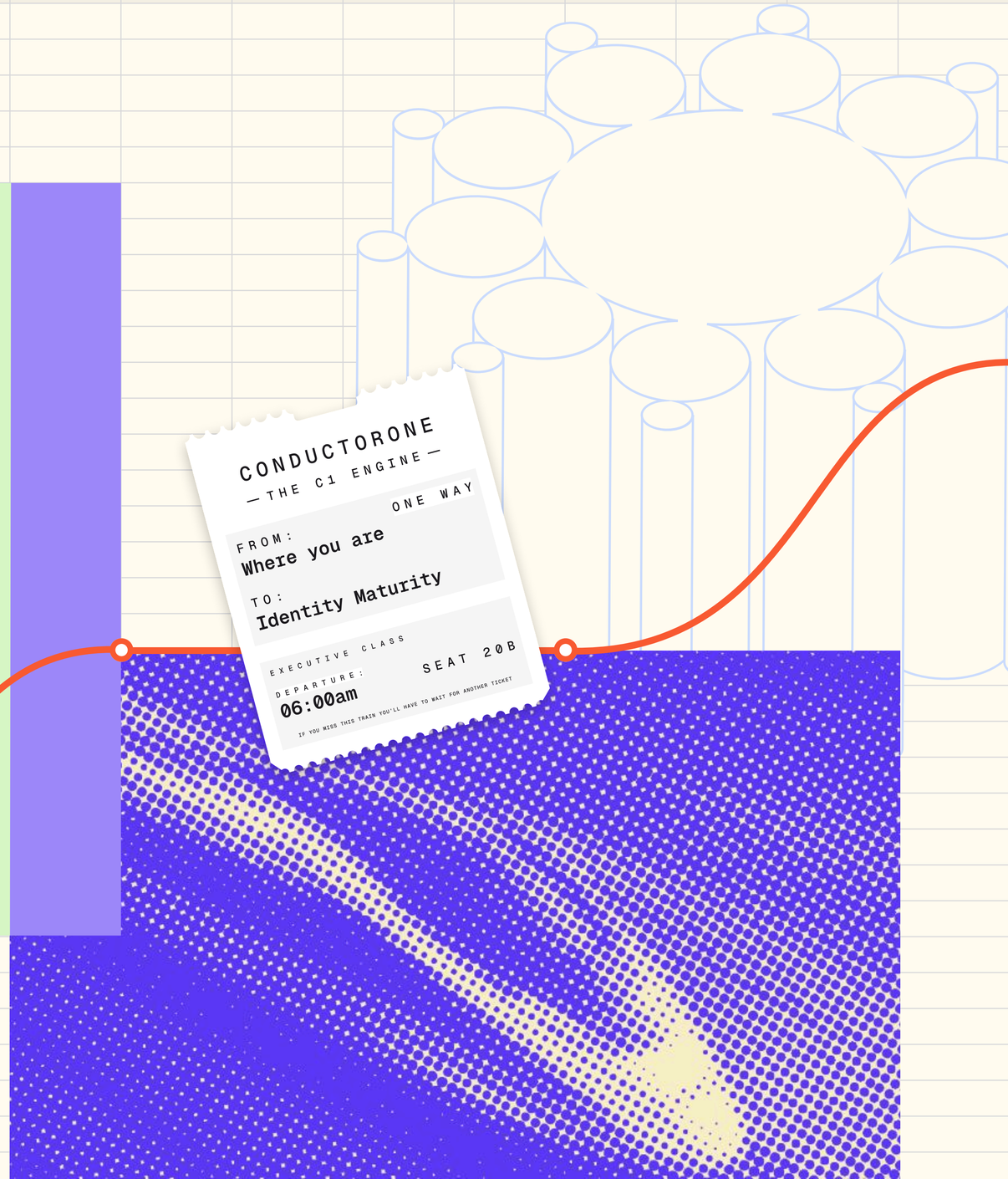
ConductorOne

GUIDE

The Path to Identity Maturity



INTRO

Every company is on its own identity journey. Some start in spreadsheets, some start with audits, some start after a close call. It matters less where you begin and more how you move forward.

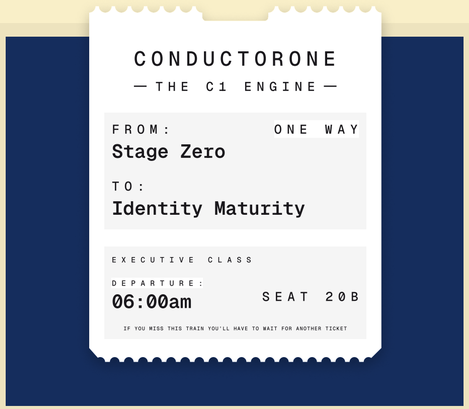
This IGA maturity path shows the real steps teams take as they go from unknown access to automated, intelligent identity security, and how you can, too.

Stage Zero: Blind Spots

In reality, no one starts at stage one. Companies just starting their identity journey are really at what we call stage zero. Here's what it looks like:

MINDSET:

You cannot secure what you cannot see.



Snapshot of reality

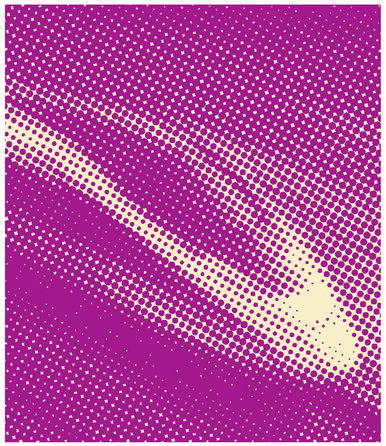
- No central view of identities or entitlements
- SaaS and shadow IT everywhere
- Spreadsheets and tribal knowledge drive access decisions
- Over-privileged accounts hiding in plain sight
- Limited ability to answer basic questions like who has access to what

Risks

- Breaches hide inside unclear access patterns
- Audit pain and higher regulatory exposure
- Toxic access combinations go undetected

Goal

Acknowledge the unknowns and prepare to discover them.



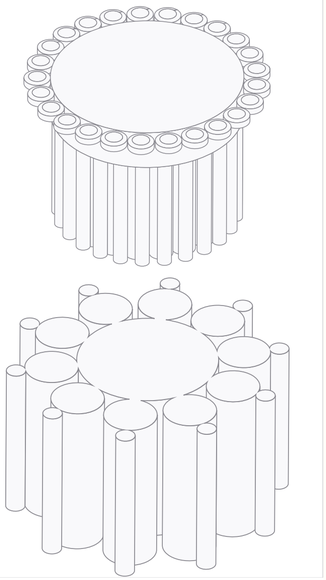
Stage One: Discovery

To get out of stage zero, you've got to start with discovery.
You can't secure what you can't see.

MINDSET: Visibility first.

What is happening

- Inventory of every identity: employees, vendors, service accounts, AI agents
- Mapping access across SaaS, cloud, and legacy systems
- Identification of privileged access
- Baseline catalog of accounts, groups, and permission sets



Key capabilities:

- Identity and entitlement catalog
- Connectors and ingestion pipelines
- Privileged account identification

Success metric:

You can answer: "Who has access to what?"
You know your highest risk accounts.

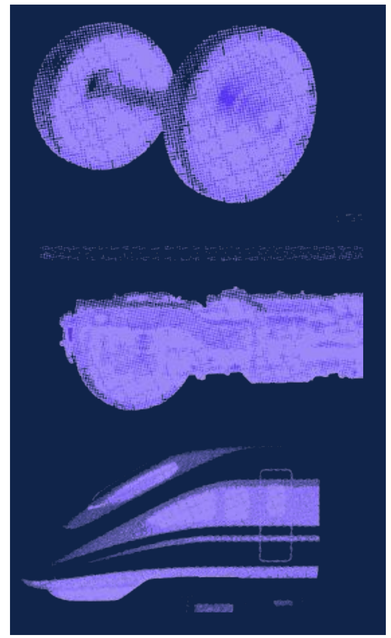
Stage Two: Hygiene and Rationalization

Once you've discovered and inventoried everything,
that's when you can start to clean up the mess.

MINDSET: Clean up the mess before you govern and automate it.

What is happening

- Deprovisioning stale users
- Removing unused permissions
- Normalizing roles and groups
- Aligning lifecycle events from HR systems
- Clearing duplicate or mis-aligned accounts



Key capabilities

- Automated orphan removal
- Role mining and rationalization
- Lifecycle alignment and identity resolution

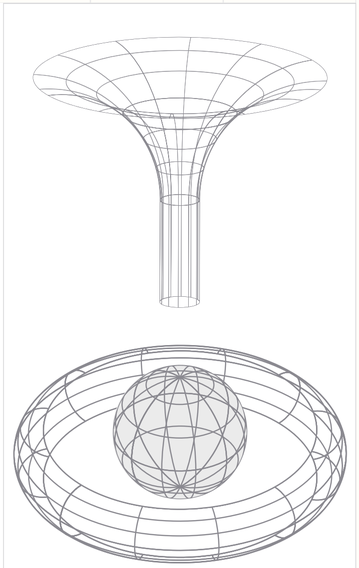
Success metric:

Reduction in zombie access, over-privileged identities, and manual cleanup cycles.

Stage Three: Governance

Once you've cleaned up your identity data, you can start governing it—creating rules, approvals, and processes that help you move forward.

MINDSET: Control with context.



What is happening

- Access reviews and certifications are running
- Approval workflows tied to risk and context
- Implementation of separation of duties checks
- Access tiers defined by sensitivity

Key capabilities:

- RBAC and ABAC enforcement
- Automated reviews and risk scoring
- Approval workflows tied to policy

Success metric:

Faster and more accurate access decisions with less user friction.

Stage Four: Just-in-Time Access and Zero Standing Privilege

Now that you have rules in place, you're able to limit privileged access and move towards zero standing privileges.

MINDSET: Standing privilege is dangerous by default.

What is happening

- Privileged access becomes temporary, not permanent
- Short-lived credentials for sensitive access
- Context-driven elevation tied to tickets or automated checks
- Access granted only when needed and removed immediately after

Key capabilities

- JIT elevation and ephemeral sessions
- Cloud policy automation
- PAM integration

Success metric:

Privilege exists only when required. Nothing sits idle.

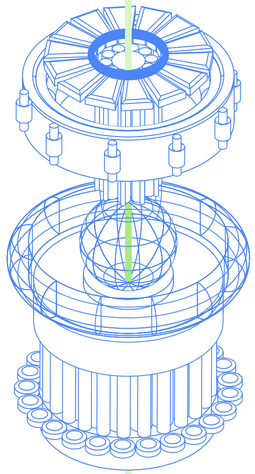
Stage Five: Autonomous Identity

The last stage of the IGA maturity path is autonomous identity. This stage relies on automation and AI-based decisions for identity security, freeing up your team's time to focus on what really matters.

MINDSET: Identity security runs itself with human oversight.

What is happening

- AI drives entitlement recommendations
- AI understands normal behavior and flags anomalies
- Intelligent policy tuning and self-healing controls
- Continuous authorization based on risk and context



Key capabilities:

- AI policy and entitlement recommendations
- Natural language policy creation
- Real-time anomaly detection and remediation

Success metric:

Identity posture adapts continuously.
Manual work becomes exception-driven, not the norm.

You cannot skip steps

You cannot	→	Until you
Govern access	→	Know who has it
Remove risk	→	See it
Enforce least privilege	→	Understand privilege
Automate decisions	→	Maintain clean baselines
Reduce standing privilege	→	Trust your entitlement map

Identity maturity builds like a staircase.
You climb one practical step at a time.

Real-world checkpoints

Wondering where you might be on the path?
Ask these questions to understand your maturity stage:

- [ ] Do we know every identity across people, machines, and AI agents?
- [ ] Can we detect privilege drift or access creep?
- [ ] Are access decisions contextual and policy based?
- [ ] How often is access temporary rather than permanent?
- [ ] How much of our identity work is automated?

Your answers define where you are and where you go next.

ConductorOne

How ConductorOne helps you mature

ConductorOne meets you where you are, guides you forward, and continuously helps you to improve.

With ConductorOne, you can:

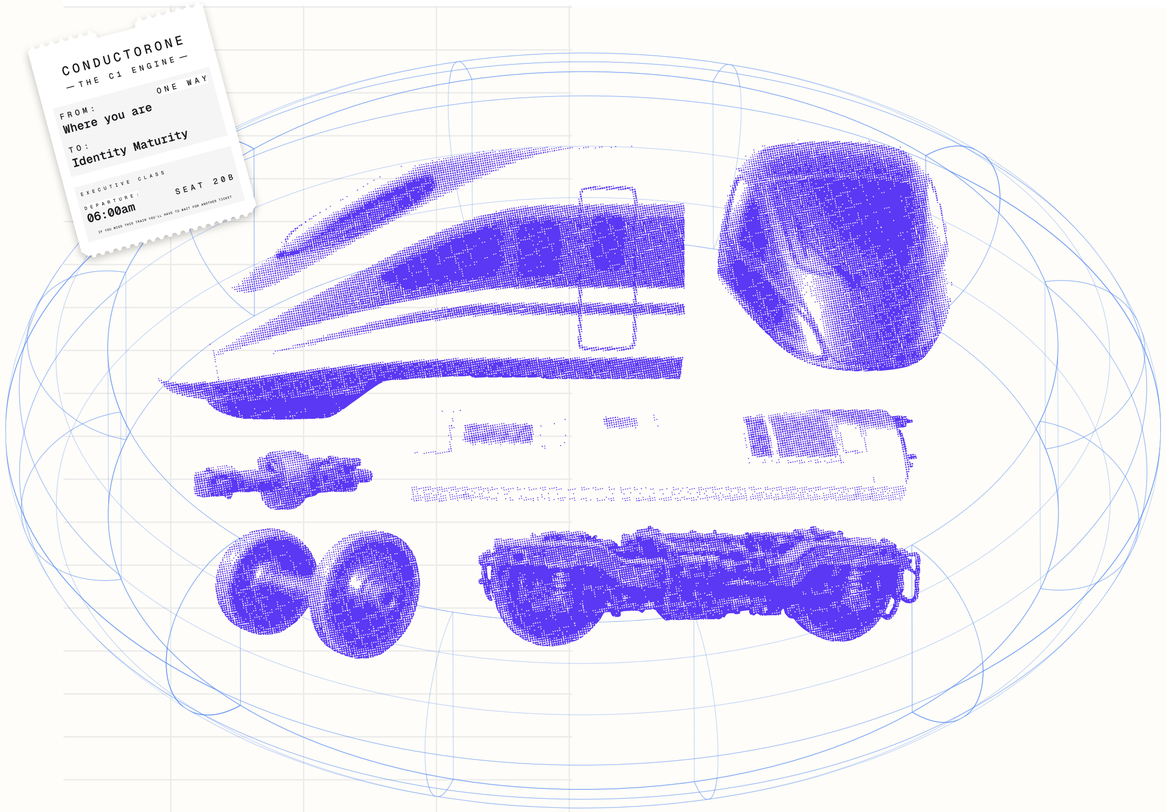
- → Discover and inventory identities across SaaS, cloud, and legacy systems
- → Clean up orphan accounts and over-privileged access
- → Apply policy-driven governance and automated certifications
- → Enforce JIT and zero standing privilege across infrastructure and SaaS
- → Move toward AI-driven autonomous identity policies

Whether you are wrangling spreadsheets or deploying ephemeral access everywhere, ConductorOne helps accelerate every stage.

Final takeaway

Identity maturity is not linear and it is not perfect.
It is a journey from unknowns, to clarity, to proactive control, and finally intelligent automation.

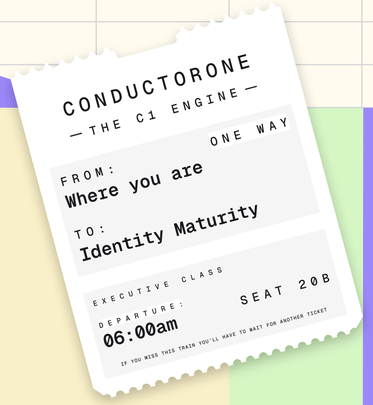
Start where you are. Move one step at a time. Automate aggressively. Embrace AI. End at zero standing privileges and autonomous governance. This is how successful security teams do it.

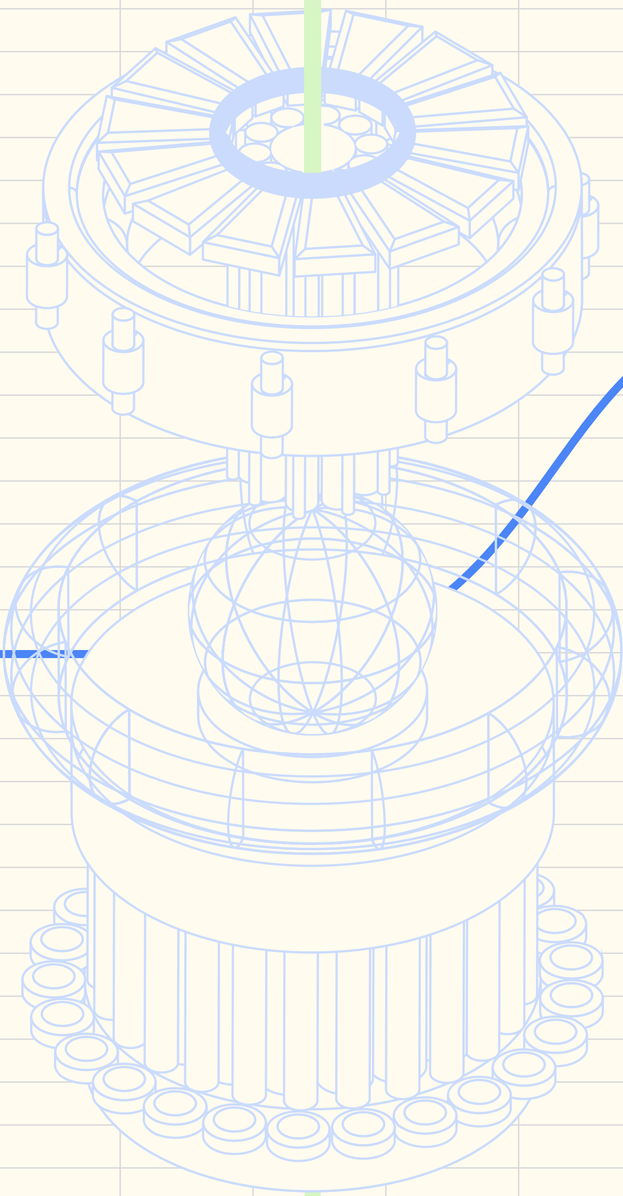


ConductorOne

GUIDE

The Path to Identity Maturity





Learn more at
ConductorOne.com