

Forum:[Hack Forums](#)

Thread: [Microsoft Defender can now automatically isolate hacked endpoints](#)

MadScientist - May 26, 2026, 11:53 am

Microsoft is testing a new Defender for Endpoint capability that will automatically isolate compromised endpoints to thwart attackers' attempts to move laterally across the network.

This is now available in preview mode and works as part of automatic attack disruption, a feature designed to contain attacks, limit their impact, and provide security teams with more remediation time.

Compromised endpoints that are automatically isolated are disconnected from the network to reduce the risk of further impact, but they retain connectivity to the Microsoft Defender for Endpoint service, which will continue to monitor the device.

"When a device in your organization is suspected to be compromised, Microsoft Defender for Endpoint can automatically isolate the device as part of automatic attack disruption," Microsoft said.

"Automatic isolation helps reduce the risk of further impact on the organization, limit attacker lateral movement, and prevent impacts such as data exfiltration and ransomware propagation."

Automatic device isolation works only on onboarded end-user workstations managed by Microsoft Defender for Endpoint.

As Microsoft explained, they can also be released from containment at any time by security operators after completing the incident investigation and mitigating the risks.

Read More -

<https://www.bleepingcomputer.com/news/microsoft/microsoft-defender-can-now-automatically-isolate-hacked-endpoints/>