3 Strategies To Rein In Access Sprawl

Lumos

Table Of Contents

3 Strategies to Rein in Access Sprawl 2

Drivers of access sprawl 4

Strategy 1

Close your integration gaps and see the full picture of access 6

Strategy 2

Develop an impact-based approach to access 8

Strategy 3

Create a culture of least privilege 9

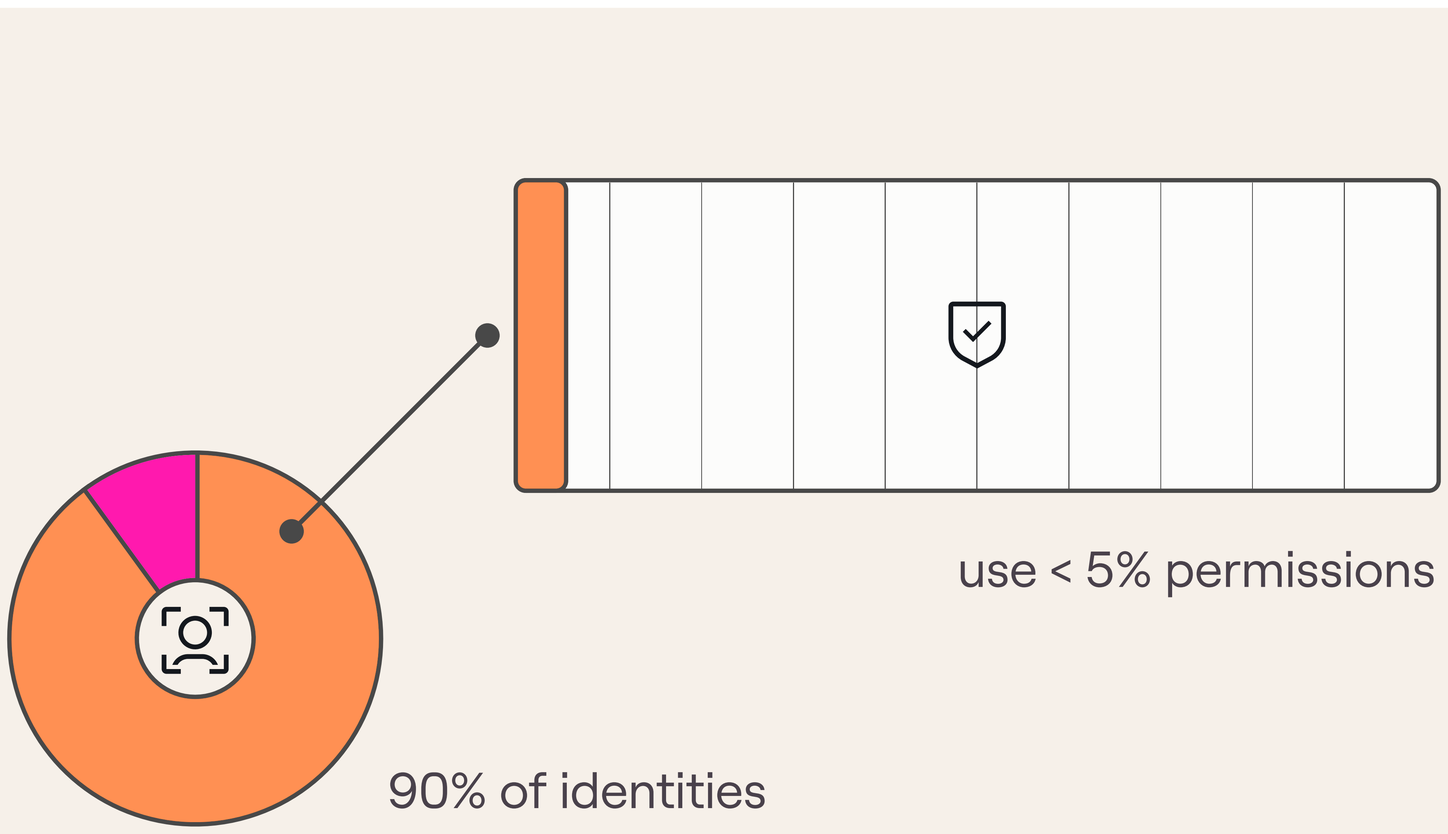
The Lumos Advantage 11

3 Strategies To Rein In Access Sprawl

Access Sprawl has been the predominant pattern of identity over the last decade. The size, scope, and complexity of identity and permissions has grown exponentially, while the capacity of IT, Security and GRC teams has, at best, grown incrementally. It wasn't so long ago that most organizations relied on just a few monolithic IT systems, hosted on-premise, with only the high-level access distinctions (i.e. "Guest", "User", "Admin"). Most of the tools we still use today for identity access, security and governance, were developed at this time.

Today's reality couldn't be more different, with companies using 600 or more apps, across cloud and on-premise, with detailed permissions governing access at the object level, and many more identities to manage, both human and non-human.

The failure to grow the capacity of identity teams to match the new scope of their work has led to unchecked access sprawl, as identities acquire more and more permissions which are never removed. In fact, Microsoft has found that 90% of identities use less than 5% of the permissions they have.



The risks associated with access sprawl are also growing. It seems like there are more security tools around every year, and companies have spent billions securing endpoints, and securing the network. But despite this investment, hackers become more successful each year. By 2024 the average cost of a data breach in the US was $9.8 million. A key reason for hackers continued success is failure to secure the identity attack surface. Hackers don't need to "hack" into your system. They just log in. 75% of all breaches depend on a compromised identity.

> "Hackers don't need to "hack" into your system. They just log in.

The good news is that, since identity is now the critical attack surface, and since most identities are extremely overpermissioned, companies that can successfully reign in access sprawl have an opportunity to improve security outcomes, in addition to increasing efficiency and reducing spend. In this whitepaper, we'll dive into the root causes of access sprawl and share three strategies you can implement to rein in access sprawl, reduce your identity attack surface and frustrate attackers looking to compromise your critical data and infrastructure.

Drivers Of Access Sprawl

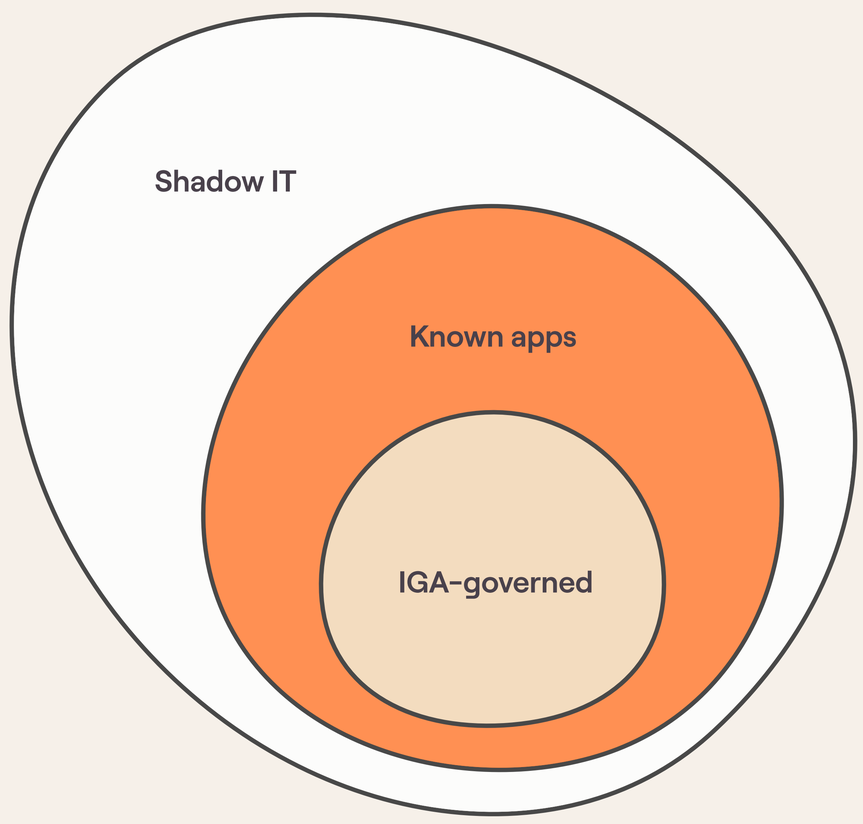
Adoption Of SaaS

SaaS offered huge benefits to companies: the ability to adopt best-class tools for each function, instead of being locked into monolithic platforms; the ability to seamlessly scale software needs with growth, and the freedom to experiment and swap out different tools as needs change.

However, it means that sensitive data and vital infrastructure has spread out across dozens or even hundreds of separate apps, each with its own authorization framework and language of permissions. Centralizing access management of SaaS requires integrating all of these disparate frameworks into a single platform for managing and securing access. Most organizations fail to do this, leading to a three-tiered system of access management with a small set of known critical apps subject to centralized governance through an IGA platform, a larger set of known apps that are managed via manual, ad hoc processes, and finally, a set of “Shadow IT” apps not known to IT and not subject to any security or governance processes.

Current status:

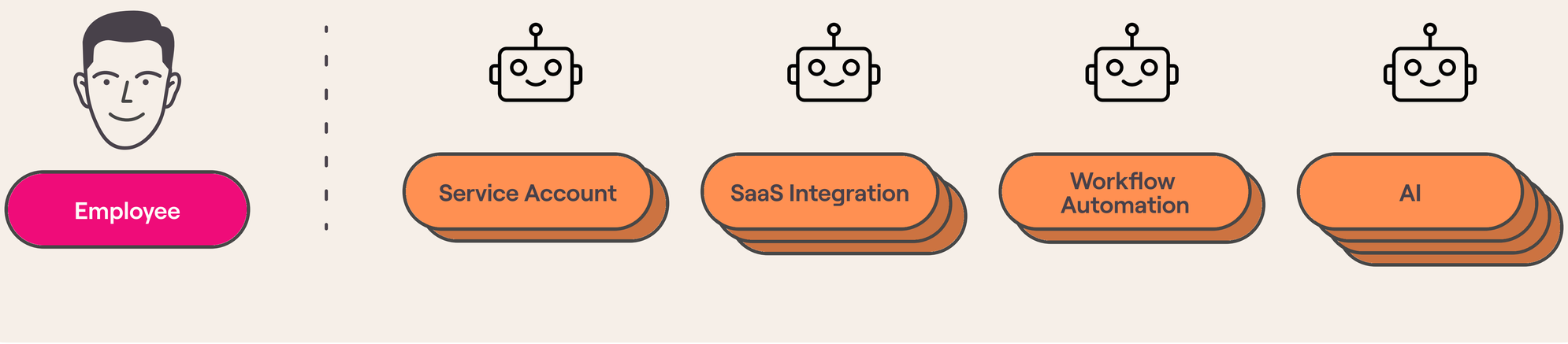
Three-tiered system of access management



Rise Of Non-Human Identities

Increased use of micro-services architecture, IPaaS, workflow automation and AI has caused an explosion in the number of non-human identities (NHIs), to the extent that companies now have between 20 and 50 NHIs for every human identity. NHIs are often completely overlooked by traditional IAM and IGA tools, which rely on HR systems as a source of truth. However, NHIs are at least as vulnerable to attack as human identities, perhaps more, given that they are usually not protected by MFA and that the credentials they use are vulnerable to discovery (for example, being found in source code).

So while the scale of managing just human identities has already become difficult for Identity teams to reach, the full problem of managing access is orders of magnitude larger still.



Access Removal Is Not Incentivized

A final and often overlooked driver of access sprawl is our work culture itself, and what kinds of work are incentivized. Employees are incentivized to complete work. Engineers must ship code, product managers must deliver features, marketers must produce measurable campaigns. All of this requires access to key data and systems, and IT and security teams face considerable pressure not to be a blocker for employees. In other words, there is always going to be more urgency to grant needed permissions, than to remove unneeded permissions.

So without a concerted effort to prioritize access removal, permissions will continue to accumulate to employees as they grow and move within the organization, creating de-facto super accounts that can be incredibly destructive if compromised or misused.

Strategy 1

Close Your Integration Gaps And See The Full Picture Of Access

The first step you must take to combat access sprawl is to establish complete visibility into access for each identity across all of your apps and systems. To find and remediate over-permissioned identities you need to be able to see all the access they have. Siloed security and governance processes won't work. But with companies using hundreds of SaaS apps, plus a mixture of cutting edge and legacy tech, custom and SaaS apps, cloud and on-premise, you need more than one method for integrating.

When evaluating an identity platform for integration completeness, you need to consider 4 key requirements:

1

Out-Of-The-Box SaaS And Cloud Infrastructure Integrations

Your modern SaaS tools will have well-documented APIs for reading and writing identity and access data, so any identity platform you consider should come with a large library of pre-built integrations.

When evaluating an integration library, look beyond just the number of integrations supported and consider:

- Are your key applications supported?
- What level of detail is supported by each integration? For example, can you see detailed access information at the object or role level? Or are you limited to seeing access at the app level?
- What capabilities does each integration support: for example are integrations read-only? Or can you actually update identities and permissions.

A Flexible Framework For Custom Integrations

However large an identity tool's integration library might be, you should expect to have to build a large number of custom integrations in order to build a complete picture of access. Tools that require you to build to a rigid development framework, limit you to developing in a single language and runtime, or require you to deploy integrations on their platform will all slow you down too much.

Look for a flexible, API-based integration framework that will allow you to build self-hosted integrations in your preferred languages and runtime. Also, make sure that you are able to create lightweight integrations focused on access to your critical data and functionality (see Strategy 2).

AI Assisted Development To Increase Velocity

Legacy IGA tools have long been held back by extended development cycles for integrations. If you're only able to onboard 5-10 applications per year, you'll never reach full visibility. The basic structure of your integrations will be similar from app to app, so look to leverage modern AI code-generation tools like Claude to spin up and test integrations fast.

In addition to increasing velocity, a well thought-out AI development program will also help you to consistently apply best practices across all your integrations.

Legacy Integration Support

Make sure you spend some time thinking about how you will integrate your older and on-premise systems. These systems are often not accessible by REST APIs or other modern connectivity protocols. So make sure your identity platform can support methods like CSV file uploads.

Don't let perfect be the enemy of good. You might not be able to support real-time integrations with your legacy systems, but a nightly or even weekly update via CSV still beats maintaining separate governance processes for old and new tech.

Strategy 2

Develop An Impact-Based Approach To Access

If you're successful at building a complete picture of access across all your apps, systems, and identities, you'll be confronted with a new problem. A decade of unchecked access sprawl means that the sheer scale of identities and access you can see will be daunting. Traditional approaches to identity governance rely on reviewing each permission one-by-one in some arbitrary order. Should Aaron have access to AWS? Should Brad have access to Bitbucket?...

Cost vs Risk

Few teams have the capacity to make this approach work across thousands and millions of permissions. To make progress, you need to acknowledge that some permissions are more important than others, either in terms of cost (such as expensive Saas licenses), or in terms of risk (such as access to sensitive data or critical infrastructure). Having achieved visibility into identities and permissions, your next step is to develop analysis and intelligence to help you find and focus on impactful access. For example, your BI tools should be able to surface:

- Identities or access that breaks known policies or best practices, such as separation of duties (SoD) violations.
- Admin-level access to apps.
- Access that is not actually used
- Outlier access such as access not shared by similar identities (same manager, same title, same geographic location, etc).

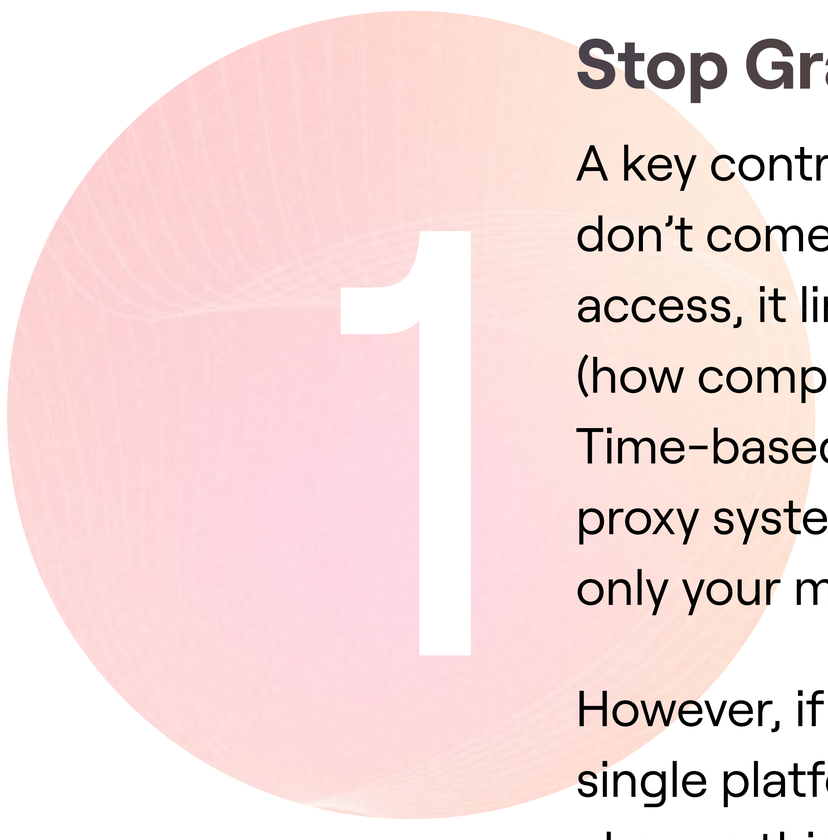
An impact-based approach stops you being paralyzed by the scale of the problem. Even if it's not possible to correct all access sprawl immediately, intelligent triage can make sure you maximize the security and cost-saving value of your work.

Strategy 3

Create A Culture Of Least Privilege

If you've been able to successfully implement strategies 1 and 2, you will have been able to make a significant dent in years-worth of access sprawl in your organization. It's now time to think about how to establish new best practices for Identity and access, and to change the practices that allowed access sprawl to become such a problem in the first place.

Here are a few ways you can get ahead of future access sprawl.



Stop Granting Forever Access

A key contributor to access sprawl is the fact that most access grants don't come with an expiration date. Unless you specifically remove access, it lingers forever, or at least until the employee is offboarded (how comprehensive are your offboarding processes by the way?). Time-based and just-in-time access do exist, but they tend to rely on proxy systems, are difficult to implement and are usually reserved for only your most critical data and infrastructure permissions.

However, if you have integrated all of your identities and apps into a single platform, and if you have the ability to update access, you can change this. Each access grant should include an end date, appropriate to the level of risk and to the business need. When the period expires, access can be re-granted if the business justification still holds, but unneeded and unused access never lingers indefinitely.

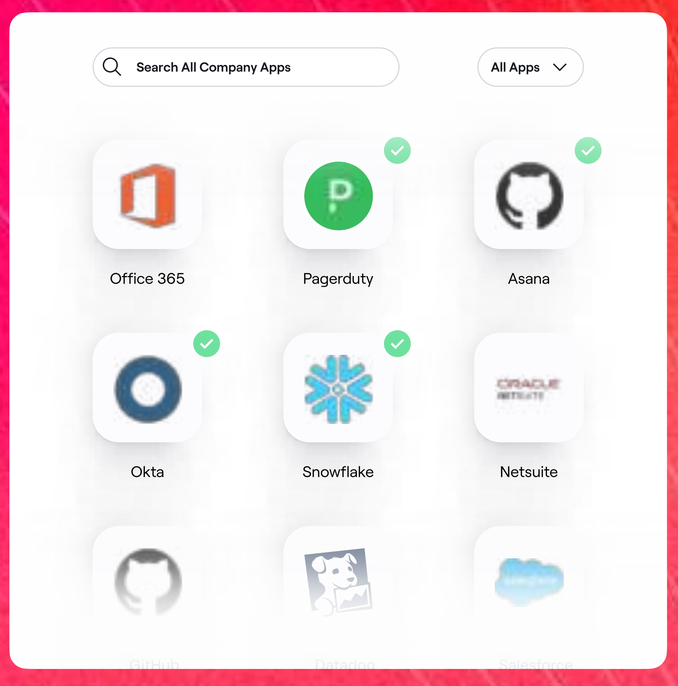
2 Automate Removal Of Unneeded Access

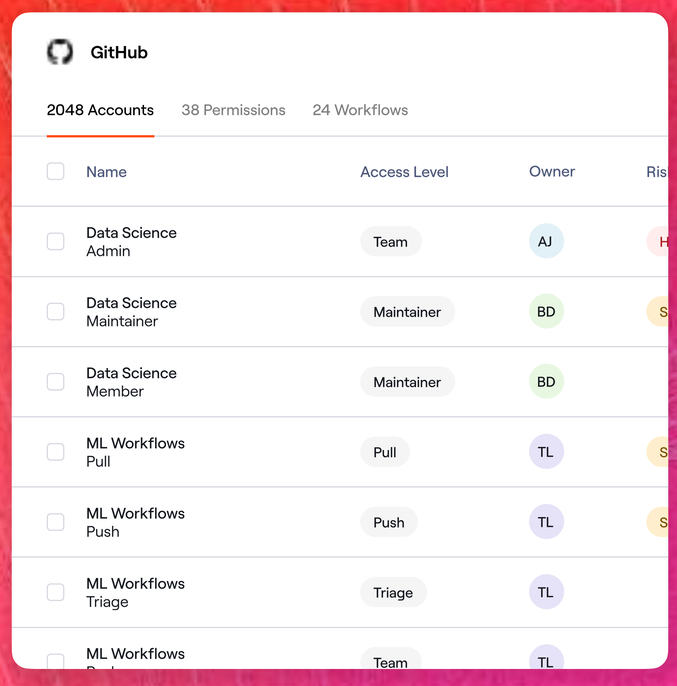
Wherever possible, your identity platform should be able to determine how often permissions are actually used. With this information, you can automate removal of unneeded access.

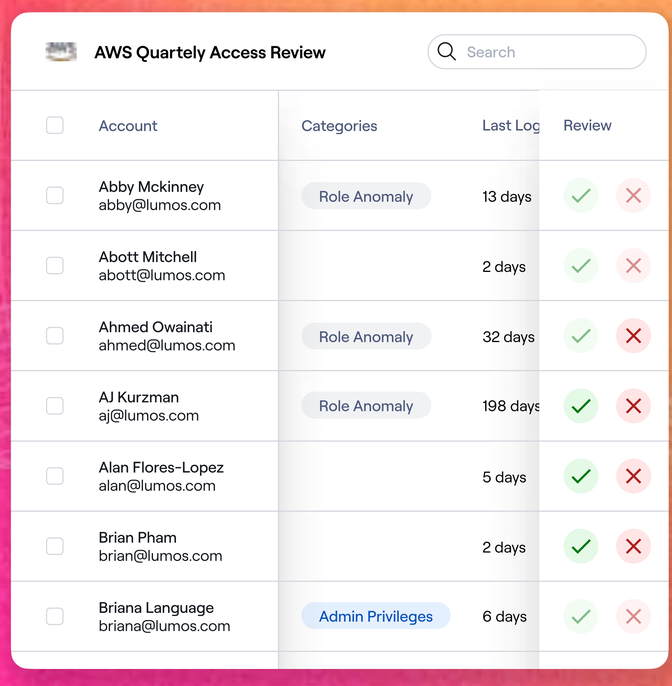
For example, if an identity has access to a critical database in Snowflake, but doesn't use that access in a 30 day period, that access should be automatically removed to be requested again when needed. A similar process can help you manage SaaS costs. If an identity has a premium license for a SaaS platform, but hasn't used any premium features this month, that identity could be automatically downgraded to a less expensive or even free tier.

3 Monitor Risky Access

Having taken steps implementing Strategy 2 to identify your most critical and risky access, don't wait for compliance-driven procedures like quarterly access reviews to revisit access to mission-critical resources. Create a discipline of reviewing risky access on a monthly or even weekly basis, and removing access that is no longer needed.







The Lumos Advantage

To learn more about how Lumos can help to stop access sprawl in your organization, schedule a personalized demo.

Lumos is the first autonomous identity platform to automatically discover and manage access across all your apps. Instead of being overwhelmed by the sprawl of apps and access, you reduce security risks, boost employee productivity, and cut costs – all in one platform.

Lumos helps you control access sprawl with:

- A full-featured integration suite including:
  1. Out-of-the-box integrations for SaaS and cloud platforms.
  2. A simple, flexible API-based development framework for building new integrations.
  3. AI-assisted integration builder to launch integrations fast.
  4. Tools for working with legacy apps, allowing for automated or near-automated capture of access data through flat file uploads.
- Access Intelligence and AI-driven insights that identify and surface high-impact access. Insights are built into common workflows like Access Reviews to make sure decision makers have the context they need.
- Automated workflows that actually help you remove insecure, outdated or unnecessary access without manual work, to stop the future spread of access sprawl.

About Lumos

Lumos is the first autonomous identity platform. It automatically discovers and manages access across all your apps. Instead of being overwhelmed by the sprawl of apps and access, Lumos empowers organizations with one unified solution that controls access on auto-pilot. Lumos customers can enhance security, cut software spend and boost employee productivity — all in one platform. Trusted by hundreds of companies, Lumos powers millions of access requests across global companies.

Learn more: https://www.lumos.com