Defender XDR from the trenches: Your blueprint for success

→ Alessandro Ryan Foti | Architect

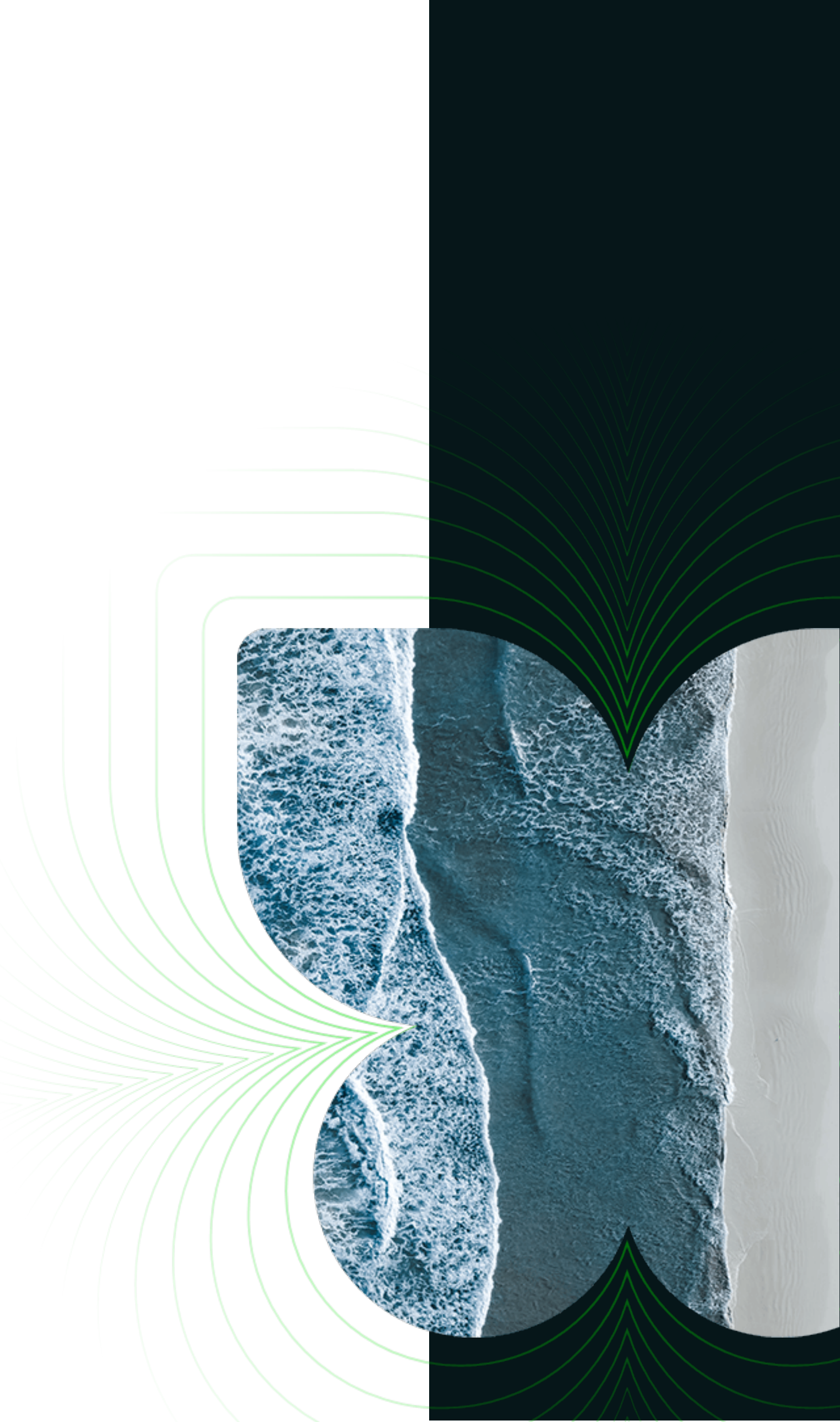
Paul Rouse | Architect

Kocho

BECOME GREATER

Agenda

- Why Microsoft Defender XDR?
- Why Kocho?
- Microsoft Defender XDR Deployment
  - Common questions
- Keys to a successful deployment
  - Microsoft Defender for Identity (MDI)
  - Microsoft Defender for Endpoint (MDE)
  - Microsoft Defender for Office 365 (MDO)
  - Microsoft Defender for Cloud Apps (MDA)
- Q&A

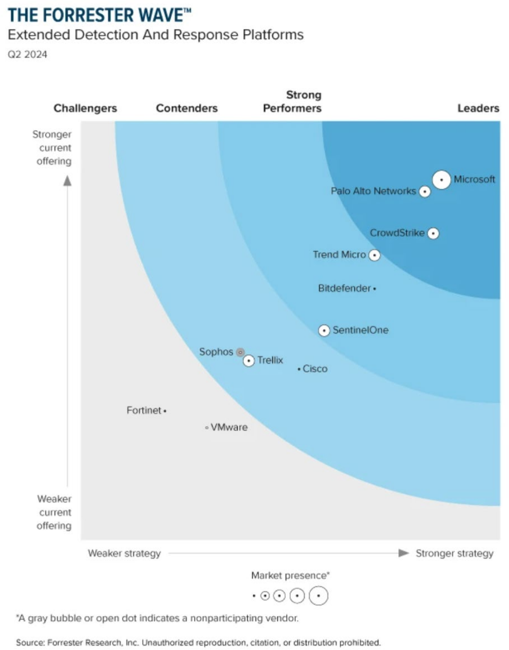


Why Defender XDR?

> *"Forrester states that "Microsoft is refining the most complete XDR offering in the market today," and called out "its dedication to innovation is demonstrated by its percentage of the R&D budget by revenue, which rivals the most innovative vendors in security."*

Microsoft is named a Leader in the 2024 Gartner® Magic Quadrant™ for Endpoint Protection Platforms ›

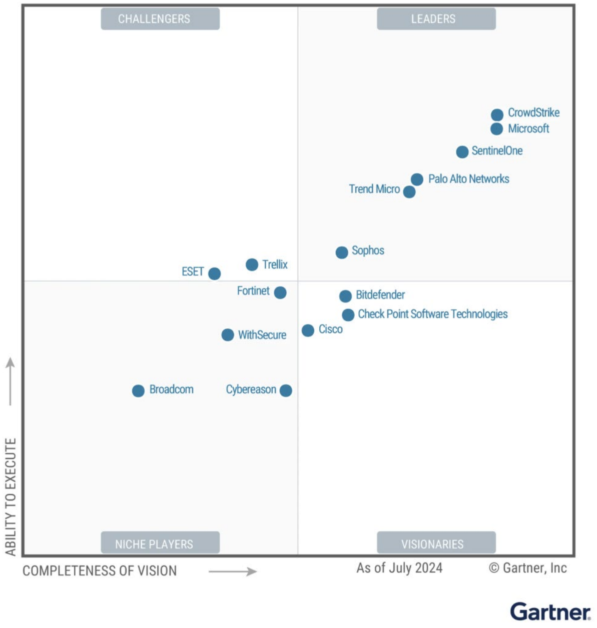
Microsoft Defender XDR demonstrates 100% detection coverage across all cyberattack stages in the 2024 MITRE ATT&CK® Evaluations: Enterprise ›

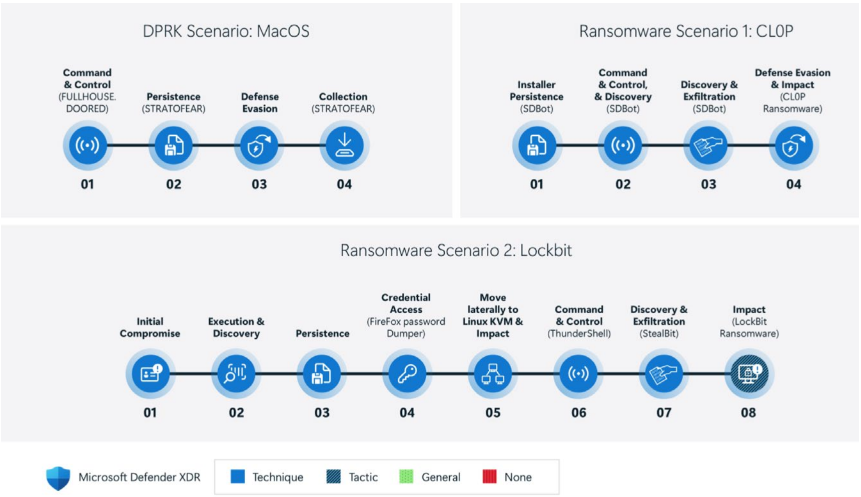

THE FORRESTER WAVE™
Extended Detection And Response Platforms
Q2 2024

*A gray bubble or open dot indicates a nonparticipating vendor.

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Figure 1: Magic Quadrant for Endpoint Protection Platforms




DPRK Scenario: MacOS
Command & Control (FULLHOUSE. DOORED)
Persistence (STRATOFEAR)
Defense Evasion
Collection (STRATOFEAR)
01
02
03
04
Ransomware Scenario 1: CL0P
Installer Persistence (SDBot)
Command & Control, & Discovery (SDBot)
Discovery & Exfiltration (SDBot)
Defense Evasion & Impact (CL0P Ransomware)
01
02
03
04
Ransomware Scenario 2: Lockbit
Initial Compromise
Execution & Discovery
Persistence
Credential Access (FireFox password Dumper)
Move laterally to Linux KVM & Impact
Command & Control (ThunderShell)
Discovery & Exfiltration (StealBit)
Impact (LockBit Ransomware)
01
02
03
04
05
06
07
08
Microsoft Defender XDR
Technique
Tactic
General
None

https://www.microsoft.com/en-us/security/blog/2024/09/25/microsoft-is-named-a-leader-in-the-2024-gartner-magic-quadrant-for-endpoint-protection-platforms/

https://www.microsoft.com/en-us/security/blog/2024/06/03/microsoft-is-named-a-leader-in-the-forrester-wave-for-xdr/

https://www.microsoft.com/en-us/security/blog/2024/12/11/microsoft-defender-xdr-demonstrates-100-detection-coverage-across-all-cyberattack-stages-in-the-2024-mitre-attck-evaluations-enterprise/

Why Defender XDR?

Deploying, managing, integrating and correlating logs and alerts across point security solution from multiple vendors

Using Microsoft Defender XDR

All your Eggs in One Basket

For the first time in history there is a reason to put all our eggs in one basket.

Honestly, its that or trying to carry 16 BASKETS with one egg in each and not drop any!

Because eggs come in cartons for a reason...

Why Kocho?

- → Secure Digital Transformation Practice staffed with highly qualified consultants and architects with decades of experience between them. Everyone shares a passion for delivering innovative, high-quality solutions to make the bad guys lives as difficult as possible
- → Deployments of Defender XDR across multiple organisations of all scales and across sectors
- → Hundreds of thousands of Users, Mailboxes, Endpoints and Servers protected
- → Close working relationship with Microsoft
  - → Microsoft Intelligent Security Association (MISA) member
  - → Regular meetings with Microsoft Product Group teams to feedback on product performance, future enhancements and roadmap features
  - → Early access to features (Design stage/Pre Private preview)

Questions for our audience

→ Who has deployed all of Defender XDR in their environment?

→ Who here has deployed any element of Defender XDR in their environment?

→ Who in here believes that they're fully utilising what they are licensed for?

→ Who is planning to deploy elements of Defender XDR in their environment?

Microsoft Defender XDR Deployment

Common Questions

Common Questions

→ Which component should I deploy first / What order should I deploy in?

→ I have an existing AV solution with X months left on the contract– what value can MDE add now?

→ How long does it take to deploy MDx?

→ What's included in my licence?

Microsoft Defender for Identity (MDI)

Keys to a successful deployment

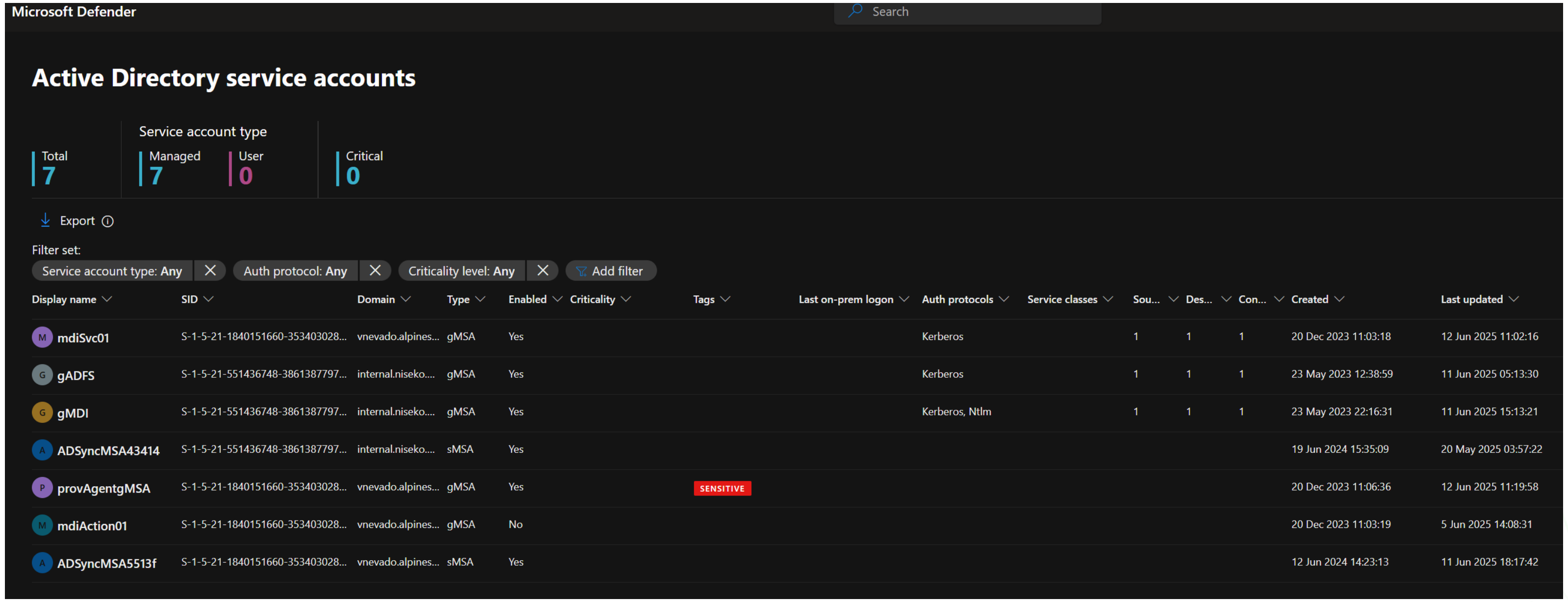
- → Sizing & Pre Reqs
- → Supported OS versions
  - → Server 2016 or newer
- → Ensure you plan to include AD FS, Entra Connect, AD CS in your coverage
- → Environment configuration (Use the fantastic PowerShell Module!)
  - → Auditing policies
  - → GMSA Account (KDS root key required)

Keys to a successful deployment

- Network Configuration
  - Sensor requires access to *.atp.azure.com on port 443
  - Required traffic can use direct internet, proxy or ExpressRoute
- Leverage Security Posture Recommendations
  - Dormant entities in sensitive groups assessment
  - Entities exposing credentials in clear text assessment
  - Security assessment: Weak cipher usage
  - Domain controllers with the print spooler service available
  - Reversible passwords found in GPOs
- Operational Considerations

Useful new stuff to be aware of

- → Service Account Discovery & Inventory



Active Directory service accounts

Service account type

Total 7 | Managed 7 | User 0 | Critical 0

Export

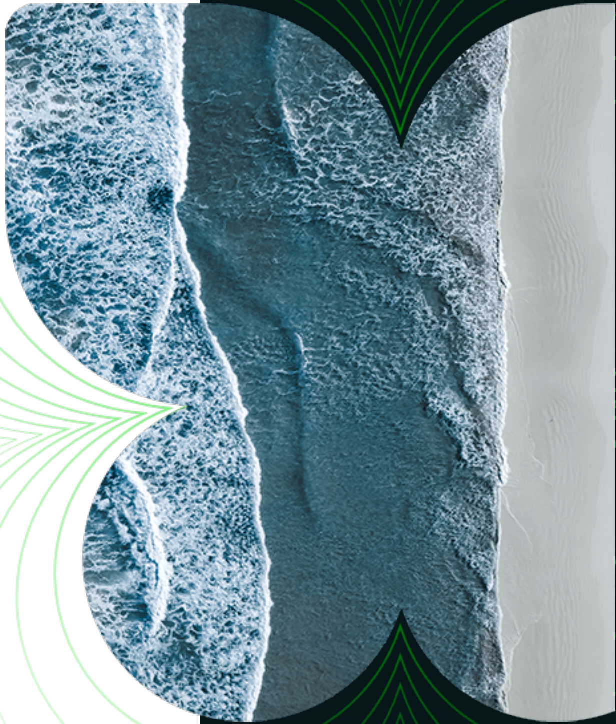
Filter set:

Service account type: Any | Auth protocol: Any | Criticality level: Any | Add filter

Display name	SID	Domain	Type	Enabled	Criticality	Tags	Last on-prem logon	Auth protocols	Service classes	Sou...	Des...	Con...	Created	Last updated
mdiSvc01	S-1-5-21-1840151660-353403028...	vnevado.alpines...	gMSA	Yes				Kerberos		1	1	1	20 Dec 2023 11:03:18	12 Jun 2025 11:02:16
gADFS	S-1-5-21-551436748-3861387797...	internal.niseko....	gMSA	Yes				Kerberos		1	1	1	23 May 2023 12:38:59	11 Jun 2025 05:13:30
gMDI	S-1-5-21-551436748-3861387797...	internal.niseko....	gMSA	Yes				Kerberos, Ntlm		1	1	1	23 May 2023 22:16:31	11 Jun 2025 15:13:21
ADSyncMSA43414	S-1-5-21-551436748-3861387797...	internal.niseko....	sMSA	Yes									19 Jun 2024 15:35:09	20 May 2025 03:57:22
provAgentgMSA	S-1-5-21-1840151660-353403028...	vnevado.alpines...	gMSA	Yes		SENSITIVE							20 Dec 2023 11:06:36	12 Jun 2025 11:19:58
mdiAction01	S-1-5-21-1840151660-353403028...	vnevado.alpines...	gMSA	No									20 Dec 2023 11:03:19	5 Jun 2025 14:08:31
ADSyncMSA5513f	S-1-5-21-1840151660-353403028...	vnevado.alpines...	sMSA	Yes									12 Jun 2024 14:23:13	11 Jun 2025 18:17:42

- → New sensor version (V3)
  - → Simplified onboarding (2019+ only)
  - → Less environmental pre reqs (GMSA account etc)

- → Scoped Access (Preview)



Microsoft Defender for Endpoint (MDE)

Keys to a successful deployment – General

Planning, planning, and more planning!

- → Both technical and operational planning are key to success
  - → Have you done your network and OS pre-requisites?
  - → Are you covering just Endpoints, or Endpoints/Servers/Mobile?
  - → Have you decided what onboarding and managing method will you use (SCCM, GPO, Intune, Security Settings Management, Ansible, etc)?
  - → Solid policy design and testing required (AV settings/Scan settings/Exclusions/Firewall)
  - → Who is the owner of the new tech?
  - → Account for ASR Technical times!

- → RBAC for Defender for Endpoint/XDR
  - → Who needs access to what?

Keys to a successful deployment – Existing AV

Existing AV

- Passive/EDR Block mode required?
- How simple is the removal process for the existing AV product?
- Are there additional settings to migrate from the existing solution (Indicators/Exclusions etc)
- Does the existing AV provide a software firewall?
  - Do we need to replace with Defender firewall and migrate rules?
  - How to deploy and manage Defender firewall?
- Exclusions
  - What applications require exclusions – are these documented?
  - Do exclusions currently exist in incumbent AV?
  - Are the reasons for the existing exclusions documented?
- Has Windows Defender AV been prevented from working (either by existing AV or GPO etc)?
- Any potential conflicting GPOs in place?

Useful new stuff to be aware of

- → Effective Settings
- → **New Attack Surface Reduction (ASR) Rules:** 2x new ASR rules are now GA:
  - → Block rebooting machine in Safe Mode.
  - → Block use of copied or impersonated system tools.
- → Support for ARM64-based Linux Servers and WSL2

Microsoft Defender for Office 365 (MDO)

Keys to a successful deployment

- → Leverage ARC Sealers and Enhanced Filtering capabilities to ease initial coexistence
- → Evaluation/PoC/Pilot (without changing your MX record)
- → Ensure users are well informed of any forthcoming changes and new behaviours they need to learn
  - → Reporting phishing attempts
  - → Accessing quarantined email/Quarantine notifications
  - → Review Junk Mail folder contents
  - → Ability to report malicious Teams messages
- → Review existing allow / block lists in your existing solution prior to migration
  - → Agree the approach with senior stakeholders

Microsoft Defender for Cloud Apps (MDA)

Keys to an effective implementation

- → **Cloud Discovery:**What are you looking to achieve with what you’ve just discovered?
  - → **Score Metrics:** App scoring is only valuable if tailored to your company and company’s priorities.
  - → **Plan for Shadow IT:** Post-discovery Governance
- → **Shadow GenAI:** Are you governing your users access to GenAI tools online?
- → **Enable App Governance**(OAuth Review): When was the last time you’ve reviewed your OAuth apps access and permissions?
- → **Connect 3rd party SaaS Apps:** Are you using Dropbox/Salesforce

Useful new stuff to be aware of

- App Governance – is a largely underused feature. It offers substantial insights and oversight regarding critical exploit vectors through, for example, policies to programmatically and automatically remove access to apps based on user defined criteria.

- Shadow GenAI – regulates access to GenAI tools for your user base.

We can help

- → Discovery / Vision Call
- → Defender XDR Workshops
- → Funded Threat Protection & SIEM workshops/trials
- → XDR Consultancy – migrations, configuration reviews
- → Security Posture Assessments
- → Anything Microsoft Security related

hello@kocho.co.uk 0800 044 5009