



BEYOND THE APPROVED LIST

Shadow IT Is a Demand Signal, Not a Discipline Problem

Why the applications your people bought without asking are the most honest roadmap you have

Giovanni Leonardi

May 2017

Shadow IT Is a Demand Signal, Not a Discipline Problem

Transformation · No. 209

Originally written May 2017 | Re-edited and re-rendered for the WhereBeyond Edition, 2025

*"Shadow IT is not the disease. It is the diagnostic —
and right now, most of us are still treating the
thermometer."*

The audit that found four hundred applications

A security review runs a discovery scan across the network and the corporate-card statements — many teams are doing exactly this in the run-up to next May's data-protection deadline. The sanctioned application register lists forty-odd systems. The scan comes back with more than four hundred.

Not four hundred security incidents. Four hundred small, cloud-hosted, mostly sensible tools that people bought because they needed to get something done: a marketing team running its own analytics and email platform, a recruiter paying nine dollars a month for a scheduling app, a product group coordinating entirely in a chat tool IT has never heard of, three separate file-sharing accounts in three separate departments. Almost all of it billed to a card and expensed as "software, miscellaneous."

The reflexive reading is that this is a governance failure to be stamped out. I want to argue the more useful thing: that inventory is the most honest piece of market research the organisation owns, and most of us are too busy being alarmed by it to read it.

What the shadow is actually telling you

Shadow IT is not new; the phrase has been around for years. What is new in the last eighteen months is the sheer ease of it. When provisioning a tool meant a server, a licence negotiation and a project code, the business had to come through IT because there was no other door. That era is over. A department head with a corporate card and a browser can be live on a capable product before lunch, cancel it before the next invoice, and never file a ticket. The friction that used to funnel demand toward the IT function has simply evaporated.

So when a team bypasses the sanctioned stack, they are not usually being reckless. They are voting. Every unsanctioned tool is a small, budgeted, deployed statement that the official option did not exist, did not work, or did not arrive in time. Read in bulk, the shadow estate is a live heat-map of where internal provision is failing and where the real work is trying to move faster than the organisation can support it.

The applications your people bought without asking are the closest thing you have to an unfiltered product backlog. Every one of them is a requirement that was urgent enough for someone to pay for it out of their own budget.

Consider what that four-hundred-item list actually encodes. Cluster it and the patterns are blunt. Five separate tools doing lightweight task tracking means the sanctioned project system is unusable for small teams. A knot of design-collaboration and prototyping tools means the product organisation has outgrown the workflow it was handed. Three file-sharing accounts mean people need to work with outside partners and the official method makes that painful. None of that is in any strategy deck. All of it is in the expense ledger.

The objection is real — and it is not the whole story

I will not be glib about the risk, because it is genuine and it is getting sharper. Customer data sitting in a tool nobody vetted, under terms nobody read, is exactly the exposure the coming data-protection regime is built to punish — and "a manager expensed it" will not be a defence a year from now. Unmanaged tools fracture identity, duplicate spend, and leave data in places no one can produce on request. Anyone who treats shadow IT as simply a good thing has not sat through a breach post-mortem.

But the standard response — hunt it, block it, threaten it — treats the symptom and misreads the cause. Lock down the cards and you do not remove the demand; you only push it further underground, where you can no longer see it at all. The teams still need the capability. They will simply get better at hiding how they get it, and you will have converted a visible signal into an invisible risk.

The more defensible move is to hold both truths at once: close the exposure and harvest the intelligence. Bring the riskiest data-handling tools into managed identity and a real contract — quickly, without a six-month procurement ritual that recreates the very friction that caused the workaround. And treat the shadow inventory as a standing input to the technology roadmap. What got bought, by whom, to solve what, reviewed each quarter, is a better demand signal than any internal survey, because people equivocate on surveys and they do not equivocate with their budgets.

What to do about it now

The instinct to regain control is right; the method is usually wrong. A practitioner reading this in the current climate could start with three unglamorous moves.

1. Count before you judge. Run the discovery once and read the result as data, not as a charge sheet. The clusters are the message.
2. Fix the fast lane, not just the fence. If it is easier to expense a tool than to request one, people will expense the tool. The unit of the problem is your own provisioning speed.

3. Give the shadow a front door. A lightweight path to sanction a popular tool — vetted for the data it touches, added to single sign-on, kept if it earns its place — turns rebellion into a pipeline. The tools that survive that path are your roadmap, chosen for you by the people doing the work.

The organisations getting this right in the current wave are not the ones with the tightest lockdown. They are the ones that stopped asking how did this get past us and started asking what is this trying to tell us. Shadow IT is not the disease. It is the diagnostic — and right now, most of us are still treating the thermometer.