AYI NEDJIMI Consultants

Microsoft Defender : Suite XDR Microsoft 365

10 mai 2026 • Mis à jour le 17 mai 2026 • 23 min de lecture • 4864 mots •

Microsoft Defender est la suite XDR de Microsoft regroupant Defender for Identity, for Office 365, for Cloud, for Servers, for IoT et for DevOps, unifié Microsoft Defender XDR (anciennement Microsoft 365 Defender). Cette pa détaille les composants, les capacités EDR (NGAV, ASR, Tamper Protection Control), le hunting KQL unifié, l'intégration Sentinel, les plans de licensing A5, Business Premium) et les comparatifs concurrentiels avec CrowdStrike SentinelOne, ESET et Bitdefender pour les PME, ETI et grands comptes en

Microsoft Defender est la suite XDR (Extended Detection and Response) de Micros unifiée de cybersécurité qui regroupe sous une marque commune les protections endpoints, les identités Active Directory et Entra ID, les charges multi-cloud (Azur boîtes Microsoft 365, les serveurs, l'IoT/OT et les pipelines DevOps. Anciennemen noms *Windows Defender Antivirus* (composant intégré à Windows depuis Vista), *M Advanced Threat Analytics (ATA)* pour l'on-premise, *Threat Prote ATP)* et *Office 365 Advanced Threat Protection (Offi* emble a été

renommé entre 2020 et 2024 pour converger vers la bannière unique **Microsoft D** (anciennement Microsoft 365 Defender). En 2026, Defender équipe par défaut plu de machines Windows et figure régulièrement en haut du quadrant Gartner Magic Endpoint Protection Platforms aux côtés de CrowdStrike Falcon et SentinelOne. Ce first détaille l'ensemble des composants de la suite, leurs capacités techniques, le licensing (P1, P2, E5, A5, Microsoft 365 Business Premium), les comparatifs concu (CrowdStrike, SentinelOne, ESET, Bitdefender) et les limites pratiques pour les PM grands comptes français qui hésitent à standardiser sur l'écosystème Microsoft.

À RETENIR

L'essentiel à retenir

Suite XDR unifiée : Defender for Endpoint, for Identity, for Cloud, for Office Servers, for IoT, for DevOps regroupés sous Microsoft Defender XDR (porta security.microsoft.com).

Capacités EDR : NGAV (Microsoft Defender Antivirus), EDR cloud, Attack S Reduction (ASR), Tamper Protection, Smart App Control, isolation automati

Hunting unifié : Advanced Hunting via KQL (Kusto Query Language) sur l'e tables (DeviceEvents, IdentityLogonEvents, EmailEvents, CloudAppEvents)

Plans : Defender for Endpoint P1 (NGAV+ASR), P2 (EDR+Threat & Vuln Mgr dans Microsoft 365 E5 / E5 Security / A5 / Business Premium (P1 only).

Multi-cloud : Defender for Cloud couvre AWS, Azure, GCP avec CSPM, CW plus de 1 200 contrôles benchmarks.

Limites PME : licensing E5 onéreux (~57 €/utilisateur/mois), E3 sans EDR, E Premium plafonné à 300 sièges, P1 sans EDR

Réponse sous 24h

Devis gratuit →