Secure Identities

Microsoft Defender for Identity (formerly Azure Advanced Threat Protection, also known as Azure ATP) is a cloud-based security solution that leverages on-premises Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.

Business Outcomes:

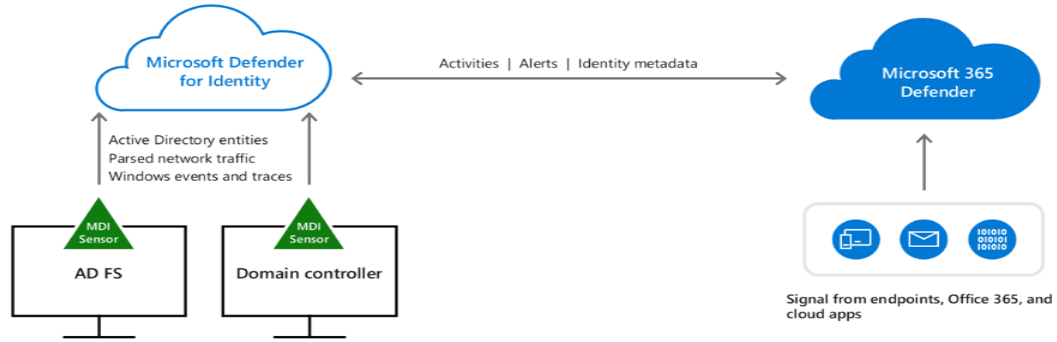
- Monitor users, entity behavior, and activities with learning-based analytics
- Protect user identities and credentials stored in Active Directory
- Identify and investigate suspicious user activities and advanced attacks throughout the kill chain
- Provide clear incident information on a simple timeline for fast triage

Approach:

- Create a Defender for Identity instance and enable investigation of identity-related threats.
- Install on domain controllers or on Active Directory Federation Services (AD FS), to monitor traffic and authentication events.
- Obtain data from Microsoft Intelligent Security Graph.
- Integrate with Syslog server through a sensor and notify when it detects suspicious activity.

> **More data will be created in the next 3 years than was created in the last 30 years combined.**
>
> **Satya Nadella,**
> **2021 Microsoft Inspire Keynote**

Defender for Identity architecture



Phase 1 – Prerequisites & Capacity Planning

The first step of Defender Architecture is to Identify requirements and planning for Capacity on Installing Sensors. The recommended and simplest way to determine capacity for Identity deployment is to use the Defender for Identity Sizing Tool

Phase 2 – Deploy

Add, download a sensor In The Defender Page and Install the Defender for Identity sensor. Create and configure a specific action account along with Sensor settings. Finally Validate the Installations and verify Defender for Identity connectivity.

Phase 3 – Investigate and Response

Microsoft Defender for Identity in Microsoft 365 Defender provides evidence when users, computers, and devices have performed suspicious activities or show signs of being compromised. Investigate for suspicious Activities and configure Alerts with Remediation actions.