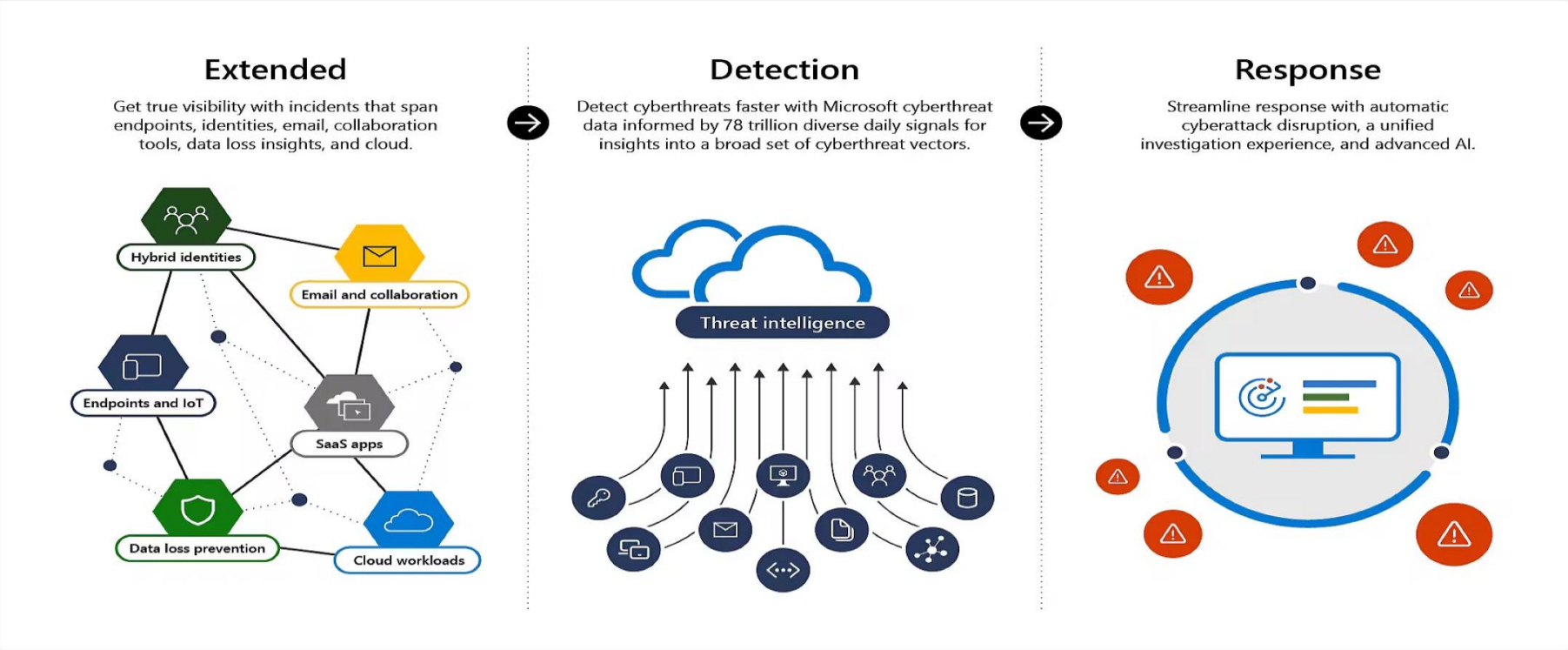
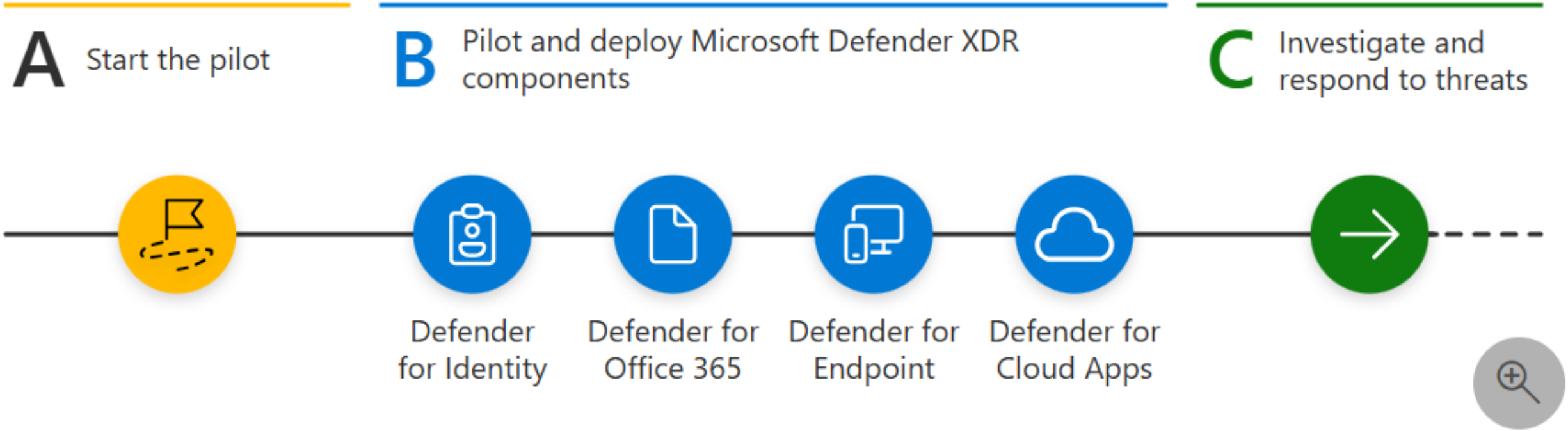


What is Extended Detection and Response (XDR)?

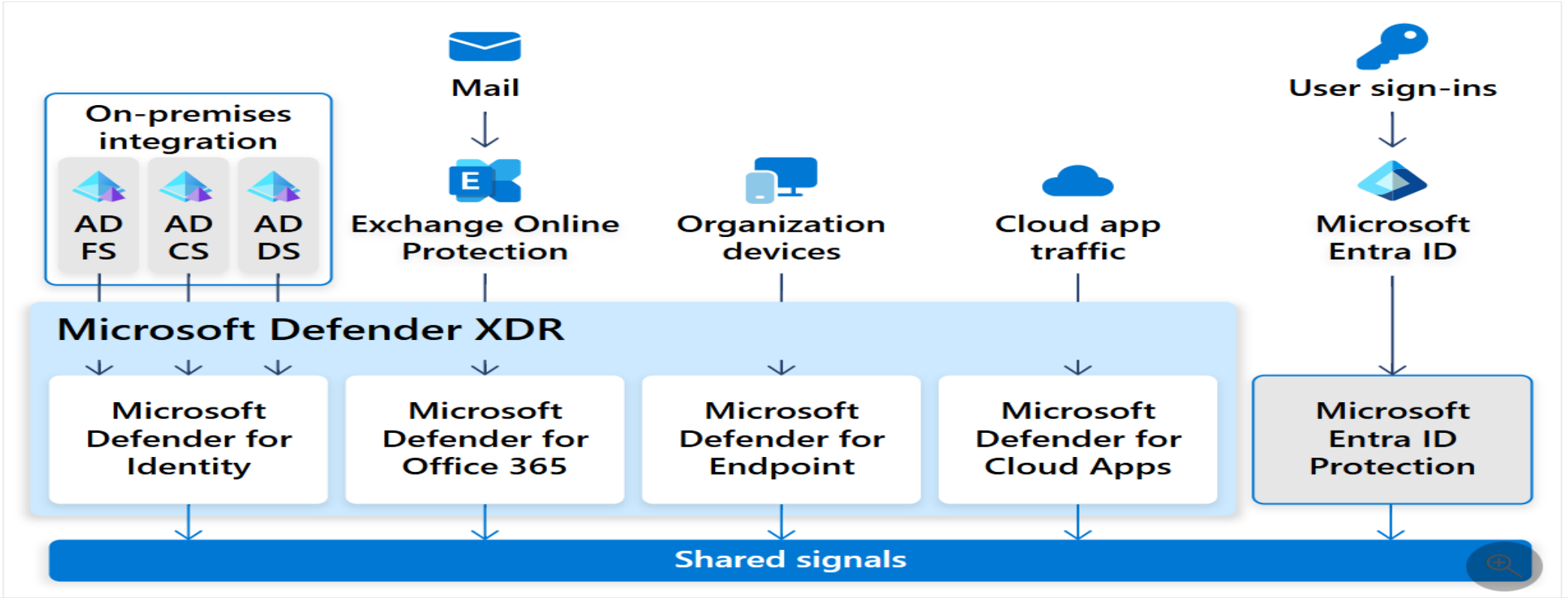
- **Extended:** Visibility across endpoints, identities, email, cloud, SaaS apps
- **Detection:** 78 trillion daily signals fuel Microsoft threat intelligence
- **Response:** Automated disruption + unified investigation with AI



Core Components of Microsoft Defender XDR

- 🧠 Defender for Identity
- 📧 Defender for Office 365
- 💻 Defender for Endpoint
- ☁️ Defender for Cloud Apps
- ✅ Investigate and respond to threats

PerparimLabs



How Defender XDR Works (Signal Correlation)

- Collects telemetry from mail, devices, apps, and identities
- Correlates them in a single XDR platform
- Enables faster, smarter response actions

PerparimLabs

XDR vs SIEM: How They Work Together

XDR (Microsoft Defender XDR)	SIEM(Microsoft Sentinel)
Focuses on **product-level telemetry**	Collects logs from **any source (cloud + on-prem)**
Pre-integrated across Microsoft 362 security tools	Offers **custom correlation rules and long-term retention**
Provides **automated investigation and response (AIR)**	Best for **compliance, analytics, and hunting across all systems**
Prioritizes **quality over quantity** of signals	

XDR = deep detection & response	SIEM = broad visibility & correlation

Defender XDR incidents can be forwarded into Sentinel for full SOC workflows

PerparimLabs