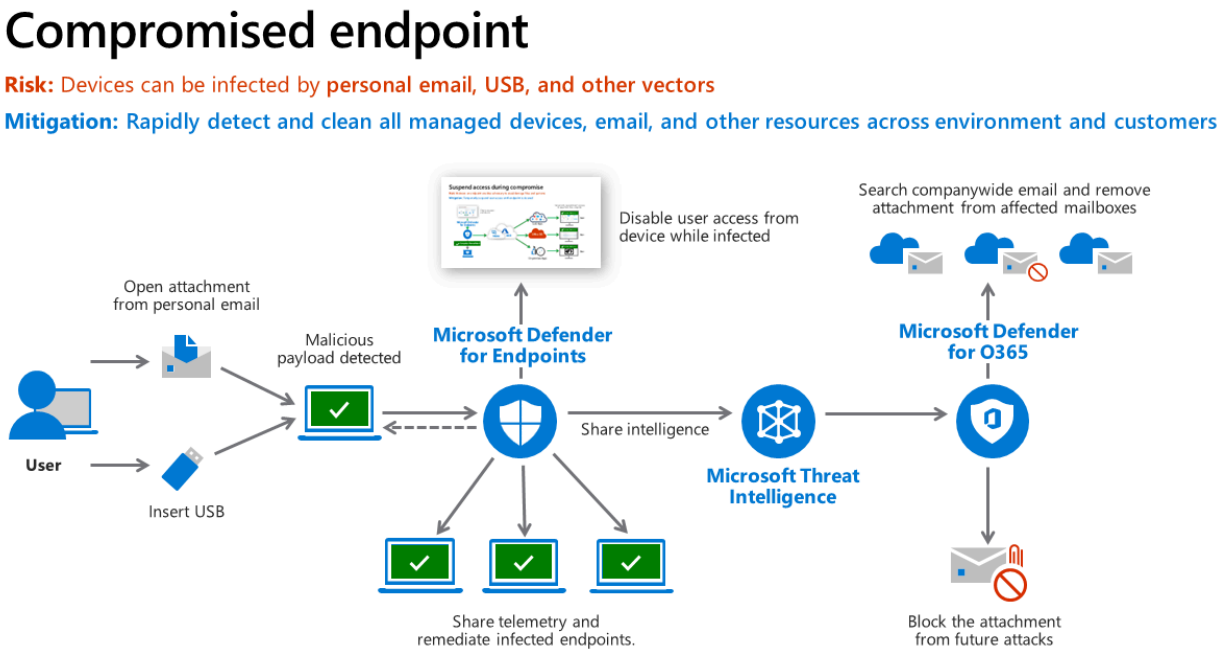
Extended Detection & Response (XDR) response use cases

By: Ryan Stewart



- *This scenario depicts a case where Microsoft Defender for Endpoint detects a malicious payload (which could come from any source, including **personal email** or a **USB drive**).*

The victim becomes a target when they receive a malicious email on a personal account, **which is outside the protection of Microsoft Defender for Office 365 (MDO)** or through a USB drive. Upon opening the attachment, the computer becomes infected with malware, all without the user's awareness. However, Microsoft Defender for Endpoints (MDE) promptly detects the attack, raising an alert to the security operations team and providing detailed threat information.

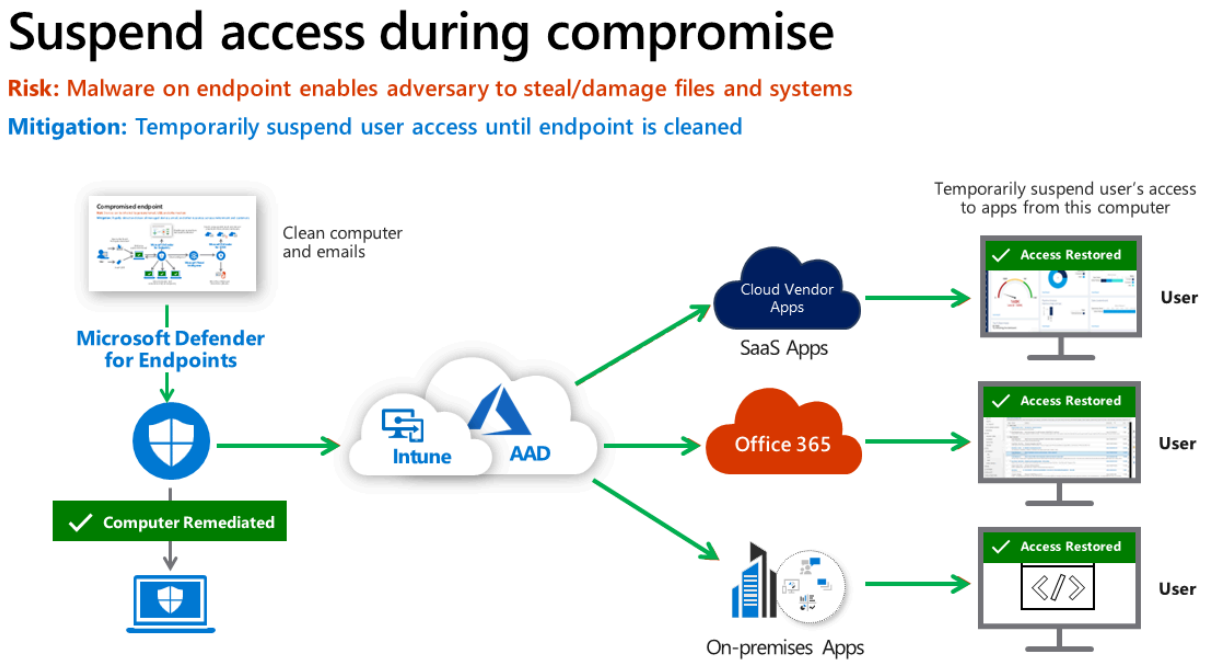
I**s MDE a SIEM?** No, Microsoft Defender for Endpoints (MDE) is not a SIEM (Security Information and Event Management) solution. MDE is an endpoint security platform, whereas a

SIEM is designed for centralized collection and analysis of security event data across the entire IT infrastructure.

To contain the risk, MDE communicates with Intune, prompting the **enforcement of a compliance policy**. An Intune Compliance Policy, configured with an MDE risk level severity, marks the affected account as noncompliant with organizational policies. A Conditional Access policy in Microsoft Entra ID subsequently blocks user access to apps.

For remediation, **MDE** takes **action**, **employing automated remediation**, security analyst approval of automated remediation, or manual investigation by analysts. Additionally, MDE addresses the threat enterprise-wide and across Microsoft Defender for Endpoints customers by integrating information about the attack into the Microsoft Threat Intelligence system.

In the process of sharing intelligence and restoring access, once the infected devices are successfully remediated, MDE signals Intune to update the device risk status. The **Conditional Access policy** in Microsoft Entra ID then permits access to enterprise resources. Furthermore, the threat signals in Microsoft Threat Intelligence are leveraged by various Microsoft tools, including MDO and Microsoft Defender for Cloud, to detect and remediate threats in **email**, **office collaboration**, **Azure**, and other components of your organization's attack surface.



Access Restricted:

Conditional Access leverages device risk information received from Microsoft Defender for Endpoint (MDE), communicated to Intune, which then updates the device compliance status in Microsoft Entra ID. **During this period, users are prohibited from accessing corporate resources.** This restriction applies to new resource requests and blocks current access to resources supporting continuous access evaluation (CAE). General internet tasks are still allowed, **but access to corporate resources is restricted.**

Access Restored:

After the threat is remediated, MDE signals Intune to update Microsoft Entra ID, prompting Conditional Access to restore user access to corporate resources. This approach effectively mitigates organizational risk by preventing attackers from accessing corporate resources through compromised devices, **while minimizing disruptions to user productivity and business processes.**