ACCESSREVOKE RESEARCH · 2026

The State of Offboarding

What IT security, compliance, and HR leaders told us about the last step nobody fully owns.

Based on direct conversations with IT security, compliance, and HR professionals across the region, at companies ranging from 10-person consultancies to national banks and telecoms.

Methodology

Between April and May 2026, we reached out to more than 70 IT security, compliance, and HR professionals, primarily across Serbia and the wider CEE region, at companies spanning software and IT services, banking and insurance, gaming, telecom, and consulting. This report draws on the in-depth, open-ended conversations we had with those who responded — security engineers, SOC analysts, IT security managers, one HR business partner, and several consultants specializing in identity and access management.

We asked a simple set of questions: what happens, today, when someone joins, changes roles, or leaves your company? Who owns it? How long does it take? Has access ever been left in place longer than it should have been? The answers were more candid, and more consistent, than we expected.

Five patterns showed up across nearly every conversation, regardless of company size, industry, or how mature the respondent considered their own process to be.

01

The mover gap is bigger than the leaver gap

Most organizations we spoke with have some real process for when someone leaves — a ticket, a checklist, an exit interview trigger. Far fewer have an equivalent process for when someone changes roles internally. Several security leads described the same pattern, independently: an employee moves teams or gets promoted, receives the access their new role needs, and keeps the access their old role had. Nobody removes it, because nobody's process treats a move with the same rigor as an exit.

> *“It's not a leaver problem — it's a mover problem,” one information security and compliance expert told us, describing it as the single most common source of what he called ‘excessive rights’ in every organization he'd worked in.*

Over a few years and a few internal transfers, an employee can end up holding permissions nobody can fully account for — not through negligence, but because the mental model of “offboarding” is built almost entirely around the exit, not the transfer. The mitigation several people pointed to wasn't better tooling; it was periodic access audits — a manual check that catches, after the fact, what the process itself doesn't prevent.

02

No one has a single, centralized tool for the whole lifecycle

Even at companies with genuinely mature security practices, access across the employee lifecycle is managed through a patchwork: an identity provider for the core directory, scripts for some systems, tickets and manual steps for the rest. “The process is partially automated, but still relies heavily on manual steps and internal procedures,” one identity and access management consultant told us. “In some cases we use scripts, but there's no centralized tool that covers the whole lifecycle.”

That same consultant described exactly the failure mode this creates: offboarding is initiated by HR or a manager, then IT manually revokes access across a half-dozen different systems — the directory, SaaS apps, VPN — and the whole thing depends on timely communication between teams that don't share a system of record. Asked directly whether access had ever been left in place too long, the answer was yes — not because of a technical failure, but a communication delay.

03

HR starts the process, then has to trust it finished

At companies with the most mature process we encountered, offboarding is genuinely cross-functional: IT, HR, the departing employee's manager, procurement for equipment, finance, sometimes legal — each responsible for their own piece. HR typically starts the process in a system, which fires off notifications to everyone else involved. But once that trigger fires, HR's visibility largely ends. They can confirm they started it. They generally can't confirm it finished — everywhere, for everyone.

> *“The ideal process is disabling the AD account, removing every group, revoking building access, email, the company phone,” one respondent said, before adding: “in practice, it's never that clean. It's usually whoever on the team has similar responsibilities, and HR promises everything and then forgets.” The same person described this happening more than once, adding that they'd simply been fortunate the departing employees hadn't noticed the access they still had.*

04

Automation is wanted — but only with a human at the final step

This was the most consistent finding, and the one that most complicates the idea that this problem just needs more automation. The most experienced security leads we spoke with weren't resistant to automating offboarding — they were specific about wanting a person to confirm the last step before it executes.

One respondent, reflecting on automation in security more broadly, put it this way: “I've seen an AI-driven tool take down half of a production environment. Automation is valuable within a defined scope, with monitoring, but the final decision has to sit with a person — no matter how good the system is, there are situations that need judgment a model wasn't trained on.” Another, at a regional bank, was more blunt: full automation of deprovisioning “isn't logically possible — at best you automate parts of it, but someone still has to go step by step and check that the user was actually removed.”

The organizations that had already automated the most — a telecom operator, a fast-growing SOC team — hadn't removed the human from the loop. They'd removed the busywork around the human: the checking, the chasing, the remembering. The decision itself stayed exactly where it was.

05

The purchase decision rarely belongs to one person

Asked who would actually decide to adopt a tool like this, almost no one named a single role. Answers ranged from “the technical director” to “senior management” to, at a larger regional group, “decisions like this are made at group level — CEOs, general managers, and HR together.” At one company, the answer was more specific still: several people, with price as the deciding factor among them.

At larger, more corporate organizations, several respondents pointed to something structural: purchases in this category tend to require a formal tender process, involving IT, HR, and finance at minimum. Whatever the exact path, the pattern was consistent — this is a committee decision, not an individual one, and any vendor selling into this space should expect to need buy-in from both a technical evaluator and a non-technical stakeholder before a deal closes.

What this means

Put together, these five patterns describe a problem that is well understood and consistently under-solved — not from a lack of awareness, but because the tooling that exists is built either for a scale these organizations haven't reached, or for a single system rather than the handful most companies actually run on. The gap isn't a mystery to the people living with it. Every person we spoke with could describe exactly where their process breaks, usually within the first minute of the conversation.

The tools that will actually get adopted in this space will need to do three things at once: cover the full lifecycle — joiners and movers, not just leavers — across every system a company actually uses, not just the primary directory; keep a human confirming the final, consequential step; and produce a record that satisfies whoever eventually asks for proof, not just whoever configured it.

This research was conducted by the team at AccessRevoke, which builds self-hosted access automation for the joiner-mover-leaver lifecycle. If you'd like to talk about what we found, or share how this looks at your own company, we'd like to hear from you — accessrevoke.com.