

BEYOND THE GATEKEEPER

# Shadow IT Won. The Mistake Now Is Trying to Win It Back

What a year of improvised tools revealed about the gatekeeping model of technology — and why re-imposing the gate is the wrong response

Giovanni Leonardi

February 2021



# Shadow IT Won. The Mistake Now Is Trying to Win It Back

Transformation · No. 256

Originally written February 2021 | Re-edited and re-rendered for the WhereBeyond Edition, 2025

---

*"The gatekeeper reads that letter as a charge sheet and starts issuing corrections. The steward reads it as a specification."*

---

## 1. When the Front Door Was Locked

---

The number that ended the debate was three hundred and forty.

That was the count of distinct software services a discovery scan turned up inside one organisation late last year — three hundred and forty tools touching corporate information, set against a sanctioned catalogue of roughly forty. The other three hundred had arrived with no business case, no architecture review, and no one in technology signing anything. They had arrived because, in the third week of March last year, people had work to finish and the front door was locked.

We have a word for those three hundred tools. For most of a decade we called it shadow IT and treated it as a hygiene problem — something to be discovered, quantified, and scrubbed away. So the instinct in the room, as the scan results went up on the screen, was the familiar one: draw up a remediation plan, rationalise the list, herd everyone back onto the approved platforms, and close the exposure before the auditors find it first.

It is an understandable instinct. Over the past eleven months I have watched it form in a dozen conversations, and I have come to believe it is the wrong one — that acting on it now is a larger risk than the sprawl it is meant to cure.

## 2. The Pandemic Did Not Create This. It Ended the Pretence.

---

The comfortable reading of the last year is that a crisis forced good people into bad habits, and that the job now is to restore order. That reading flatters us. It lets technology functions cast themselves as the responsible adults cleaning up after a necessary emergency.

The less comfortable reading is the true one. The tools did not appear because discipline collapsed. They appeared because the official route could not move at the speed the work demanded, and everyone quietly already knew it. When the offices emptied, the gap simply became impossible to hide.

Consider the arithmetic that every one of those three hundred choices ran through, whether the person made it consciously or not. The sanctioned way to acquire a new capability took, on a good day, six to eight weeks — a request form, a security questionnaire, an architecture slot, a procurement negotiation, a data-protection sign-off, a licence order. The unsanctioned way took four minutes and a corporate card, or nothing at all beyond an email address. When a team needs to run a client workshop on Thursday and it is Tuesday, that is not a close contest.

*Shadow IT is not a failure of employee discipline. It is a market signal. Every unsanctioned tool is a small, precise statement that the official channel was too slow, too rigid, or too absent to serve a real need in time.*

One example stays with me. A finance team ran three consecutive quarterly closes out of a shared spreadsheet held in one manager's personal cloud account, because the sanctioned ledger could not be reached cleanly from home and the fix was stuck in a queue behind forty other requests. Nobody in that team was reckless; every one of them would have told you they were doing the responsible thing, keeping the numbers moving while the official system caught up. They were right. The recklessness, if it sat anywhere, sat in an organisation that had made the compliant path the impossible one and then expected compliance.

For years the gatekeeping model rested on an unstated bargain: technology would be the single door through which capability entered the organisation, and in return it would provision fast enough that no one needed another door. The first half of that bargain was enforced with policy. The second half was quietly never kept. Remote working did not break the model. It removed the physical friction — the shared network, the managed desktop, the person two desks away who could say you can't use that — that had been propping up a model already hollow at the centre.

### 3. The Objection Is Not Wrong

Here is where the honest version of this argument has to slow down, because the case for reasserting control is not a caricature. It is serious, and anyone who has sat through a breach post-mortem feels its weight.

Three hundred unmanaged tools is a genuine exposure, not a rhetorical one. Corporate information now sits in personal file-sharing accounts that no leaver process will ever reach. Client data flows through services whose hosting location no one has checked — and after last summer's ruling on transatlantic data transfers, where the data rests is no longer a footnote for a European organisation but a live legal question. Few of those tools sit behind the single sign-on that lets us cut access the day someone leaves; fewer still feed the logs that would tell us if something had gone wrong. The winter's great security story — a compromise buried inside trusted, widely deployed software — was a reminder that the supply chain we do vet is dangerous enough, before we add three hundred services we have never looked at.

All of that is real. None of it is an argument for the gate.

Because the gate does not make those tools safe. It makes them invisible. The three hundred we can see are the ones adopted in the open, by people who assumed the choice was reasonable. Announce a crackdown and rationalisation programme, and you do not remove the need those tools were meeting — you remove only the candour. The spreadsheet moves to a personal laptop. The file-sharing link stops being mentioned in meetings. The visible sprawl you were about to inventory becomes an invisible one you cannot. We would be trading a governance problem we can see for a security problem we cannot, and calling it progress.

#### 4. From Gatekeeper to Steward

So the question the topic poses — now what? — deserves a better answer than now we take it back. The more useful reframing is to stop trying to own the choice of tool and start governing the things that actually carry the risk.

That is a real shift in what a technology function is for, and it is worth being concrete about the difference.

| The old posture                               | The steward's posture                                          |
|-----------------------------------------------|----------------------------------------------------------------|
| Technology owns which tools may be used       | Technology owns the standards any tool must meet               |
| Control is exercised at the point of purchase | Control is exercised at the points of identity, data, and exit |
| Default answer is no, pending review          | Default answer is yes, within a guarded lane                   |
| Success is a short, enforced catalogue        | Success is a known, well-governed estate however long          |
| The measure is tools blocked                  | The measure is data protected and access controlled            |

In practice this means picking the few battles that matter and conceding the many that do not. Identity is the first battle: make single sign-on the non-negotiable price of entry, so that whatever a team adopts, access is granted and revoked centrally and a departure closes every door at once. Data is the second: classify what actually cannot leave the building, and put real controls around that, rather than pretending everything is equally sensitive and therefore protecting none of it well. Exit is the third: know how information gets out of a service and back under control if it fails or is dropped, because the tool a team loves this quarter is not guaranteed to survive the next.

Everything outside those guarded lanes can be allowed to breathe. And the piece most technology functions still resist is the one that makes the rest work: replacing the slow no with a fast yes. If a team can get a governed, single-sign-on-enabled, data-classified answer in two days instead of eight weeks, the incentive to go around the process largely evaporates. Shadow IT is, in the end, an arbitrage on institutional slowness. Close the speed gap and you close the arbitrage far more effectively than any policy ever will.

There is a bottleneck to name here, because it is almost always a person rather than a policy. In most organisations the slow no has a single face: one security architect, or one

small review board, through whom every request must pass, and whose queue grows without bound because approving is careful work and there is only so much of one person to go round. The steward's model does not fire that person; it changes their job from approver of every case to author of the lane — codifying, once, what a safe adoption looks like, so that the ninety routine requests approve themselves against a published standard and the scarce expert judgement is spent only on the ten that are genuinely novel. That is the difference between a control that scales and one that simply accumulates a backlog and calls it rigour.

---

*"You cannot police your way out of a problem your own slowness created. You can only out-serve it."*

---

I am not arguing for surrender, and it would be dishonest to pretend the steward's model is comfortable. It asks technology leaders to give up the clean defensibility of it was on the approved list and accept a messier accountability for outcomes across an estate they no longer fully choose. It asks for investment in identity and data plumbing that never demonstrates on a slide as neatly as a rationalised catalogue does. That is a harder story to tell a board than a remediation programme with a tidy end date. But it has the singular advantage of describing the world as it now is.

## 5. What "Now What" Actually Asks

---

The organisations that will come out of this period well are not the ones that most successfully turn the clock back to a February that is not coming again. They are the ones that read those three hundred tools correctly — not as a lapse to be corrected, but as the most honest piece of user research their technology function has had in years.

Every one of those tools is a sentence in a very long letter from the organisation about where the official channel failed it. The gatekeeper reads that letter as a charge sheet and starts issuing corrections. The steward reads it as a specification.

The tools are not going back behind the gate, because there was never really a gate — only a queue that people were willing to stand in until, one week last spring, standing in it stopped being an option. The task now is not to rebuild the queue. It is to become the kind of technology function fast and trustworthy enough that no one wants to leave it.