Microsoft Security solution feature guide

Microsoft Defender for Endpoint

Take full advantage of your investment and rapidly stop attacks. Advance beyond endpoint silos and mature your security based on a foundation of extended detection and response (XDR) and Zero Trust.

What are the necessary actions to elevate your security posture with Defender for Endpoint?

Discover how to protect your endpoints and organizational data while efficiently scaling your security resources with the features highlighted on the next page.

Note: Before enabling these features, we recommend you inventory your devices within the organization. Utilize Microsoft Defender Vulnerability Management and Microsoft Defender for Endpoint to support this effort.

Microsoft Security

Defining manual response actions ›

Manual response actions are actions that your security team can take when threats are detected on endpoints or in files that have been compromised.

Explore automated investigations ›

Utilize inspection algorithms to examine alerts and take immediate action to resolve breaches.

Enable endpoint reporting and policy settings ›

Prioritize alerts effectively, gain visibility into the full scope of a breach, and respond to remediate threats by integrating Defender for Endpoint with Intune.

Engage in advanced threat hunting ›

Proactively inspect events in your network to locate threat indicators and entities with flexible access to data, enabling unconstrained hunting for known and potential threats.

Understand active vs. passive mode for antivirus ›

Depending on your operating systems and integration of Microsoft Defender for Endpoint with antivirus protection, there are various considerations for how to protect against threats.

» For a self-guided experience to learn more about how to enable these features, please **visit our learning collection**.

Microsoft Security