Microsoft Defender AV with **Acronis** EDR

Microsoft Defender: Outmatched by today's threats. Overpriced to solve.

MSPs relying solely on Microsoft Defender AV face critical protection gaps — limited visibility, no multitenant management and lack of automated response. Defender's built-in capabilities fall short against advanced threats like ransomware and zero days. Yet, Microsoft's advanced security options are prohibitively expensive for SMBs. Service providers need a cost-efficient way to elevate threat protection and scale their security services — without ditching existing Defender deployments.

Augment Microsoft Defender with Acronis EDR, built for MSPs

Acronis EDR seamlessly layers advanced, AI-guided detection and response onto Microsoft Defender — no migration, no added complexity. Designed for MSPs, it delivers centralized, multitenant visibility, automated response and recovery capabilities that align with the full NIST Framework. Now, MSPs can scale protection and profitability — without replacing Defender.

Benefits for your MSP business

- Enhance clients' protection and reduce risks from nowadays threats.
- Build profitable MDR services without abandoning Microsoft Defender.
- Gain centralized visibility across tenants, assets and threats.
- Automate response actions: isolation, rollback, recovery and patching.
- Meet Microsoft Partner Program requirements without through-the-roof costs.
- Outsource security management via Acronis MDR if needed.
- Deliver enterprise-grade security to SMB clients—without enterprise complexity.

AI-guided EDR, built for service providers

Leverage AI-powered detection and response with centralized, multitenant visibility on top of Microsoft Defender — no "rip and replace."

Enterprise-grade security at SMB-friendly costs

Deliver advanced protection, recovery and response at a fraction of the cost that it will take you to deliver MDR with Microsoft or enterprise-grade EDRs.

Recovery-ready response across the NIST framework

From identifying and protecting assets to advanced detection, response and even rollback and recovery — ensure continuity in any attack scenario.

Top use cases

Address critical gaps Microsoft Defender leaves behind

Ransomware protection

Detect, block and auto-recover from ransomware — even variants that bypass traditional antivirus tools.

Zero-day attack defense

Identify suspicious behavior and stop zero-day exploits with behavioral and AI-based detection — not signatures.

Advanced persistent threats (APTs)

Spot stealthy intrusions and lateral movement across endpoints using context-rich threat intelligence.

Business continuity and recovery

Roll back affected files and restore operations instantly — integrated recovery minimizes downtime.

Fileless attack detection

Monitor PowerShell, WMI and memory-based activity to detect threats that leave no traceable files.

Multitenant management

Manage all client environments from a single pane of glass with full visibility and control.

Centralized visibility

Aggregate threat telemetry, response insights and compliance data across clients and workloads.

Award-winning endpoint protection

- AV-TEST Top Product for Corporate Endpoint Protection
- SE Labs AAA rating for Enterprise Advanced Security
- IDC MarketScape: Worldwide Cyber-Recovery Leader
- Frost Radar™: Endpoint Security Leader
- G2 Grid Leader for Endpoint Protection Suites

Layer resilience and response on top of Microsoft Defender

Ready to unlock full-spectrum protection with Microsoft Defender? Discover how Acronis EDR helps MSPs deliver scalable, profitable security with built-in resilience.

LEARN MORE

GET A DEMO

Acronis

Learn more at www.acronis.com