SHADOW AI

The Ungoverned Tool in Your Governed Environment

Employees are using AI tools you did not approve, on accounts you cannot see, with data you cannot recover. This is not a future risk. It is a current condition in most professional services environments.

59%	$670K	47%	20%
of employees use AI tools not approved by their organization	additional average breach cost when shadow AI is involved	of workplace AI usage runs through personal, unmanaged accounts	of organizations have already experienced a shadow AI security breach

Sources: Cybernews (2025) · IBM Cost of Data Breach Report (2025) · Netskope Cloud & Threat Report (2026) · IBM / Reco (2025)

WHAT SHADOW AI ACTUALLY LOOKS LIKE

Shadow AI is not a rogue actor or an attacker. It is a paralegal summarizing a deposition in ChatGPT. It is a financial advisor drafting client correspondence in a personal Claude account. It is an associate pulling contract language into an unapproved browser-based tool to save an hour. The intent is productivity. The result is data leaving the organization through a channel that cannot be monitored, logged, or recovered.

Among executives and senior managers, the rate of shadow AI use is higher — not lower. One survey found 93% of senior leaders use unapproved AI tools at work. The people with the most access to sensitive information are the most likely to use ungoverned tools.

WHY EXISTING CONTROLS DO NOT STOP IT

Shadow AI operates at the browser layer. It does not require an application install. It does not trigger endpoint alerts. It does not generate a security event. An employee on a managed device, behind a corporate firewall, fully enrolled in Intune, can open a personal ChatGPT account in a browser tab and paste client data into it — and no existing control will detect it, flag it, or stop it unless the environment is specifically configured to prevent it.

The gap is not at the perimeter. The gap is at the identity and device layer — specifically, whether personal accounts can authenticate to AI tools from a managed device, and whether data can leave the governed environment through an uncontrolled browser session.

WHAT A GOVERNED ENVIRONMENT REQUIRES

Control	Requirement	What It Addresses
Managed endpoints only	No personal device can access any governed resource	Personal devices running ungoverned AI tools
Personal accounts blocked	Conditional Access enforces work identity only	Employees authenticating to AI tools with personal accounts
Downloads to OneDrive only	File downloads routed to governed storage	AI-generated content saved outside the governed environment
Work profile enforced	Microsoft Edge for Business, Intune-managed	Browser-layer access to unapproved AI platforms

These controls are not policies. Policies can be ignored. These are enforced conditions — the environment either permits the action or it does not. There is no exception process. There is no workaround. The governed environment does not negotiate.

WHAT CARRIERS ARE NOW REQUIRING

Cyber insurance underwriters have shifted from questionnaires to evidence. In 2026, a "yes" on a renewal application is not sufficient. Carriers expect documentation: telemetry logs, control coverage reports, backup test results, and incident response records. Organizations that cannot produce this evidence at renewal face higher premiums, reduced limits, or denial.

Shadow AI has accelerated this shift. Carriers are introducing AI-specific exclusions and riders that condition coverage on documented governance of AI usage inside the environment. An organization that cannot demonstrate control over how AI tools are accessed — which accounts, which devices, which data — is presenting an unquantifiable risk. Underwriters are pricing that accordingly.

The controls required for cyber insurability and the controls required to govern shadow AI are the same controls. MFA enforced on every identity. EDR in block mode on every endpoint. Managed devices as the only path to governed resources. Immutable backup with tested recovery. Continuous monitoring with a documented record. An organization operating inside a governed environment does not assemble this evidence at renewal. It already exists.

THE GOVERNANCE BOUNDARY

AnchorOne governs the environment AI runs in — not the AI itself. Which AI tools an organization adopts, how staff are trained to use them, which workflows are automated — those decisions belong to the organization. What AnchorOne enforces is that those tools operate inside a governed perimeter: on managed devices, under verified identities, with data that stays inside the environment.

Shadow AI is not a technology problem. It is a governance problem. The technology to address it already exists inside Microsoft 365. What most organizations lack is the authority to enforce it — and the standard that defines what enforcement requires.