[Joint Solution Brief]

Microsoft 365 E7: The Security Architecture Hiding in Your Current Investment

The Identity Controls Most Organizations Have Licensed but Not Enforced

OVERVIEW

Most enterprises are already running Microsoft at scale. Windows runs on more than 70% of enterprise desktops worldwide. Four in five Fortune 500 companies run Microsoft 365. 85% run Azure. Entra ID governs 720 million monthly active users.

Microsoft 365 E7 unifies that existing footprint into a single platform tier, combining Microsoft 365 E5, the full Entra Suite, Copilot, and Agent 365. Microsoft has made an architectural declaration: human identities, AI agents, NHI, and automated workloads must be governed from the same control plane. The architecture positions Entra ID as the control plane for governing human identities, AI agents, and automated workloads across the environment most security teams are already operating in.

71%	4 in 5	85%	720M
Windows Share of Global Enterprise Desktops	Fortune 500 Companies Running Microsoft 365	Fortune 500 Companies Running Azure	Monthly Active Users on Entra ID

Organizations running E3 or E5 today are using roughly 70% of included capabilities. E7 doesn't close that gap on its own. Operationalizing what's already licensed is what changes the security posture and the cost structure.

IMPACT OF MICROSOFT 365 E7 ON INFORMATION SECURITY

IDENTITY IS THE NEW PERIMETER

AI introduces non-human identities (NHIs) which most security architectures are not designed to handle. AI agents, automated workflows, and Copilot-driven actions authenticate, access systems, and trigger business processes with little to no human oversight. Without a unified identity governance framework, these workloads operate outside the organization's security perimeter.

E7 consolidates the tooling to close the gap between AI governance and identity security. Entra ID Governance, Privileged Identity Management, Conditional Access, and Continuous Access Evaluation now apply to both human and non-human identities. Organizations that configure this architecture before agentic AI scales will have governed, documented access controls in place.

KEY CAPABILITIES ACTIVATED UNDER E7:

1. **Entra ID Governance:** Lifecycle, access reviews, and entitlement management for humans and agents
2. **Privileged Identity Management:** Just-in-time access for Tier 0 workloads including AI service accounts
3. **Defender XDR:** Unified threat detection across endpoints, identity, and cloud workloads
4. **Microsoft Purview:** Data governance and compliance across AI-generated and human-generated content

REDUCING COMPLIANCE EXPOSURE AND RISK BY CONVERGING IAM AND AI GOVERNANCE

MOST IGA FRAMEWORKS WERE NOT BUILT FOR THIS

Most identity governance and administration (IGA) programs are built around human joiner/mover/leaver lifecycles, but AI agents do not follow that model. Instead, they are provisioned programmatically, assigned permissions at scale, and often accumulate entitlements that lack visibility. The result is an expanding attack surface outside existing governance controls.

Regulatory requirements are moving in the same direction. Financial services regulators, state privacy frameworks, and emerging AI governance standards are beginning to require auditable access trails for automated systems. Organizations that have not extended their IGA frameworks to cover AI workloads carry both compliance exposure and security risk.

WHAT MODERN AI IDENTITY GOVERNANCE REQUIRES:

1. **NHI Lifecycle Management:** Provisioning, rotation, and deprovisioning of AI agent credentials
2. **Entitlement Management for AI Workloads:** What each agent can access and under what conditions
3. **Continuous Access Evaluation:** Real-time policy enforcement for agents acting autonomously
4. **Auditable Access Trails:** AI-driven actions audit-ready for regulatory and legal review

AI AUTOMATION AND THE IDENTITY CONTROL PLANE

THE 70/30 REALITY

Most organizations running E3 or E5 today are using roughly 70% of included security and identity capabilities. Entra ID Governance may be licensed but not configured, PIM enabled but not enforced, lifecycle workflows present but inactive. E7 doesn't close that gap automatically. Operationalizing what's already licensed, before July pricing takes effect, is what changes the security posture and the cost structure.

AI automation compounds this. As Agent 365 and Copilot Studio enable organizations to deploy agents at scale, those agents inherit whatever access model exists at the time of deployment. If the underlying identity architecture is ungoverned, every new agent widens that surface.

AUTOMATION REQUIRES GUARDRAILS

Agentic AI deploys autonomous agents that act on behalf of users and organizations. Without governance controls, those agents operate with permissions that are invisible, unauditable, and outside the organization's risk model.

Microsoft's 365 E7 stack provides the native tooling to build these guardrails using Conditional Access policies scoped to workload identities, Entra Permissions Management for least-privilege enforcement, and Sentinel for behavioral anomaly detection across human and non-human identities.

HOW SDG HELPS: FROM STRATEGY TO EXECUTION

SDG assesses, architects, implements, and operationalizes, before transferring ownership to your team. We provide documented runbooks, trained internal owners, and a governance cadence that runs without SDG present. Every engagement produces a running function, not a report.

ENGAGEMENT	WHAT SDG DOES	OUTCOME
E7 Readiness & Licensing Strategy	Audit E3/E5 utilization. Map unused capabilities to security gaps. Build a phased E7 adoption roadmap with July price increase urgency factored in.	License rationalization plan with ROI model and migration timeline.
Entra Identity Architecture & Zero Trust	Design and implement Entra ID Governance, PIM, Conditional Access, and Lifecycle Workflows. Architect Zero Trust controls for hybrid and cloud environments.	Fully governed identity environment with documented policies and internal runbooks.
AI & NHI Governance	Extend IGA to cover AI agents, service principals, and managed identities. Build entitlement management and access review cadence for NHIs.	AI workloads governed under the same policy framework as human identities.
Automation Guardrails & Policy Design	Define Conditional Access policies for Agent 365 and Copilot workload identities. Configure Permissions Management for least-privilege enforcement.	AI agents operate within a defined, auditable, and enforceable access model.
AI Security Assessment & Red Teaming	Pressure-test AI agent permissions, identity federation, and governance controls. Deliver a prioritized remediation roadmap.	Validated security posture for AI workloads with a closed-finding program.
Managed Identity Services	Ongoing advisory, governance reviews, and operational support as AI workloads scale. Quarterly milestones tied to E7 adoption progress.	Sustained program ownership with quarterly governance cadence and E7 adoption milestones.

THE OUTCOME

A fully governed identity environment, with AI workloads under the same policy framework as human identities, and a Microsoft investment that's fully utilized.

ABOUT US

With more than 30 years of experience partnering with global enterprises on complex business and IT initiatives, SDG is a trusted provider of advisory, transformation, and managed services. The firm empowers organizations to strengthen cyber resilience by integrating AI into identity, threat, and risk management solutions that protect digital assets and deliver measurable business value. Learn more at www.sdgc.com.

Contact us to assess your current E3/E5 utilization and build a roadmap *before* July pricing takes effect:

Contact Us: solutions@sdgc.com

SDG
75 North Water Street
Norwalk, CT 06854
203.866.8886
sdgc.com