# Defender XDR

A diagram of a system

Description automatically generated

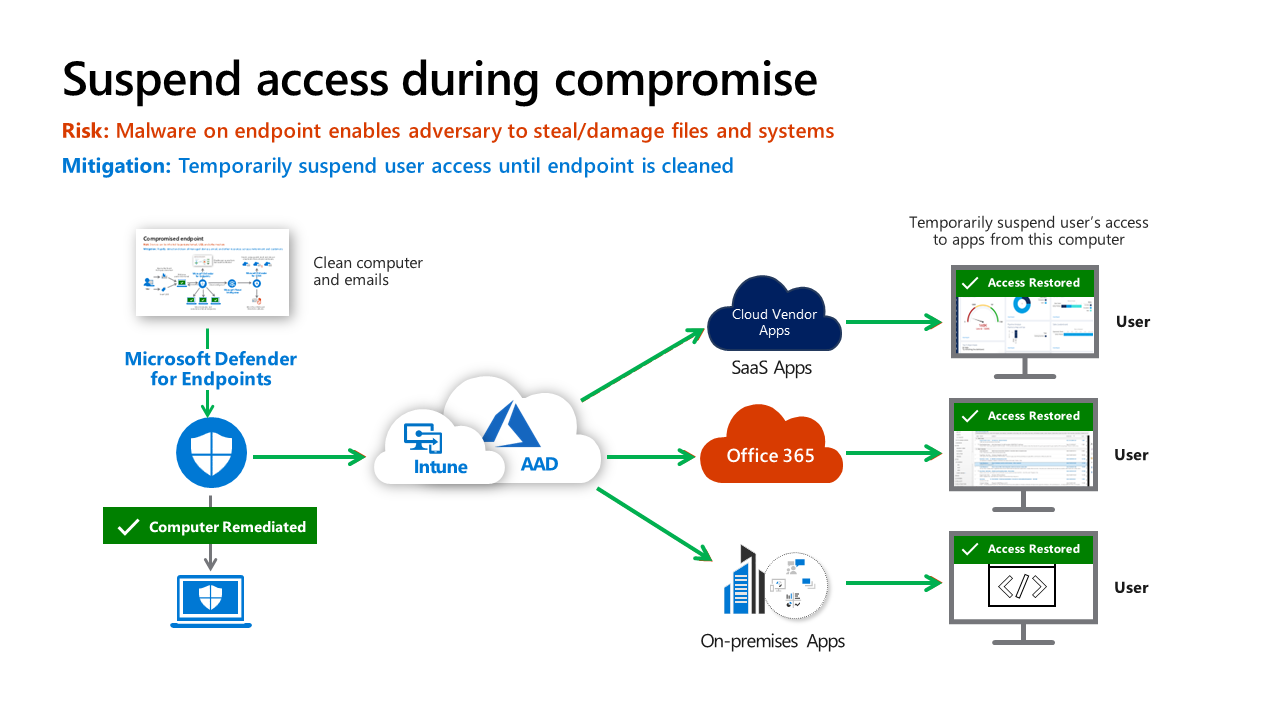
* Protection suite with solutions that detect malicious activity across
  + Email
  + Endpoints
  + Applications
  + Identity

## Detection of Threat

A diagram of a computer system

Description automatically generated

* EDR Detecting a malicious payload which would come from any source, including personal email or a USB drive.
* MDE communicates with Intune. An Intune Compliance Policy configured with MDE risk severity and marks the account as non-compliant with organizations policy. The conditional Access created in Microsoft Entra ID blocks user access to apps.
* Restore access.
  + The threat signals in MTI are used by Microsoft tools securing other parts of your orgs attack surface.
  + MDO and MDC use signets to detect and remediate threats in email, office collaboration, Azure and more.



### Restrict and Grant Access inside Process.

A diagram of a software system

Description automatically generated

## Defender XDR in SOC

An overview of how XDR and Microsoft Sentinel are integrated in a SOC.

A diagram of security operations

Description automatically generated

### Security Operations Model

SOC is composed of several distinct functions. Each function has a primary focus area and must collaborate with other functions and outside teams to be effective.

A diagram of a threat intelligence

Description automatically generated with medium confidence

**Automation**: Resolution of known types with automation. These are well-defines attacks that the organization has been seen many times.

**Triage (Tier 1):**

* Rapid remediation of high volume of well-known incidents that require quick human judgement.
* Identify anything anomalous or interesting that might need further investigation by Tier 2.

**Investigation (Tire 2):**

* Handles issues escalated from Tier 1.
* Conducts deeper investigations on complex attacks.
* Deals with new / unfamiliar alert types to document processes for **Triage team and automation**.

**Hunt (Tire 3):**

* Focused on identifying attackers that could have slipped through the process and handle major business-impacting events.
* Pro-actively hunts for undetected threats and refines alerts/automation.