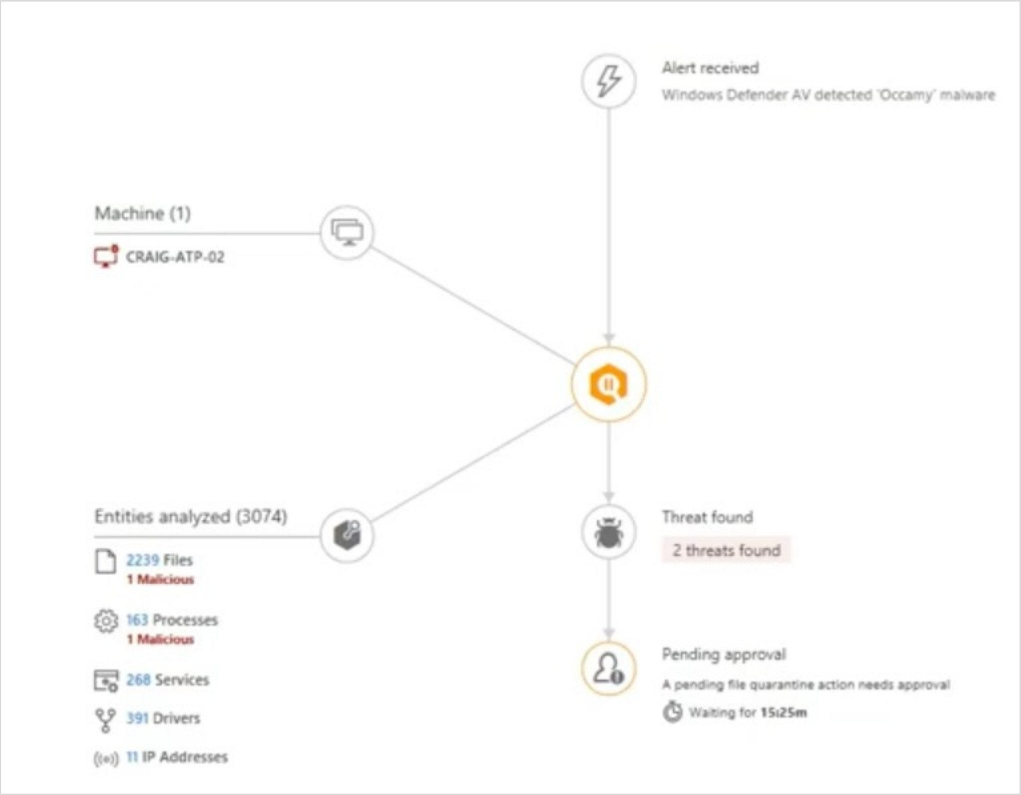
- ***Automation levels***

  Not protected
  Semi - require approvals for all folders
  Semi - require approvals for non-temp folders
  Semi - require approvals for core folders
  Full - remediate threats automatically

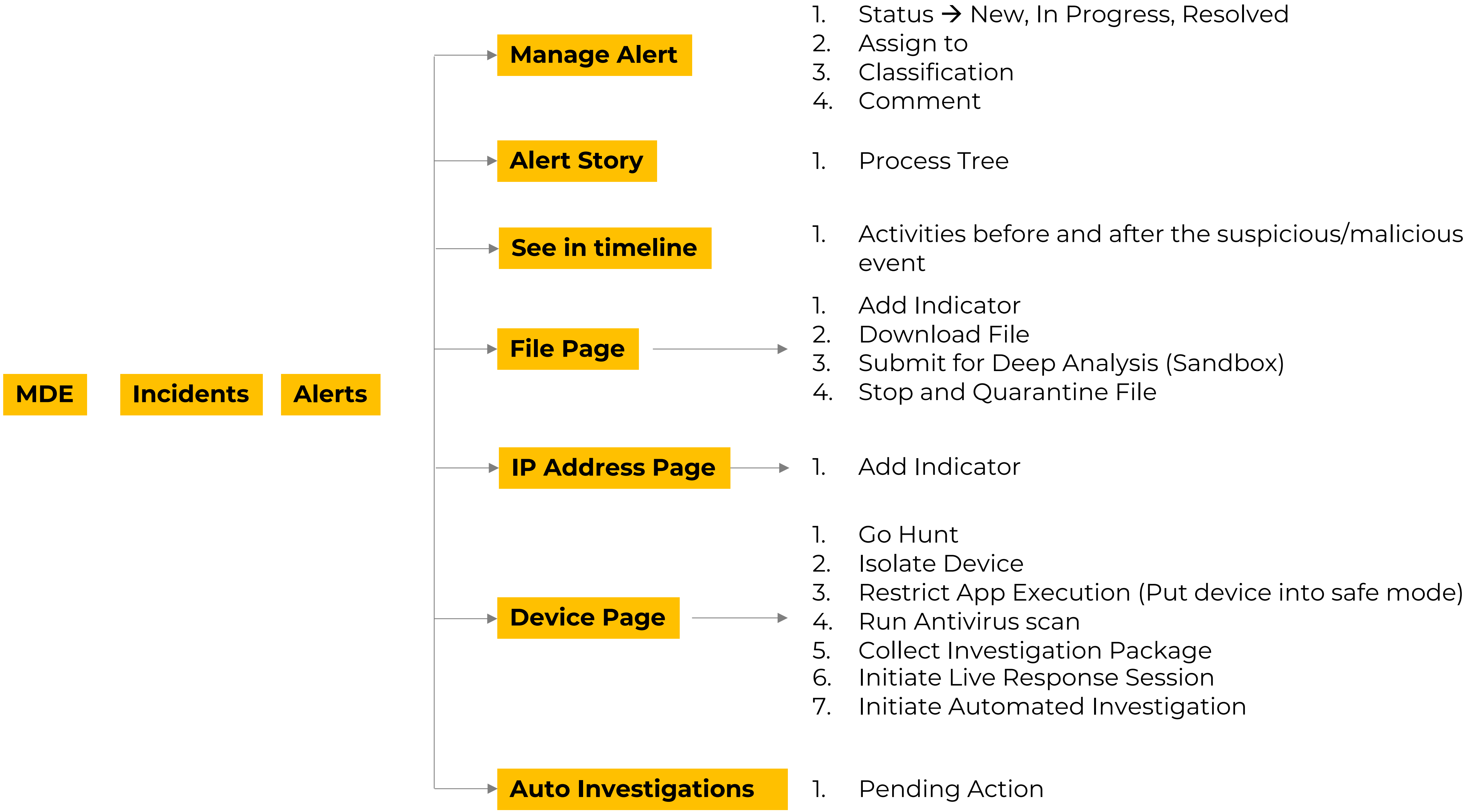
- All automated investigations will be listed.

- Each Investigation has ***Investigation Graph*** - Entities Analyzed, Machines Involved, Pending approval

- ***Pending Actions*** --> Approve, Decline (can be done individually or in bulk)



MDE – Analyst Actions



MDE

Incidents

Alerts

Manage Alert

1. Status → New, In Progress, Resolved
2. Assign to
3. Classification
4. Comment

Alert Story

1. Process Tree

See in timeline

1. Activities before and after the suspicious/malicious event

File Page

1. Add Indicator
2. Download File
3. Submit for Deep Analysis (Sandbox)
4. Stop and Quarantine File

IP Address Page

1. Add Indicator

Device Page

1. Go Hunt
2. Isolate Device
3. Restrict App Execution (Put device into safe mode)
4. Run Antivirus scan
5. Collect Investigation Package
6. Initiate Live Response Session
7. Initiate Automated Investigation

Auto Investigations

1. Pending Action

MDE - Alerts

1. Office process dropped and executed a PE file
2. Windows defender AV detected *Malware_Name* malware
3. Suspicious process injection observed
4. Suspicious service registration
5. Multiple threat families detected on one endpoint
6. Unexpected behaviour observed by a process run with no command line argument
7. An anomalous scheduled task was created
8. Suspicious task scheduler activity
9. *'Malware_Name'* malware was detected
10. PowerShell dropped a suspicious file on the machine
11. Suspicious behaviour by Microsoft Word was observed
12. 'ApplicationName' unwanted software was prevented
13. Detecting users adding themselves to local administrators group with details
14. Startup Registry Key MITRE ATT&CK T1060
15. Horizontal port scan initiated
16. Suspicious System Network Connections Discovery
17. Suspicious LDAP query

MDE

Advanced Hunting

Advanced hunting is a query-based threat-hunting tool that lets you explore up to 30 days of raw data.

Kusto Query Language (KQL) is used for querying.

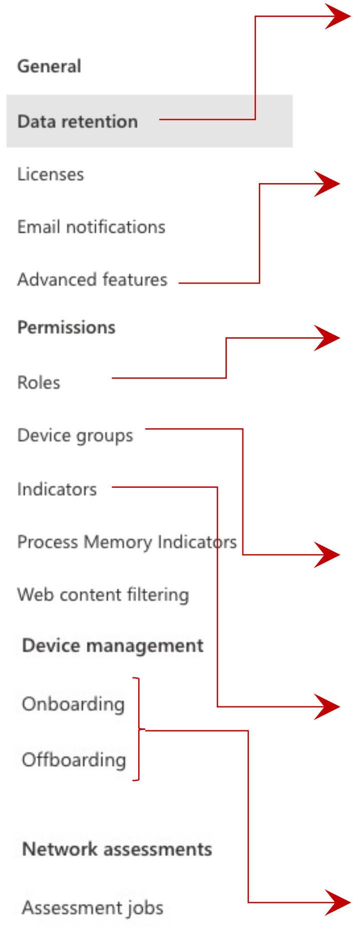
KQL Commands	Splunk Equivalent	Important Tables (schema) and Field Names
`where`	`search`	`AlertInfo`
`extend`	`eval`	`DeviceInfo`
`summarize`	`stats`	`DeviceFileEvents`
`project`	`table`	`DeviceProcessEvents`
`render`	`chart`	`DeviceRegistryEvents`
`order`	`Sort`	`DeviceNetworkInfo`
`distinct`	`dedup`	

You can use the same threat-hunting queries to build custom detection rules. These rules run automatically to check for and then respond to suspected breach activity, misconfigured machines, and other findings.

MDE

Administration

MDE - Settings



Data Retention – The default data retention in MDE tenant is 180 days.

Advance Features – Discussed in further slides

Roles - Different roles can be created to give different access to different teams
The usual roles crated include: Security Analyst, Senior Security Analyst, MDE Admin

Device Groups – A group of computers having common features like location, OS, department etc. can be grouped together in Device Group. It will help in applying different automation levels to different groups.

Indicators – All the indicators (file, IP, URL/Domain) will be appearing here

Onboarding/Offboarding – Discussed in further slides

Onboarding

Deployment Planning

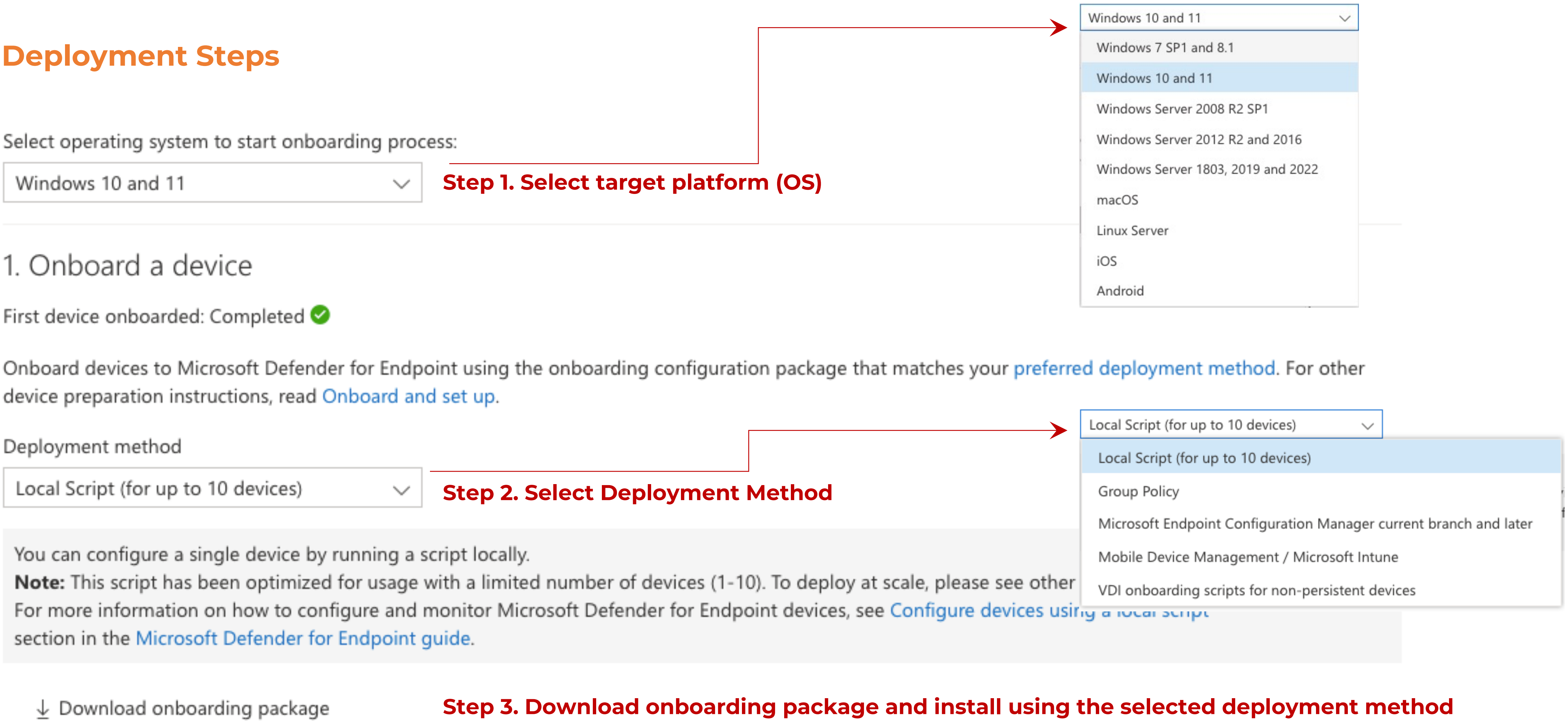
POC/Evaluation	5 – 50 devices (different platform)	Test by enabling all important features
Pilot Deployment	200 – 500 devices	Different method of deployment Issues that can occur
Organization wide rollout	All possible devices	Based on the learnings from POC and Pilot deployment

Consideration before deployment

- Endpoint count & Server Count
- Platforms (operating systems)
    - *Windows, Linux, Mac*
- Deployment and management by?
    - *GPO, SCCM, Microsoft Endpoint Manager*

Onboarding

Deployment Steps



Select operating system to start onboarding process:

Windows 10 and 11

Step 1. Select target platform (OS)

Windows 10 and 11
Windows 7 SP1 and 8.1
Windows 10 and 11
Windows Server 2008 R2 SP1
Windows Server 2012 R2 and 2016
Windows Server 1803, 2019 and 2022
macOS
Linux Server
iOS
Android

1. Onboard a device

First device onboarded: Completed ✓

Onboard devices to Microsoft Defender for Endpoint using the onboarding configuration package that matches your preferred deployment method. For other device preparation instructions, read Onboard and set up.

Deployment method

Local Script (for up to 10 devices)

Step 2. Select Deployment Method

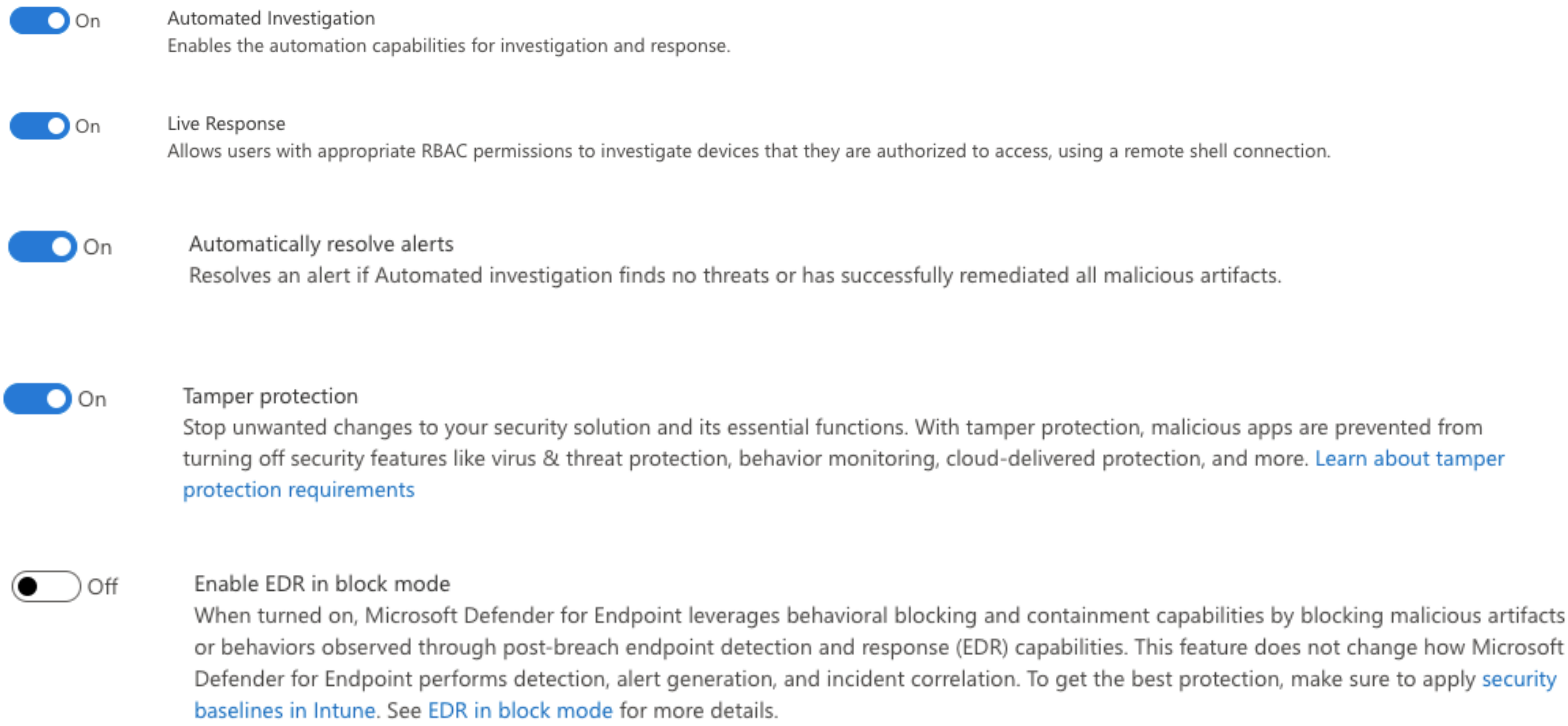
Local Script (for up to 10 devices)
Local Script (for up to 10 devices)
Group Policy
Microsoft Endpoint Configuration Manager current branch and later
Mobile Device Management / Microsoft Intune
VDI onboarding scripts for non-persistent devices

You can configure a single device by running a script locally.
Note: This script has been optimized for usage with a limited number of devices (1-10). To deploy at scale, please see other
For more information on how to configure and monitor Microsoft Defender for Endpoint devices, see Configure devices using a local script
section in the Microsoft Defender for Endpoint guide.

↓ Download onboarding package

Step 3. Download onboarding package and install using the selected deployment method

Advance Features



On — Automated Investigation
Enables the automation capabilities for investigation and response.

On — Live Response
Allows users with appropriate RBAC permissions to investigate devices that they are authorized to access, using a remote shell connection.

On — Automatically resolve alerts
Resolves an alert if Automated investigation finds no threats or has successfully remediated all malicious artifacts.

On — Tamper protection
Stop unwanted changes to your security solution and its essential functions. With tamper protection, malicious apps are prevented from turning off security features like virus & threat protection, behavior monitoring, cloud-delivered protection, and more. Learn about tamper protection requirements

Off — Enable EDR in block mode
When turned on, Microsoft Defender for Endpoint leverages behavioral blocking and containment capabilities by blocking malicious artifacts or behaviors observed through post-breach endpoint detection and response (EDR) capabilities. This feature does not change how Microsoft Defender for Endpoint performs detection, alert generation, and incident correlation. To get the best protection, make sure to apply security baselines in Intune. See EDR in block mode for more details.

Additional Resources

Become a Microsoft Defender for Endpoint Ninja (watch the Security Operations Fundamental, Intermediate and Expert videos)
https://techcommunity.microsoft.com/t5/microsoft-defender-for-endpoint/become-a-microsoft-defender-for-endpoint-ninja/ba-p/1515647#_Toc45281213

Short & sweet educational videos on Microsoft Defender for Endpoint
https://techcommunity.microsoft.com/t5/microsoft-defender-vulnerability/short-amp-sweet-educational-videos-on-microsoft-defender-for/ba-p/1021978

Ninja Show
https://adoption.microsoft.com/en-us/ninja-show/

MDE Trial
https://aka.ms/MDETrial

Log Analytics demo for KQL Practice
https://aka.ms/lademo

Additional Resources

Job Description (CV points)

- Design of the service architecture for endpoint detection and response service using / utilizing Microsoft Defender Portfolio (Microsoft Defender for Endpoint, Microsoft Defender for Identity, Microsoft Defender for Office 365, Microsoft Defender for Cloud App).
- Must have strong knowledge in Windows Server, Windows Client, Active Directory and, or Azure Active Directory.
- Performing migration of legacy endpoint security technologies to Microsoft technology stack for all the endpoint security modules of a suite (Endpoint detection and response, Antivirus, DLP, Encryption)
- Must have working knowledge on MS Defender for Cloud (Security Center) and MS Admin Center.
- Experience in device(s) onboarding and off-boarding.
- Must have experience on AIR (Automated Investigations and Remediation) based on the alerts received.
- Must have knowledge on Attack Surface Reduction (ASR) capabilities for the alerts received.
- Integration of EDR with Customer's Incident Response processes.
- Performing Threat Hunting and EDR assessments.
- Developing EDR strategic advisory and roadmap to Clients
- Supporting Sales related activities such as Proof-of-Concept, proposal presentations, Due-Diligence, solution campaigns, etc.
- Connect with other EDR colleagues through collaboration and mentoring.
- Defining maturity model and conducting maturity assessments.