

Microsoft E3 vs. E5

Compliance at Scale Powered by AI, Delivered by RKON

Microsoft E3: Foundational Security & Compliance

Microsoft E3 establishes a strong, cost-effective foundation across identity, endpoint management, and core compliance, giving organizations a standardized baseline for security and governance. Stepping up to E5 is where that foundation becomes a force multiplier: materially reducing risk exposure, accelerating threat detection and response, and strengthening audit readiness with deeper visibility and automation.

E3 is best for organizations establishing baseline controls and standard operations:



What E3 Includes (Security + Compliance)

- **Identity:** Microsoft Entra ID Plan 1 (baseline Conditional Access) in Microsoft 365 E3 (or via EMS E3 in an Office 365 + EMS model).
- **Endpoint management:** Microsoft Intune Plan 1.
- **Endpoint protection:** Microsoft Defender for Endpoint Plan 1.
- **Cloud app visibility:** Defender for Cloud Apps Discovery (visibility into unsanctioned apps).
- **Purview core:** Information Protection (labels), DLP for email and files, retention policies.
- eDiscovery Standard and Audit Standard (default 180-day retention for logs generated on/after Oct 17, 2023).
- Compliance Manager (risk-based compliance score and improvement actions).



E3 Limitations

- Investigations may require more manual effort and shorter evidence windows compared to premium tiers.
- Advanced audit retention, advanced eDiscovery workflows, and advanced insider/comms programs require E5-level Purview licensing/add-ons.
- Cloud app governance and advanced threat response depth are more limited than E5's advanced security stack.

Microsoft E5: Advanced Security + Advanced Compliance

Microsoft E5 builds on E3 with advanced threat protection and advanced compliance investigation capabilities, supporting improved risk posture and reduced operational burden during incidents, audits, and litigation.

E5 is best for advanced threat response and compliance investigations (role-based).



What E5 Adds (Security + Compliance)

- **Identity:** Entra ID Plan 2 (available via Microsoft 365 E5 or EMS E5).
- **Endpoint protection:** Defender for Endpoint Plan 2 (advanced detection and response).
- **Cloud app security:** Full Defender for Cloud Apps (beyond discovery).
- **Identity detection:** Defender for Identity; Email/collaboration protection: Defender for Office 365 Plan 2.
- **Audit (Premium):** Default 1-year retention for key workloads for appropriately licensed users; retention policies support additional retention scenarios (longer retention possible via add-ons).
- eDiscovery (Premium) and advanced Purview capabilities such as Insider Risk Management and Communication Compliance.



Why E5 Changes the Game

- Faster, more defensible investigations via premium audit retention and advanced eDiscovery workflows.
- Reduced breach exposure by strengthening identity and endpoint detection/response for high-impact roles.
- Improved SaaS governance and control with full cloud app security (vs discovery visibility).

When to Evaluate E5

Evaluate E5-level capabilities when outcomes require higher-confidence investigations (audit/eDiscovery), reduced breach cost and response time for high-value roles, stronger audit readiness, or broader SaaS governance and control.

E3 vs. E5 at a Glance (Security + Compliance)

Capability	E3	E5 (Advanced)
Identity	Entra ID Plan 1	Entra ID Plan 2
Endpoint management	Intune Plan 1	Intune Plan 1 (plus broader security stack in E5)
Endpoint protection	Defender for Endpoint Plan 1	Defender for Endpoint Plan 2
Cloud apps	Defender for Cloud Apps Discovery	Full Defender for Cloud Apps
Audit	Audit (Standard) – default 180 days for logs generated on/after Oct 17, 2023	Audit (Premium) – default 1 year for key workloads for appropriately licensed users
eDiscovery	Standard	Premium
Insider / communications risk	Baseline controls (advanced solutions require E5-level Purview)	Insider Risk Management + Communication Compliance

Not sure what's right for your organization

RKON can assess requirements by persona and workflow, confirming where E3 is sufficient and where E5-level capabilities reduce risk and investigation time—without unnecessary broad upgrades.

The RKON Advantage

- Microsoft Security & Compliance experts with proven E3→E5 roadmap execution.
- Deployment + operationalization: policies, alerts, investigation workflows, and governance.
- Licensing-aligned, audit-safe guidance centered on “users who benefit must be licensed.”