

# Microsoft Defender AV mit Acronis EDR



## Microsoft Defender: Den heutigen Bedrohungen nicht gewachsen und für einen umfassenden Schutz zu teuer.

MSPs, die ausschließlich auf Microsoft Defender AV vertrauen, sehen sich mit kritischen Sicherheitslücken konfrontiert. Dazu zählen eine eingeschränkte Transparenz, die fehlende Möglichkeit einer mandantenfähigen Verwaltung und das Fehlen automatisierter Reaktionsfähigkeiten. Die integrierten Funktionen von Defender reichen nicht aus, um komplexe Bedrohungen wie Ransomware und Zero-Day-Angriffe abzuwehren. Die erweiterten Sicherheitsoptionen von Microsoft sind für KMUs jedoch unerschwinglich. Service Provider benötigen daher eine kosteneffiziente Möglichkeit, um den Schutz vor Bedrohungen zu verbessern und ihre Sicherheitsdienste zu skalieren, ohne dabei bestehende Defender-Bereitstellungen aufgeben zu müssen.

## Erweitern Sie Microsoft Defender um eine speziell für MSPs entwickelte Lösung: Acronis EDR

Acronis EDR erweitert Microsoft Defender nahtlos um fortschrittliche, KI-gestützte Erkennungs- und Reaktionsfunktionen, ohne dass eine Migration notwendig ist oder die Komplexität zunimmt. Die speziell für MSPs entwickelte Lösung bietet zentralisierte, mandantenfähige Transparenz sowie automatisierte Reaktions- und Wiederherstellungsmaßnahmen, die alle NIST-Kategorien abdecken. Damit sind MSPs nun in der Lage, ihre Schutzdienstleistungen zu skalieren und ihre Gewinne zu steigern, ohne Defender ersetzen zu müssen.

### Vorteile für Ihr MSP-Geschäft

- Verbessert den Schutz Ihrer Kund:innen und reduziert Risiken durch aktuelle Bedrohungen.
- Entwickeln Sie profitable MDR-Services, ohne dabei auf Microsoft Defender verzichten zu müssen.
- Sie erhalten einen zentralen Überblick über alle Mandanten, Assets und Bedrohungen.
- Automatisieren Sie Reaktionsmaßnahmen: Quarantäne, Rollback, Wiederherstellung und Patching.
- Erfüllen Sie die Anforderungen des Microsoft Partnerprogramms ohne explodierende Kosten.
- Lagern Sie bei Bedarf das Sicherheitsmanagement an Acronis MDR aus.
- Bieten Sie KMUs Sicherheit auf Enterprise-Niveau, aber ohne die Komplexität einer solchen Lösung.



### KI-gestütztes EDR, speziell für Service Provider entwickelt

Nutzen Sie zusätzlich zu Microsoft Defender die KI-gestützten Erkennungs- und Reaktionsfunktionen von Acronis EDR mit zentraler, mandantenfähiger Transparenz. Ein vollständiger Austausch von Defender ist nicht erforderlich.



### Sicherheit in Unternehmensqualität zu KMU-freundlichen Kosten

Bieten Sie Ihren Kund:innen einen fortschrittlichen Schutz mit Wiederherstellungs- und Abwehrmöglichkeiten zu einem Bruchteil der Kosten, die Ihnen die Bereitstellung einer Microsoft-basierten MDR-Lösung oder anderer Enterprise-EDR-Lösungen verursachen würde.



### Gegenmaßnahmen (inkl. Wiederherstellungsfähigkeiten) gemäß NIST-Framework

Von der Identifizierung und Absicherung von Assets bis zur Erkennung und Abwehr von Angriffen (einschließlich Rollbacks und Wiederherstellungen) – Sie können die Geschäftskontinuität Ihrer Kund:innen bei jedem Angriffsszenario gewährleisten.

## Wichtige Anwendungsfälle

### Acronis EDR schließt kritische Sicherheitslücken, die Microsoft Defender offenlässt

#### Schutz vor Ransomware

Erkennen und blockieren Sie Ransomware – selbst Varianten, die herkömmliche Antivirus-Software umgehen – und stellen Sie Daten automatisch wieder her.

#### Schutz vor Zero-Day-Angriffen

Identifizieren Sie verdächtiges Verhalten und stoppen Sie Zero-Day-Exploits mithilfe von verhaltens- und KI-basierter Erkennung – nicht mit Signaturen.

#### Advanced Persistent Threats (APTs)

Erkennen Sie verdeckte Eindringversuche und laterale Bewegungen auf Endpoints mithilfe von kontextreicher Threat Intelligence.

#### Geschäftskontinuität und Datenwiederherstellung

Stellen Sie betroffene Dateien und Vorgänge mithilfe der integrierten Wiederherstellungsfunktion sofort wieder her,

um Ausfallzeiten zu minimieren.

#### Erkennung von dateilosen Angriffen

Überwachen Sie PowerShell-, WMI- und arbeitsspeicherbasierte Aktivitäten, um auch Bedrohungen zu erkennen, die keine nachverfolgbaren Dateien hinterlassen.

#### Mandantenfähiges Management

Verwalten Sie alle Kundenumgebungen über eine zentrale Übersicht, die Ihnen vollständige Transparenz und Kontrolle bietet.

#### Zentrale Übersicht

Aggregieren Sie Bedrohungstelemetrie, Response-Insights und Compliance-Daten über Clients und Workloads hinweg.

## Preisgekrönter Endpunktsschutz



AV-TEST: Top-Produkt für den Endpunktsschutz in Unternehmen



SE Labs: Bestnote für Enterprise Advanced Security



IDC MarketScape: Weltweiter Cyber-Recovery Leader



Frost & Sullivan Frost Radar™: Endpoint Security Leader



G2 Grid: Top-Platzierung bei Endpoint Protection Suites

#### Statten Sie Microsoft Defender mit Resilienz und Reaktionsfähigkeiten aus!

Sind Sie bereit, einen umfassenden Schutz auf Basis von Microsoft Defender freizuschalten? Erfahren Sie, wie Acronis EDR MSPs dabei unterstützt, skalierbare und profitable Sicherheitsdienste mit integrierter Resilienz anzubieten.

[MEHR ERFAHREN](#)

[DEMO VEREINBAREN](#)