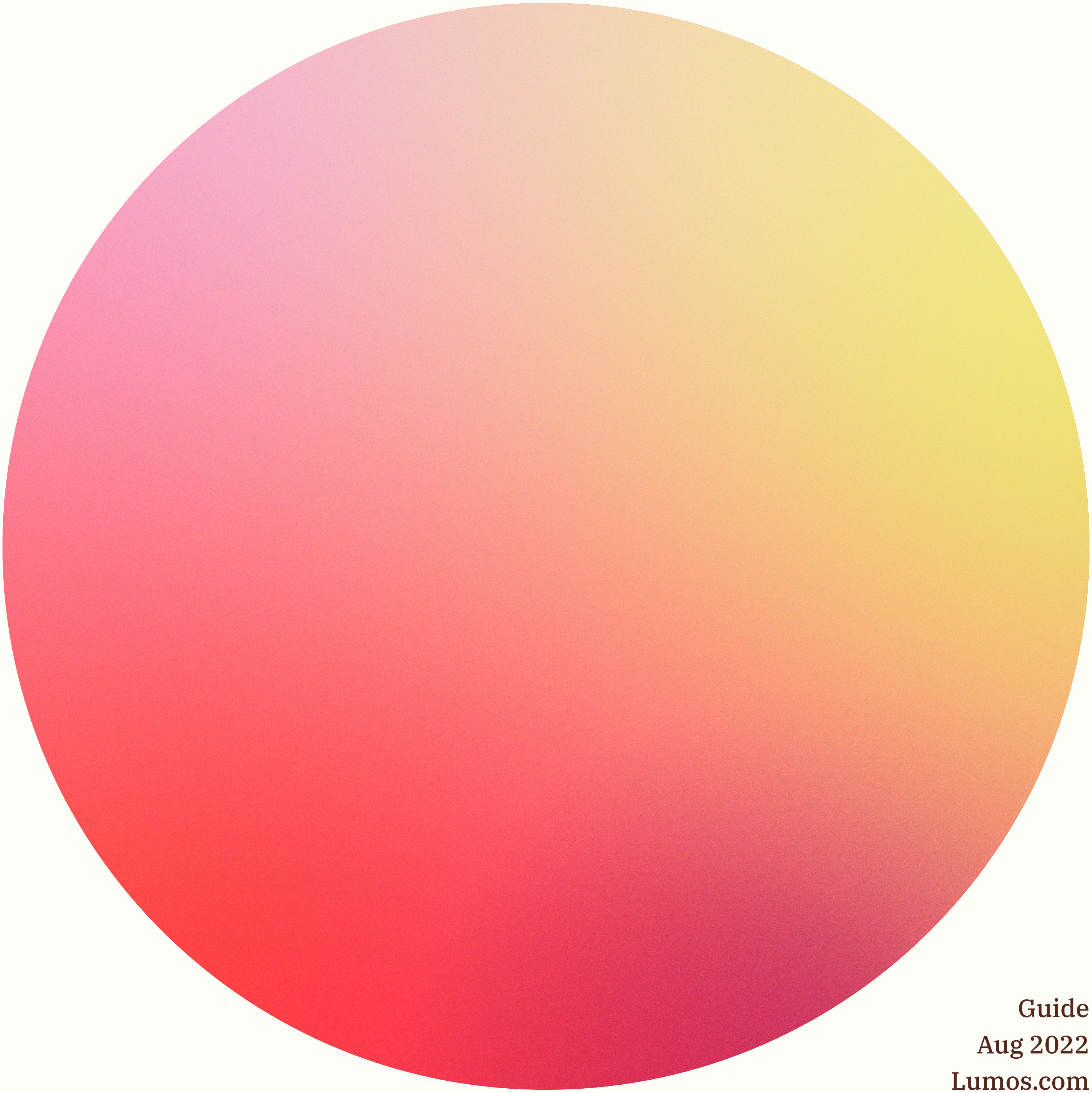
# Least Privilege Access: The Good, The Bad, and The Better Way

By Alan Flores-Lopez
Co-Founder @Lumos



Guide
Aug 2022
Lumos.com

# Introduction

Least privilege access is something all IT teams shoot for–but achieving it is easier said than done. It’s a powerful approach that grants the least amount of privilege necessary depending on who is requesting access and the context of the request. It’s the difference between having a key that works on every door and one that only opens certain rooms, depending on who you are.

It’s not uncommon for employees to have access to hundreds of company-sanctioned apps. Each employee must have enough access to do their jobs but not too much access to cause security threats or compliance issues. It’s a fine line between too little, too much, and just right.

Okta was hacked in January 2022. Hackers breached a third-party customer service firm, controlled a support engineer’s machine and used that person’s access to view Okta’s customer data!

In a “Zero Trust” environment, you assume that people will get compromised. Protecting yourself starts with reducing privileged access. Unfortunately, people often have more access than they need.

Least
Privilege

Or, once they receive access they never lose it. In fact, Segment did an analysis in 2020 regarding internal AWS admin privileges. Basically, they calculated the number of access points that had an admin role and how many of them were actually used. They had 689 admin access points and 60% of them were NOT used in the last 30 days.

People having too much access can lead to major problems. After the hack, Okta is further modifying their customer support tool to restrictively limit what information a technical support engineer can view. So, next time somebody gets compromised the blast radius is limited.

What happens when IT departments can't *perfectly* walk the least privilege tightrope? It creates access offenders. And those offenders can open you up to threats, bog you down, cost you money–or worse–your business.

IT centralizes access requests and reviews to make the process more efficient while keeping the company cost-efficient, compliant, and safe. But centralization and the admin work that goes along with it makes things worse for everyone. Employees are stuck waiting while IT is trying to surf the huge wave of requests.

More importantly, how can IT teams adhere to least privilege access and ensure their access reviews are up-to-date–without spending every minute of every day manually reviewing?

## Centralization + The Admin Work Web = The Enemy of Least Privilege

That’s why we’ve created this guide. This article is about how to implement least-privilege in your company to  protect yourself against security threats. You might think: “Phew, least-privilege is hard to implement.” It doesn’t have to be. The question is…why does it seem so hard to implement?

We’ll walk you through the list of offenders, why least privilege access is still a problem, and give you a step-by-step guide showing you how to fix it without setting yourself up for late nights and early mornings.

*Let’s get started.*

## The Access Offenders

First, let’s talk about the who’s who list of access offenders. One of the biggest issues here is that this problem covers a large surface area:

**The overprivileged admin:** It’s easy to dole out admin privileges because employees will never have to request additional access. But people with admin privileges who don’t actually need them are dangerous: **80%** of all hacks can be attributed to privilege abuse.

**The background lurker:** Employees likely have access to apps they don’t need or access they don’t even know they have–and it puts a dent in the bottom line. Fun fact: **25%** of all licenses allocated are not used.

Fun fact: 25% of all licenses allocated are not used

**The ticket submitter:** Employees are assigned access based on their roles and teams, but standard access can result in underprovisioning. If employees don’t have enough access they submit IT ticket requests–which creates more work for IT teams, slows their productivity, and can negatively impact company revenue.

**The (privilege) creeper:** Giving employees more permissions than they need is common, but overprovisioning comes at a cost. The difference between what they have and what they need is privilege creep. Privilege creep opens up a greater attack surface, giving hackers more opportunity to infiltrate.

## The Issue With The SOC 2 Framework

**Oh, and the SOC 2 compliance framework isn't much help.** A second issue is that there's no guidance:

SOC 2 compliance is important, but the framework around least privilege is vague. The guidelines say that companies are "required to follow least-privilege policy," but offer no roadmap to get there. It's up to each IT team to determine what compliance looks like for their company.

We've established that achieving least privilege access is super important, but it's also extremely difficult. And that begs the question: **Why hasn't this problem been solved?**

**Because it's a leaky bucket.** Companies are using tons of apps and they're adding more all the time. IT must assign permissions for each app and user and one or two admins are tasked with removing privileges or licenses that are no longer needed. And nobody has time for that.

Outside of accepting that some things will fall through the cracks, what can you do? Stop doing things the old way. You're managing an APPocalypse. No one team can manage the influx of permissions requests and access reviews. There simply isn't enough time in the day. Instead, focus on self-governance with time-based access.

## Self-Governance as a Solid Solution

*Let's start with the principles of self-governance.*

Self-governance starts with decentralization. Rather than relying on IT teams to manage and monitor permissions and privileges, users can get what they need on their own with the click of a mouse.

Think of it like a vending machine. People put in their money (or in this case, credentials), get their snack, and walk away. No IT help needed at all.

Self-governance gives admins peace of mind because employees only use the apps and permissions they need and lose access once their needs change. Individuals become more productive while the enterprise is more cost-efficient, compliant, and safe.

Self-Governance

## Getting Started With Self-Governance

- **Make it convenient.** Employees will almost always take the easiest path to value. In order to make individuals act in a responsible way, the compliant path must also be the most convenient path.
- **Banish the bottleneck.** A central entity creates bottlenecks. It's also the leaky bucket. Employees request access from IT and then they wait. And if IT is busy, they sometimes wait some more. Decentralization allows companies to eliminate IT access request tickets, get them access to what they need, and make sure employees don't have access to things they shouldn't.
- **Relinquish control.** Instead of being the centralized execution arm, IT can become the company-internal platform that enables employees with the right infrastructure to act responsibly and effectively.
- **Lean on experience.** From buying phone apps to food to gas, we DIY every day. The enterprise can enable employees to solve any app problem on their own in a compliant and effective way. Instead of asking for support, companies can enable employees to help themselves quickly and responsibly.

40-50% of Access & Permission Request IT Tickets have a TTR of 19 hours. Companies that leverage the Lumos platform experience a TTR of around 4 minutes.

Check this out - 40-50% of Access & Permission Request IT tickets have a TTR of 19 hours through ITSM. Companies that leverage the Lumos platform experience a TTR of around 4 minutes. That's the power of self-governance in action.

## Time-Based Access Gets Its Due

*Next, we'll move on to time-based access.*

A number of companies use role-based access control, or RBAC, to manage permissions. RBAC can be great–to a point. The downside of RBAC is that it views access as static. It also doesn't account for users who may need temporary access for a specific period to complete a designated task.

Instead, time-based access treats privileges as dynamic rather than specific to a role or team. Time-based access is often used in conjunction with activity-based access management. Users are given a window of time to perform a specific activity. Once the window closes and activity ceases the person's access to the app or specific permissions is removed. For example, Segment used a combination of time-based access and activity-based access removals to reduce permission sprawl by 90%. Yes, you read that right.

Getaround performed both quarterly access reviews and access reviews when an employee's role changed. If a person moved into a new position the manager was asked to recertify access. These two simple reviews allowed Getaround to remove more than 1,000 unused licenses.

### The Access Review Checklist:

- □ **Get the right app data**
- □ **Perform a VLookUp with HRIS**
- □ **Create columns for "accept access," "reject access," and "modify access"**
- □ **Send this form to app admins to complete**
- □ **Change users in the system and upload evidence (app admin)**
- □ **Send complete report to auditors**

Least privilege access is something every organization should have on lock (pun intended). Consider focusing on self-governance with time-based access and follow our checklist to ensure your organization is as secure as possible. Let’s avoid being the next headline about a massive breach!

## About the Author

Alan is a technical co-founder at Lumos, the AppStore for companies. Previously he was an engineer at Samsara.  He has BS/MS degrees in Computer Science from Stanford. He was the Head TA for the computer security course and did research in the empirical security research group. From time to time, Alan will go on opinionated rants about the future of technology.

Follow Alan on **LinkedIn**

## About Lumos

Employees shouldn't be admins for hundreds of web apps with excessive permissions. But then again, nobody wants to be stuck in IT ticket queues for days to get the right access. With Lumos, you make your company more productive and compliant with self-service app requests, access reviews, and license removals.

**Click here to try Lumos out**