Microsoft Defender XDR

Paul Schnackenburg

30th October 2024

Image courtesy of Adobe Firefly

CYBER SECURITY PRODUCT CHALLENGES

- Point solutions
- Integration challenges
- Security Orchestration, Automation & Response SOAR
- Endpoint Detection and Response EDR
- Network Detection and Response NDR
- eXtended Detection and Response XDR
- Continuous Threat Exposure Management CTEM

DEFENDER XDR

- Defender for Endpoint
- Defender for Office
- Defender for Identity
- Defender for Cloud Apps

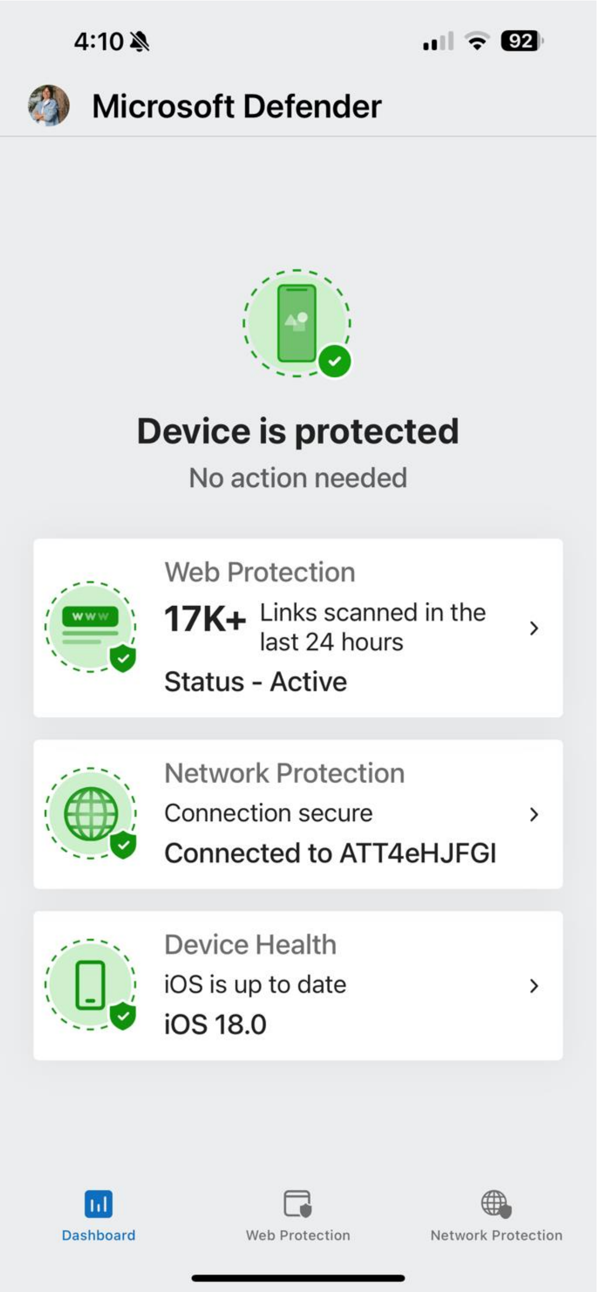
- Defender External Attack Surface Management
- Defender Threat Intelligence
- Defender for IoT / OT
- Exposure Management / Secure Score
- Sentinel
- Intune

LICENSING BASICS

- Business Premium (max 300 users)
- M365 E3
- M365 E5
- Defender for IoT add-on
- Defender for OT
- Defender Vulnerability Management add-on

DEFENDER FOR ENDPOINT

- Endpoint Detection and Response (EDR)
- A sensor is deployed to each device.
  - Sensor collects telemetry data and sends it up into the portal
  - Its goal is to watch the behavior of processes / drivers and report back
- Supported operating systems
  - Windows 7 SP1 + Server 2008 R2 and forward
  - MacOS and iOS
  - Android
  - Popular Linux distributions
  - However older OS's mostly report only



Microsoft Defender

Device is protected

No action needed

Web Protection

17K+ Links scanned in the last 24 hours

Status - Active

Network Protection

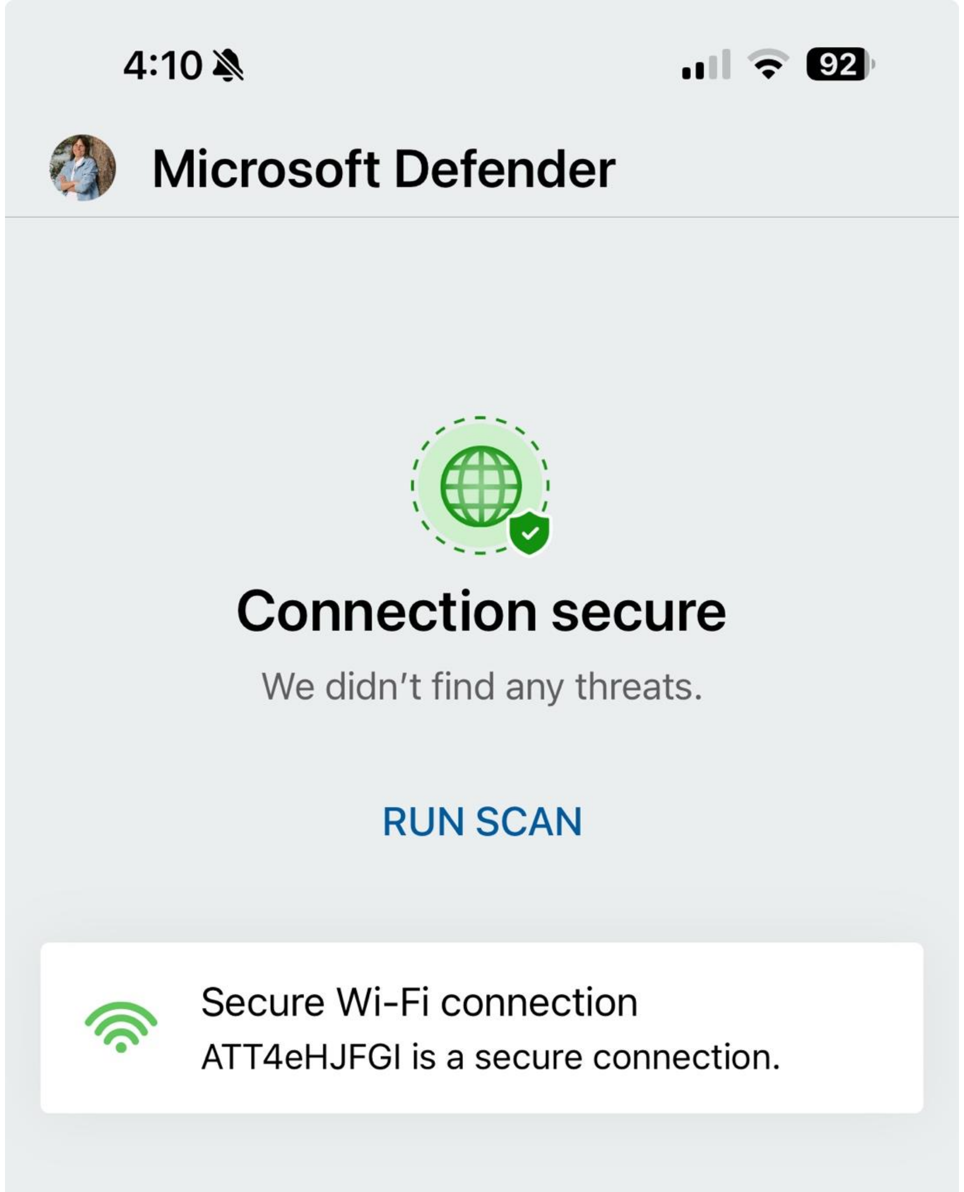
Connection secure

Connected to ATT4eHJFGI

Device Health

iOS is up to date

iOS 18.0



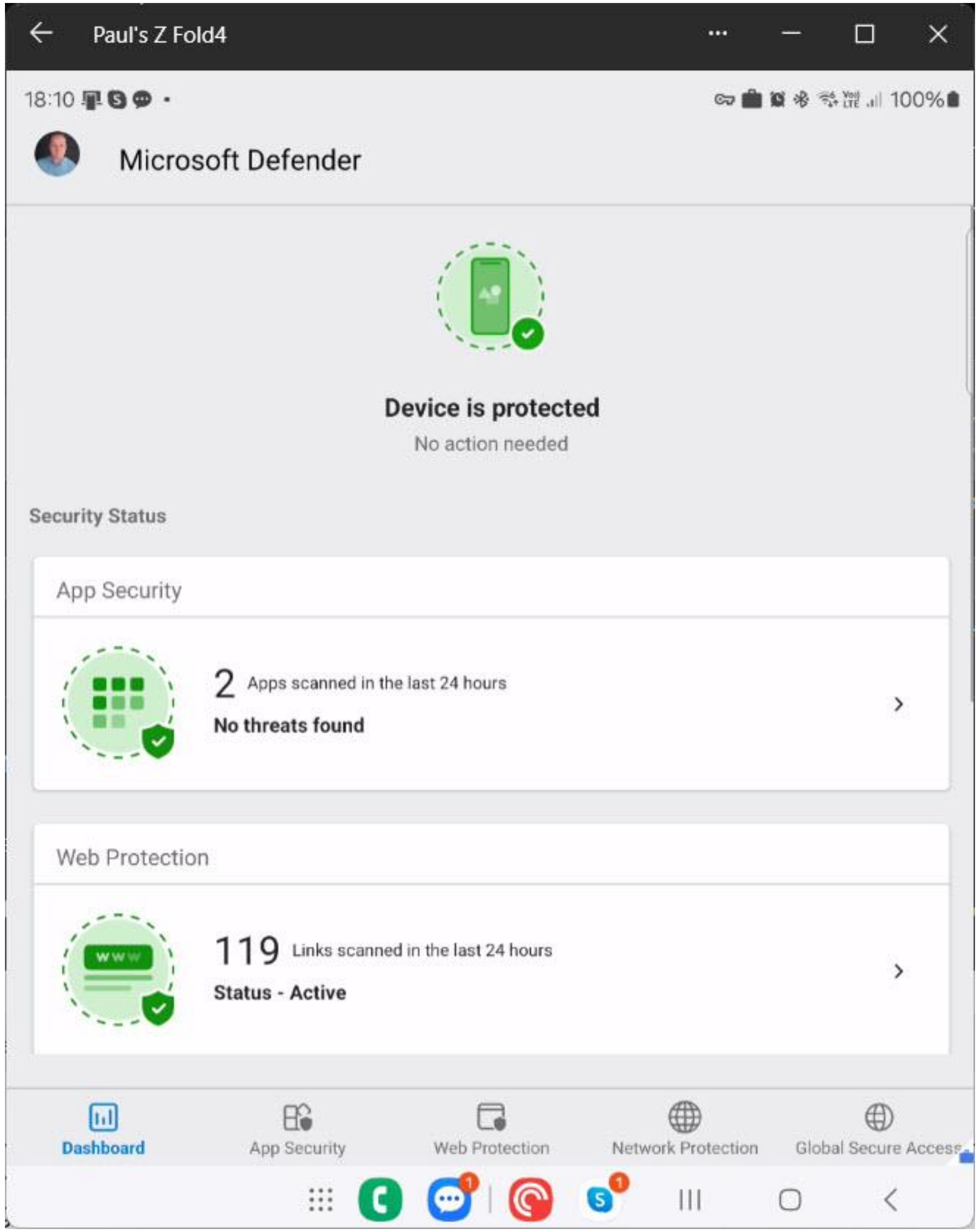
Microsoft Defender

Connection secure

We didn’t find any threats.

Secure Wi-Fi connection

ATT4eHJFGI is a secure connection.



Microsoft Defender

Device is protected

No action needed

Security Status

App Security

2 Apps scanned in the last 24 hours

No threats found

Web Protection

119 Links scanned in the last 24 hours

Status - Active

HOW IT WORKS

- Telemetry data is uploaded
- Local and cloud-based ML models
- Data is quickly reviewed for matches to known malware
- Activity is reviewed for suspiciousness
- Suspicious files and activity are run in a sandbox to further determine what they are trying to do
- Results are fed into knowledgebase, correction action takes place, results are logged in the portal

INTEGRATIONS WITH OTHER FEATURES

- Attack surface reduction rules – Intune
- Mobile Device Management – Intune
- Client Firewall – windows
- Device control – Intune

- Mac and Linux: telemetry, vulnerability management and antimalware
- iOS and Android: Tunnel, malicious app scanning, phishing link protection, reporting

DEFENDER FOR IDENTITY

- Active Directory & Federation Services & Entra ID Connect servers
- The security Graph
  - Learns from user & device accounts what normal behaviour looks like
- Honey token accounts
- Sets enforcement level based on account sensitivity
- Breaks lateral movement
- Can disable accounts automatically

ENTRA ID COMPONENTS OF P2

- Identity secure score
- Conditional Access (P1+)
- User risk
- Sign-in Risk
- MFA registration

DEFENDER FOR OFFICE 365

- Protects against business email compromise
  - Reputation
  - DNS authentication
  - Malware, spam, phishing, grey and bulk email
- Covers Office 365
  - SharePoint, OneDrive, Teams and Office 365 applications

- Additional protections
  - Impersonation protection
  - Learns each individuals common contacts
  - Phishing aggressiveness settings
  - Safe attachments and safe links
  - Sorts bulk mail
  - Scans for malware including attachments via detonation
  - Zero Hour Auto Purge (ZAP)
  - Custom transport rules
  - End user training and education campaigns

EXCHANGE ONLINE PROTECTION

- TABL for block & allow (can take up to ~~24 hours~~ 5 minutes)
- Anti-Malware policy
- Anti-Spam policy
- Anti-Phishing

DEFENDER FOR CLOUD APPS

- Cloud Security Access Broker (CASB)
- Tracks, manages, protects SaaS applications and activities within them
- Discover Shadow IT: block or allow
- Protects Third party Cloud services
  - Dropbox, Google workplace, Salesforce, Slack, etc
- Logs for investigation of app activity
  - Create policy based on activity
- Manages oAuth apps
- App activity policy
- Session policy
- Reverse proxy to integrate cloud app security into conditional access rules

PERMISSIONS OPTIONS IN DEFENDER XDR

- Basic (Security Administrator / Global Administrator / Security Reader)

  OR

- Role Based Access Control (RBAC)

- One-time choice, no option to go back to Basic
- For larger security teams to split tasks / permissions across XDR workloads / scoped for different geographies
- Device groups & tagging in MDE

ATTACK SURFACE REDUCTION (ASR) RULES

▪ ASR rules	➢ Restricts what apps and commands can do
▪ Controlled Folder Access	➢ Limits write access to most folders
▪ Exploit Protection	➢ Blocks legacy features of the OS
▪ Network protection	➢ Layer 3 protection and custom indicators blocks
▪ SmartScreen	➢ Blocks risky websites and apps
▪ Web filtering	➢ Blocks categories of websites

ASR “PROPER”

- Block credential sealing form the Windows local security authority subsystem (LSASS.exe)
- Block abuse of exploited vulnerable signed drives
- Block persistence through WMI event subscription
- ____
- Block Adobe Reader from creating child processes
- Block all Office applications from creating child processes

- Block executable content from email client and webmail
- Block executable files from running unless they meet a prevalence, age or trusted list
- Block execution of potentially obfuscate scripts
- Block JavaScript/VBScript from launching downloaded executable contents
- Block Office applications from creating executable content
- Block Office applications from injecting code into other processes
- Block Office communication application from creating child processes
- Block process creating originating from PSExec and WMI commands
- Block untrusted and unsigned processes that run from USB
- Block Win32 API calls from Office macros
- Use advanced protection against Ransomware

EXPOSURE MANAGEMENT – 1 (PUBLIC PREVIEW)

- Initiatives to strengthen protection for one risk area:
  - Business Email Compromise
  - CIS M365 Foundations benchmark
  - Cloud Security
  - Critical Asset Protection
  - Endpoint Security
  - Enterprise IoT Security
  - External Attack Surface Protection
  - Identity Security
  - Ransomware Protection
  - SaaS Security
  - Vulnerability Assessment
  - Zero Trust (foundational)

EXPOSURE MANAGEMENT - 2

- Initiatives to protect against particular threat actors
- XSPM relies on a graph database, not just lists of vulnerabilities & assets, but also how they're connected, this lets you do things like:
- Attack surface map
- Attack paths ("Device allows lateral movement to device", "Device allows lateral movement to user account" and "Device allows lateral movement to group")

SUMMARY

- Modern defense relies on integrated security solutions
- Microsoft XDR is *very* integrated
- Different Defenders for various threat vectors
- Copilot for Security (if you've won the lottery)