Lumos

The Modern Access Review Playbook

Turning a quarterly compliance burden into a continuous security control.

Why access reviews stopped working

Traditional access reviews were designed for a world that no longer exists. The control was built for annual compliance cycles in a few on-prem systems. But today, most enterprises use hundreds of SaaS apps, adding new ones every week. The same review framework, built on static spreadsheets that track slow-moving environments, is now supposed to manage a moving target.

The result is a process that feels cumbersome and yields little. Managers must certify hundreds of entitlements without knowing what each one does. IT teams chase down signatures across Slack, email, and tickets. When the cycle finally ends, much of the access that was "reviewed" remains unchanged. The audit gets cleared, but the risk does not.

The sneaking cost of broken reviews

Every quarter, identity teams pay a tax in three currencies: time, trust, and security.

Manager fatigue

Reviewers face countless checkboxes without knowing what each entitlement actually grants. After a few hours, every screen looks the same. Rubber-stamping becomes a survival tactic. The cost is paid twice: once by the manager doing the work, and again by the security team later when an incident is traced back to access that was signed off as appropriate.

Drift between cycles

A review is a snapshot, not a film. Joiner-mover-leaver workflows handle joiners and leavers reasonably well, but movers—employees who change roles, get promoted, or take on interim projects—end up accumulating access that is appropriate one moment and inappropriate the next. Most over-provisioned access happens not due to mistakes but because people are doing their jobs.

Audit gymnastics

Evidence gets pieced together from spreadsheets, screenshots, and exports. Auditors covering SOC 2, ISO 27001, HIPAA, and FedRAMP increasingly ask for fresh evidence rather than quarterly attestations. The window in which a once-a-quarter review can be seen as "continuous" by an auditor is closing.

As identity continues to rapidly shift, traditional access reviews are falling further behind on both fronts: auditors expect compliance from environments too large for teams to handle, and environments growing too rapidly to audit are leaving teams unable to maintain secure access.

Where the existing toolkit falls short

The market has tried to tackle this problem in three ways. Each approach solves part of the issue, but none solve all of it.

The problem lies in timing. Each category was developed when a different challenge was urgent, and the boundaries between them were drawn before SaaS, cloud infrastructure, and AI agents changed what “access” means in the enterprise. The tools function well in their specific areas, but they don’t connect across the gaps where modern access risk really exists.

The compliance-era playbook		Modern access reviews
Legacy IGA platforms Built for on-prem, with limited SaaS coverage and heavy integration maintenance	→	A real-time access graph spanning every SaaS, infrastructure, and on-prem app in the environment
Standalone UAR tools Good at orchestrating campaigns, but blind to provisioning and remediation	→	Reviews that connect directly into provisioning and remediation, so a “revoke” actually revokes
HRMS-driven workflows Catch joiners and leavers, but miss movers and entitlement drift	→	Continuous detection of drift, dormant access, and risky combinations between cycles
Spreadsheets and ticket queues Flexible, but unscalable and unauditable	→	Audit-ready evidence generated as the work happens, not reconstructed afterward.

None of these tools were designed for the volume of decisions a modern reviewer faces today. The solution isn’t a faster spreadsheet, a prettier ticket queue, or another integration point. It requires a different operating model—one that starts with a constantly updated view of access, applies intelligence to the decisions that need to be made, and treats remediation as part of the same workflow as detection.

As environments grow exponentially, the path to modernizing access reviews is through Identity Security Agents that can reduce the operational load on teams."

The four pillars of a modern access review

A modern access review program isn't just about running campaigns more frequently, it's about changing the unit of work. Reviewers need to see the decisions that matter, while low-risk access and is managed automatically by identity security agents. When a decision is made, the remediation should happen immediately, with an audit trail produced as a byproduct and not a separate project.

This model differs from simply “doing the same thing, but with a better interface.” It acknowledges that the number of access decisions in a modern enterprise is too high for human attention to scale linearly, and that the right approach is to focus human attention only on the decisions where context is missing or risk is real. Everything else should be handled by the agents built to handle those tasks for your unique organizational needs.

Modern, Agentic Access Reviews

Context-rich certifications

Identity security agents collect usage data, last-access dates, peer comparisons, and risk signals, and present the priorities to reviewers. Decisions take seconds, not minutes, and rubber-stamping fades away.

Automated decisioning

Low-risk, clearly appropriate access is certified automatically by the agent. Human reviewers concentrate only on edge cases, including privileged access, dormant accounts, anomalies, and toxic combinations.

Remediation built in

When a reviewer revokes access, the identity security agent instantly removes it across all impacted systems. There's no ticket queue, no manual follow-up, and no “pending” items for the next cycle.

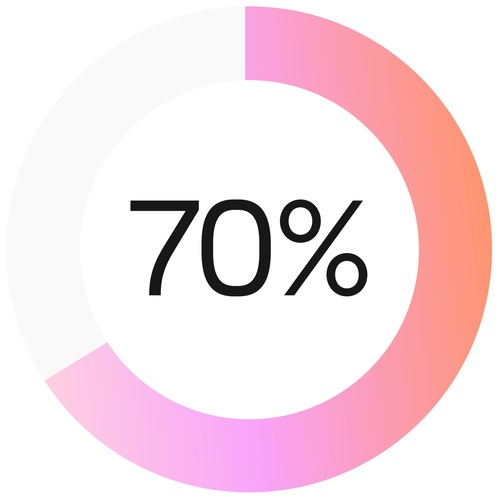
Audit-ready by default

Every decision, signal, and approval is tracked in a continuous evidence trail. Auditors get a real-time view rather than scrambling at audit time.

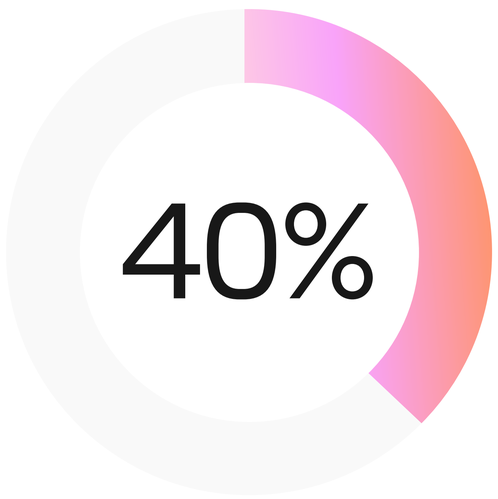
Identity security agents are built around these pillars, transforming access reviews from an event you endure into a continuous control you can run without needing to expand the team. Access is continuously certified, drift is detected between cycles, and the review process integrates into everyday access governance instead of being just a quarterly burden.

Proof from the field

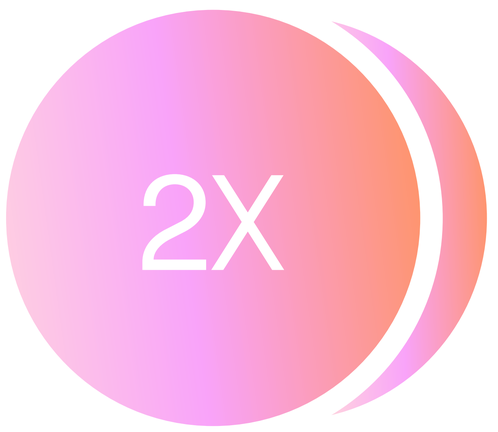
Identity teams conducting agentic access reviews with Lumos are already benefitting from the time savings, security improvements, and increased audit confidence. Here are three examples from public Lumos customer stories:



Faster access reviews at Netskope, with an 80% reduction in standing access.[1]



Less time on access reviews at Marqeta, across 150+ managed apps.[2]



Access reviews completed at ChargePoint, with zero compliance errors.[3]

This is a clear pattern: when the work shifts from tracking checkboxes to assessing real risk while agents handle the rest, teams complete more reviews with less effort and end up with cleaner access than they started with.

1. https://www.lumos.com/stories/netskope
2. https://www.lumos.com/stories/marqueta
3. https://www.lumos.com/stories/chargepoint

A reviewer's checklist for the next cycle

If you are preparing for your next access review cycle, use this checklist to test your current approach against the modern playbook. Any "no's" indicate a starting point for improvement.

- Reviewers see the context they need to make informed decisions—not just entitlement names.
- Low-risk, clearly appropriate access is auto-certified, allowing reviewers to focus on edge cases.
- Privileged access, dormant accounts, and toxic combinations are flagged automatically before the cycle opens.
- Revocations remove access instantly across all connected systems.
- Drift between cycles is monitored continuously, not delayed.
- Reviewer effort is decreasing, even as the number of apps grows.
- Audit evidence is created as the work happens, not put together during audits.

See it in action

Lumos transforms access reviews from a quarterly burden into a continuous control. It's built on a real-time access graph, with reviewer context, automated decision-making, and instant remediation all in one platform.

To see how Lumos can shorten your next review cycle while strengthening your access posture, request a personalized walkthrough at lumos.com.

Book a Demo