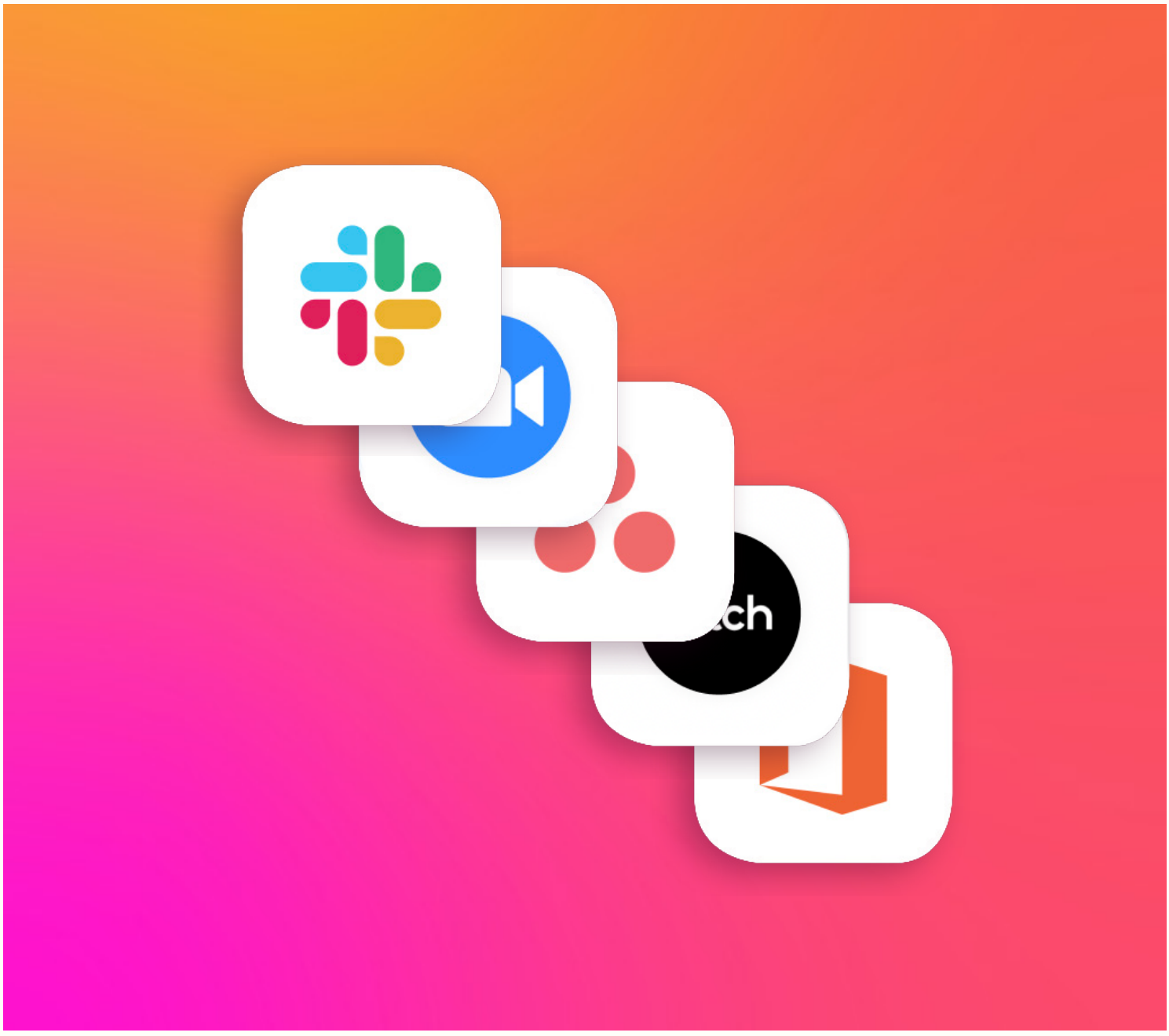
The **Lumos** Guide To

Identity Access Management

We break down the steps you need to take – and the questions to ask – as you lay the foundation for modernizing your Identity Access Management systems.



Introduction

The days of having a few servers on campus that power everything on a company's network have been ancient history for the better part of the last two decades. Networks today are sprawling, complex, and don't have physical perimeters.

While cloud apps and services have modernized the way people communicate at work and access information, they have also created a new security challenge for the stakeholders who manage identity and access management systems. With so many endpoints, and people using different usernames and passwords across services, IT teams with legacy identity and access management systems have a tougher job ensuring the wrong person isn't able to access confidential information, or launch a sophisticated cyber attack after infiltrating one of many endpoints.

"Older legacy identity management products have a real challenge with cloud integrations," said George Finney, CEO of Well AwareSecurity and author of Project Zero Trust. "As you get into bigger organizations, you can also start to worry about too much sprawl. That means that over time they get more and more permissions to do different things, and unless you're managing all of those different services' permissions globally, that is going to be a challenge."

It could also be a security nightmare. One report summed it up best: "Infrastructure access is snowballing out of control."

Zero Trust

While the industry is moving toward a Zero Trust model, where “never trust, always verify” is the motto, adopting a modern Identity Access Management approach can be a foundational step for companies who want to bolster their identity and access management systems and eventually adopt what is becoming a new industry standard.
“Having an identity and access management system is an accelerator for zero trust,” Finney said.

The term “Zero Trust” has been around since 2010, however the move toward it has accelerated after President Joseph R. Biden signed a White House Executive Order in May 2021, which calls on federal government agencies to implement plans to “advance toward Zero Trust architecture.” Many IT leaders, including those at companies that might conduct business with the federal government or hope to in the future, are also strategizing about how they can get on the path to eventually adopting a Zero Trust model.

Zero Trust may be the long term goal, however many IT leaders are taking a slower, methodical approach before fully adopting it. Just 30% of IT leaders surveyed say adopting a Zero Trust model is a priority this year. By comparison, 80% of IT leaders from the same group say improving access management is one of their main strategic initiatives this year.

“Identity and zero trust do go hand in hand, particularly with the kind of the new technology models that are coming out, whether that’s secure access or service edge,” Finney said.
As IT leaders seek to integrate modern Identity Access Management into their IT architecture as part of their Zero Trust journey, here are some questions to ask and steps to take along the way.

Take inventory of your current Identity Access Management systems

The first step to adopting Identity Access Management begins with understanding how identities are currently managed. An estimated 60% of corporate data is stored in the cloud. And we're not talking about one singular place, but many. Now is the time to audit current access policies and user permissions – and chances are you'll have many, many places to look and will find varying policies. Think of some of the services employees use every day to check emails, send large files, chat with teams online and over video, pull analytics, and so much more.

Another important question to ask is "Who is managing permissions?" Verifying identities and granting access is already a tedious task leaving tickets piled up in the queue at IT desks, not to mention the time spent tracking down managers and other stakeholders who also need to sign off before someone new can log into a system. It goes without saying that this is not great for productivity. In one survey, more than half (53%) of people say it can take anywhere from hours to weeks for an infrastructure access request to be approved. A majority (88%) of respondents say those requests require at least two people to grant and approve access, while one-quarter say they have to wait on four or more people to get the job done.

Taking an in-depth look at how Identity Access Management currently operates will help you to identify gaps and areas where a modern Identity Access Management system can help improve the company's security posture.

Assess Your Goals

An important part of laying the groundwork on the road to Zero Trust is determining how Identity Access Management will fit into the micro parts of your company – think at the organizational level. Not every group will have the same needs, but ultimately your goals should align with the company's overall security architecture and requirements.

Partner with an identity and access manager

After understanding the current state of identity and access management across the company and identifying goals, the next step is to lay the foundation for a new Identity Access Management system.

"The foundation of zero trust is going to be built on identities," John Watts, a Gartner analyst, said on a podcast. "For example, if you have an identity provider, you can attribute who somebody is through that provider. That's very foundational to the zero trust philosophy. In fact, a lot of the zero trust concepts and the security policies are built around the concept of an identity and knowing who somebody is with some assurance, and being able to add context to that and say, 'If we don't know who somebody is, maybe we can add another level of assurance.'"

Set Up a Governance Team

Having a governance team in place is vital to making sure Identity Access Management runs smoothly throughout a company. Finney recommends that at least a few members of the team are people who have “deep, institutional knowledge” about the IT architecture across the organization.

“It ties your identity team, which is probably mostly technical people, back to the business. One of the unique things about identity is that it requires you to have a deep understanding of not just how business works, and what business processes there are, but also what department needs there are,” he said.

Educate Employees

Employees can be your biggest weak spot, or your first line of defense. If you haven’t already, now is a good time to set up Multi Factor Authentication to mitigate any risks of stolen credentials and unauthorized access. Employees should also receive regular cybersecurity information that educates them about strong passwords, safe browsing, and how to identify and report suspicious activity.

Document Everything

Foster a collaborative culture where stakeholders work with IT to document processes and share them in an organized place managed by the governance team.

“It’s such a great value add both for you as a security team, to be able to build that institutional knowledge, and be able to use it to train up new folks coming through,” Finney said. “It’s also a great way to give back to the business, because oftentimes processes are anecdotal and aren’t necessarily written down.”

The best part of implementing a “document everything” policy? It makes compliance so much easier, saving IT teams from scrambling due to issues or time sensitive requests.

“We’ve talked a lot in the industry about aligning security in the business. That’s what identity is, right?” Finney said. “That’s why I think identity is so key to success, when it comes to security.”
Interested in learning more about how setting up solid IAM paves the way for strong zero trust foundation? Let’s chat.