Welcome and we will start shortly

Microsoft Security

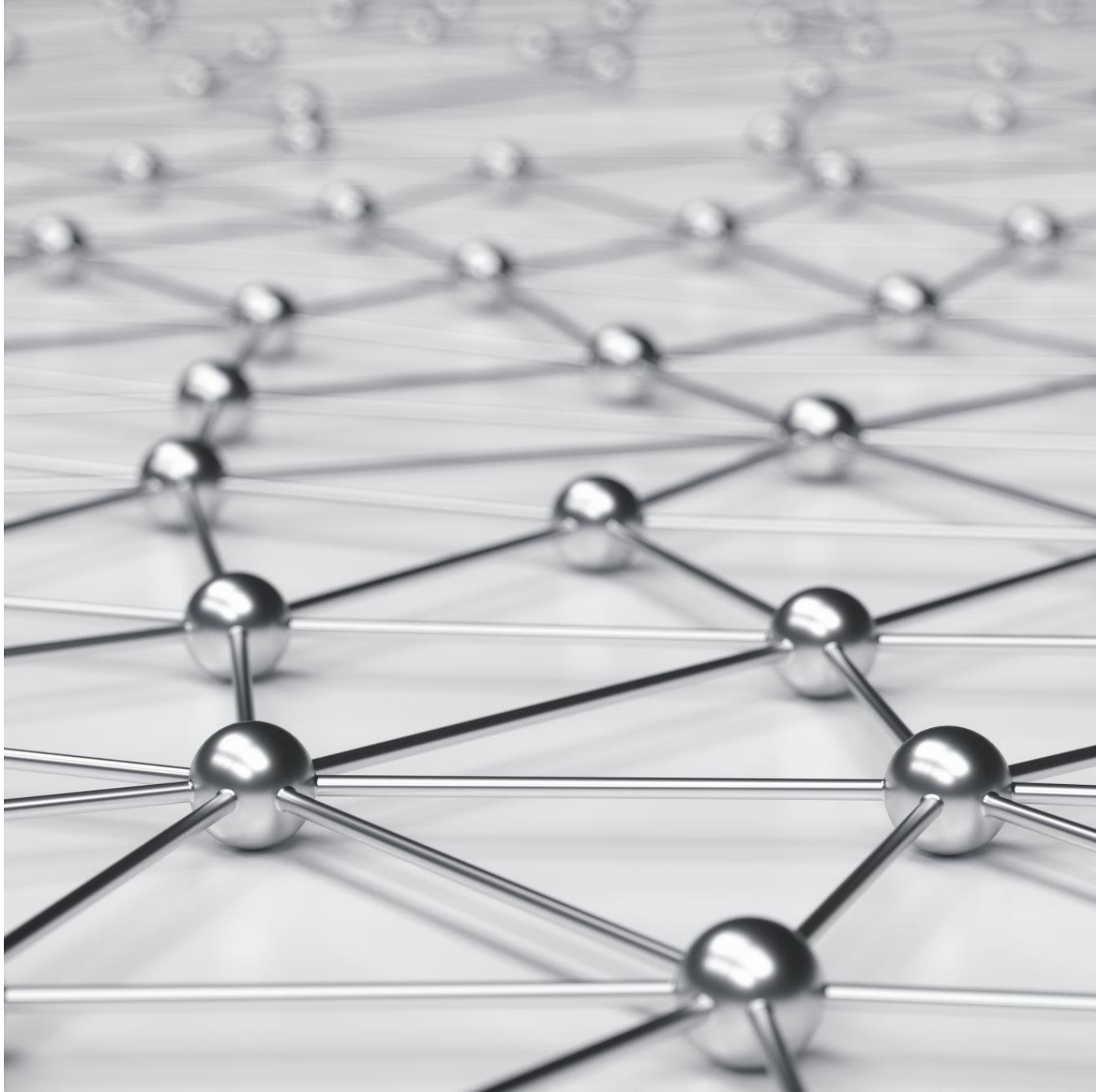
Microsoft Defender for Endpoint on macOS (MDE on macOS)

Max Velitchko
Software Developer Engineer

Yong Rhee
Product Manager

Modern Security and SOC – Product Group (PG)
Microsoft Corp.

Learn



An industry leader in endpoint security

Gartner names Microsoft a Leader in 2021 Endpoint Protection Platforms Magic Quadrant.

Forrester names Microsoft a Leader in 2021 Endpoint Security Software as a Service Wave.

Forrester names Microsoft a Leader in 2020 Enterprise Detection and Response Wave.

Our antimalware capabilities consistently achieve high scores in independent tests.

Microsoft leads in real-world detection in MITRE ATT&CK evaluation.

Microsoft Defender for Endpoint awarded a perfect 5-star rating by SC Media in 2020 Endpoint Security Review

Microsoft won six security awards with Cyber Defense Magazine at RSAC 2021:

- Best Product Hardware Security
- Market Leader Endpoint Security
- Editor's Choice Extended Detection and Response (XDR)
- Most Innovative Malware Detection
- Cutting Edge Email Security

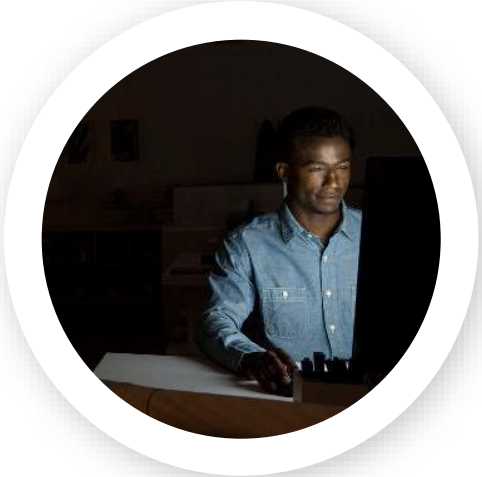
Let’s talk about what it means to protect endpoints in an organization

Navigating a shifting world

Conventional security tools have not kept pace

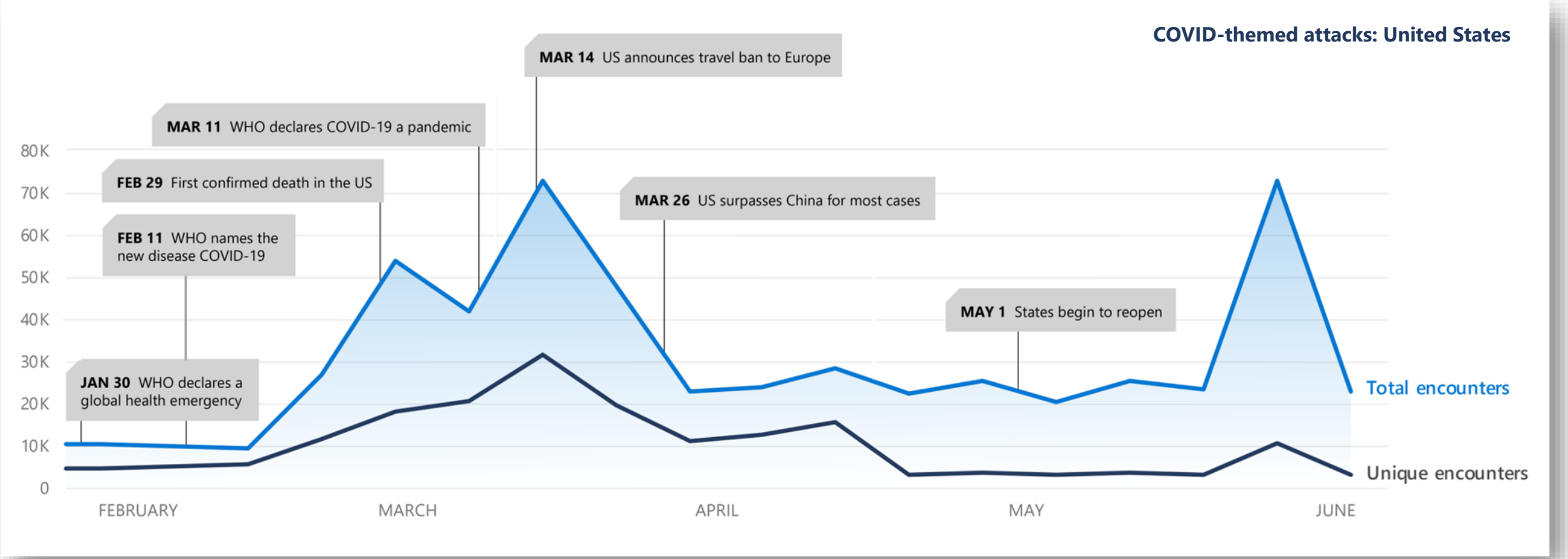
The nature of business and work have changed

Cost of breaches and regulations are increasing



Today's threats: criminal groups follow opportunities

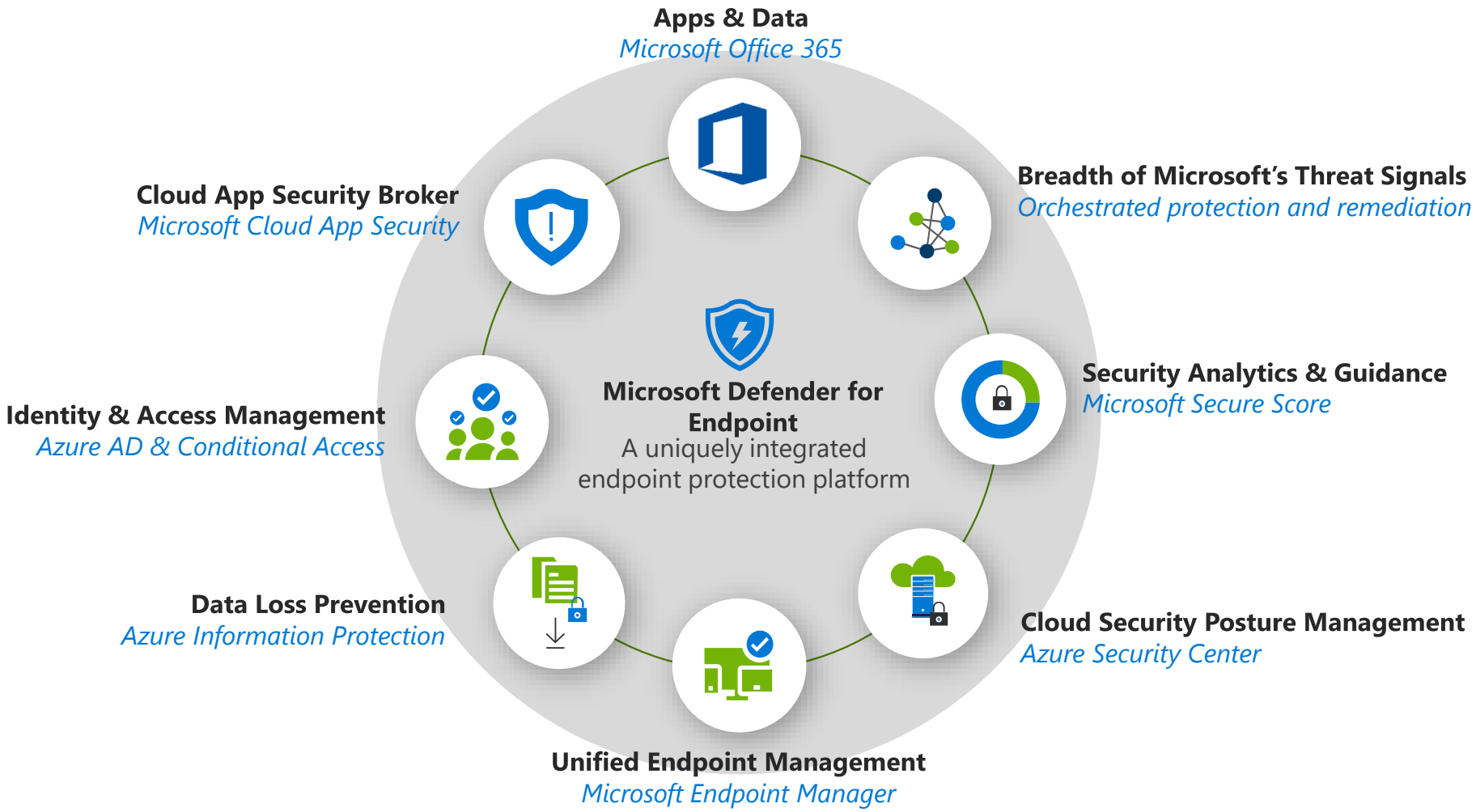
Malware encounters align with news headlines



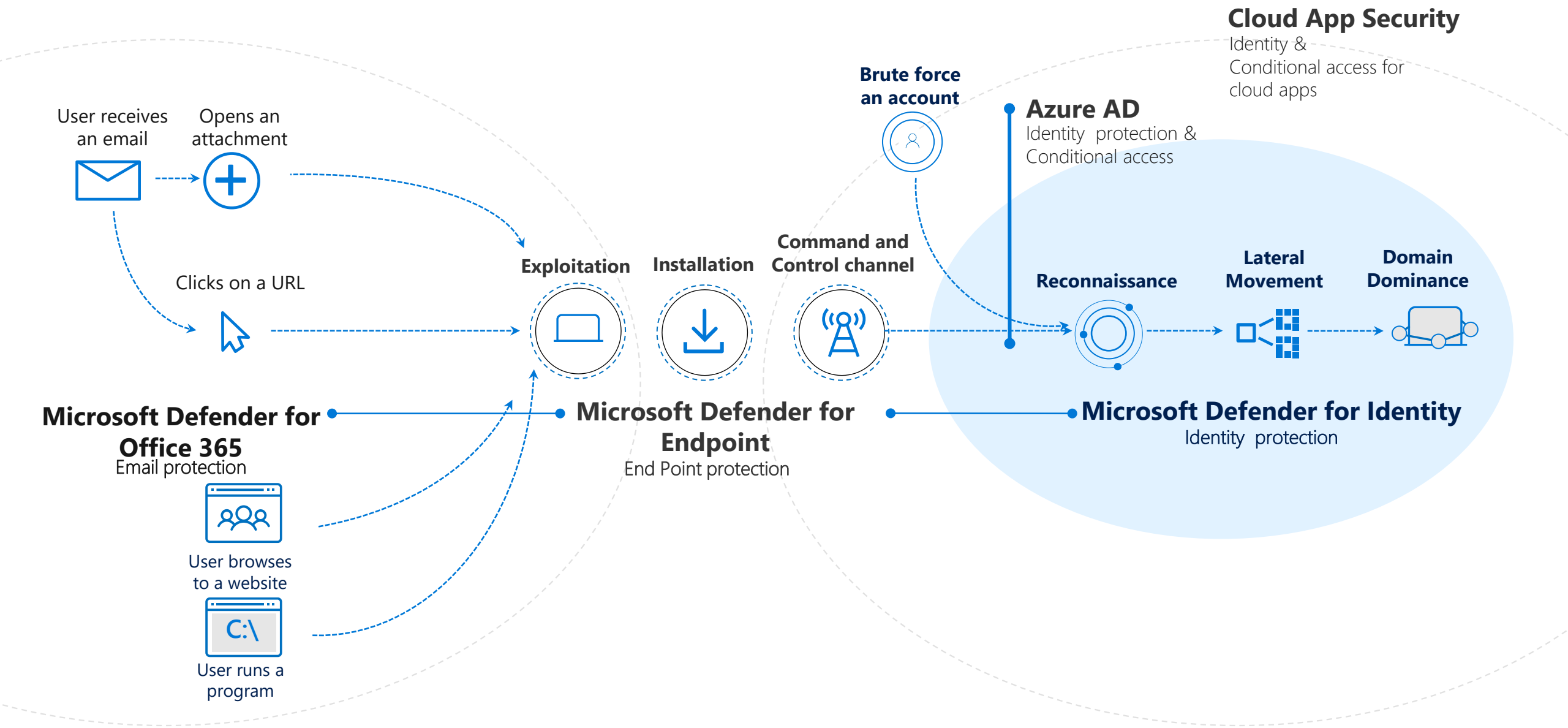
Source: Microsoft Digital Defense Report 2020

Microsoft Defender for Endpoint

Elevate the security for all your workloads



Attack Stages



Delivering endpoint security across platforms

Windows macOS

Endpoints and servers

iOS

Mobile device OS

Windows 365

Azure Virtual Desktop

Virtual desktops

Cisco

Juniper Networks

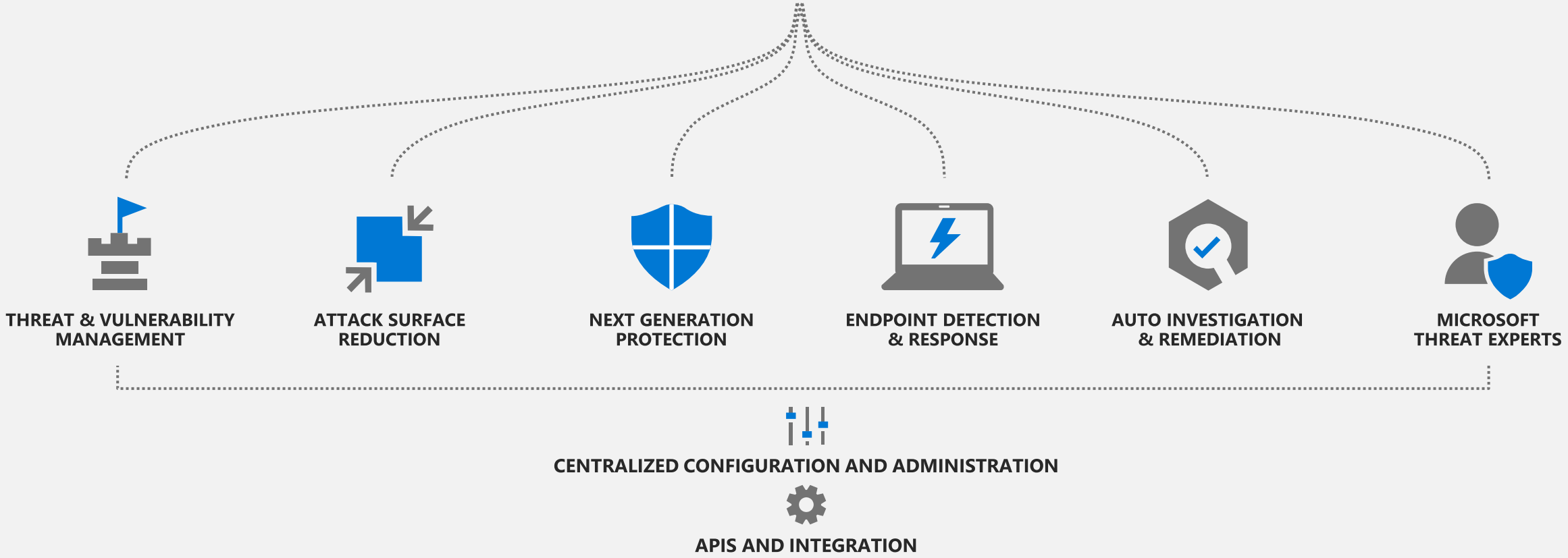
HP Enterprise

Palo Alto Networks

Network devices

Microsoft Defender
for Endpoint

Threats are no match.



Customer environments are heterogenous and complex

LEGACY SYSTEMS

DIVERSE CLIENT ESTATE

VIRTUAL DESKTOP ENVIRONMENTS

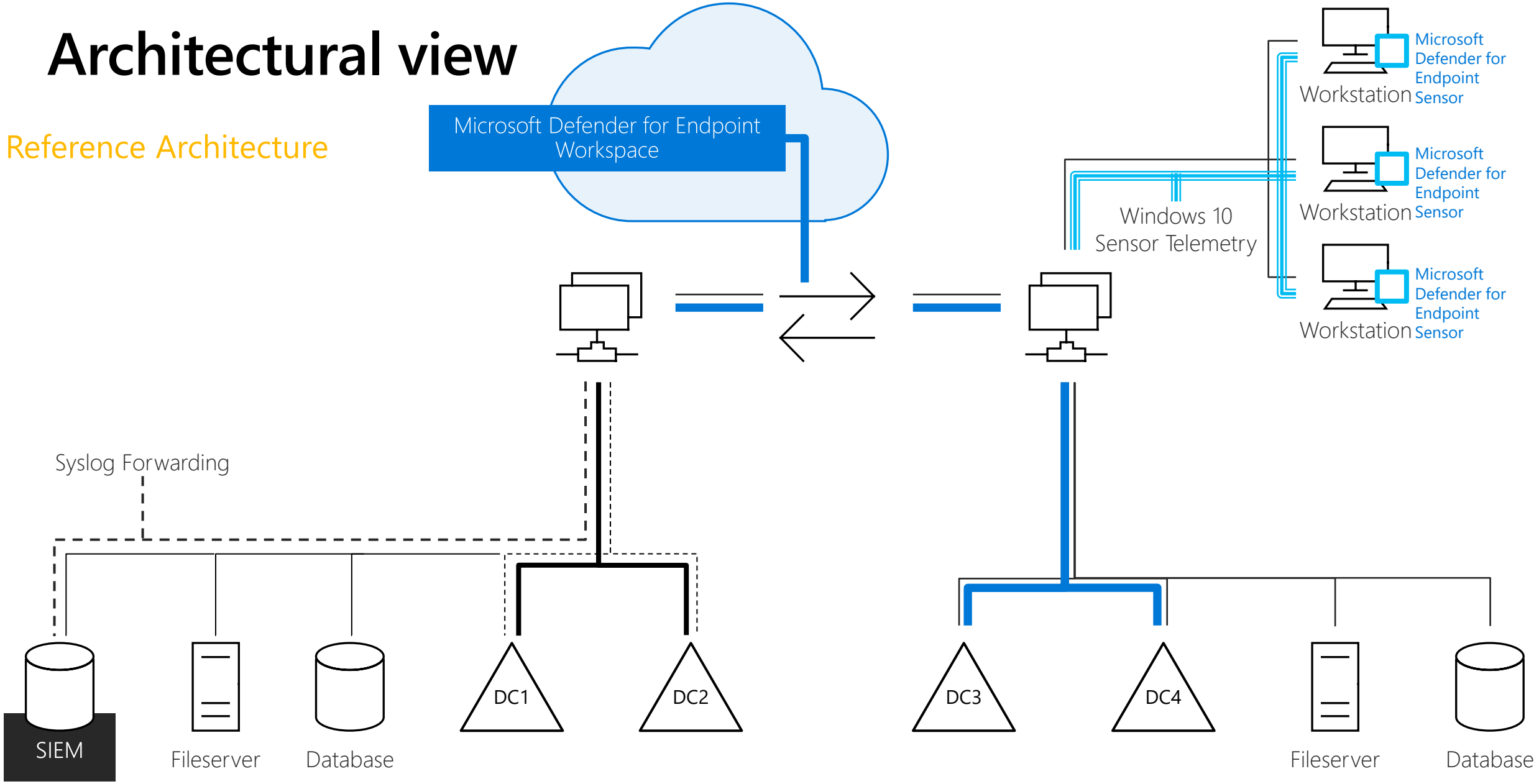
ON PREM / IN CLOUD WORKLOADS

CONTAINERS

MOBILE DEVICES

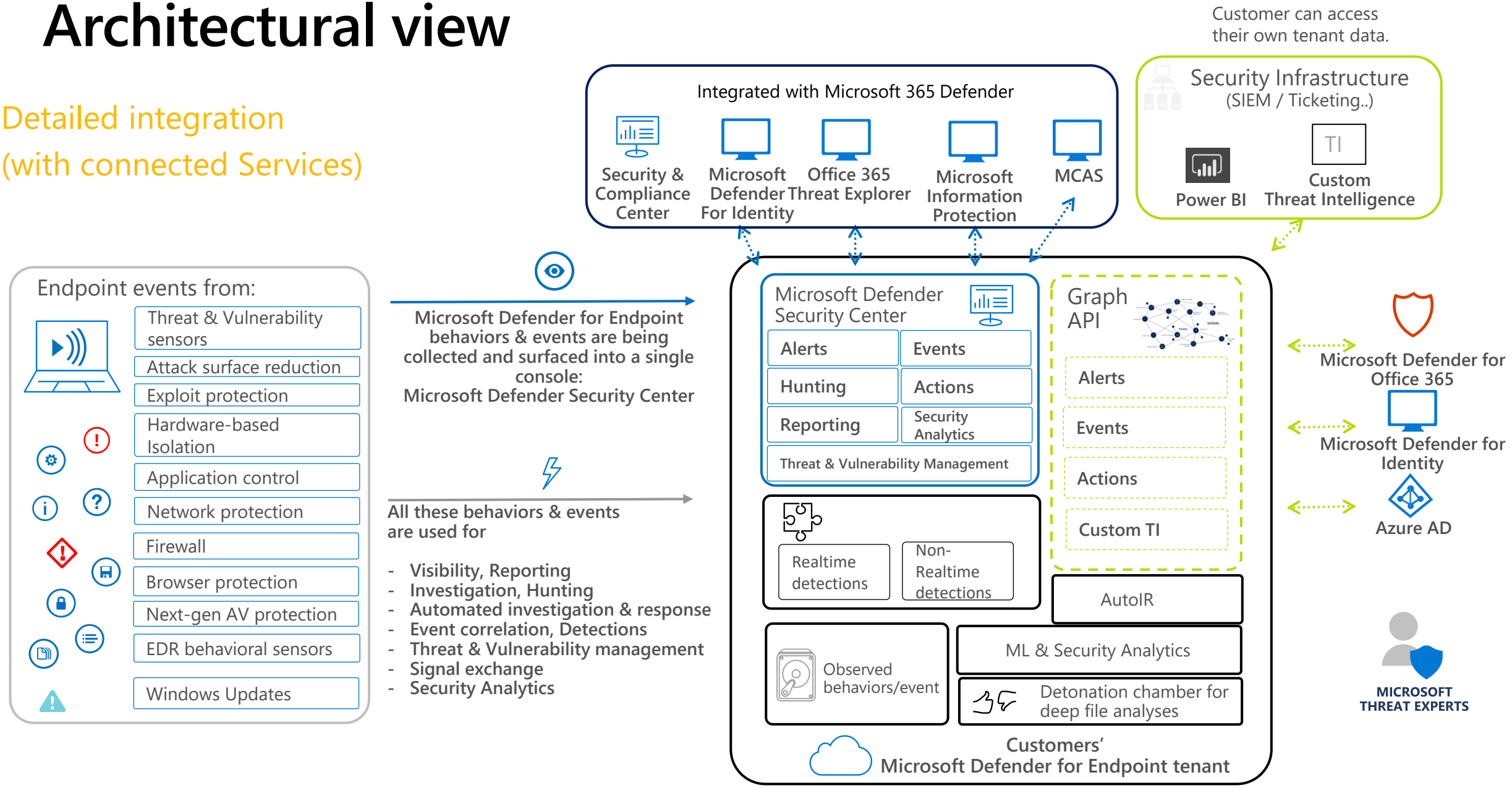
Architectural view

Reference Architecture

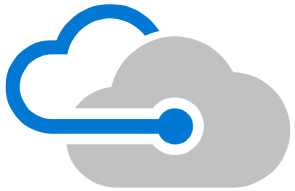


Architectural view

Detailed integration (with connected Services)



Why we're different



Cloud powered

No delays
or update compatibility
issues. Always up to date.

Unparalleled optics

Built on the industry's
deepest insight into
threats and shared signals
across devices, identities,
and information.

Automated security

Take your security to a
new level by going from
alert to remediation in
minutes—at scale.

Mac Current Offerings

AV & EDR

Threat landscape for non-Windows platforms

techradarpro

Mac threats outpace Windows for the first time

By Anthony Spadafora 3 days ago

Mac threats increased by more than 400 percent year-over-year

WIRED

BRIAN BARRETT

SECURITY 01.25.2020 12:10 PM

The Sneaky Simple Malware That Hits Millions of Macs

How the Shlayer Trojan topped the macOS malware charts—despite its "rather ordinary" methods

ZDNet MENU UK

macOS users targeted with new Tarmac malware

Tarmac malware deployed via malvertising campaigns across the US, Italy, and Japan.

By Catalin Cimpanu for Zero Day | October 11, 2019 -- 13:00 GMT (14:00 BST) | Topic: Security

Forbes

12,753 views | Jan 28, 2019, 10:30am

Mac Users Being Targeted By A Sneaky Image-Based Malware Attack

Lee Mathews

Sudo Bug Lets Non-Privileged Linux and macOS Users Run Commands as Root

February 03, 2020 Mohit Kumar

CVE-2019-18634

New Sudo Vulnerability

Don't drink & root

INTEZER

EvilGnome: Rare Malware Spying on Linux Desktop Users

Written by Paul Litvak - 17 July 2019

cybereason

NEW PERVASIVE WORM EXPLOITING LINUX EXIM SERVER VULNERABILITY

Top Count

1. United State
3. Canada
4. Netherlands
5. Germany

ZDNet MENU UK

New security flaw impacts most Linux and BSD distros

Issue is only a privilege escalation flaw but it impacts a large number of systems.

By Catalin Cimpanu for Zero Day | October 25, 2018 -- 23:15 GMT

Android phones hacked; hundreds of millions' cameras, GPS, microphones affected

Google finds malicious sites pushing iOS exploits for years

Google finds exploits for 14 iOS vulnerabilities, grouped in exploit chains, deployed in the wild since September 2016.

Jeff Bezos 'Hacked' After Receiving WhatsApp Message From Saudi Crown Prince: Report

iOS

https://aka.ms/macOSandAM

Support Model

- Defender for Endpoint supports the 3 latest major releases of macOS
  - 13 (Ventura)
  - 12 (Monterrey)
  - 11 (Big Sur)
  - ~~10.15 (Catalina)~~
- Beta versions of macOS are <u>not</u> supported
- X64 (EMT64 and AMD64) and ARM64 (e.g. M1, etc…) processors are supported as of agent version 101.40.84
- Microsoft Support (Customer Service and Support (CSS)
  - supports n-2 versions of production channel agent.

Microsoft Defender for Endpoint (Mac)

The first step in our cross-platform journey

Threat prevention

- Realtime MW protection for Mac OS
- Malware detection alerts visible in the Microsoft Defender for Endpoint console

Rich cyber data enabling attack detection and investigation

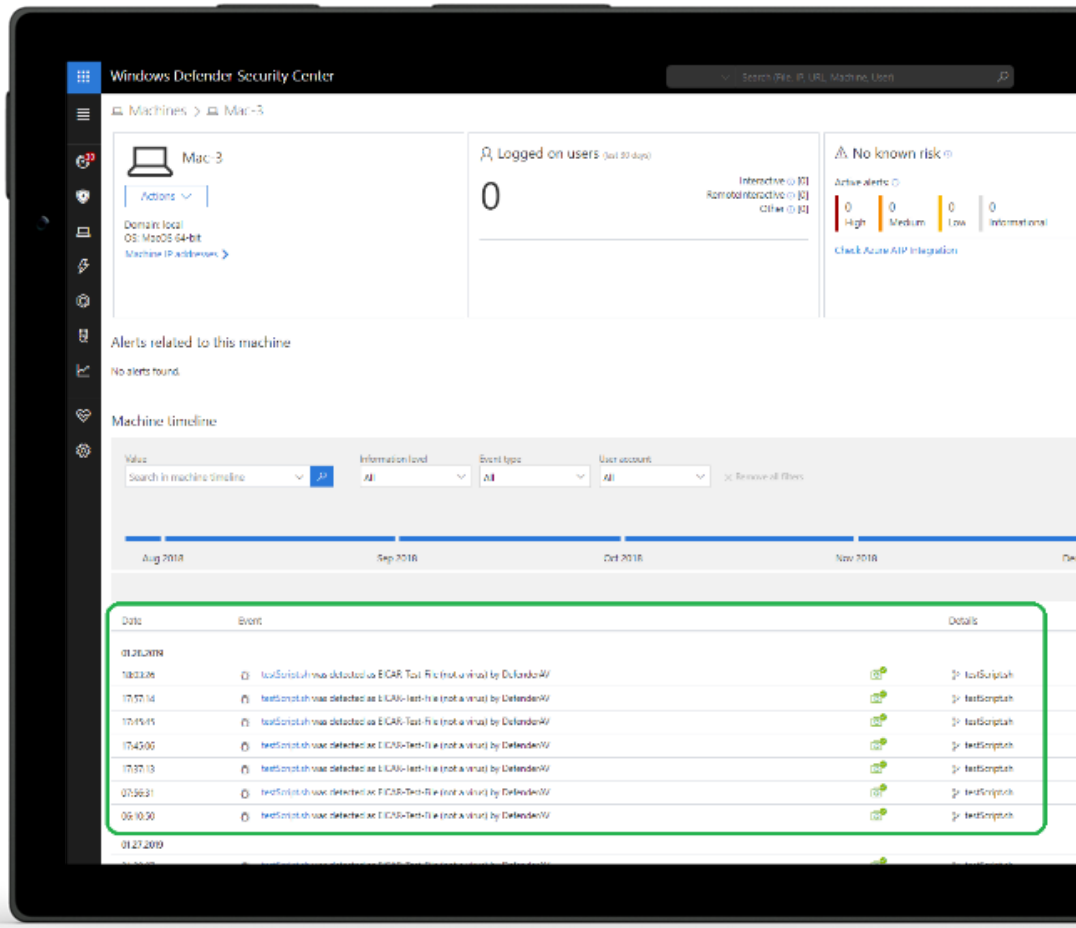
- Monitors relevant activities including files, processes, network activities
- Reports verbose data with full-scope of relationships between entities
- Provides a complete picture of what's happening on the device

Enterprise Grade

- Lightweight deployment & onboarding process
- Performant, none intrusive
- Aligned with compliance, privacy & data sovereignty requirements

Seamlessly integrated with Microsoft Defender for Endpoint capabilities

- Detection dictionary across the kill chain
- 6 months of raw data on all machines inc Mac OS
- Reputation data for all entities being logged
- Single pane of glass across all endpoints Mac OS
- Advanced hunting on all raw data including Mac OS
- Custom TI
- API access to the entire data model inc Mac OS
- SIEM integration
- Compliance & Privacy
- RBAC



Pre-breach

Mac AV

Current Offerings

Status: GA

CPU
X64
ARM64

macOS
Ventura (13)
Monterey (12)
Big Sur (11)

Client

- **Anti-tampering**
- **AV prevention** [i.e., Block and Quarantine]
- **Full command line experience** (scanning, configuring, agent health)
- **Network Protection**
  - **Web Threats** (URL reputation,anti-phising, aka Smart screen)
  - **Web Content Filtering**
  - **MCAS enforcement**
- **Device Control** [i.e., USB , iOS, Android, Firewire (IEEE1394), etc…]
- **Data Loss Prevention** (DLP)

Portal

Antivirus alerts:

- Severity
- Scan type
- Device information (hostname, machine identifier, tenant identifier, app version, and OS type)
- File information (name, path, size, and hash)
- Threat information (name, type, and state)
- Device Health Reporting

Device information:

- Machine identifier
- Tenant identifier
- App version
- Hostname
- OS type
- OS version
- Computer model
- Processor architecture
- Whether the device is a virtual machine

- Same UX across all investigation and Hunting flows
- GCC, DOD environments support

Post-breach

Mac EDR

Current Offerings

Status: GA

Data Collection

- Process tree
- Process creation
- File creation
- Network events

Threat and Vulnerability

- **Secure score** algorithm [security best practices across the fleet]
- **Vulnerability assessment** [OS patches and applications] + Reporting

Portal

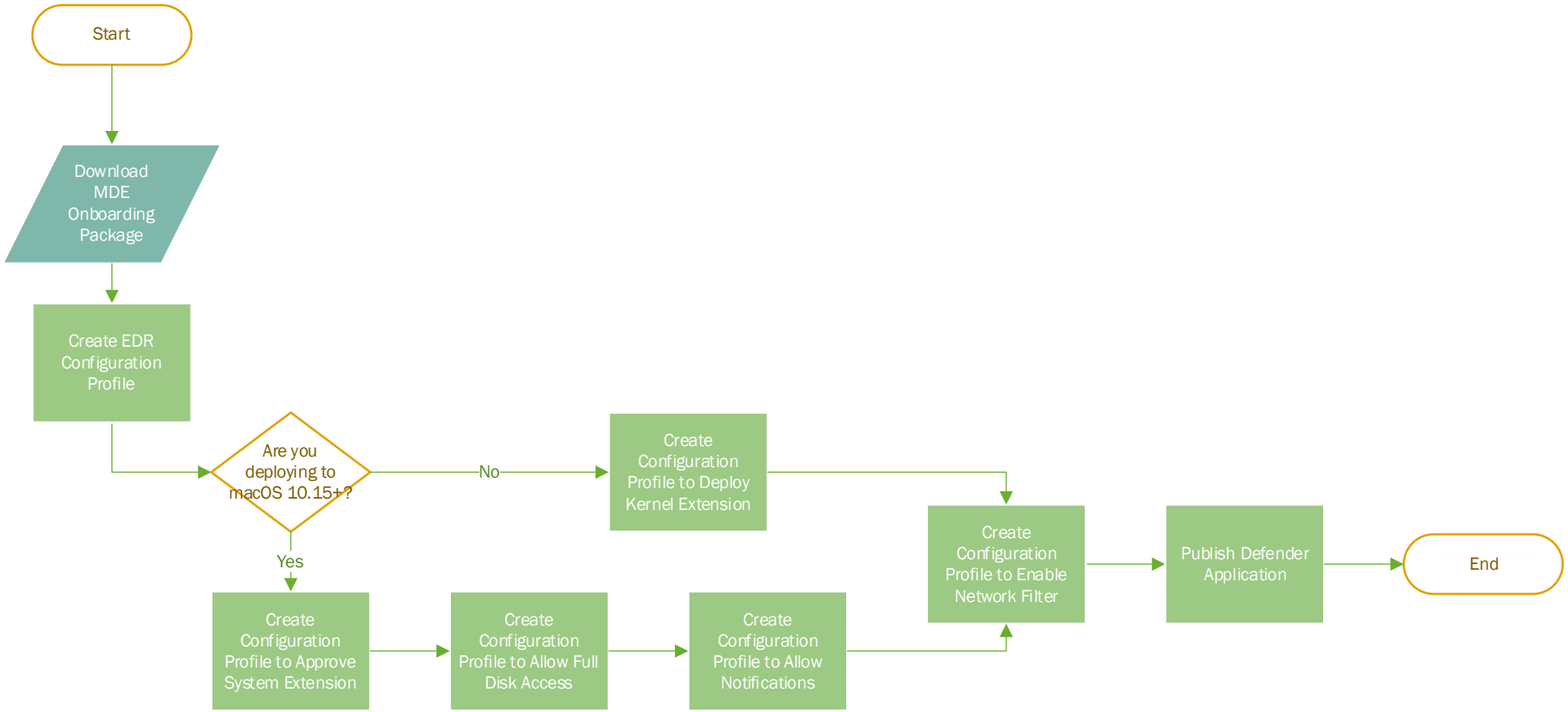
- **Single pane of glass**
- **Machine page**
- **Machine tagging**
- **Machine timeline**
- **Advanced hunting** (30 days, can be extended to 2 years with MDE Streaming API or a SIEM (e.g. Azure Sentinel)
- **6 months of raw data** on all machines inc macOS
- **Custom file/IP/URL allow/block**
- **Custom detections**
- [Response]:
  - **Live Response** on the machine (cmd and scripts)
  - **Isolate** (Network quarantine)
  - **Initiate remote AV scan**
  - **Collect Investigation package** (Machine Screenshot), for triage deep investigation
  - Block file upon demand

Differences in Configuration Standards

	Windows	Linux	macOS
Standard Mechanism	Registry	Configuration File	plist
Config Mechanism	OS-hosted jetpack database	Defined by application	XML \ Binary XML
Access Control	Registry file + key ACL	File system ACL	File system ACL
Configuration Management	• Group Policy • CM Platform	• Local Config • CM Platform	• Mobile Device Management (MDM)

Configuration Differences between Intune and JAMF

Microsoft Intune	JAMF
Every setting is a different configuration profile	Ability to set multiple configurations in one profile
Supports merging antivirus exclusions from multiple configuration profiles	Antivirus setting is explicit, not merged
Will fail the configuration profile if kernel extensions are configured for Apple silicon	Claims to gracefully handles Apple Silicon with kernel extensions configured per docs (not per my experience though)



MDE on macOS Deployment Process Overview

Configuration Profiles

Name	MDE
MDE Onboarding	X
System Extensions	X
Kernel Extension	X
Full Disk Access	-
+ com.microsoft.wdav, com.microsoft.wdav.epsext	X
+ com.microsoft.dlp.daemon	
Network Filter	X
Notifications	X
Accessibility	X

Premade mobileconfig files are available for required permissions (excluding MDE Onboarding):
https://github.com/microsoft/mdatp-xplat/tree/master/macos/mobileconfig/profiles

Customers can also use a single combined mobileconfig:
https://github.com/microsoft/mdatp-xplat/blob/master/macos/mobileconfig/combined/mdatp-nokext.mobileconfig

Deploying MDE on macOS via JAMF

TIP: Screen shots available at
Deploying Microsoft Defender for Endpoint on macOS with Jamf Pro
https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/mac-install-with-jamf?view=o365-worldwide

Creating JAMF Configuration Profiles

- Create a new configuration profile
  - Distribution Method: Install Automatically
  - Level: Computer Level
- Configure settings
- Set deployment scope using Scope tab
- Return to the Options tab

Configuring Onboarding using JAMF

- Download the MDM onboarding package from Defender portal
- Click on the Application & Custom Settings option, then External Applications
  - Click Add
  - Specify com.microsoft.wdav.atp in the Preference Domain
  - Select “Upload File (PLIST file)”
  - Upload the PLIST file from the onboarding package

Configure Microsoft AutoUpdate (MAU)

- Click on Application & Custom Settings \ Payload if not already there
- Click the “Add” button
- Enter the following under the preference domain field: com.microsoft.autoupdate2
- Copy the XML from the Microsoft AutoUpdate section of the JAMF deployment to the Property List field

Configuring Notifications using JAMF

- Click “Notifications” tab on left-hand navigation
- Add MDAV notification settings
  - Click “Add”
  - Bundle ID: com.microsoft.wdav.tray
  - Click Include on each item under settings, configure as customer prefers (ideally enable)
- Add AutoUpdate notification settings
  - Click “Add”
  - Bundle ID: com.microsoft.autoupdate.fba
  - Click Include on each item under settings, configure as customer prefers (ideally enable)

Granting Defender full disk access using JAMF

- Click on Privacy Preferences Policy Control, then Configure
- Use the following identifier: com.microsoft.wdav
- Ensure Identifier type is set to Bundle ID
- Paste the following under Code Requirement:
```
identifier "com.microsoft.wdav" and anchor apple generic and certificate
1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate
leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate
leaf[subject.OU] = UBF8T346G9
```
- Click Add under App or Service
- Choose “SystemPolicyAllFiles”, access “Allow” and click Save

Granting Defender full disk access using JAMF (cont'd)

- Click the "+" under App Access
- Enter com.microsoft.wdav.epsext as the identifier
- Ensure Identifier Type is set to Bundle ID
- Enter the following in the Code Requirement box:
  ```
  identifier "com.microsoft.wdav.epsext" and anchor apple generic and
  certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate
  leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate
  leaf[subject.OU] = UBF8T346G9
  ```
- Click the "Add +" button under App or Service
- Choose "SystemPolicyAllFiles", access "Allow"

Approve the MDE Kernel Extension (macOS<= 10.15)

- Do not use this to configure Apple silicon systems – the entire configuration profile will fail
  - Apple silicon does not support kernel extensions
  - JAMF documents claim to handle Apple silicon gracefully per their docs, but in my experience it does not
  - Consider creating a differently scoped policy for this configuration, or just a different configuration profile (messy, but easy ☺)
- Click on “Approved Kernel Extensions” and click “Configure”
- Enter the following under Approved Team ID
  - Display Name: Microsoft Corp.
  - Team ID: UBF8T346G9

Approve System extensions for MDE

- Click on System Extensions, then Configure
- Change “System Extensions Types” drop-down to “Allowed System Extensions”
- Enter the following under team identifier: UBF8T346G9
- Click add under “Allowed System Extensions” and add the following
  - com.microsoft.wdav.epsext
  - com.microsoft.wdav.netext

Configure Network Extension

- Click on “Content Filter” in the left-hand navigation
- Enter the following configurations (all others blank)
  - Filter Name (optional): Microsoft Defender Content Filter
  - Identifier: com.microsoft.wdav
  - Filter Order: Inspector
  - Socket Filter: com.microsoft.wdav.netext
  - Socket Filter Designated Requirement:
    identifier "com.microsoft.wdav.netext" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = UBF8T346G9
- Save the policy

Creating the Defender for Endpoint package

- Download the installation package from the Defender portal
- Rename the package with the date to keep track of age
- Click on Management Settings in the far left-hand navigation
- Click on Computer Management, then Packages
- Click on the “+ New” button
- Click “Choose File” and upload the package you downloaded & renamed
- Set the package display name to “Defender for Endpoint <date>”
- Click the save button

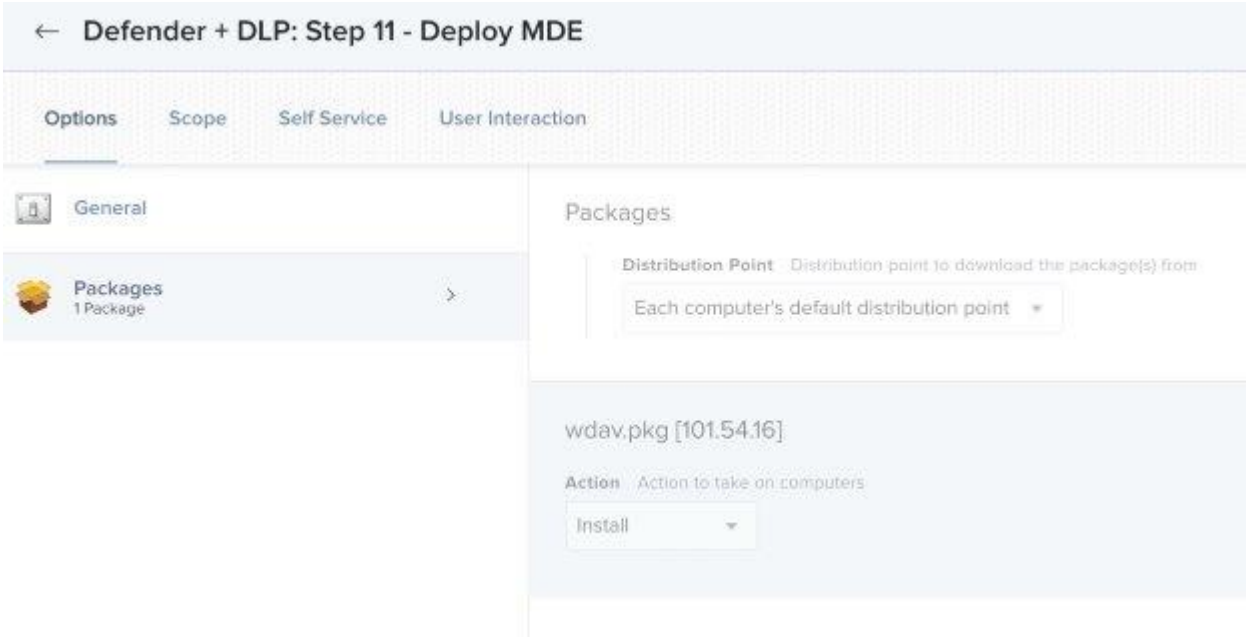
Assigning the MDE package

- Click “Computers”, then “Polices” in the left-hand navigation
- Click the “+ New” button
- Enter the following information
  - Display Name: Microsoft Defender for Endpoint
  - Trigger: Recurring Check-in
- Click on “Packages” in the left-hand navigation, then click “Configure”
- Find the package you created in the previous step and click “Add”
- Click on the Scope tab on the top to set your deployment scope
- Save the policy

Considerations for Deployment

- Consider using the same computer groups for the configuration profile and package deployment
- You can set everything in one configuration profile if you prefer, or use multiple
- You may want to separate your deployment configuration profile from your AV configuration deployment
- You may want to deploy the configuration profile ahead of the package to avoid user prompts
- You can force a JAMF client to check-in using the following command:
  `sudo jamf policy`

Deploy wdav.pkg



Deploying via MEM

TIP: Screen shots available at
Deploy Microsoft Defender for Endpoint on macOS with Microsoft Intune
https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/mac-install-with-intune?view=o365-worldwide

Creating the EDR Configuration Profile

- Create a configuration profile
  - Platform: macOS
  - Profile type: Templates
  - Template name: Custom
- Set a name for the Configuration Profile
- Set up the Configuration Profile
  - Set a name for the configuration profile (this is what will be displayed to users)
  - Deployment channel: Device channel
  - Upload the WindowsDefenderATPOnboarding.xml from the onboarding package
- Configure scope tags and assignments

Approve MDE kernel extensions (macos <= 10.15)

- Create another configuration profile
  - Platform: macOS
  - Profile type: Templates
  - Template name: Extensions
- Assign a name to the configuration profile
- Expand Kernel Extensions
  - Set team identifier to UBF8T346G9
- Configure Scope tags & Assignments

Do not deploy this to Apple Silicon (M1) devices. Kernel extensions are not supported on this platform and the policies will fail

Approve MDE system extensions (macOS >10.15)

- Create another configuration profile
  - Platform: macOS
  - Profile type: Templates
  - Template name: Extensions
- Assign a name to the configuration profile
- Expand System extensions and add the following
  - Bundle identifier: com.microsoft.wdav.epsext
    Team identifier: UBF8T346G9
  - Bundle identifier: com.microsoft.wdav.netext
    Team identifier: UBF8T346G9
- Configure Scope tags & Assignments

Granting MDE full disk access (macOS > 10.15)

- Download the full disk access config
  - https://raw.githubusercontent.com/microsoft/mdatp-xplat/master/macos/mobileconfig/profiles/fulldisk.mobileconfig
- Create a configuration profile
  - Platform: macOS
  - Profile type: Templates
  - Template name: Custom
- Set a name for the Configuration Profile
- Set up the Configuration Profile
  - Set a name for the configuration profile (this is what will be displayed to users)
  - Deployment channel: Device channel
  - Upload the fulldisk.mobileconfig file
- Configure scope tags and assignments

Granting MDE network filter access (macOS > 10.15)

- Download the full disk access config
  - https://raw.githubusercontent.com/microsoft/mdatp-xplat/master/macos/mobileconfig/profiles/fulldisk.mobileconfig
- Create a configuration profile
  - Platform: macOS
  - Profile type: Templates
  - Template name: Custom
- Set a name for the Configuration Profile
- Set up the Configuration Profile
  - Set a name for the configuration profile (this is what will be displayed to users)
  - Deployment channel: Device channel
  - Upload the fulldisk.mobileconfig file
- Configure scope tags and assignments

Granting MDE notification access (macOS > 10.15)

- Download the full disk access config
  - https://raw.githubusercontent.com/microsoft/mdatp-xplat/master/macos/mobileconfig/profiles/notif.mobileconfig
- Create a configuration profile
  - Platform: macOS
  - Profile type: Templates
  - Template name: Custom
- Set a name for the Configuration Profile
- Set up the Configuration Profile
  - Set a name for the configuration profile (this is what will be displayed to users)
  - Deployment channel: Device channel
  - Upload the fulldisk.mobileconfig file
- Configure scope tags and assignments

Publishing MDE to macOS

- Click Apps from the MDE left-hand navigation
- Click macOS under “By platform”
- Click Add
  - App type: Microsoft Defender for Endpoint \ macOS

Run an Antimalware (aka AV) detection test

- curl -o ~/Downloads/eicar.com.txt http://www.eicar.org/download/eicar.com.txt

Configuring Antimalware using JAMF

- Download the configuration schema from Defender's GitHub repository
- Choose or create a configuration profile
  - Level: Computer Level
  - Distribution Method: Install Automatically
- Under Applications & Custom Settings choose "External Applications"
- Click the "Add" button and choose "Custom Schema" as the source
  - Enter com.microsoft.wdav as the Preference Domain
  - Click "Add Schema" and upload the schema.json file from Defender's GitHub repository
- Settings should be configurable after you click "Save"
- When you are done, click "Save" on the bottom right

Configuring Antimalware

- MDE for macOS (MDATP for macOS): List of antimalware (aka antivirus (AV)) exclusion list for 3rd party applications.

https://yongrhee.wordpress.com/2020/10/14/mde-for-macos-mdatp-for-macos-list-of-antimalware-aka-antivirus-av-exclusion-list-for-3rd-party-applications/

- Common mistakes to avoid when defining exclusions

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/common-exclusion-mistakes-microsoft-defender-antivirus?view=o365-worldwide

How can we really tell something is being excluded?

- File/folder: Drop EICAR in excluded path or as excluded name, does it detect? No = you are good.
  Process exclusions: A bit trickier. Only way I know to do this is via logging with these steps:
  1) Put the exclusion for the process in place.
  2) Turn logging verbose with "mdatp log level set --level verbose"
  3) Run the process
  4) Turn logging back to info with "mdatp log level set --level info"
  5) Export diag info with "mdatp diagnostic create"
  6) Open the diagnostic and look for file "\library\Logs\Microsoft\mdatp\microsoft-defender_core.log"
  7) Search the file for the excluded process. In this example, we excluded "nano":
- [7651][2021-01-27 18:43:33.864344 UTC][debug]: **RTP: Not scanning** '{"key":{"last_modified":0,"scan_reason":"read","process":{"id":8282,"start_time":1611773013856546,"path":"/usr/bin/**nano**"},"parent_process":{"id":1788,"start_time":0},"is_file_created":null},"value":{"file":"/private/etc/nanorc","ignore_exclusions":false}}' **due to process exclusion** [7651][2021-01-27 18:43:33.864362 UTC][debug]: agent, realTimeAntivirusEngine, [53, result, {"$type":"optional<threat_data>","value":null}]

Scheduled Scans

Scheduled scans are not an in-box capability today

To schedule a scan on macOS, [create a plist for use with launchd]

Easiest way to accomplish this would be a shell script.

We provide an example bash script to accomplish this [on GitHub]

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
  "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>Label</key>
    <string>com.microsoft.wdav.schedquickscan</string>
    <key>ProgramArguments</key>
    <array>
        <string>sh</string>
        <string>-c</string>
        <string>/usr/local/bin/mdatp scan quick</string>
    </array>
    <key>RunAtLoad</key>
    <true/>
    <key>StartCalendarInterval</key>
    <dict>
        <key>Day</key>
        <integer>3</integer>
        <key>Hour</key>
        <integer>2</integer>
        <key>Minute</key>
        <integer>0</integer>
        <key>Weekday</key>
        <integer>5</integer>
    </dict>
    <key>WorkingDirectory</key>
    <string>/usr/local/bin/</string>
</dict>
</plist>
```

Check for Platform Update (Product Update)

- /Library/Application Support/Microsoft/MAU2.0/Microsoft AutoUpdate.app/Contents/MacOS
- ./msupdate --install --apps wdav00

Check for Update definition

- mdatp --definition-update

Privacy for Microsoft Defender for Endpoint on macOS

- Privacy for Microsoft Defender for Endpoint on macOS
- https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/mac-privacy?view=o365-worldwide

Resources for Microsoft Defender for Endpoint on macOS

- Resources for Microsoft Defender for Endpoint on macOS
- https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/mac-resources?view=o365-worldwide

mdatp cmd line basics ?

`mdatp config`	
`mdatp connectivity test`	Tests connectivity with cloud endpoints
`Mdatp definitions`	
`Mdatp diagnostic`	
`Mdatp diagnostic`	
`Mdatp edr`	
`Mdatp exclusion`	
`Mdatp health`	

Troubleshoot installation issues

- Troubleshoot installation issues for Microsoft Defender for Endpoint on macOS
- https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/mac-support-install?view=o365-worldwide

- Note: The list of URL's that need to be added are in:

  - Commercial:
  https://download.microsoft.com/download/6/b/f/6bfff670-47c3-4e45-b01b-64a2610eaefa/mde-urls-commercial.xlsx

  - GCC/GCC High:
  - https://download.microsoft.com/download/6/a/0/6a041da5-c43b-4f17-8167-79dfdc10507f/mde-urls-gov.xlsx

Troubleshoot installation issues cont…

- Checking to see if the system extensions need a reboot

systemextensionsctl list

```
demoadmin — -zsh — 185×24
Last login: Thu May 13 20:11:29 on ttys000
demoadmin@DemoAdmins-Air ~ % systemextensionsctl list
4 extension(s)
--- com.apple.system_extension.network_extension
enabled active  teamID  bundleID (version)      name    [state]
                UBF8T346G9      com.microsoft.wdav.netext (101.27.50/101.27.50)Microsoft Defender ATP Network Extension [terminated waiting to uninstall on reboot]
*       *       UBF8T346G9      com.microsoft.wdav.netext (101.29.61/101.29.61)Microsoft Defender ATP Network Extension [activated enabled]
--- com.apple.system_extension.endpoint_security
enabled active  teamID  bundleID (version)      name    [state]
                UBF8T346G9      com.microsoft.wdav.epsext (101.27.50/101.27.50)Microsoft Defender ATP Endpoint Security Extension      [terminated waiting to uninstall on reboot]
*       *       UBF8T346G9      com.microsoft.wdav.epsext (101.29.61/101.29.61)Microsoft Defender ATP Endpoint Security Extension      [activated enabled]
demoadmin@DemoAdmins-Air ~ %
```

In this example, no reboot is required, unless you want to offload the older system extensions.

Troubleshoot kernel extension issues

Note: Only applicable for Catalina and older versions

- Troubleshoot kernel extension issues in Microsoft Defender for Endpoint on macOS
- https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/mac-support-kext?view=o365-worldwide

Troubleshoot license issues

- Troubleshoot license issues for Microsoft Defender for Endpoint on macOS
- https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/mac-support-license?view=o365-worldwide

Troubleshoot cloud connectivity

- Troubleshoot cloud connectivity issues for Microsoft Defender for Endpoint on macOS
- https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/troubleshoot-cloud-connect-mdemac?view=o365-worldwide

Supported type of proxies for MDE on macOS

- Manual static proxy configuration
- Proxy autoconfig (PAC)
- Web Proxy Autodiscovery Protocol (WDAP)

Check for successful network connection

curl -w ' %{url_effective}\n' 'https://x.cp.wd.microsoft.com/api/report ' 'https://cdn.x.cp.wd.microsoft.com/ping

Taking care of False Positives (FP’s) and False Negatives (FN’s).

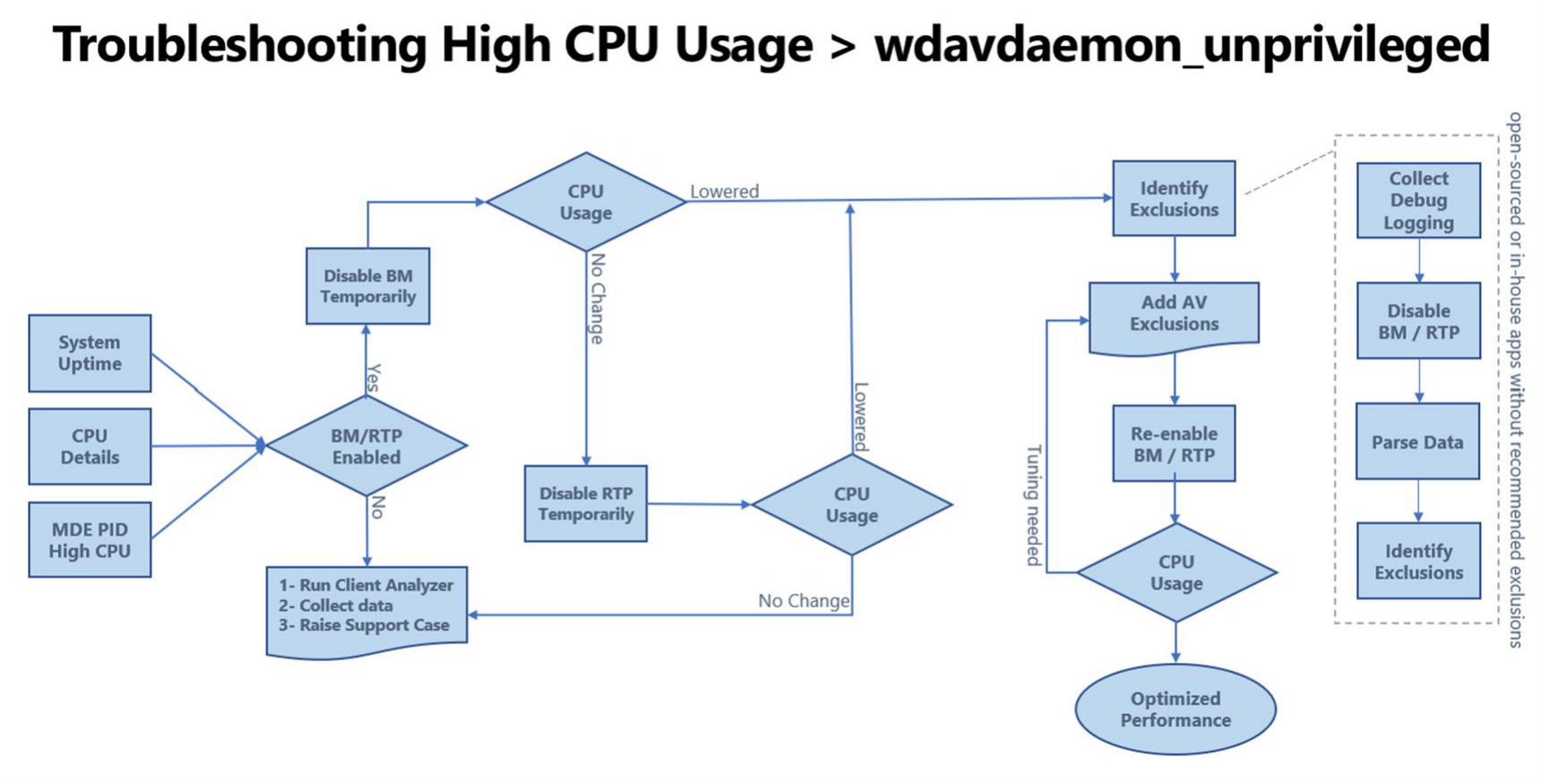
- Submit the FP’s and FN’s to https://aka.ms/MDSI

- Address false positives/negatives in Microsoft Defender for Endpoint

Taking care of High CPU issues

Process	What MDE Component	Comments
wdavdaemon	core (aka privileged)	Need to open a Microsoft support ticket if there is a high cpu here.
wdavdaemon_unprivileged	antimalware (antivirus)	Troubleshoot performance issues for Microsoft Defender for Endpoint on macOS https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/mac-support-perf?view=o365-worldwide
wdavdaemon_enterprise	edr	Need to open a Microsoft support ticket if there is a high cpu here.

Troubleshooting High CPU issues in wdavdaemon_unprivileged



Troubleshooting High CPU issues in **wdavdaemon_unprivileged** cont…

1. sudo mdatp log level set --level debug
   TIP: If the issue is occurring during startup, you might have to use this instead: sudo mdatp log level persist --level debug
2. mdatp config real-time-protection --value enabled
3. While the issue is reproducing...
4. mdatp diagnostic real-time-protection-statistics --output json > real_time_protection.json

- Reference: https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/mac-support-perf?view=o365-worldwide#troubleshoot-performance-issues-using-real-time-protection-statistics

Troubleshooting High CPU issues in **wdavdaemon_unprivileged** cont…

- Sample script to parse the log real_time_protection.json
- If you have a macOS system:

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/mac-support-perf?view=o365-worldwide#troubleshoot-performance-issues-using-real-time-protection-statistics

- If you have a Windows system:

https://github.com/YongRhee-MDE/Scripts/blob/master/MDE_macOS_High_CPU_json_parser.ps1

Troubleshooting High CPU issues in **wdavdaemon_unprivileged** cont…

Based on the previous step, add to the AV exclusions via:

The mdatp command line for testing purposes:

- file (aka processes)

mdatp exclusion file [add\|remove] --path [path-to-file]

e.g.

mdatp exclusion file add --path processname

or

mdatp exclusion file add --path /var/log/test.log

- folder (aka directory)

mdatp exclusion folder [add\|remove] --path [path-to-directory]

e.g. mdatp exclusion folder add --path /var/log/

- extension

mdatp exclusion extension [add\|remove] --name [extension]

e.g. mdatp exclusion extension add --name .test

- Reference: https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/mac-exclusions?view=o365-worldwide
- Also review Common mistakes to avoid when defining exclusions

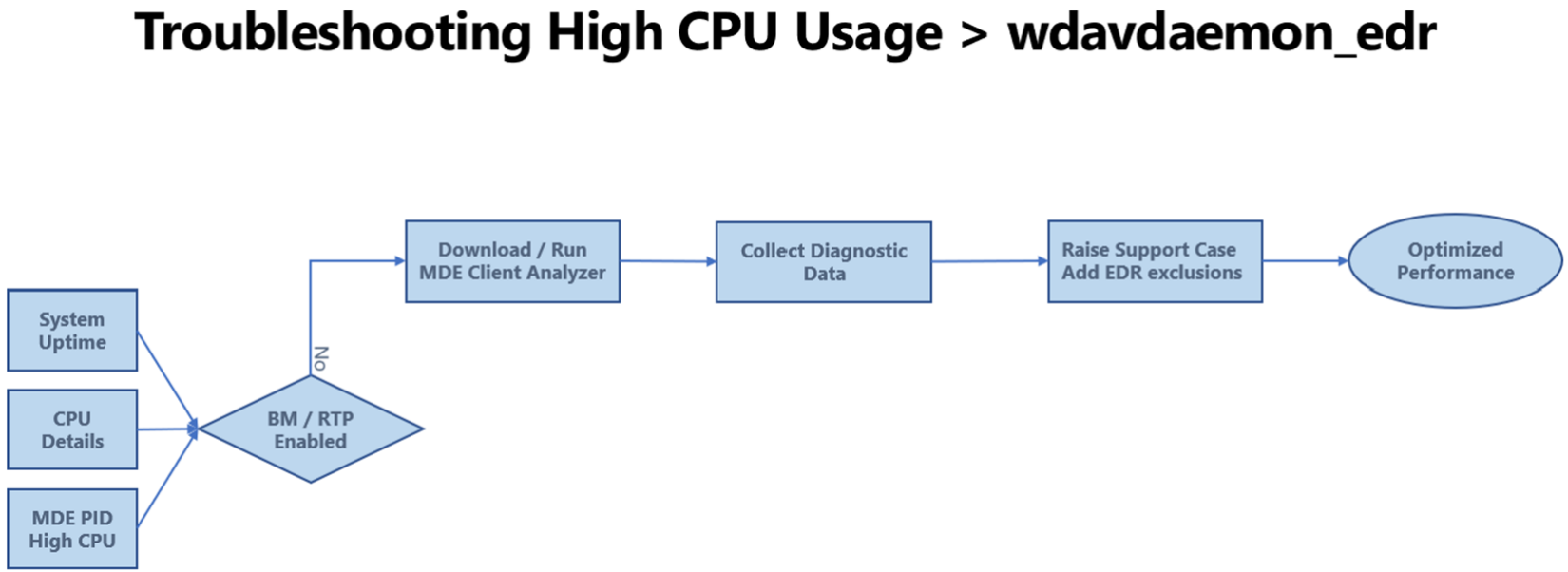
Troubleshooting High CPU issues in **wdavdaemon_unprivileged** cont…

- Once you verify that the AV exclusions are working as intended, please add it to the Settings Preferences (akin to the MDM policy / GPO policy in Windows)
- Property list for JAMF full configuration profile

or

- Intune full profile

Troubleshooting High CPU issues in wdavdaemon_edr



Note: The instructions for MDE Client Analyzer are in slide 82.

MAU (Microsoft AutoUpdate)

- Read about how to deploy MAU policies

https://learn.microsoft.com/en-us/deployoffice/mac/update-office-for-mac-using-msupdate

- Read about how to deploy MAU policies via JamF:

https://docs.jamf.com/technical-papers/jamf-pro/microsoft-office/10.18.0/Microsof_Office_Distribution.html

Collecting diagnostic data

- Run the client analyzer on macOS and Linux
- https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/run-analyzer-macos-linux?view=o365-worldwide
- https://aka.ms/XMDEClientAnalyzerBinary

- Terminal:

```
spctl --add /Path/To/MDESupportTool
sudo ./MDESupportTool –d
```

or

```
sudo ./MDESupportTool –performance
```

Uninstall MDE on macOS for troubleshooting

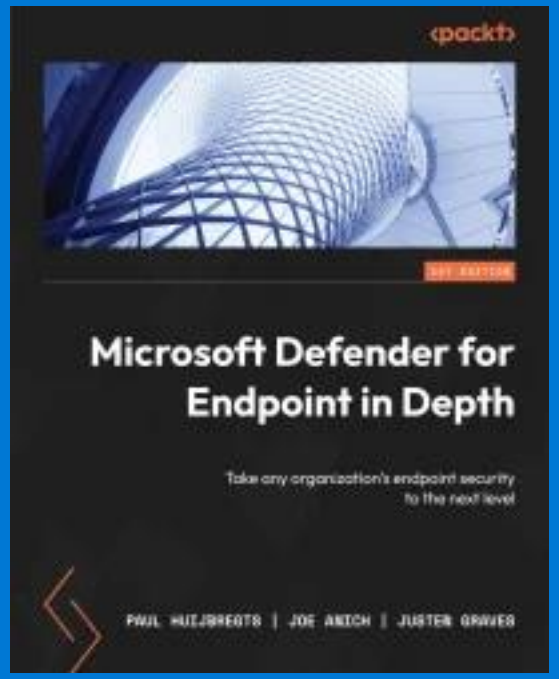
- Before you uninstall, you should consider offboarding MDE on macOS. It will prevent duplication of the Device in the “Device List”, which will remain in the portal for 180 days.

- If you really need to uninstall, make sure that you move the macOS to a policy where MDE on macOS Tamper Protection is either in audit mode or disabled.

- How to uninstall MDE on macOS?
- https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/mac-resources?view=o365-worldwide#uninstalling

Contact Microsoft Defender for Endpoint support

- Contact Microsoft Defender for Endpoint support
- https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/contact-support?view=o365-worldwide



If you are interested in learning more about Microsoft Defender for Endpoint, please check out this new book called

"Microsoft Defender for Endpoint in Depth"

Packt publisher https://aka.ms/MDE-Book

Authors:

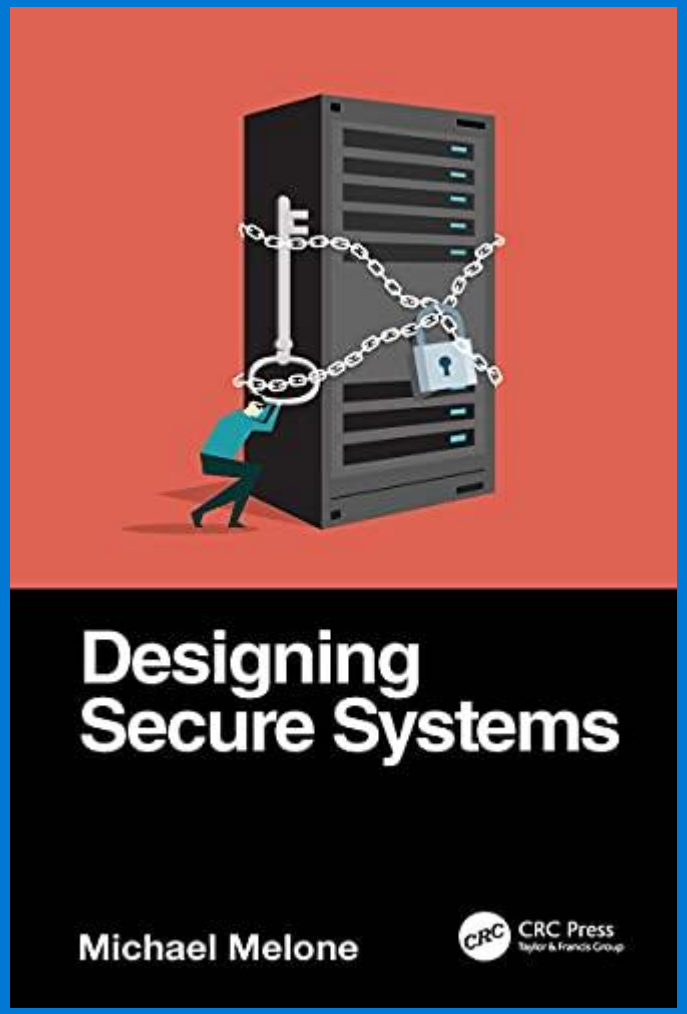
- Paul Huijbregts – Microsoft Defender for Endpoint Product Manager
- Joe Anich – Microsoft Incident Response (formerly known as DART)
- Justen Graves – Microsoft IT SOC

Microsoft Defender for Endpoint Deployment

Jeffrey Appel
Microsoft MVP

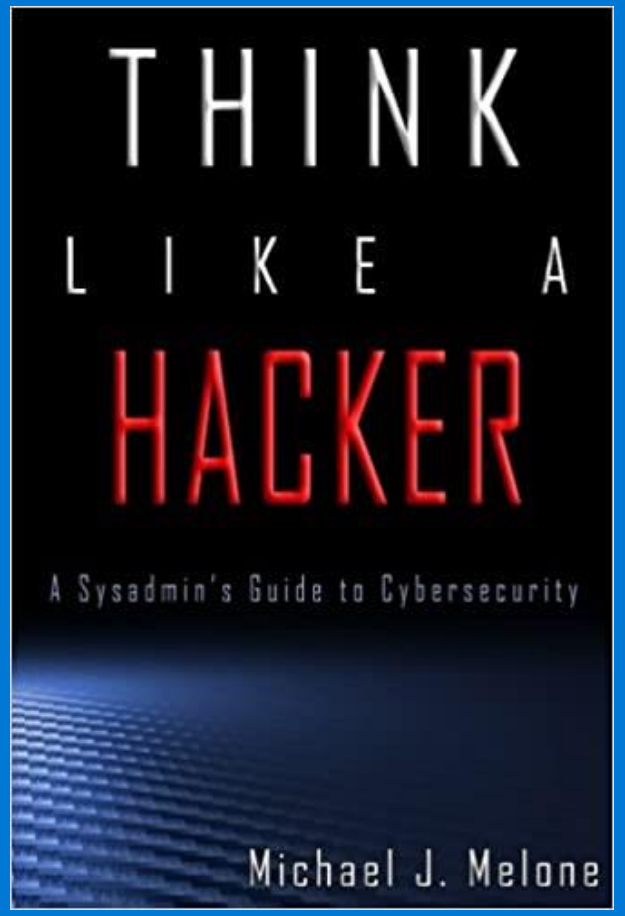
PowerShell Automation and Scripting for CyberSecurity: Hacking and Defense for Red and Blue Teamers

Miriam C. Wiesner
Microsoft Defender for Endpoint Security Researcher



Designing Secure Systems

Michael Melone
Microsoft Defender Experts XDR - researcher



Think Like a Hacker: A Sysadmin's Guide to Cybersecurity

Michael Melone
Microsoft Defender Experts XDR - researcher

Note: Wrote it while being in Microsoft DART, now called Microsoft Incident Response (Microsoft IR)

We'd love your feedback!

Fill out the survey to let us know what upcoming features are of the greatest importance to you:
https://forms.office.com/r/ctbTgmjV5h

Q&A

Microsoft Security

Thank you!