Table of Contents

[Defender XDR 2](#_Toc164085052)

[Detection of Threat 2](#_Toc164085053)

[Restrict and Grant Access inside Process. 3](#_Toc164085054)

[Defender XDR in SOC 4](#_Toc164085055)

[Security Operations Model 4](#_Toc164085056)

[M365 Defender 5](#_Toc164085057)

[Microsoft Defender AV and MDE alert severities. 8](#_Toc164085058)

[Suppress alerts. 8](#_Toc164085059)

# Defender XDR

A diagram of a system

Description automatically generated

Protection suite with solutions that detect malicious activity across

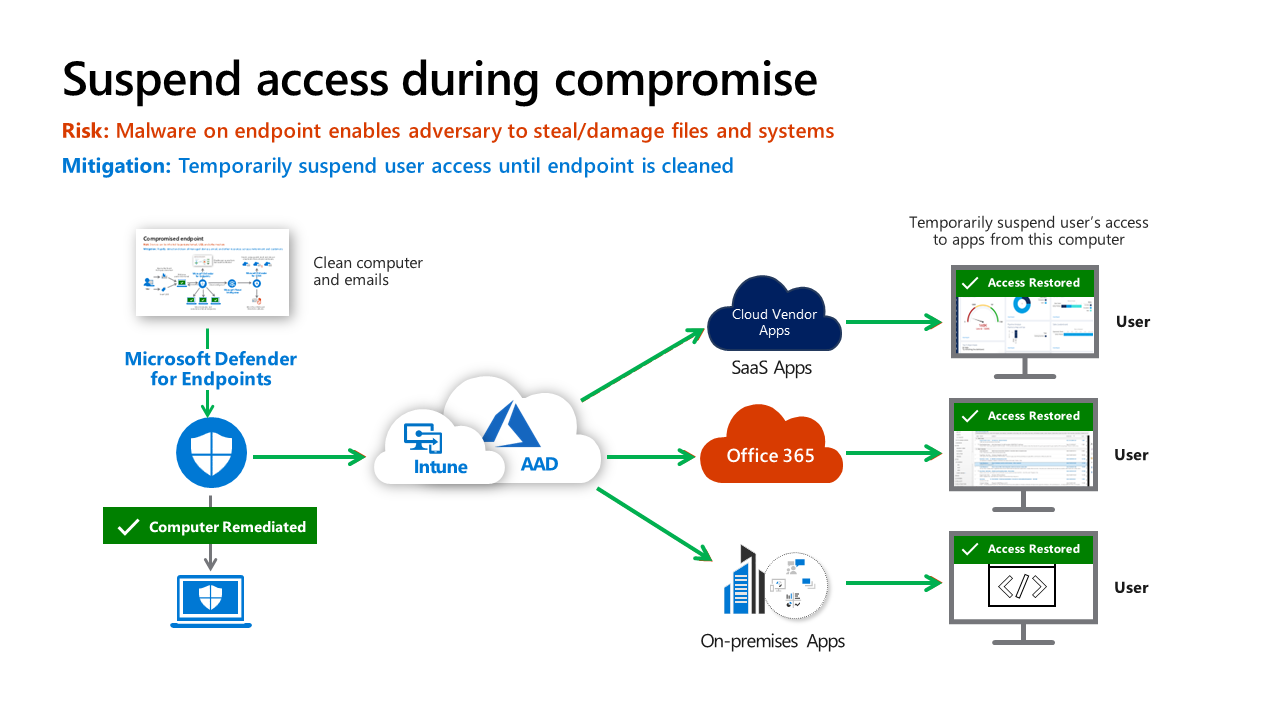
* Email
* Endpoints
* Applications
* Identity

## 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.

## M365 Defender

M365 Defender aka Defender XDR is a unified pre- and post-breach enterprise breach suite that natively coordinates detection, prevention, investigation, and response across

* Endpoints
* Identities
* Email
* Applications

Microsoft Defender portal combines protection, detection, investigation, and response to emails, collaboration, identity, device, and top threats in a central place.

The single pane of glass brings the functionalities of existing Microsoft security portals like:

* ***Microsoft Defender for Office 365***
* ***Microsoft Defender for Endpoint***
* ***Microsoft Defender for Cloud Apps***
* ***Microsoft Defender for Identity***
* ***Microsoft Defender Vulnerability Management***

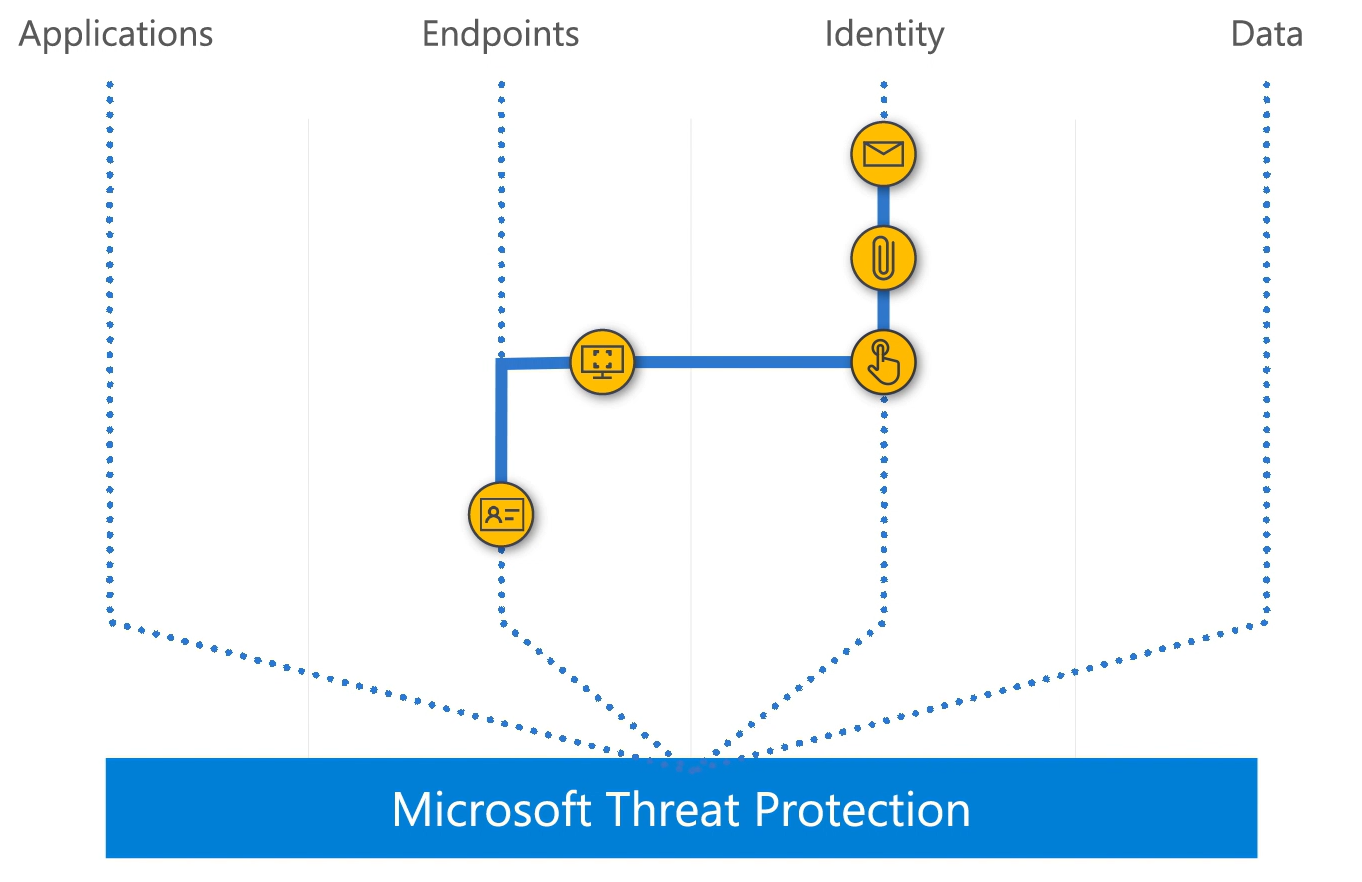
List of more portals.

* ***Microsoft purview compliance portal***
* ***Microsoft Entra ID***
* ***Microsoft Entra ID Protection***
* ***Azure Information Protection***
* ***Microsoft Defender for Cloud***

Microsoft Defender XDR is used to investigate threats. It provides a cross-domain threat correlation.

Incidents are based on related alerts created when a malicious event or activity is seen on your network.

Individual alerts provide valuable clues about an on-going attack. Piecing individual clues together can be a challenging and time-consuming.

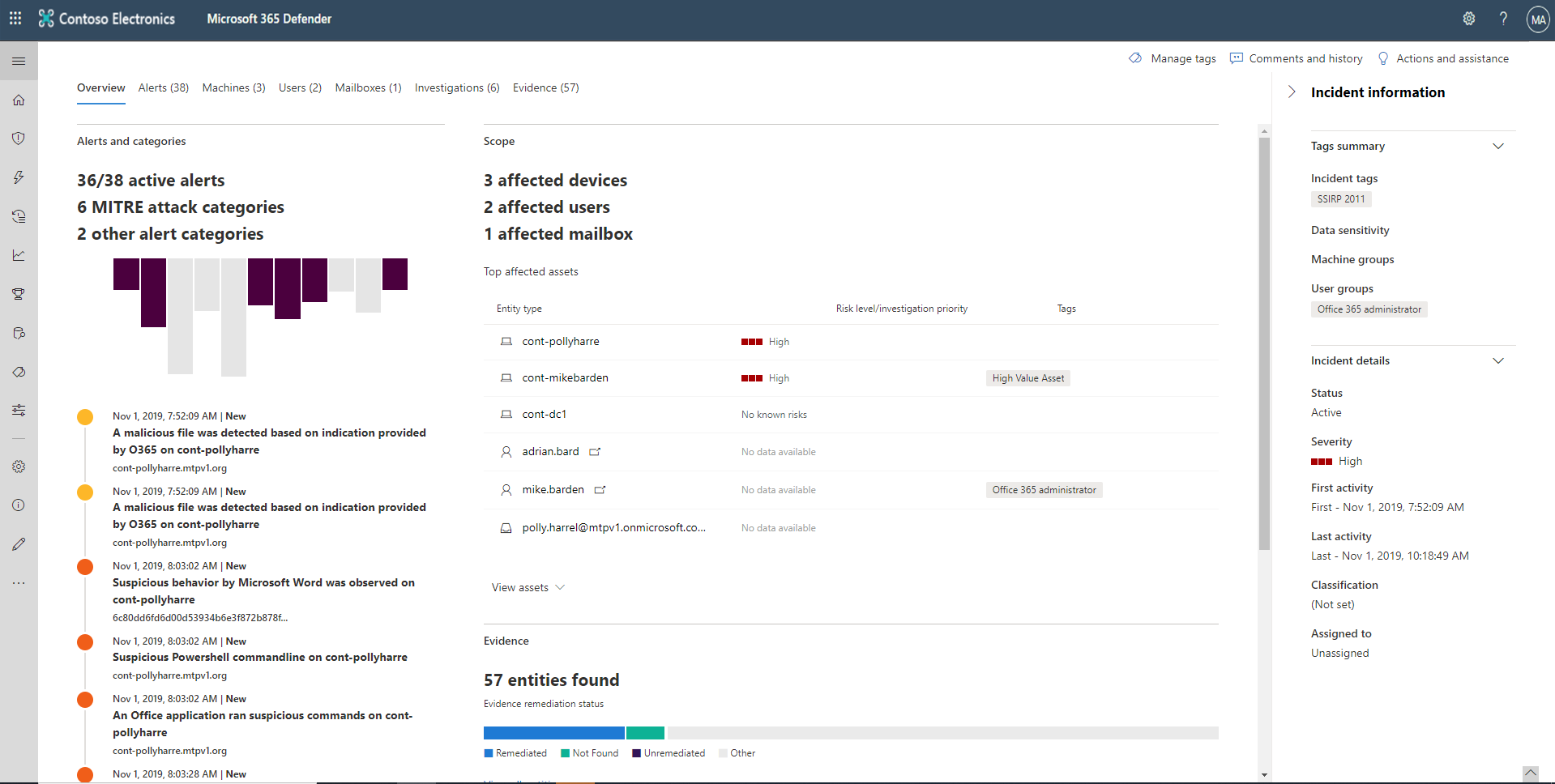


A line of yellow circles with black text

Description automatically generated

<https://www.microsoft.com/en-us/videoplayer/embed/RE4Bzwz?postJsllMsg=true>

* An incident is a collection of correlated alerts that makes up the story of an attack.
* XDR aggregates malicious and suspicious events that are found in different device, user, and mailbox entities in the network.
* XDR provides the information of
  + Where the attack is started, What tactics were used.
  + How far the attack has gone into the network.
  + Visibility on scope of an attack. Like how many devices, users and mailboxes were impacted.
  + How severe the impact was.
  + Details about affected entities.
* By default, the incident queue shows incidents seen in last 30 days.
* The most recent incident is at top of the list.
* **Incident overview page.**



* + Attack categories
    - The attack categories give you a visual and numeric view of how advanced the attack has progressed against the kill chain.
  + Scope
    - List of top impacted assets that are part of this incident.
  + Alerts timeline
    - Chronological order in which the alerts occurred and the reasons that these alerts linked to this incident.
  + Evidence
    - Summary of how many different artifacts were included in the incident and their remediation status.
* **Devices**
* **Users**
* **Mailboxes**
* **Apps**
* **Investigations**
  + Here you can see all the automated investigations triggered by alerts in this incident.
  + The investigations perform remediation actions or wait for analyst approval of actions.
  + You can check the remediation status by clicking on an investigation.
  + Actions will appear in **pending actions tab** for approvals as part of the investigation.
* **Evidence and Responses**
  + Suspicious entities in the alerts, providing you information about the important files, processes, services, emails, and more.

## Microsoft Defender AV and MDE alert severities.

MDAV and MDE alert severities are different because they represent different scopes.

* MDAV threat severity represents the absolute severity of the detected threat ***(potential risk to an individual device)***.
  + Focuses on how bad a single threat (like malware) is for one device.
* MDE thereat severity represents the actual severity of the detected threat ***(potential risk to the organization)***.
  + Focuses on how serious a suspicious activity is for your entire organization. It considers both the risk to a single device and the potential for wider harm across your network.
* Alert severity
  + Informational
    - Detected a threat that was prevented and didn’t infect the device.
  + Low
    - Commercial malware was detected while executing but blocked and remediated by MDAV.
    - It may have caused some damage to the individual device but no organizational threat.
  + Medium or high
    - Threat that can pose a threat not only to the individual device but to the organization.
    - Regardless of if it is blocked will be ranked “Medium” or “High”.
* The ***alert category*** is aligned with the tactics and techniques in the MITRE ATT&CK matrix.
* You can create a new incident from the alert or link to an existing incident.

## Suppress alerts.

You suppress alerts from appearing in Microsoft Defender Security Centre. Suppression rules can be created from an existing alert. They can be disabled or re-enabled if needed.

* When suppression rule is created, it takes effect from the point when the rule is created.
* The rule won’t affect existing alerts already in the queue.
* The rule will only be applied to alerts that satisfy the conditions set after the rule is created.

Two contexts for a suppression rule that you can choose from

* Suppress alert on this device.
* Suppress alert in my organization.

## Protecting identities with Entra ID Protection

This helps to automatically detect, remediate, and investigate identity-based risks for your organization.

### Microsoft Entra ID Protection

Microsoft Entra that’s designed to protect your identities through a three-part process.

* Detect
* Investigate
* Remediate

### Risks

#### 

Risks are categorized in two ways.

***User risk*** – actions that users take after signing in.

* **Unusual behaviour.**
* **Leaked credentials.**

***Sign-in risk*** – suspicious activity and actions by users when they sign-in.

* **Unfamiliar sign-in properties.**
  + Identity protection remembers and learns user’s sign-in history. Detection is triggered when a sign-in occurs from an unusual location for a user.
* **Atypical travel.**
  + Two or more sign-ins occur from distant locations in a short time period.
* **Malware-linked IP address.**
* **Anonymous IP address.**

### Entra ID Protection workflow

* Self-remediation workflow