Shadow IT: A Hidden Threat

Idea In Short

Treat shadow information technology (IT) as a visibility problem, not a discipline problem, and fund discovery before you fund enforcement. Combine network and identity logs with a short, non-punitive survey to find the tools employees already depend on, then sort each one into approve, restrict or retire rather than issuing a blanket ban. Speeding up legitimate approval requests removes the underlying reason employees go around IT in the first place, which does more to reduce risk than any policy memo.

The Everyday Shortcuts Behind Shadow IT

A salesperson shares a customer list through a personal Google Drive account. A marketing manager pastes an unpublished campaign plan into a free artificial intelligence (AI) tool. A developer spins up a cloud database for a quick test and forgets to close it afterward. None of them intends to put the company at risk; they are simply trying to finish a task. That is precisely what makes shadow IT difficult to control, because it usually grows from convenience rather than malicious intent, and it can stay invisible until sensitive data is exposed, an employee leaves or an incident forces the company to investigate systems it never knew existed.

What Shadow IT Actually Means

Shadow IT is hardware, software or a cloud service used for business purposes without the knowledge or approval of the organization's information technology (IT) department. The term covers far more than unauthorized applications. It extends to personal laptops, cloud storage accounts, browser extensions, messaging apps, AI platforms, development environments, application programming interfaces (APIs), virtual machines and subscription-based software that individual departments purchase directly.

The UK National Cyber Security Centre (NCSC) describes shadow IT as unknown assets used within an organization but not accounted for through normal asset management or

corporate IT processes, and that distinction matters. An application does not have to be inherently dangerous to create risk; the problem is that nobody responsible for security knows it is being used, what information it holds or who can access it. Shadow IT should not be confused with malware planted by an attacker. It is normally introduced by authorized employees or contractors using an unapproved resource to complete legitimate work.

Bring Your Own Device, known as BYOD, is not automatically shadow IT either. A personal phone enrolled in the company's device-management system and covered by an approved BYOD policy is a known, managed asset. That same phone becomes a shadow IT concern the moment it stores corporate files without encryption, monitoring or access controls.

What Shadow IT Looks Like in Practice

Cloud storage is one of the easiest places for shadow IT to take root. An employee cannot send a large file through the company email system, so they upload it to a personal Dropbox, Google Drive, OneDrive or Box account, and the workaround takes minutes and solves the immediate problem. The file may then sit in that personal account for years. Analysis from the 1 consistently finds that credential misuse and unmanaged access points remain among the leading paths attackers exploit, and unmanaged storage accounts fit that pattern precisely.

Communication tools create similar gaps. A project group might move conversations to WhatsApp, Telegram, Slack or another platform simply because it is more convenient than the approved system, and important decisions, attachments and customer information now sit outside the organization's retention and access policies. Project management and design platforms follow the same pattern. A team can open a free Trello, Asana, Canva or similar account without involving IT or procurement, and problems often surface later, once the free account becomes central to daily work and holds months of internal information.

Personal hardware belongs in the same conversation. USB drives, home computers, wireless printers, external hard drives and smart devices can all handle company information without ever appearing in the official asset inventory. Even security and privacy products can become shadow IT. An employee preparing for a business trip might install a consumer virtual private network (VPN) on their own initiative. Review sites such as The Best VPN can help individuals compare providers through hands-on testing, but a well-reviewed consumer service is not automatically approved for corporate work, since IT still

needs to assess where business traffic is routed, how the provider handles data and whether its use conflicts with company policy.

Then there is shadow AI. Employees increasingly use public chatbots, transcription platforms, writing assistants and automation tools to save time, and the risk begins when they enter customer records, contracts, source code, financial information or internal strategy documents without understanding how the service stores and processes that data. IBM's research shows how quickly adoption has outpaced governance. The 2025 Cost of a Data Breach Report found that 63% of surveyed organizations lacked policies for managing AI or preventing shadow AI, and among organizations that reported an AI-related security incident, 97% lacked proper AI access controls.

Why Employees Bypass IT

Shadow IT is often framed as an employee-discipline problem, and that explanation is convenient but usually incomplete. People turn to unauthorized tools when approved systems make ordinary work unnecessarily difficult, whether they cannot share a file with a client, collaborate with an external contractor, access a service remotely or obtain software before a project deadline. Sometimes the approved alternative simply does not perform the required task.

Consider a design team that must wait three weeks for approval to use a new collaboration platform, while the client expects a first draft in five days. One employee opens a free account, invites the team and keeps the project moving, and from that employee's perspective, the decision looks practical rather than reckless. Research summarized by 2 reaches a similar conclusion: most policy violations trace back to employees prioritizing task completion over compliance, not indifference to security. The underlying security problem remains real, but punishment alone will not solve it. If the original obstacle stays in place, employees will find another workaround and simply become more careful about hiding it.

Why Shadow IT Becomes a Security Problem

The most serious issue is not necessarily weak software; it is the absence of organizational control. IT cannot patch an application it does not know exists. It cannot remove access when an employee leaves, verify that multifactor authentication is enabled, preserve records, monitor suspicious activity or include the system in an incident-response plan, and

this gap creates several overlapping risks.

Sensitive information can leave approved systems without triggering data-loss controls. A personal storage account may use a weak password or remain accessible on an old device. Public links may be forwarded well beyond their intended recipients, and data may end up stored in a country or environment that does not meet the organization's contractual or regulatory requirements. Guidance from the 3 identifies exactly this loss of visibility, rather than any single vulnerable product, as the defining characteristic of shadow IT risk.

Shadow IT also expands the number of accounts an attacker can target. Employees frequently reuse passwords, grant broad permissions to integrations or connect applications through "Sign in with Google" or "Sign in with Microsoft," so a compromised third-party account can expose far more than the isolated application itself. Access also tends to outlive its original purpose: a contractor finishes an assignment but their account remains active, an abandoned software-as-a-service (SaaS) subscription continues holding customer information, and an application programming interface token created for a temporary test is never revoked. The result is a security environment built partly from systems that nobody maintains and few people remember.

Operational problems can prove just as disruptive. If a department builds an important workflow around one employee's personal account, the company may lose access entirely when that employee leaves. Data may not be backed up, exported or compatible with approved systems, and what began as a shortcut gradually becomes infrastructure the business quietly depends on.

How Shadow IT Discovery Works

The first goal is visibility, not immediate blocking. The NIST Cybersecurity Framework 2.0 quick-start guide recommends maintaining an inventory of hardware, software, systems and services, and it asks organizations to consider which technologies employees actually use to perform their work and whether those technologies are both secure and approved.

A basic software inventory will not reveal everything. Browser-based tools leave little evidence on a device, and remote employees may access them entirely outside the corporate network, so discovery has to combine several types of information. Firewall, proxy, domain name system (DNS) and endpoint logs can reveal connections to cloud

services that never appear in the approved application catalog. Identity-provider logs show which third-party tools employees have connected to corporate accounts, and expense reports and company-card statements can uncover subscriptions that individual departments purchased directly.

Cloud Access Security Brokers, commonly known as CASBs, automate much of this work by analyzing traffic and categorizing cloud services based on their security and compliance characteristics. For scale, Microsoft's Cloud App Discovery documentation describes a catalog containing more than 31,000 cloud applications assessed against more than 90 risk factors. That technology still has limits, since it may miss applications absent from its catalog, activity performed entirely on unmanaged devices or traffic hidden from normal network monitoring. Technical discovery should therefore be supported by direct conversations with employees. A short, non-punitive survey can reveal tools that logs cannot. Ask teams what slows them down, which services they pay for themselves, where they exchange large files and which AI tools they use, and the answers double as useful product feedback for IT.

Managing Shadow IT Without Stopping Useful Work

A blanket ban sounds decisive but often pushes the same behavior further out of sight. A better strategy distinguishes between tools that can be approved, tools that require restrictions and tools that create unacceptable risk, a triage approach the 4 recommends over across-the-board prohibition.

Approval should move faster, because employees are less likely to bypass IT when requests receive a clear answer within days rather than disappearing into a lengthy review, and low-risk applications should not require the same process as systems handling financial, health or identity data. Employees should not have to search through policy documents to find out which file-sharing, messaging, AI or project-management tools they may use, so a simple internal catalog of approved alternatives proves more useful than a long list of prohibitions.

The review itself should match the data at stake. A basic scheduling app and a platform processing customer records do not carry the same risk, so reviews should weigh what information the tool receives, where that information is stored, how access is controlled and whether data can be deleted or exported. Discovering an unauthorized application does not always mean it must be removed either. If it meets a genuine business need, IT may be able

to purchase an enterprise plan, enable single sign-on, apply retention rules and transfer ownership from an individual employee to the company.

A safe reporting route matters just as much as any technical control. Employees should be able to disclose an unapproved tool without expecting automatic punishment, because otherwise IT learns about shadow systems only when something breaks. Training should use situations employees recognize, such as uploading a file to a personal account, installing a browser extension, connecting a chatbot to company email or buying software with a corporate card. Generic warnings about "unauthorized technology" are easy to ignore, since many employees do not realize their everyday shortcuts qualify.

Shadow IT will never be eliminated completely. New tools appear too quickly, and employees will keep looking for faster ways to work. The realistic objective is to find those tools early, understand why people adopted them and bring useful technology under appropriate control before a convenient workaround becomes a hidden security problem.

- 1Verizon Data Breach Investigations Report
- 2Harvard Business Review
- 3SANS Institute
- 4Cloud Security Alliance

Summary

Shadow IT persists because approved systems often move slower than the work employees need to finish. Finding these tools early, understanding why people adopted them and bringing useful technology under management closes the gap between convenience and control.