

# #POWERCON2022

Protezione dei dispositivi mobili e server con  
Microsoft Defender for Endpoint

**Roberto Tafuri**

*Cloud Solution Specialist – Project Informatica*

*roberto.tafuri@project.it*

*www.robertotafuri.it*



/ictpower

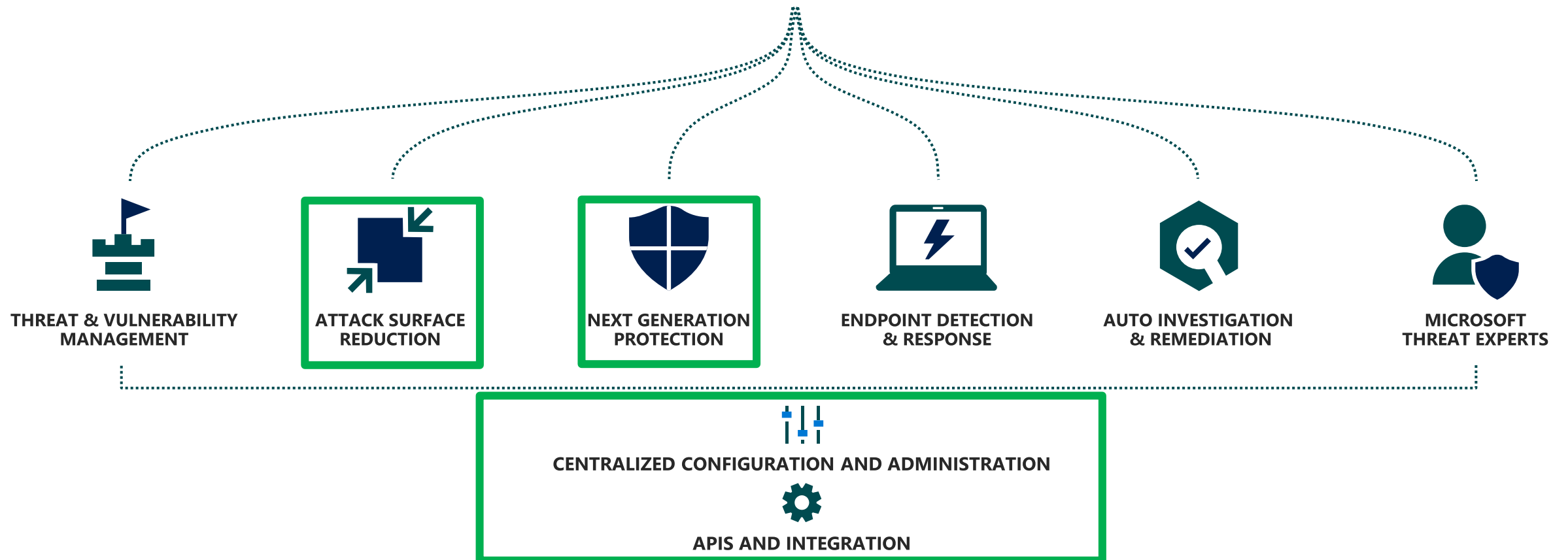


@ictpower\_it






# Microsoft Defender for Endpoint

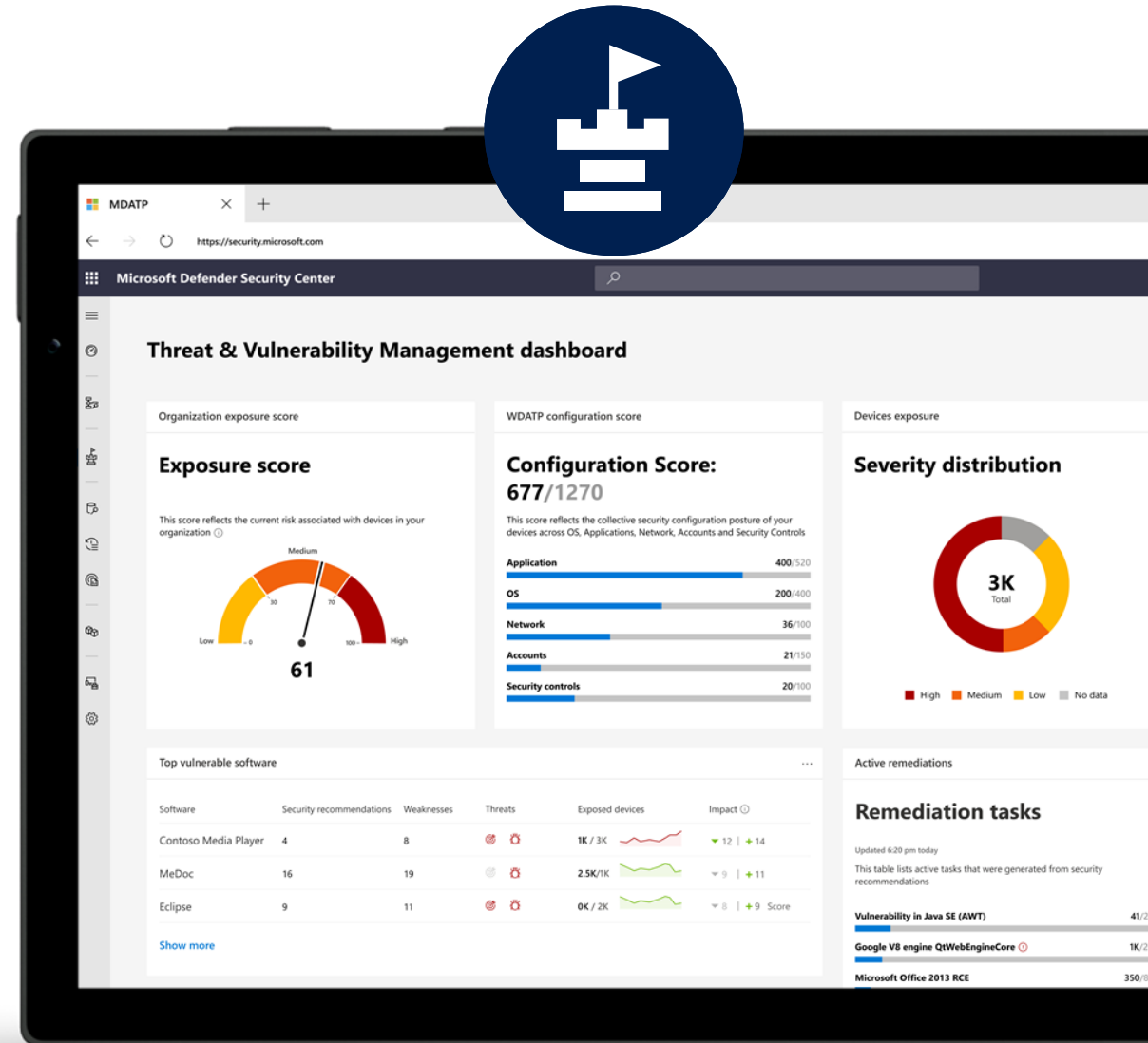
Threats are no match.



# Threat & Vulnerability Management

A risk-based approach to mature your vulnerability management program

-  1 Continuous real-time discovery
-  2 Context-aware prioritization
-  3 Built-in end-to-end remediation process



# Continuous Discovery

## Extensive vulnerability assessment across the entire stack

Easiest to exploit



Application extension vulnerabilities

Application-specific vulnerabilities that relate to component within the application.

For example: Grammarly Chrome Extension (CVE-2018-6654)



Application run-time libraries vulnerabilities

Reside in a run-time libraries which is loaded by an application (dependency).

For example: Electron JS framework vulnerability (CVE-2018-1000136)



Application vulnerabilities (1<sup>st</sup> and 3<sup>rd</sup> party)

Discovered and exploited on a daily basis.

For example: 7-zip code execution (CVE-2018-10115)



OS kernel vulnerabilities

Becoming more and more popular in recent years due to OS exploit mitigation controls.

For example: Win32 elevation of privilege (CVE-2018-8233)



Hardware vulnerabilities (firmware)

Extremely hard to exploit, but can affect the root trust of the system.

For example: Spectre/Meltdown vulnerabilities (CVE-2017-5715)

Hardest to discover

# Attack Surface Reduction

Eliminate risks by reducing the surface area of attack



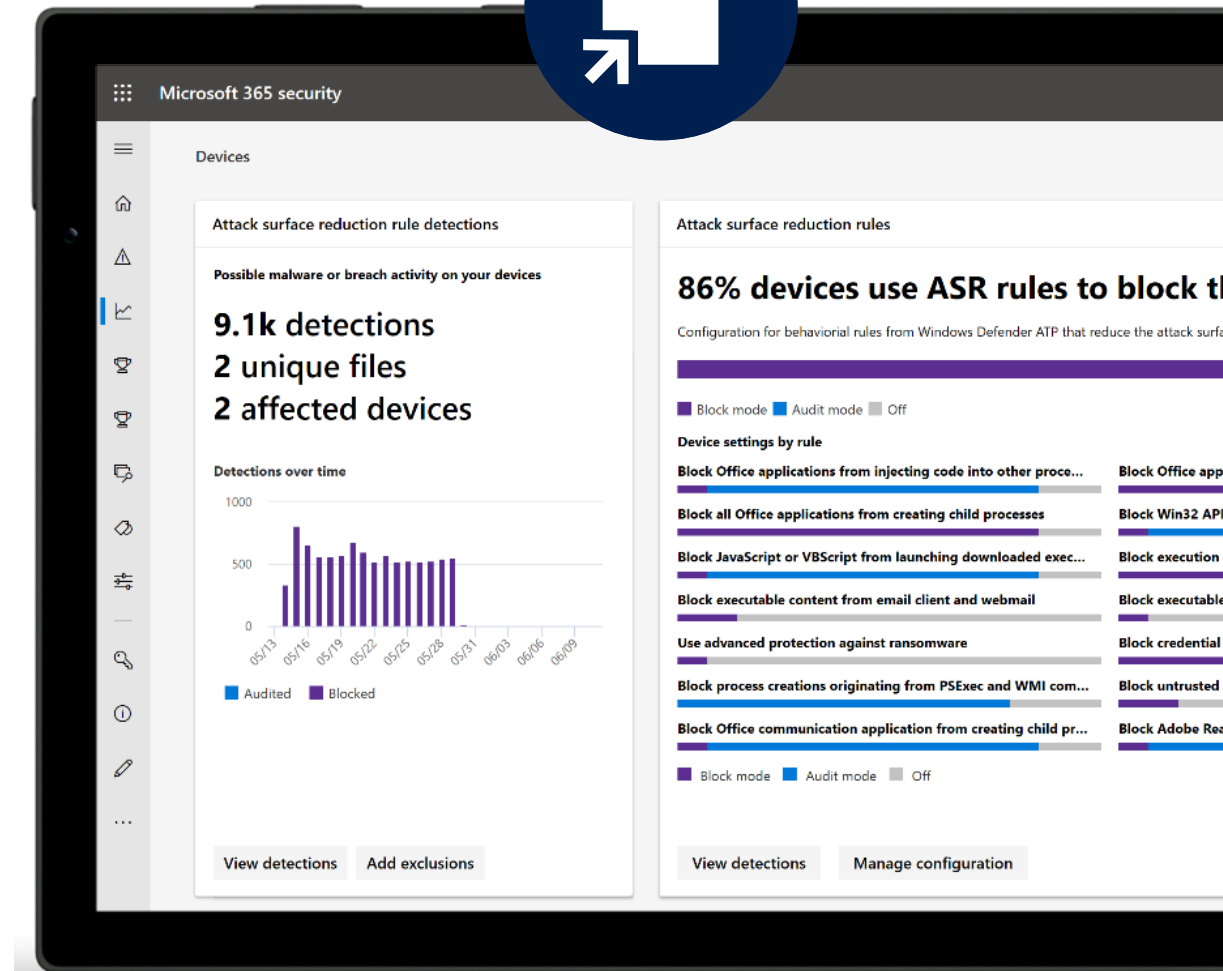
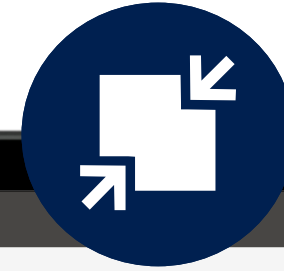
System hardening without disruption



Customization that fits your organization

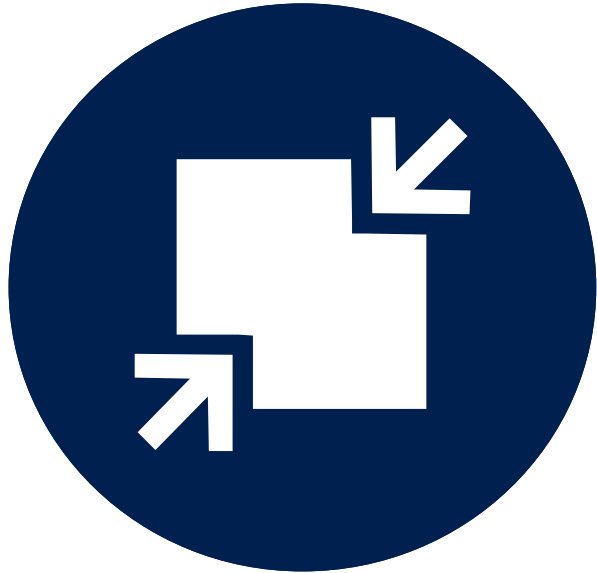


Visualize the impact and simply turn it on



# Attack Surface Reduction

Resist attacks and exploitations



HW based isolation

Application control

Exploit protection

Network protection

Controlled folder access

Device control

Web protection

Ransomware protection

Isolate access to untrusted sites

Isolate access to untrusted Office files

Host intrusion prevention

Exploit mitigation

Ransomware protection for your files

Block traffic to low reputation destinations

Protect your legacy applications

Only allow trusted applications to run

# Next Generation Protection

Blocks and tackles sophisticated threats and malware



Behavioral based real-time protection



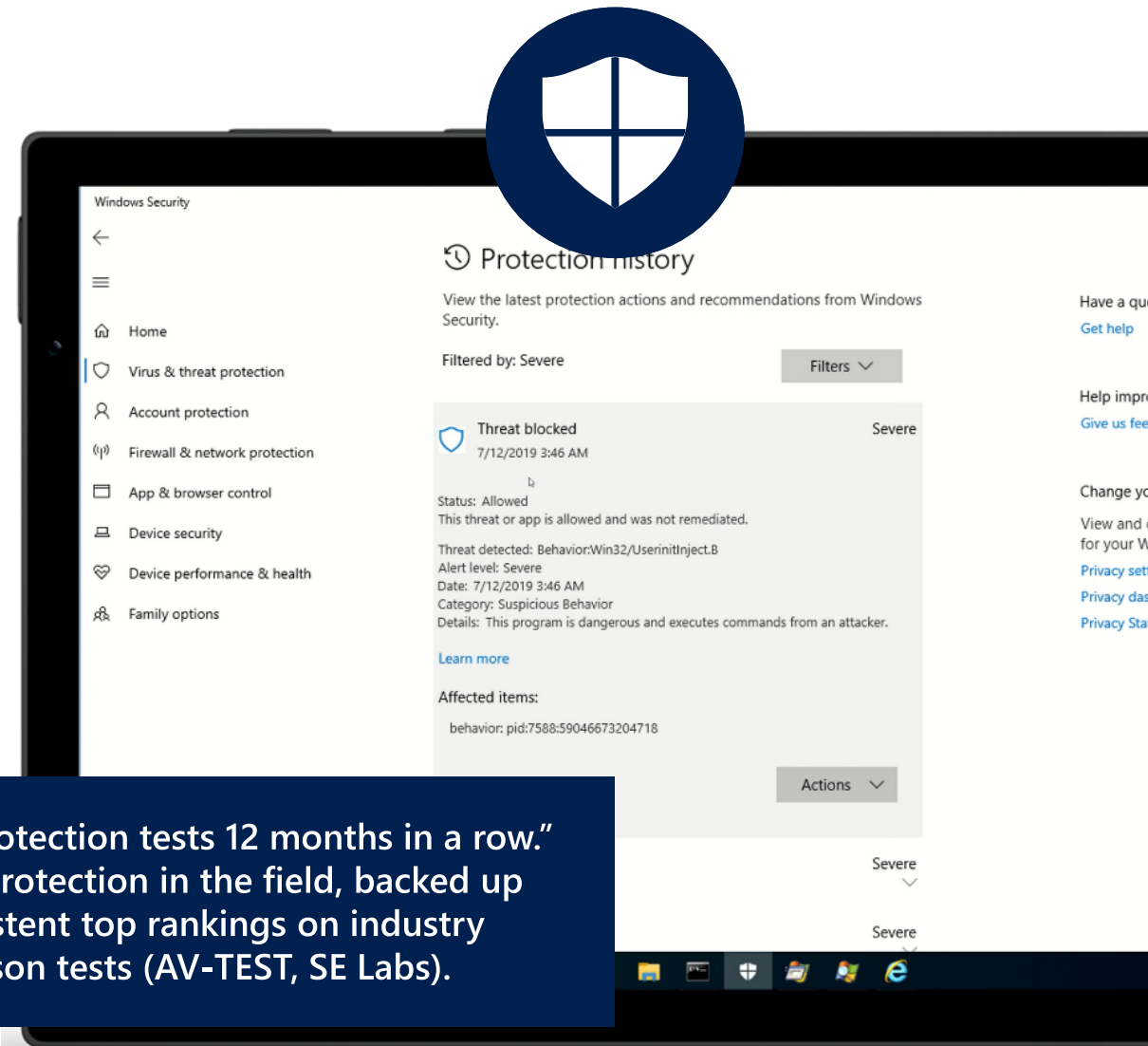
Blocks file-based and fileless malware



Stops malicious activity from trusted and untrusted applications



“Aced protection tests 12 months in a row.”  
Proven protection in the field, backed up  
by consistent top rankings on industry  
comparison tests (AV-TEST, SE Labs).



# Endpoint Detection & Response

Detect and investigate advanced persistent attacks



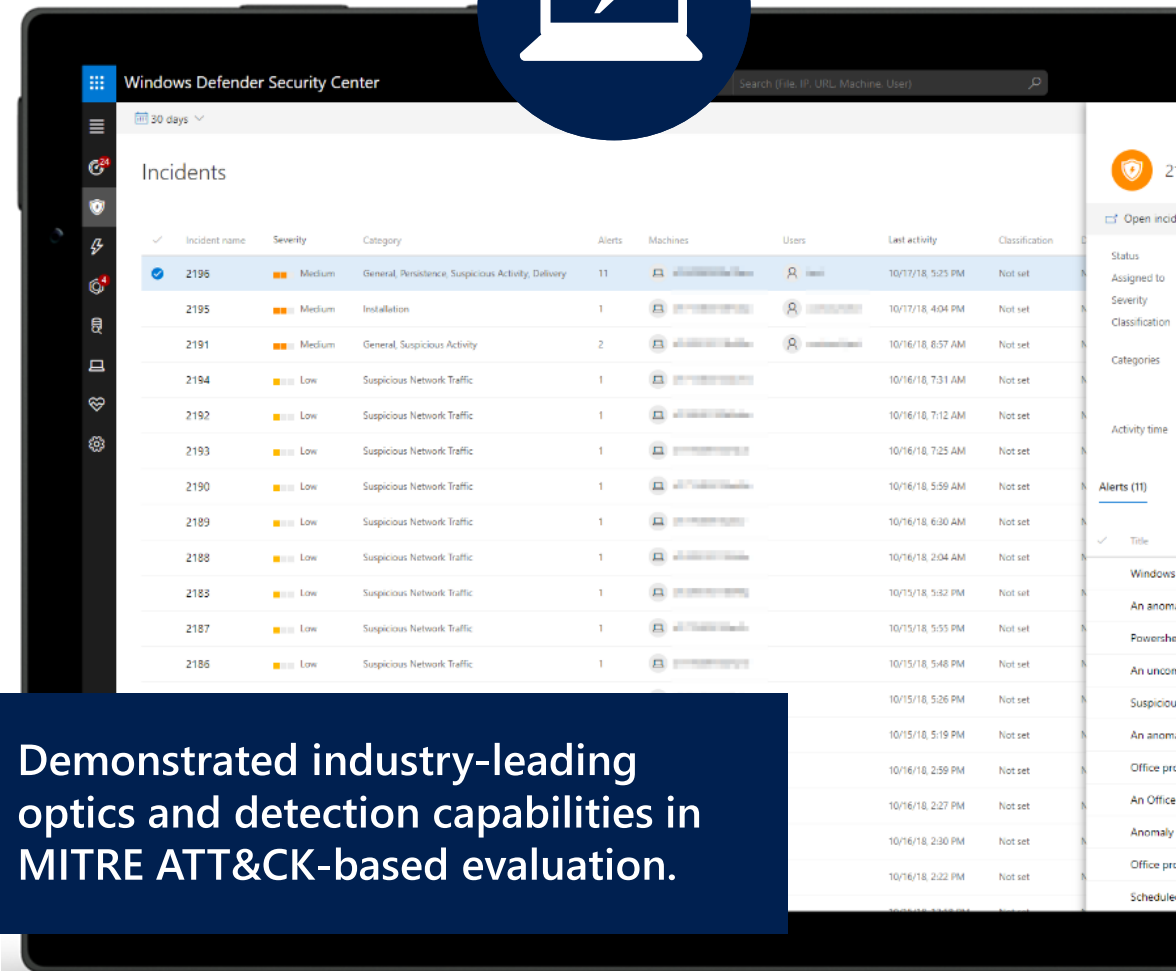
Correlated behavioral alerts



Investigation & hunting over 6 months of data



Rich set of response actions



Demonstrated industry-leading optics and detection capabilities in MITRE ATT&CK-based evaluation.



# Endpoint Detection & Response



Correlated post-breach detection

Investigation experience

Incident

Advanced hunting

Response actions (+EDR blocks)

Deep file analysis

Live response

Threat analytics

# Auto Investigation & Remediation

Automatically investigates alerts and remediates complex threats in minutes



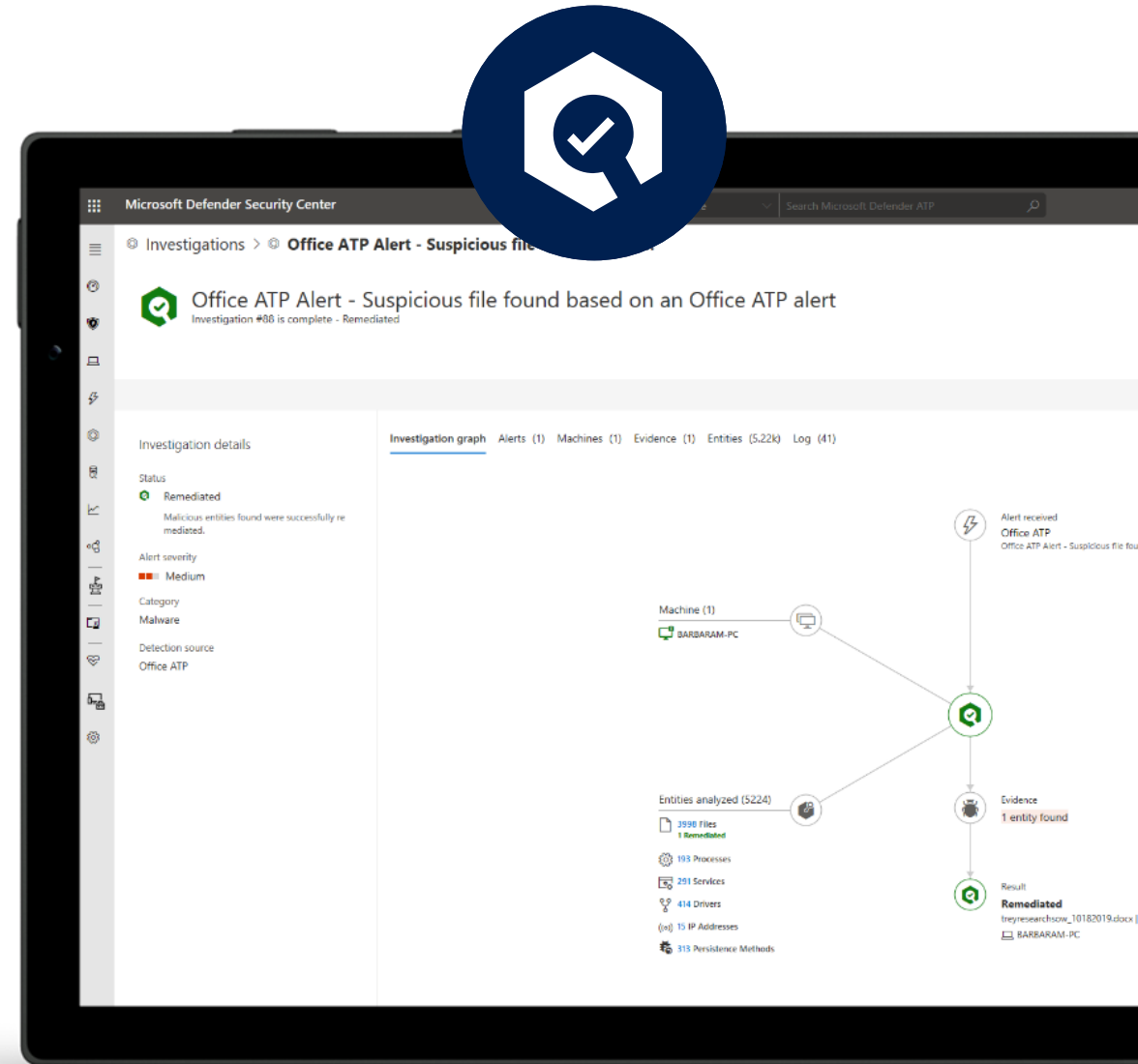
Mimics the ideal steps analysts would take



Tackles file or memory-based attacks



Works 24x7, with unlimited capacity



# Security Management

Assess, configure and respond to changes in your environment



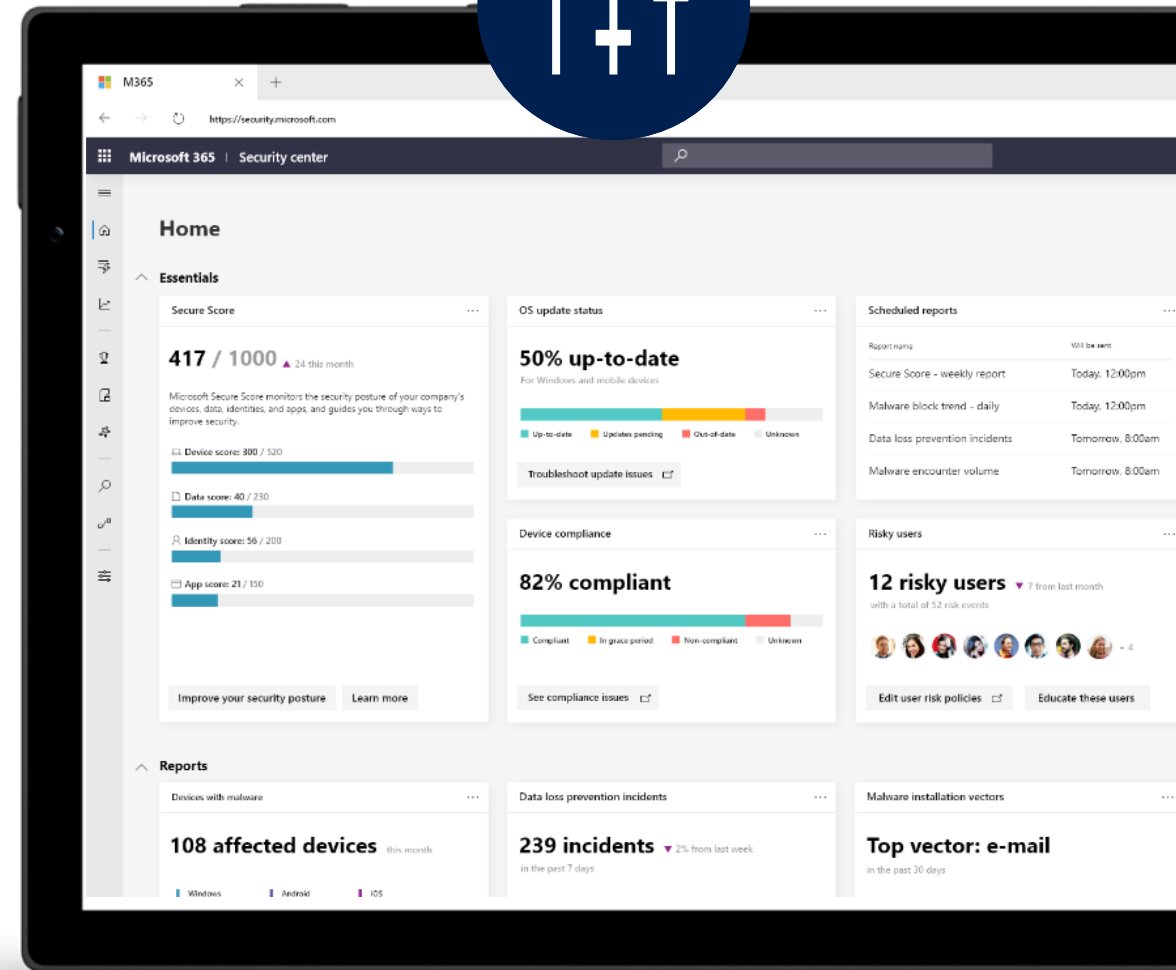
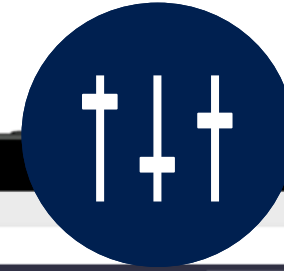
Centrally assess & configure your security



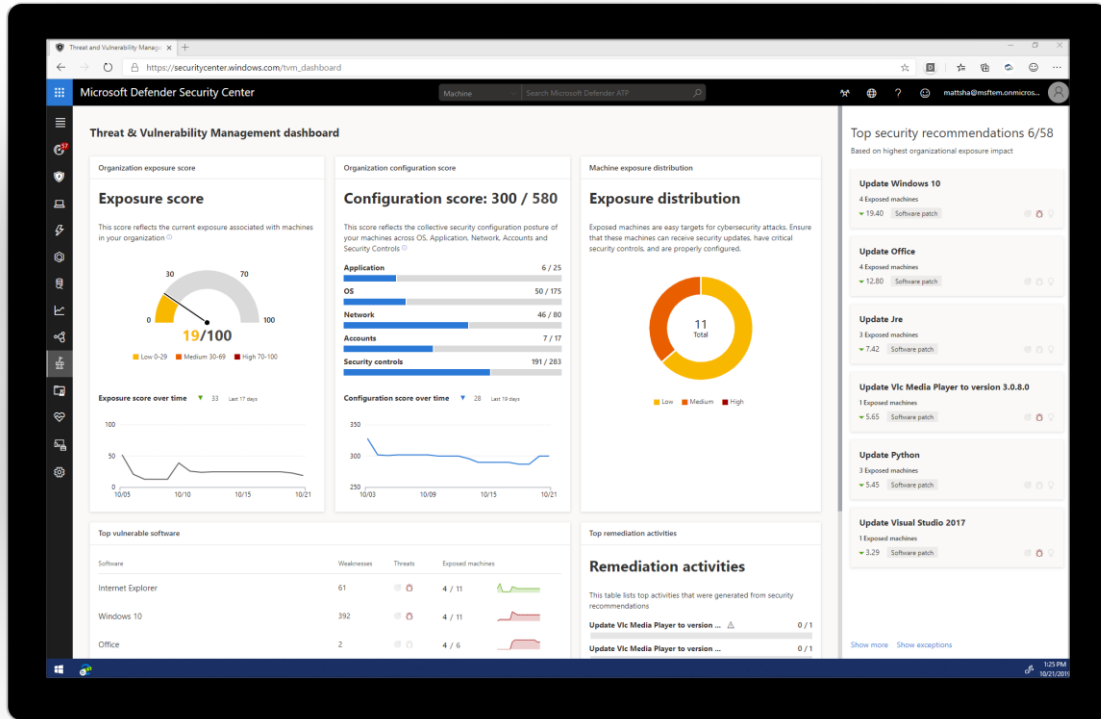
Variety of reports and dashboards for detailed monitoring and visibility



Seamless integration between policy assessment and policy enforcement



# Seamless integration



**Microsoft Defender for Endpoint**  
Policy Assessment

The screenshot displays the Microsoft Azure Device Security - Security tasks table. The table contains the following data:

Name	Priority	Status	Source	Impacted Devices	Created Date	Due Date	Assigned To
Update .net Framework	None	Pending	ATP		10/21/19, 11:56 AM	10/25/19, 6:56 PM	
Update Vlc Media Player to versi...	High	Completed	ATP		10/17/19, 1:34 PM	10/18/19, 8:32 PM	
Update Vlc Media Player to versi...	None	Pending	ATP		10/21/19, 11:54 AM	10/23/19, 6:54 PM	
Update Jre	Low	Pending	ATP		10/21/19, 11:54 AM	10/26/19, 6:54 PM	
Update Vlc Media Player to versi...	None	Pending	ATP		10/21/19, 11:55 AM	11/02/19, 6:55 PM	
Update Python	High	Pending	ATP		10/21/19, 11:55 AM	11/09/19, 6:55 PM	
Update Visual Studio 2017	Low	Pending	ATP		10/21/19, 11:56 AM	10/25/19, 6:56 PM	

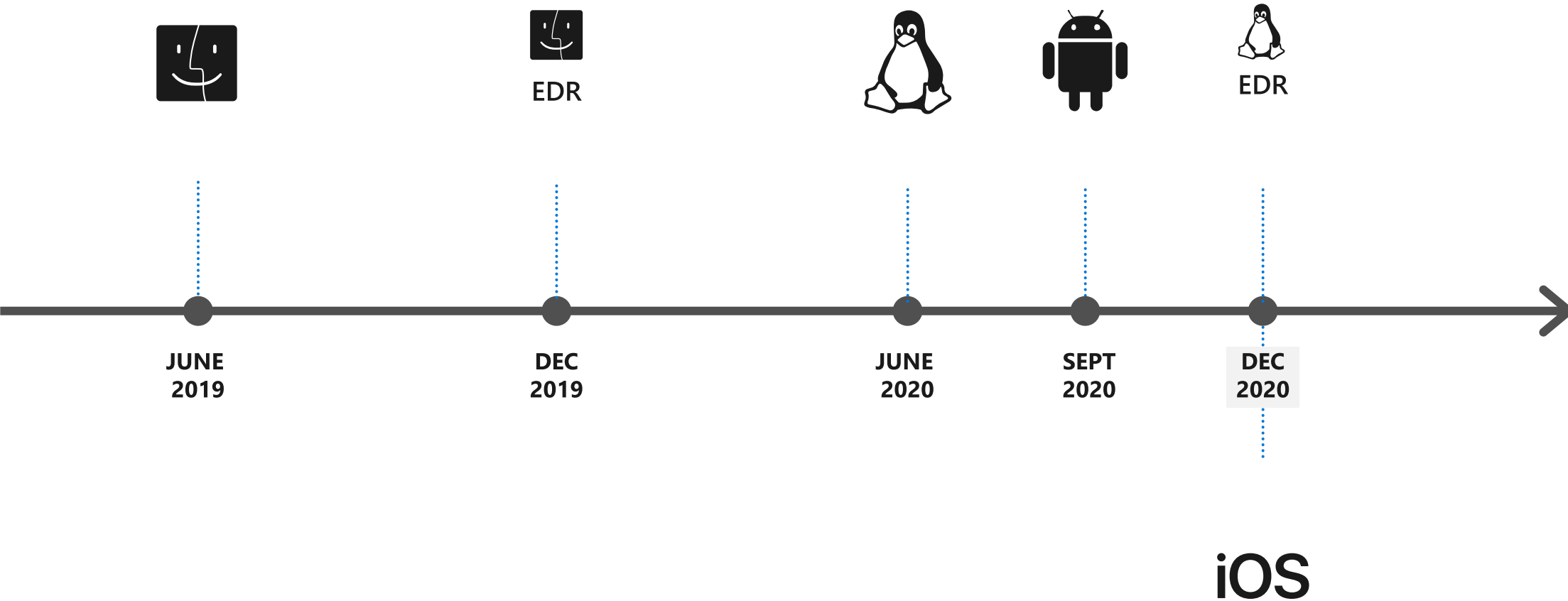
**Microsoft Endpoint Manager**  
Policy Enforcement



# Cross-platform

---

# Delivering industry leading endpoint security across platforms



# 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

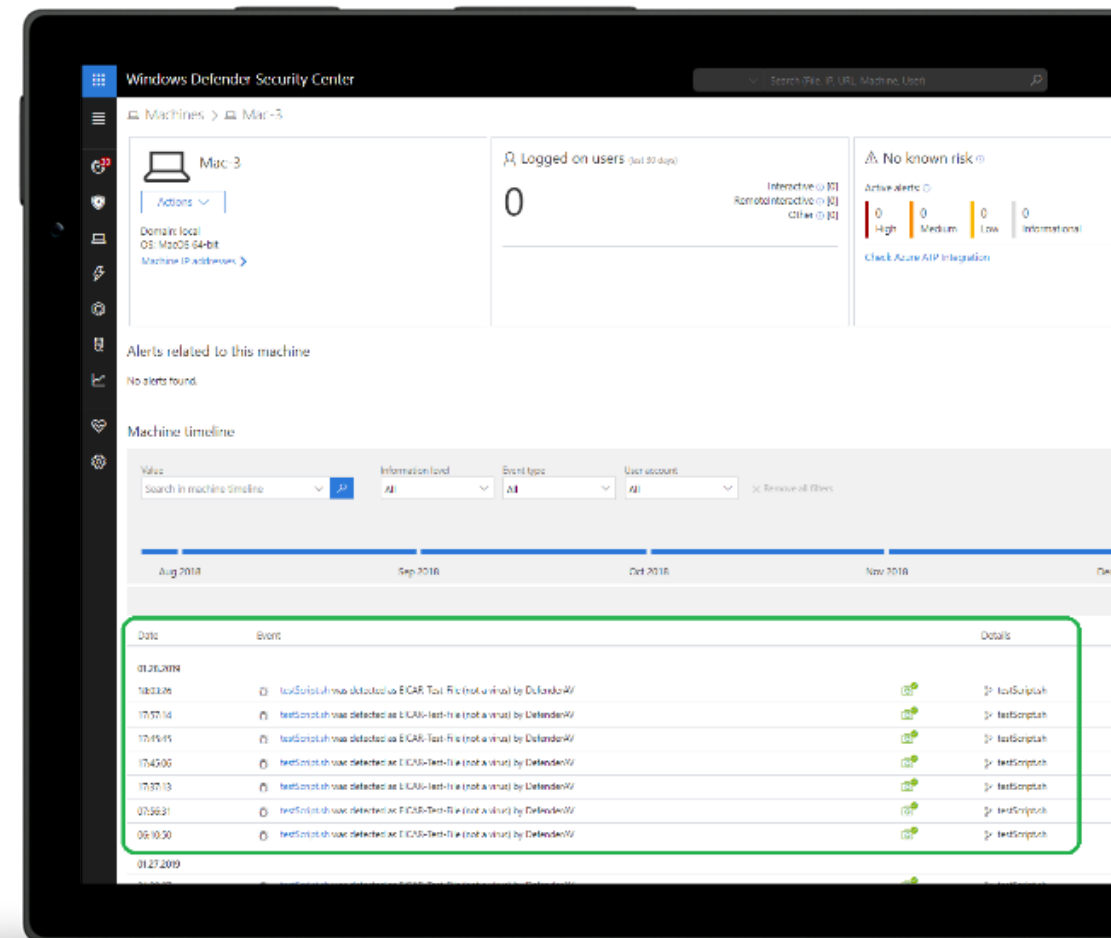
- Monitors relevant activities including files, processes, network activities
- Reports verbose data with full-scope of relationships between entities
- Provides a complete picture of what's happening on the device

### 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



# Microsoft Defender for Endpoint (Linux)

## On the client:

- AV prevention
- Full command line experience (scanning, configuring, agent health)

```
File Edit View Search Terminal Help
parallels@ubuntu:~$ mdatp
-h [ --help ]          Display help
--trace                Begins tracing Microsoft Defender's ac
--verbose              Verbose output
--retry                Retry attempts to connect
--diagnostic            Gathers log files and packages them to
                      compressed file in the support directo
--definition-update    Checks for new definition updates
--pretty               Displays the output in human-readable
--health [metric]      Display health information (Optional p
                      report just one metric)
--notice               Display third party notice
--logging              Logging options (see below)
--config [name] [value] Change configuration
--threat               Threat operations (see below)
--scan                 Scan operations (see below)
--exclusion             Exclusion operations (see below)
--connectivity-test    Run connectivity test
--edr                  EDR config (see below)

-logging options:
--set-level arg        Sets the current diagnostic logging leve
--view-logs            Outputs the contents of log files to the

-threat options:
--add-allowed arg      Adds allowed threat
--remove-allowed arg  Removes allowed threat
--get-details arg      Gets threat details
--list                 Lists all detected threa
--quarantine arg       Quarantines threat (by t
--restore arg           Restores threat (by thre
--remove arg            Removes threat (by threa
--type-handling [threat_type] [action]
                      Changes the way certain
                      threats are handled

-scan options:
--path path            Scans provided path
--quick                Performs quick scan
--full                 Performs full system scan
--cancel               Cancels current scan (either quick, full
                      one)

-exclusion options:
--list                 List exclusions
--add-file arg         File path
--add-folder arg       Folder path
--add-extension arg    File extension
--add-process arg      Process name
--remove-file arg      File path
--remove-folder arg    Folder path
--remove-extension arg File extension
```



In the Microsoft Defender Security Center, you'll see basic alerts and machine information.

EDR functionality will be gradually lit up in upcoming waves.

## 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 information:

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



# Microsoft Defender for Endpoint (Android) current offering



## Web Protection

- Anti-phishing
- Block unsafe network connections
- Custom indicators: allow/block URLs



## Malware Scan

- Alerts for malware, PUA
- Files scan
- Storage and memory peripheral scans



## Single Pane of Glass Reporting

- Alerts for phishing
- Alerts for malicious apps
- Auto-connection for reporting in Microsoft Defender Security Center



## Conditional Access

- Block risky devices
- Mark devices non-compliant



## Supported Configurations

- Device Administrator
- Android Enterprise (Work Profile)



## Licensed by Microsoft

- Included in per user licenses that offer Microsoft Defender for Endpoint
- Part of the 5 qualified devices for eligible licensed users
- Reach out to your account team or CSP

# Microsoft Defender for Endpoint (iOS) current offering



## Web Protection

- Anti-Phishing
- Block unsafe network connections
- Custom Indicators: allow/block URLs



## Single Pane of Glass Reporting

- Alerts for phishing
- Auto connection for reporting in Microsoft Defender Security Center



## Supported Configurations

- Supervised
- Unsupervised

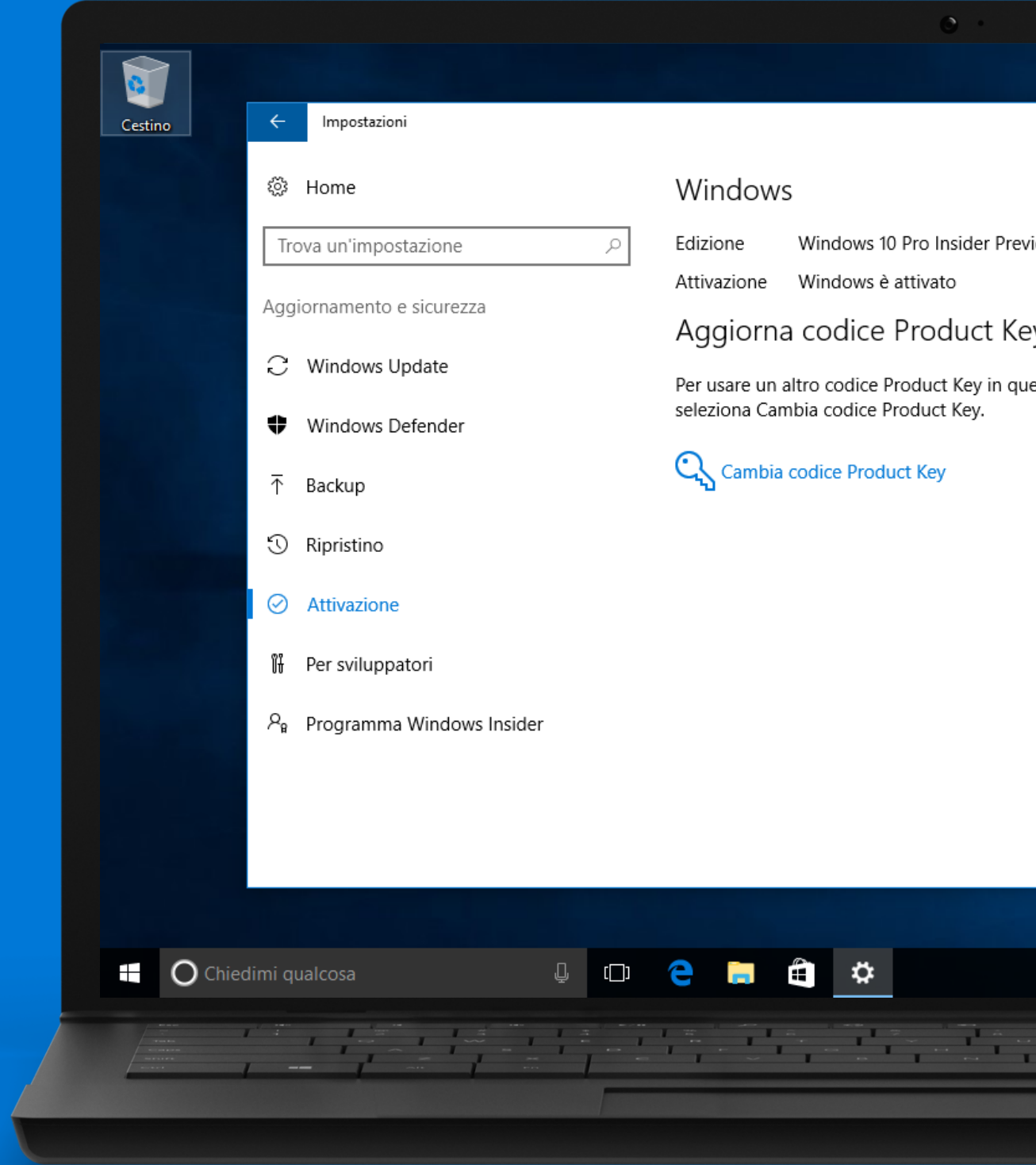


## Licensed by Microsoft

- Included in per user licenses that offer Microsoft Defender for Endpoint
- Part of the 5 qualified devices for eligible licensed users
- Reach out to your account team or CSP

# DEMO

## EVALUATION LAB



# Grazie

Roberto Tafuri

*Cloud Solution Specialist – Project Informatica*

*roberto.tafuri@project.it*

*www.robertotafuri.it*



/ictpower



@ictpower\_it