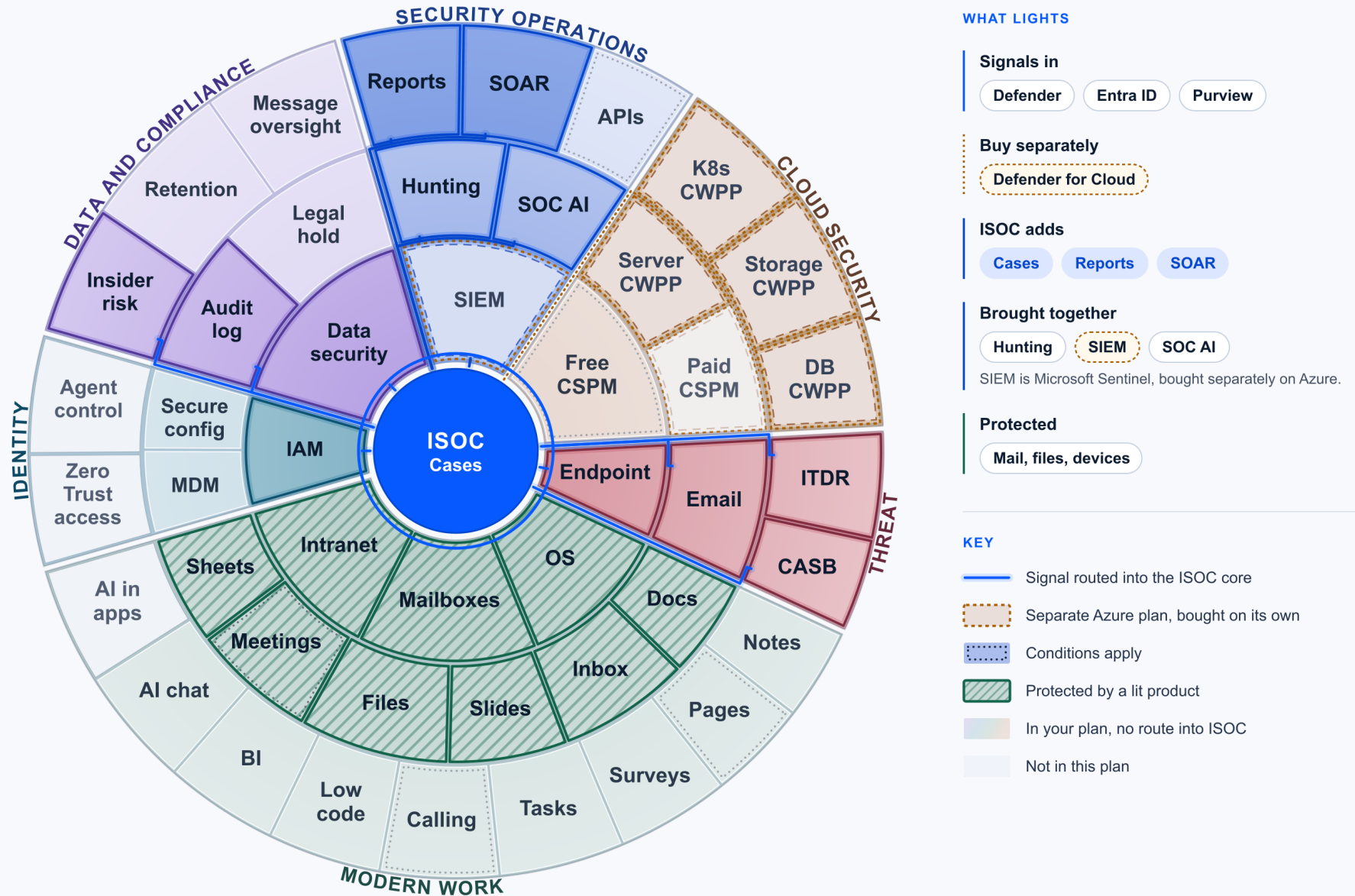


Microsoft 365 E5, lit for ISOC.

Lit means it can feed or serve ISOC on this plan; gold dashed parts are bought separately on Azure. Nothing is switched on in your tenant.



MVP DETAIL

What each lit part needs.

The same Microsoft 365 E5 picture, with the conditions the big picture leaves out. Nothing here is switched on in a tenant.

Signals in: Defender, Entra ID, Purview

Defender XDR alerts arrive natively, with no separate ingestion; Entra ID Protection risk data is in the ISOC data benefit. Purview data security signals join them, each with a condition below.

[ISOC data and billing](#)

With conditions

Data security Data loss alerts reach the Defender incident queue with E5 level rights, once an admin turns off the built-in rule that keeps them out.
[Data loss alerts in Defender](#)

Insider risk Insider Risk alerts in Defender are prerelease and need the data sharing setting.
[Insider Risk alerts in Defender](#)

Audit log Audit evidence arrives through an ISOC workspace connector.
[ISOC data and billing](#)

Buy separately: Defender for Cloud

Defender for Cloud workload plans, gold dashed. No Microsoft 365 plan includes them; their alerts arrive natively once bought.

[Defender for Cloud in Defender XDR](#)

ISOC adds: Cases, Reports, SOAR

Cases in the middle, workbooks (Reports) and automation rules (SOAR), in preview.

[ISOC overview](#)

Brought together: Hunting, SIEM, SOC AI

Incidents and hunting (Hunting) come with Defender XDR. Sentinel (SIEM) runs on its own workspace and usage, bought separately on Azure. Security Copilot (SOC AI) runs on its own capacity, which Microsoft 365 E5 and E7 include as rollout reaches your tenant.

[ISOC overview](#)

[Security Copilot inclusion](#)

Before you plan

Current ISOC preview eligibility lists Defender Suite, Microsoft 365 E5 and E7 without an active Sentinel workspace. Existing Sentinel deployments should be preserved. Product entitlement alone does not establish preview availability.

[ISOC preview eligibility and workspace requirements](#)

Current preview documentation excludes active Sentinel workspaces. Microsoft announces a choice for eligible existing customers to move to ISOC starting November 15, 2026. Keep production workspaces connected and confirm the available migration route.

[ISOC preview eligibility and workspace requirements](#)

[Microsoft ISOC commercial eligibility and data-benefit FAQ](#)

A qualifying license does not establish tenant access or deployment. ISOC workspace creation requires an Azure subscription and specified Entra and Azure roles. Microsoft commercial eligibility also lists an Azure subscription; confirm requirements for the selected route.

[ISOC preview eligibility and workspace requirements](#)

[Microsoft ISOC commercial eligibility and data-benefit FAQ](#)

[ISOC workspace prerequisites and permissions](#)

Protected: Mail, files, devices

Mail, files, meetings, Office apps and Windows devices that Defender for Office 365, Defender for Endpoint and Purview protect show softly. Their alerts reach ISOC through those protections.

[Defender for Office 365](#)

[Safe Links in Office apps](#)

[Defender for Endpoint](#)

[Purview data loss prevention](#)