ConductorOne

Guide to Modern IGA

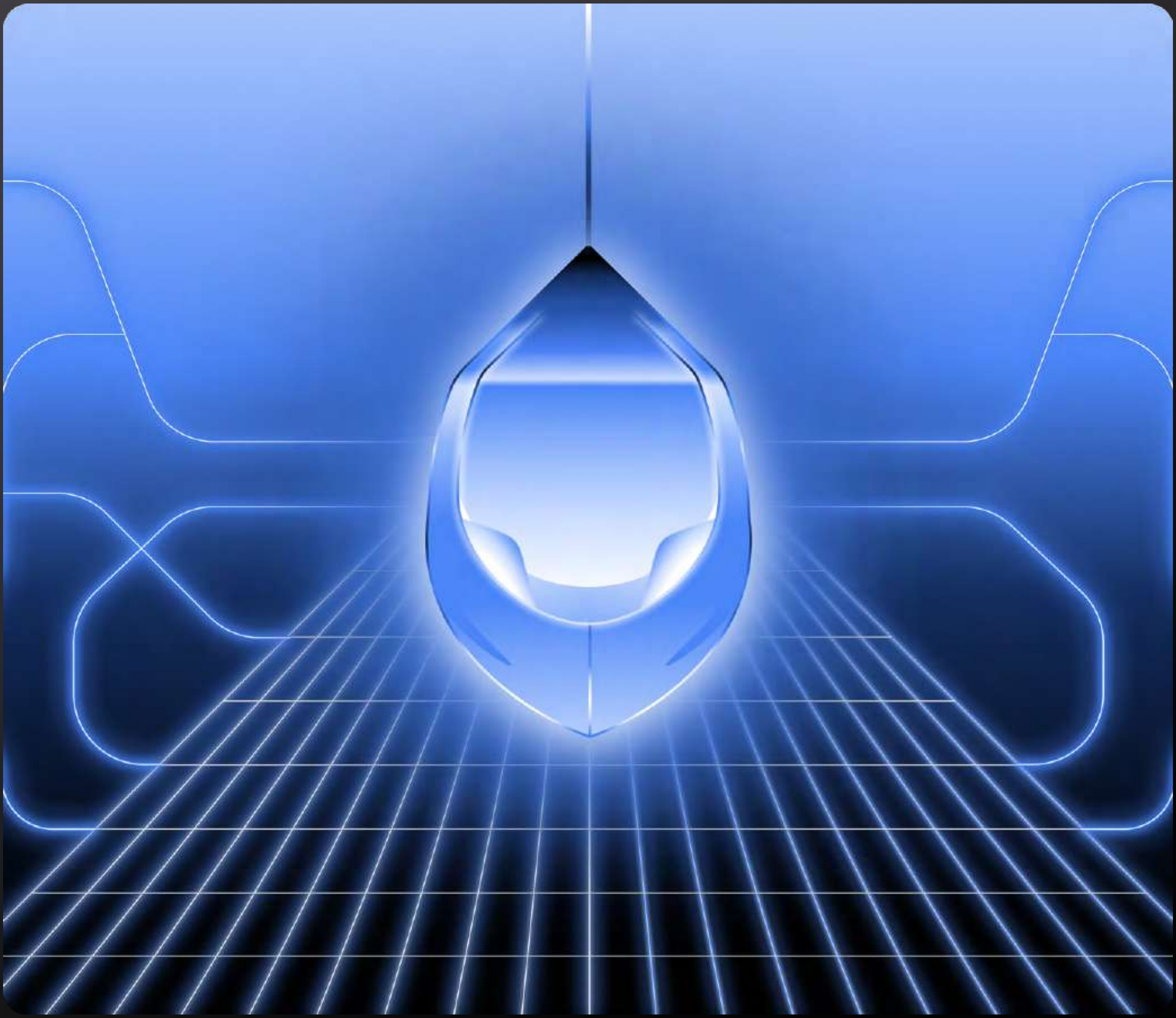


Table of Contents

Introduction

It’s been over a decade since Gartner officially recognized “identity governance and administration” (IGA) tools as a growing category in the identity and access management (IAM) market. These tools, which combined provisioning and governance capabilities, were developed to help large enterprises ensure that only the right people got access to sensitive digital data—to improve data security and comply with emerging cybersecurity regulations.

Today IGA is a well-established market dominated by legacy players who’ve been around for more than twenty years, since well before the category had a name. In that time, the essential goals of IGA haven’t changed, but the challenges—and stakes—of meeting those goals have increased dramatically.

The amount of data we now produce, and the ways in which it’s created, stored, and accessed, have exploded, and cloud computing and remote work have transformed where and how identities interact with that data. The number of identities with potentially sensitive access—including employees, contractors, third-parties, and non-human identities—has skyrocketed.

This new landscape has exponentially expanded organizations’ potential attack surface areas—compromised identities with sensitive permissions have become a leading cause of data breaches. Getting control of access sprawl is now a critical security concern for companies of all sizes.

Twenty-year-old IGA solutions, built for the pre-cloud, pre-remote era, aren’t equipped to respond to this new reality. Modern business environments demand a fundamentally new approach to IGA that can meet today’s identity security and compliance challenges with the speed and flexibility of today’s technology. The identity security landscape has evolved—and IGA is evolving as well.

This guide will cover what’s changed since legacy IGA first hit the market, the security and compliance gaps created by those changes, and how modern IGA platforms are disrupting the category to create better security outcomes than the previous generation of tools. You’ll come away with a clear understanding of the benefits of modern IGA and what to look for in a modern IGA solution.

DigitalOcean

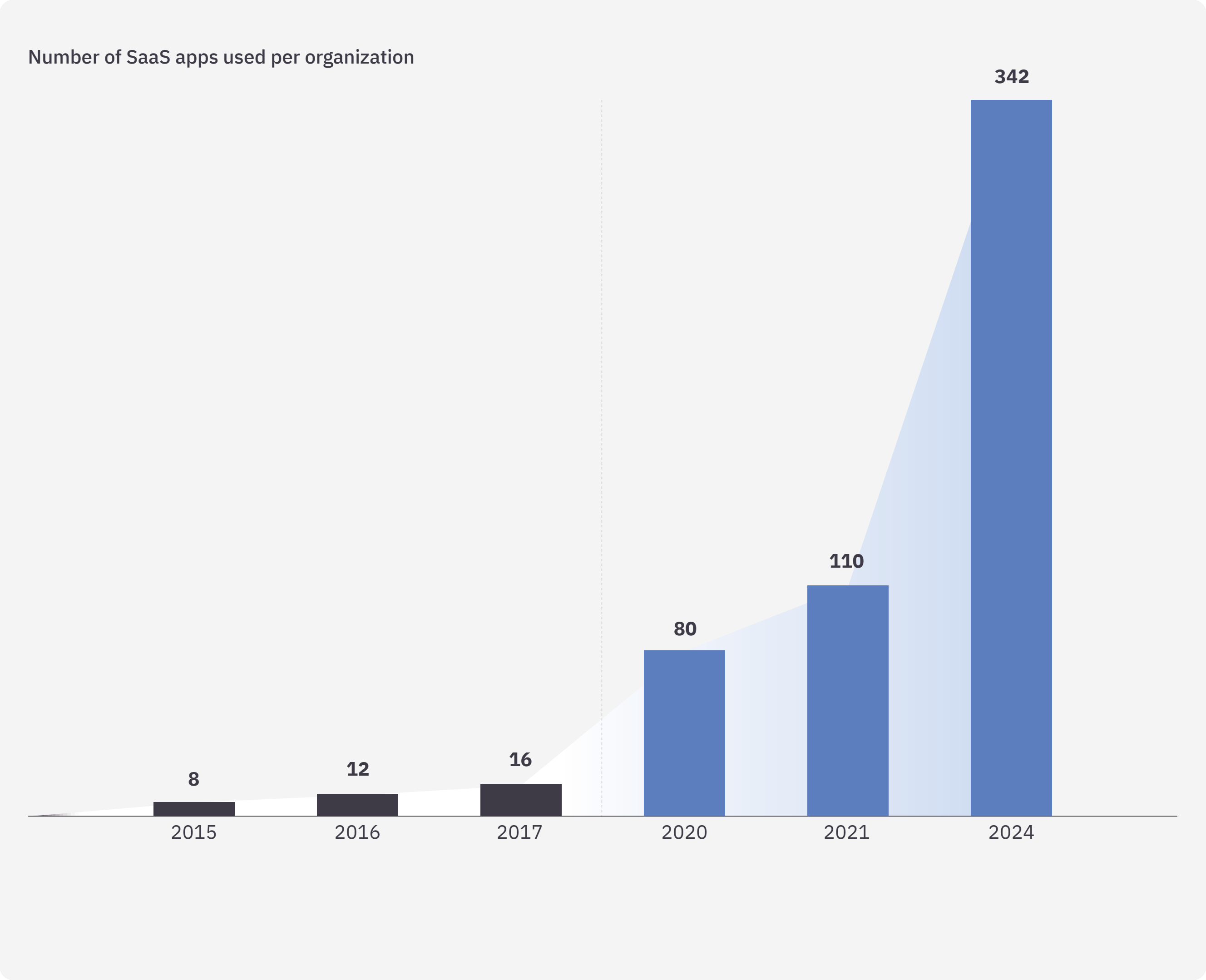
"Having a tool that can do this in a timely fashion, iteratively and repeatedly, enables very real security control."

Tim Lisko, Director of Product and Infrastructure Security, DigitalOcean

A new identity security landscape

RAPID CLOUD ADOPTION

Since 2015, the average number of SaaS applications used by organizations has skyrocketed from under ten to well over 300, and IaaS usage is growing just as fast. Gartner now forecasts that by 2025, enterprise IT spending on cloud computing will overtake that of traditional IT — and the trend shows zero sign of slowing down.



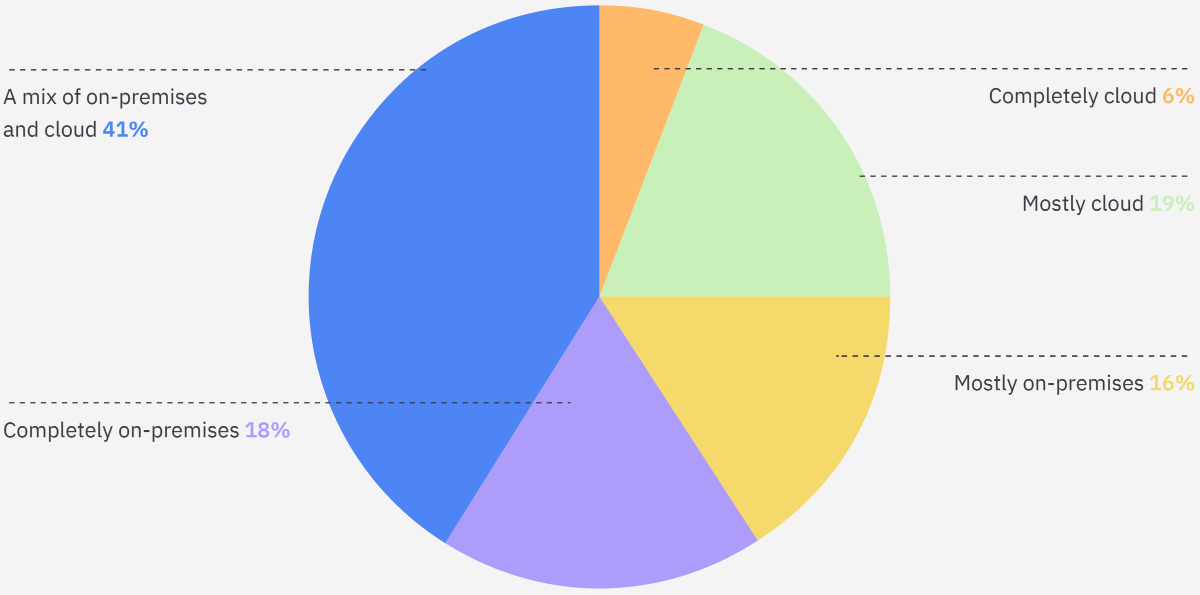
Multiply the increasing numbers of cloud-based software and infrastructure accounts by the number of employees, contractors, third-parties, and non-human identities accessing them and you get an explosion of permissions that can exponentially increase a company's attack surface area.

IT and Security teams are scrambling to keep up with this proliferation of cloud-based access, but momentum is against them. Depending on a company's size and needs, just a single cloud-based tool like AWS can comprise hundreds or more accounts and role-based permissions to provision and manage. Securing identity is no longer a human-scale task—teams need modern tools designed to simplify and automate management of these new systems and permission schemas.

COMPLEX ENVIRONMENTS

Of course, traditional on-prem systems haven't gone away. Of the over 500 IT and security leaders surveyed for ConductorOne's 2024 Identity Security and Outlook Report, 76% reported managing access across both on-prem and cloud systems. Hybrid environments are the norm.

How would you currently describe your company's technology environment?



These environments often comprise a tangled mix of legacy and newer apps and infrastructure, including homegrown apps and commercial off-the-shelf (COTS) software systems, each with its own permissions model and security vulnerabilities. Companies may also have multiple sources of identity "truth" to juggle in the form of identity providers (IdPs) human resource information systems (HRISs). Understanding what users have access to and how entitlements interact across these environments is critical to maintaining security, but companies are struggling to get full visibility into their systems, creating access blindspots that put their business at risk.

RAPID CLOUD ADOPTION

> *77% of security leaders reported instances of cyberattacks or data breaches at their organization in the past year due to improper or overprivileged access.* [*]

As security technologies have become better at detecting and thwarting attempts to break into systems, attackers have shifted strategies. Instead of breaking in, they're finding ways to simply walk through the front door, exploiting identity-related vulnerabilities created by today's access environments. With the advent of generative AI, phishing attacks in particular are getting incredibly sophisticated—falling victim to one is not a matter of "if" but "when."

Ensuring only the right people have access to sensitive data, and only for as long as that access is needed, is no longer an aspirational goal of a zero trust program—it's a critical must-do for reducing the risk of identity-related breaches. Recent overhauls to major compliance frameworks like the National Institute of Standards and Technology (NIST) Cybersecurity Framework and the New York Department of Financial Services (NYDFS) Part 500 that include tighter identity security protocols confirm this new imperative.

SYSTEM1

"Being able to show ConductorOne to internal auditors for SOX compliance, where they can generate time-stamped, immutable reports and see logs in one console, was impressive."

Jack Chen, Director of Information Technology, System1

Where legacy IGA falls short

Twenty years ago, only large enterprises with tens of thousands of employees and lots of on-prem systems needed (and could afford) the tools to help them govern access and maintain compliance. Today, companies of all sizes are struggling to manage access sprawl across disparate systems, and compliance with identity security best practices is business critical for every organization. But legacy IGA tools are still built with the assumptions of serving yesterday's enterprise customers.

According to Gartner, 50% of legacy IGA deployments end up in distress. While that number is shocking, it's no surprise to the many who've experienced it firsthand. Here's the far-too-common failure mode: twelve months into implementation and well over budget, having spent two times the cost of software on services, teams find themselves with only three apps integrated. These tools simply were not built to connect with newer technology and handle today's quickly evolving access landscape.

Legacy IGA pain points

LONG IMPLEMENTATION TIMES

Gartner cites overly ambitious initiatives and incomplete use case documentation as just two of the reasons why legacy IGA deployments fail. The underlying cause of both is outdated data models that require customers to do extensive, exacting systems and data prep before a legacy tool can be implemented. In a world where sophisticated SaaS and IaaS tools can be deployed in seconds, waiting multiple quarters to see ROI is hard to justify.

HIGH COSTS AND HIDDEN EXPENSES

Because implementation of legacy IGA solutions is convoluted and time-consuming, customers are typically advised to use professional services at a cost well beyond the contract price. Deployment fees can easily exceed the annual software price, usually at least doubling the first year cost. And some customers report having to buy additional hardware or services just to get things functioning as promised—after the contract is signed.

UNNECESSARY COMPLEXITY

Legacy IGA tools are positioned as solutions built to manage highly customized, on-prem environments, but customers complain the tools themselves create unwanted complexity. They have clunky, outdated user interfaces and gratuitous shelfware, and staff must go through weeks of training—to the point of needing certification—to operate them with confidence. This puts the IGA project in failure mode: when a tool is hard to use, users often find a way to work around it.

LACK OF INNOVATION

While legacy IGA solutions claim to be keeping up with technological changes, there's little investment in bringing their platforms up to date or innovating novel capabilities. Instead, updates come in the form of tacked-on features and third-party providers. Teams accustomed to configuring their environment "as code" and building workflows using tools like Terraform and webhooks will be frustrated by legacy IGA's lack of modern tooling, lack of extensibility, and slow (or no) response to feature requests.

POOR SECURITY OUTCOMES

Ultimately, a tool that's only partially deployed and can't be quickly updated or extended is a liability. Without full visibility and control across today's environments, companies are left with identity security gaps that leave them vulnerable. Further, legacy IGA was developed to manage identity in an era of birthright access, standing privileges, and once-a-year user access reviews—all considered security liabilities today. Modern companies who want to move to just-in-time access, zero standing privileges, and continuous compliance will find it harder to achieve these goals with legacy tools.

Even auditors—who are cautious to recommend new tools—are starting to discourage companies from purchasing legacy IGA products. In the end, long or stalled deployments of governance tools do nothing to improve compliance.

DigitalOcean

"ConductorOne is innovating in an area underserved by the technology industry, and solving problems a lot of teams have to do manually. That has a really big value for DigitalOcean."

Heather Cannon, Security Engineering Leadership, DigitalOcean

A new way to IGA

Governing access has historically involved a tradeoff between productivity and security. Whether done manually or with the help of legacy IGA tools, processing access requests, ensuring compliance with security policies, and regularly auditing access have always required significant time and effort. When resources and patience are stretched thin, shortcuts—like rubberstamping access approvals or granting unnecessary standing privileges—are taken in the name of keeping the business moving, despite the security risks involved.

Modern IGA solutions reject this tradeoff. They employ intelligence, opinionated workflows, flexible connectors, and automation and AI to remove complexity and streamline processes wherever possible. They're purpose-built to be quickly deployed and scaled so companies can achieve real security AND efficiency wins right away. Modern companies can't afford to wait to see value from their IGA tools, or to take productivity shortcuts that put their data at risk.

How modern IGA changes the game

TIME TO VALUE

Modern companies accustomed to cloud-based, immediately deployable software and infrastructure expect quick time to value from the security tooling they adopt. They want better security now—not in six months. Modern IGA solutions are designed to meet today's companies where they are and integrate with their existing technology stack quickly, providing security and compliance benefits in a matter of days to weeks.

FULL VISIBILITY AND CONTROL

Companies' greatest identity security challenge today is understanding and gaining centralized control over access in complex, hybrid environments. At their core, modern IGA solutions are sophisticated data platforms designed to solve this challenge—they intelligently ingest, normalize, and orchestrate fine-grained identity and entitlement data froma customer's systems to provide complete visibility and access control. This model inverts legacy IGA's approach to data, which requires customers to adjust their systems to fit the IGA tool's data model—resulting in vexing, complicated implementation, limited visibility, and inaccuracies.

SIMPLE, INTUITIVE DESIGN

Modern IGA tools are designed with admins and end users in mind. They strike a functional balance between flexibility and simplicity that makes them quick to set up, highly configurable, and intuitive to learn and use—no extensive training necessary. By integrating with tools end users are already familiar with, like Slack, Microsoft Teams, helpdesks, and CLI, modern IGA solutions support a "secure by default" approach to identity security. They provide access requesters, approvers, and reviewers a seamless experience that makes the most secure behaviors painless to perform.

EXTENSIBLE AND SCALABLE

Today's IT and security teams want flexible security tools that can be easily adapted to the system configurations, policies, and use cases unique to their organization. Modern IGA solutions have comprehensive APIs and support for tools like Terraform, webhooks, and CLI that allow developers to extend and scale the solutions as their needs evolve.

COMMITTED TO INNOVATION

Modern IGA solutions were born out of the need for innovation in a stale market and understand how quickly today’s identity security landscape is evolving. They maintain a swift clip of updates and feature releases essential to keeping customers secure, compliant, and productive.

SECURITY-FIRST GOVERNANCE

Unlike legacy tools designed with an IT-oriented view of identity governance, modern IGA tools prioritize security. They enable intelligent, risk-based access controls and provide real-time tracking of problematic access—like orphaned, unused, overprivileged, and conflicting access—that allow companies to put proactive security policies in place and mitigate risks before they become a problem.

	Legacy IGA	Modern IGA
Time to value	Year+ deployments not uncommon; 50% of deployments in distress*	Live in weeks
Implementation cost	Heavy professional services can be 2-3x software cost	Included in purchase
Integrations	Outdated integration technology limits visibility across modern systems	Out-of-the-box integrations for cloud, infrastructure, and on-prem
Extensibility	Requires specialization to customize	Modern API, command line, webhook, and Terraform interfaces
User experience	Clunky UI frustrates IT and security teams and discourages secure behaviors from end users	Intuitive UI and seamless experience in web app, Slack, MS Teams, and CLI
Use cases	IT-focused; not built to address modern security needs	Security-driven governance with just-in-time access, automated offboarding, and policy-based access controls

*Gatner , “Avoid These Top 5 Mistakes When Deploying IGA”

igsenergy

> *"ConductorOne was not only the best option that met our needs at the time, but showed a willingness and flexibility to engage in a more strategic partnership long term."*

Chris Hatfield, Manager of Security and Infrastructure at IGS Energy

ConductorOne

IGA for the modern enterprise

ConductorOne is the first access control and governance solution designed to address modern identity security needs. The platform intelligently ingests and orchestrates access data from across your tech stack to get you up and running and achieving security and efficiency gains right away.

1

month avegrage time to go live

97%

less time to process access requests

95%

less time to prepare access reviews

One platform — comprehensive control and compliance

DISCOVER AND REMEDIATE IDENTITY-BASED RISKS

Strengthen your overall security posture and reduce the risk of a data breach by identifying shadow apps, unused and orphaned accounts, overprivileged users, and more.

MOVE TO ZERO STANDING PRIVILEGES

Automate just-in-time access with self-service requests and custom approval policies to enforce zero standing privileges for critical resources and infrastructure—without sacrificing productivity.

STREAMLINE REGULATORY COMPLIANCE

Meet the requirements of data protection frameworks such as SOC 2, ISO, SOX, HIPAA, and GDPR with fully automated user access reviews, separation of duties enforcement, onboarding, offboarding, role-based access controls, and one-click reporting for auditors.

DRIVE AUTOMATION AND EFFICIENCY

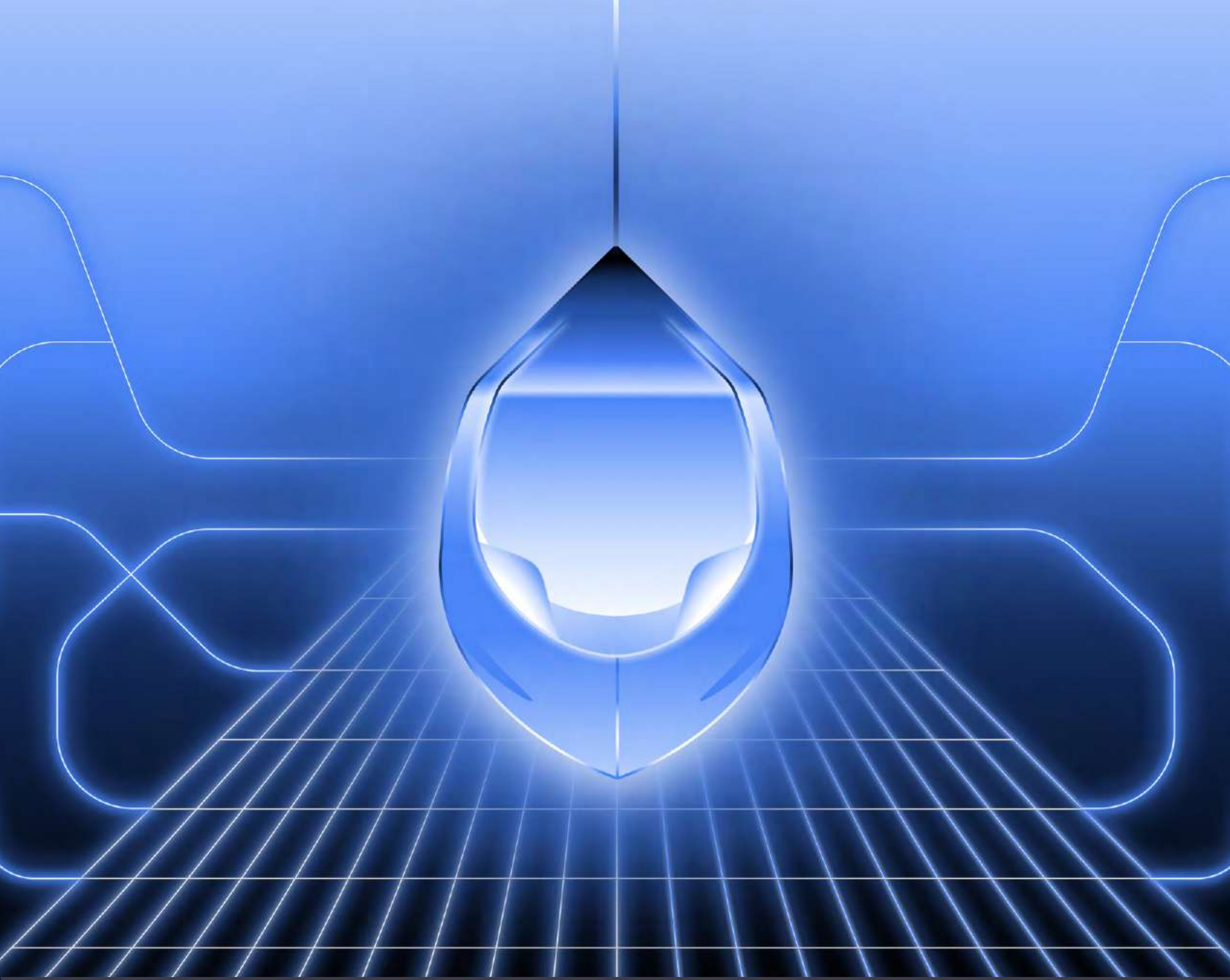
Unburden IT with self-service access requests, helpdesk automation, auto-approval workflows, zero-touch provisioning, and more to drive significant efficiencies while ensuring security policies are upheld.

CREATE A BETTER USER EXPERIENCE

Ensure the most secure action is always the easiest to take by providing a great user experience in the tools users already use, like web app, Slack, CLI and helpdesk systems such as Jira and ServiceNow.

ENABLE TECHNICAL TEAMS

Support technical users on your security team with tools and interfaces that developers love, including modern APIs, command line tools, Terraform for automated configuration, and webhooks for workflow orchestration.



ConductorOne

Legacy IGA was built to serve yesterday's governance needs. ConductorOne is built to handle the identity security challenges facing companies today—and tomorrow. Talk to our team to learn how ConductorOne can help you simplify and streamline access governance and secure your company.

Visit conductorone.com or book a demo to learn more

Get a demo