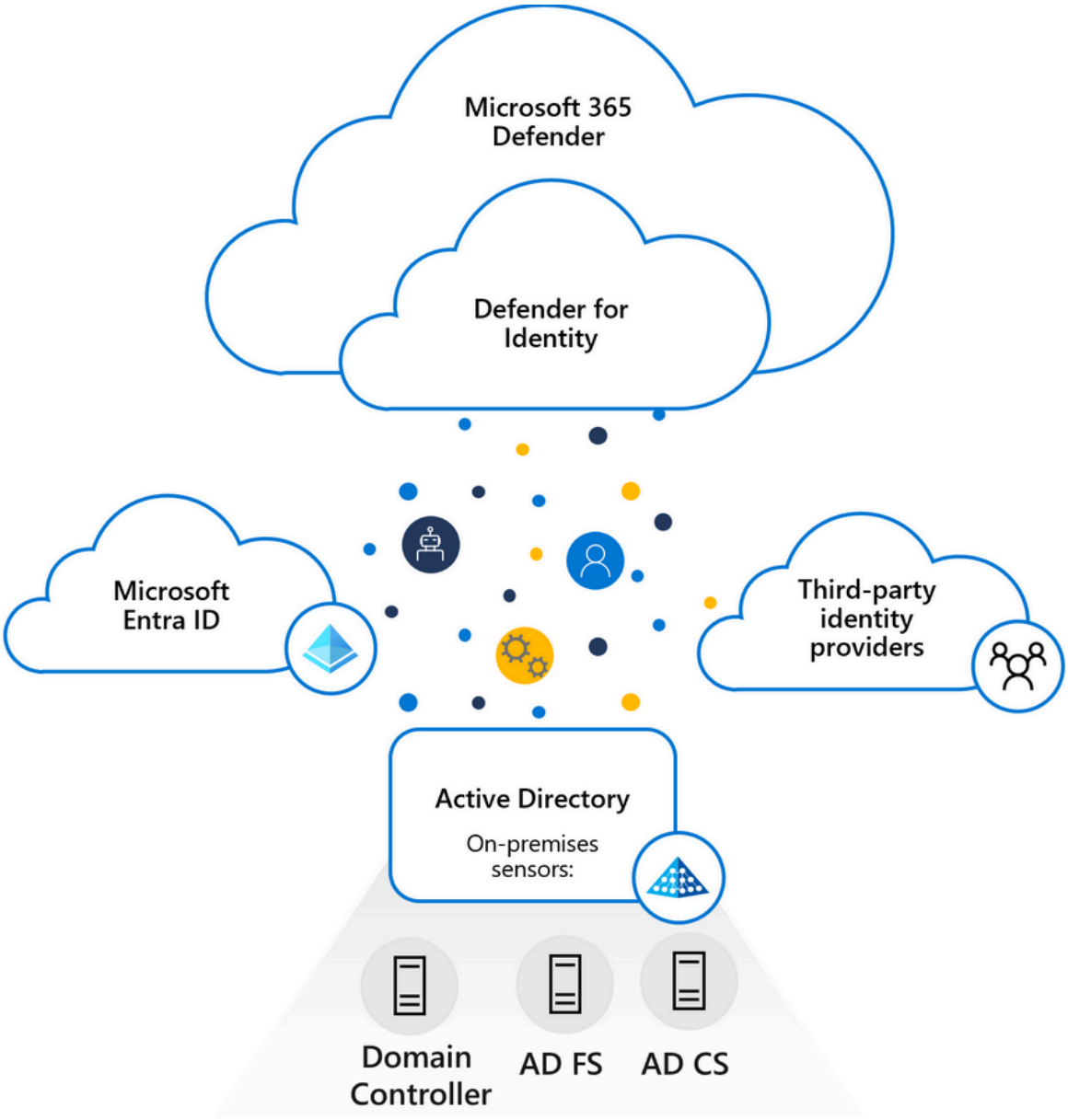
Microsoft Defender for Identity architecture

By: Ryan Stewart



The following image shows how Defender for Identity is layered over **Microsoft Defender XDR**, and works together with other Microsoft services and third-party identity providers to monitor traffic coming in from **domain controllers** and **Active Directory** servers.

Installed directly on your domain controller, Active Directory Federation Services (AD FS), or Active Directory Certificate Services (AD CS) servers, the Defender for Identity sensor accesses the event logs it requires directly from the servers. After the logs and network traffic are parsed by the sensor, Defender for Identity sends only the parsed information to the Defender for Identity cloud service.

Defender for Identity components

Defender for Identity consists of the following components:

- **Microsoft Defender portal**
  The Microsoft Defender portal creates your Defender for Identity workspace, displays the data received from Defender for Identity sensors, and enables you to monitor, manage, and investigate threats in your network environment.

- **Defender for Identity sensor** Defender for Identity sensors can be directly installed on the following servers:

    - **Domain controllers**: The sensor directly monitors domain controller traffic, without the need for a dedicated server, or configuration of port mirroring.
    - **AD FS / AD CS**: The sensor directly monitors network traffic and authentication events.
- **Defender for Identity cloud service**
  Defender for Identity cloud service runs on Azure infrastructure and is currently deployed in the US, Europe, Australia East, and Asia. Defender for Identity cloud service is connected to Microsoft's intelligent security graph.

Defender for Identity sensor

The Defender for Identity sensor has the following core functionality:

- Capture and inspect domain controller network traffic (local traffic of the domain controller)
- Receive Windows Events directly from the domain controllers
- Receive RADIUS accounting information from your VPN provider
- Retrieve data about users and computers from the Active Directory domain
- Perform resolution of network entities (users, groups, and computers)
- Transfer relevant data to the Defender for Identity cloud service

Defender for Identity sensor reads events locally, without the need to purchase and maintain additional hardware or configurations. The Defender for Identity sensor also supports Event Tracing for Windows (ETW) which provides the log information for multiple detections. ETW-based detections include Suspected DCShadow attacks attempted using domain controller replication requests and domain controller promotion.

Domain synchronizer process

The domain synchronizer process is responsible for synchronizing all entities from a specific Active Directory domain proactively (similar to the mechanism used by the domain controllers themselves for replication). One sensor is automatically chosen at random from all of your eligible sensors to serve as the domain synchronizer.

If the domain synchronizer is offline for more than 30 minutes, another sensor is automatically chosen instead.

Resource limitations

The Defender for Identity sensor includes a monitoring component that evaluates the available compute and memory capacity on the server on which it's running. The monitoring process runs every 10 seconds and dynamically updates the CPU and memory utilization quota on the Defender for Identity sensor process. The monitoring process makes sure the server always has at least 15% of free compute and memory resources available.

No matter what occurs on the server, the monitoring process continually frees up resources to make sure the server's core functionality is never affected.

If the monitoring process causes the Defender for Identity sensor to run out of resources, only partial traffic is monitored and the health alert "Dropped port mirrored network traffic" appears in the Defender for Identity sensor page.

Windows Events

To enhance Defender for Identity detection coverage related to NTLM authentications, modifications to sensitive groups and creation of suspicious services, Defender for Identity analyzes the logs of specific Windows events.

To ensure that the logs are read, make sure that your Defender for Identity sensor has advanced audit policy settings configured correctly. To make sure that Windows Event 8004 is audited as needed by the service, review your NTLM audit settings