

INDEPENDENT EDUCATIONAL FIELD GUIDE

Yesterday to Today.

An honest comparison begins with your environment. Today is an assembled operating model, not a claim that a new entitlement is live in your tenant.

Yesterday: begin with your actual starting point.

Defender without Sentinel: deployed protections can already contribute evidence.

Active Sentinel: preserve the workspace. Defender and Sentinel may already share incidents and hunting.

Mixed estate: keep your endpoint choice. Microsoft identity and email protections can contribute when licensed and deployed.

Exploded: separate the responsibilities.

Native Defender evidence and workspace-ingested events follow different routes. License, deployment, permissions and availability are separate checks.

Today: put the parts to work together.

Connect related evidence, an investigation owner, a supported action and a checked result. Optional agents need available evidence, permitted tools and appropriate capacity.

What this guide does not assume

No automatic license activation. No assumed connector deployment. No universal savings, new retention promise or guaranteed ISOC rollout. A portal move is not a commercial transition.

Public sources**[Connect Microsoft Sentinel to Microsoft Defender](https://learn.microsoft.com/en-us/azure/sentinel/microsoft-sentinel-onboard)**

<https://learn.microsoft.com/en-us/azure/sentinel/microsoft-sentinel-onboard>

[Advanced hunting in Microsoft Defender](https://learn.microsoft.com/en-us/defender-xdr/advanced-hunting-microsoft-defender)

<https://learn.microsoft.com/en-us/defender-xdr/advanced-hunting-microsoft-defender>

[Agents in Microsoft Security Copilot](https://learn.microsoft.com/en-us/copilot/security/agents-overview)

<https://learn.microsoft.com/en-us/copilot/security/agents-overview>