A Practical Guide for IT Leaders choosing E3, E5, or E7

Aligning Your Security Needs to Your Microsoft License

Let Your Security Posture Guide Your Strategy

Microsoft 365 E3, E5, and E7 do not represent small, incremental improvements to the same set of tools. From a security standpoint, they represent three different assumptions about what kind of problem you're trying to solve. Choosing the wrong one for the wrong reasons costs organizations more than just money.

E7 is the first new enterprise tier Microsoft has introduced since E5 launched a decade ago. Of course, the security and AI environment that existed in 2015 didn't include AI agents operating autonomously across enterprise systems like it does now. The tiers have changed to reflect that.

Each tier assumes a different security posture, serves different roles, and carries different risk implications. This guide is a decision tool to help you see those differences clearly enough to act.

E5: Where Security Becomes Proactive

E5 is the baseline the other options are measured against. What you give up with E3 and what you gain with E7 both make more sense when you understand what a mature E5 environment looks like.

E5 includes the full Microsoft Defender suite (Defender for Endpoint P2, Defender for Office 365 P2, Defender for Identity, Defender for Cloud Apps), Entre ID P2 with Privileged Identity Management and Risk-Based Conditional Access, Microsoft Sentinel integration for unified threat detection and response, eDiscovery Premium, and advanced data compliance/security/governance capabilities.

But the point of E5 is the shift in posture, not its list of features. E3 security is reactive: you respond to alerts and incidents after they happen. E5 security is proactive: you hunt for threats before they materialize, you enforce least-privilege access in real time, and you investigate insider risk patterns before they become incidents.

SoftwareOne's audits for enterprise environments often reveal that organizations holding E5 licenses are operating at roughly E3-level security maturity. A typical E5 audit might reveal that Defender for Identity was deployed but never configured, that Privileged Identity Management was set up during onboarding but has remained untouched for years, or that the Insider Risk policies never made it to the finance, HR, or legal teams that actually needed them.

If your organization is evaluating E5 or E7, the first question shouldn't be whether the features justify the cost. Instead, ask if you have the operational capacity to configure and use what you're already paying for.

The organizations that get the most value from E5 are the ones that run Sentinel, enforce PIM, and maintain Conditional Access policies blocking anomalous logins in real time.

Those organizations have a security program. The others have a subscription, and a license is not a security posture.

E5 is right for:

- Large enterprises with centralized IT operations and dedicated security teams
- Regulated industries including finance, healthcare, energy, government, and critical infrastructure
- Organizations with elevated cyber risk, material data exposure, or compliance obligations that require granular identity governance and audit capability

---

E3: Solid Productivity, Baseline Security

E3 covers the core Office applications, Exchange Online, SharePoint, Teams, Entre ID P1 with standard Conditional Access, data loss prevention, sensitivity labels, and standard auditing. Microsoft added Defender for Office 365 Plan 1 to E3 at no extra cost starting in 2026, a meaningful security improvement for organizations on this tier.

E3 is a strong productivity platform. It is not a security platform. Organizations that can operate on E3 typically have low data sensitivity across most roles, meaningful external security layers (third-party EDR, a SIEM, threat intelligence feeds) that offset what E3 doesn't include, and limited regulatory exposure.

For organizations in regulated industries, or where sensitive data flows through financial, HR, legal, or compliance functions, the shortfalls in E3 are harder and more expensive to address through add-ons than the cost difference to E5. When your compliance officer asks whether E3 is sufficient, the honest answer is that it depends on what you're trying to be compliant with. For organizations with SOX, HIPAA, or PCI obligations, the audit trail and identity governance capabilities in E3 are often insufficient. Entre ID P2 and Sentinel, both E5 features, are where those requirements actually get met.

E3 is right for:

Mid-market organizations with modern productivity needs and limited data-sensitive roles, and for general staff and frontline workers. Organizations with strong external security layers that don't need Microsoft's native security stack to cover their exposure.

E7: Security for the Agentic Enterprise

E7 includes everything in E5, plus Microsoft 365 Copilot, Agent 365 (AI agent identity and governance), Work IQ for advanced productivity analytics, and the full Microsoft Entra Suite including advanced identity governance and Security Service Edge.

Because the security features are not significantly different from E5, the most meaningful difference is the introduction of a new class of actor: the AI agent.

E5 was designed to secure human workers and the data they access. E7 extends that same control framework to AI agents, software entities that operate at machine speed, across systems, on behalf of users. Agent 365 provides a central registry for agents, policy enforcement, and integration with E5's existing Defender suite so that agents can be audited, secured, and governed the same way privileged users are.

In just the first weeks of preview availability, tens of millions of agents appeared in the Agent 365 registry. Organizations are already running agents, often without visibility into what those agents can access, what they're doing, or whether they're operating inside acceptable boundaries.

The caveat that matters most:

E7 is not a security upgrade. It is a security multiplier. If your permissions model is poorly managed, if your directory is cluttered, or PIM has never been meaningfully enforced, an AI agent operating inside that environment will accelerate those problems. E7 amplifies your existing security posture. It doesn't repair it.

SoftwareOne advises customers to treat E7 readiness as a question of E5 maturity. Before E7 makes sense, you need a clean directory, working Privileged Identity Management, a configured Purview environment, and proven Copilot adoption generating real productivity value. Without that foundation, E7 is an expensive way to amplify existing risk.

E7 is right for:

A targeted subset of users, including power roles, innovation teams, and security and governance leads, where Copilot is already delivering measurable productivity value and where agent usage is operationally relevant.

Matching Tiers to Roles, Not Headcount

Most enterprise organizations should not be on a single tier across all users. The licensing model that makes sense for a SOC analyst is not the same model that makes sense for a frontline worker scheduling appointments. Treating them identically either means overspending on low-risk roles or under-protecting high-risk ones.

In practice, SoftwareOne sees most organizations defaulting to single-tier deployments, often because mixed licensing introduces management complexity, or because purchasing decisions are made at the organizational level before role analysis is complete. The mixed-tier model is the right answer for most large enterprises.

A practical role-based framework:

Role	Recommended Tier	Rationale
General staff, frontline workers	E3	Low data sensitivity, no elevated regulatory exposure
Security team, SOC analysts	E5	Requires full Defender suite, Sentinel, threat hunting
Finance, legal, HR, compliance	E5	Regulatory obligations, sensitive data, audit requirements
Executives, board members	E5	High-profile targets, sensitive communications
Innovation/Copilot pilot users	E5 + Copilot add-on	Measure ROI before committing to E7
Power users with proven Copilot value, mature governance	E7	Only after E5 foundation is solid

Four Questions Before You Assign a Tier

Does this role handle regulated data or material business decisions?

If yes, E3 is likely insufficient. Audit trails, identity governance, and access controls in E5 are where regulated data environments get their footing.

Does it carry compliance obligations?

SOX, HIPAA, and PCI environments require capabilities that E3 doesn't include natively. Entre ID P2 and Sentinel are where those requirements are met.

Is it a high-value target for insider or external threats?

Executives, finance leads, and security personnel are disproportionately targeted. The Defender suite and Insider Risk capabilities in E5 exist specifically for these profiles.

Does Copilot or agent automation deliver measurable productivity value here?

If Copilot ROI hasn't been established at the E5 level first, E7 is a premature commitment. Pilot before you bundle.

Based on those answers, assign the tiers and run a 90-day pilot for your highest-priority tier assignments, measure security incidents, Copilot adoption, and feature utilization, and use that data to build the cost and risk model before rolling out org-wide.

How July 2026 Pricing Changes Affect Your Decision

Microsoft has announced price increases effective July 2026. E5 moves to $60 per user per month; E3 moves to $39. The E5 increase is roughly 5%, about $3 per user per month, but context matters.

For organizations currently running E5 with Copilot as a standalone add-on, the math on E7 is worth a fresh look before renewal. At current pricing, E5 ($57) plus Copilot ($30) puts you at $87 per user.

E7, at $99 for the full bundle, represents approximately a 15% savings compared to buying those components separately, according to SoftwareOne's licensing advisory team. That savings only materializes if you're really using everything the bundle includes.

The threshold SoftwareOne advisors pose to customers is: if you're not fully using E5, not running Agent 365, and not actively using the Entra suite, then you're already leaving value on the table at $90 per user. Paying $99 for additional unused capability doesn't solve that problem.

For E3 organizations, the widening distance between E3 ($39) and E5 ($60) strengthens the case for mixed-tier licensing. Upgrading your entire organization to E5 is a significant cost increase, but upgrading only high-risk roles (including the security, finance, legal, and executive teams) while keeping E3 for general staff becomes more defensible as the per-seat price difference grows.

Don't treat the pricing moment as a routine renewal. Treat it as an audit trigger. SoftwareOne's licensing advisory engagements are built to answer exactly this question: does your current tier mix actually match your security posture and compliance obligations? That's a different conversation than procurement.

Before Your Next Renewal: Five Questions

Use your license renewal as the forcing function it should be. Before you sign, you'll need clear answers to these questions:

Maturity audit: Are your E5 teams actually using E5 capabilities, including PIM, Sentinel, and Insider Risk, or are you paying for features that have never been configured?

Role mapping: Have you mapped organizational roles to tiers based on data sensitivity and regulatory exposure, or are you on a single tier by default?

Compliance alignment: Does your tier selection meet the audit requirements of your compliance frameworks? If your compliance team relies on identity governance and incident forensics, E3 is not sufficient.

Agent readiness: If E7 is on the table, do you have a mature identity governance foundation, including a clean directory, working PIM, and a configured Purview environment? If not, E7 will amplify your current risk rather than reduce it.

Copilot ROI: Have you piloted Copilot with an E5 + Copilot add-on to measure adoption and business value before committing to E7 at scale?

If you can't answer these clearly before your next renewal, a conversation with SoftwareOne's Microsoft experts is the right starting point. Visit us at SoftwareOne.com to learn more.

Contact us today.

Find out more at
www.softwareone.com

SoftwareOne AG | Headquarters
T. +41 44 832 41 69
E. info@softwareone.com