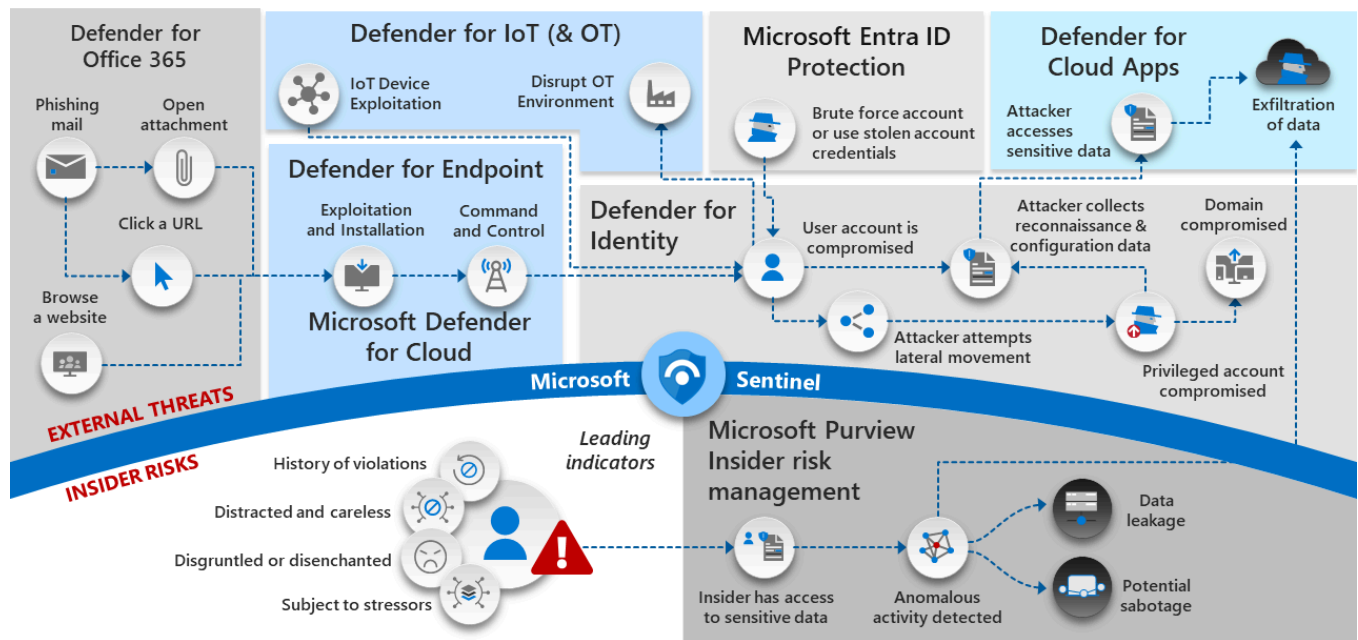


Defend across attack chains

Insider and external threats

Microsoft December 2021 – <https://aka.ms/MCRA>



(A Microsoft attack chain example, see the attacker activity visible to each Microsoft Defender XDR product)

Microsoft Defender XDR is an integrated suite of threat protection solutions designed to identify **malicious activities** spanning email, endpoints, applications, and identity. These comprehensive solutions offer a **holistic view** of the entire attack chain, providing a thorough understanding of the threat landscape. This insight empowers organizations to effectively remediate and fortify defenses against future attacks.

In the illustrative attack chain graphic, observe the visibility of **attacker activities** within each Microsoft Defender XDR product. The accompanying diagram highlights the array of **Microsoft Defender XDR tools** strategically positioned to safeguard against various attack chains.

As a **Security Operations Analyst** implementing Microsoft Defender XDR solutions at your company, it is crucial to comprehend how **Extended Detection and Response (XDR)** integrates signals from **endpoints, identity, email, and applications**. This integration enhances the detection and mitigation capabilities, ensuring a **robust defense** against evolving threats.

- **Microsoft Entra ID Protect**
- **Defender for IoT/ICS**
- **Defender for Office 365**
- **Defender for Cloud Apps**

