tines

Essential Guide

Unlocking IT agility with automation and orchestration

Vol 2: Identity and access management

Contents

Foreword
Scott Bean, Senior IAM and Security Engineer, MongoDB

Identity is fundamental to every part of a business. It's the digital reflection of your workforce, shaping everything from securing cloud systems to ordering a company lunch.

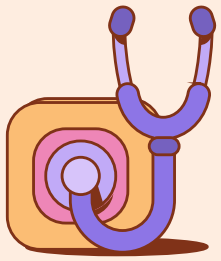
The idea isn't new. As far back as the 1400s, King Henry V issued "safe conducts" to control who could cross borders. Identity and Access Management (IAM) is today's version of that system. Except the borders are digital, and the scale is global.

The challenge is that IAM hasn't kept pace. Each application adds its own setup, and new standards rarely close the gaps. IT teams face tens of thousands of signals daily, all of which need to be normalized and acted on in real time, without slowing down the business.

When identity breaks, the consequences can be severe. Microsoft's recent Midnight Blizzard breach exploited reused passwords across multiple apps. Mailchimp suffered three breaches in one year, all tied to compromised employee credentials. And the 2014 JPMorgan Chase breach, which hit 76 million households, started with a single overlooked authentication gap.

These events show just how fragile IAM can be, and why IT teams need new ways to make it consistent, scalable, and secure.

Identity and access management



When identity controls can't keep up

For advanced organizations, IAM is foundational to secure, efficient operations. From onboarding new employees and granting access to the right tools, to ensuring that contractors, service accounts, and partners have appropriate permissions, IAM touches every corner of the business. It enables collaboration, protects sensitive data, supports compliance, and ensures that people can do their jobs without unnecessary friction.

But when IAM breaks down, whether through misconfigured roles, orphaned accounts, or inconsistent controls, the consequences ripple across departments. This leads to productivity delays, audit failures, and even costly security incidents.

The stakes are high. Ninety-one percent of organizations rank identity security as a top-five priority, with 42% calling it their top concern. Yet with hundreds of apps, cloud and on-prem systems, contractors, and service accounts to manage, the workload quickly becomes more than what most teams can handle. And businesses are paying the price.

According to IBM's 2025 Cost of a Data Breach Report, the global average cost of a breach is $4.44 million, while in the U.S. it's $10.22 million, driven higher by regulatory penalties and slower detection.

This guide explores why IAM practices break down, where the pressure comes from, and how orchestration and automation can help IT and security teams increase operational efficiency, minimize end user friction, and mitigate security risk.

The problem

Identity: simple in theory, harder in practice

Why does IAM break down? Three root causes stand out.

A patchwork of identity tools, systems and processes

Some applications integrate with SSO in minutes, while others demand weeks of back-and-forth or expensive upgrades. At scale, across hundreds of systems, this inconsistency creates fragile environments that are difficult to govern. Even minor missteps can escalate, as seen by Microsoft in 2023, where an IAM misconfiguration (a legacy non-production test tenant account without multi-factor authentication) was compromised via password spraying. This enabling a nation-state attacker (Midnight Blizzard) to access a number of senior corporate email accounts.

Scaling access, scaling risk

Managing 20 users is straightforward. Managing hundreds or thousands across a patchwork of systems and apps is something else entirely. Each joiner, mover, or leaver triggers a chain of changes, every one an opportunity for accounts to linger or privileges to accumulate. As organizations grow, even core apps are replaced with enterprise platforms, introducing yet more churn and risk. And now, with shadow AI tools adopted outside formal IT processes, identity gaps are multiplying faster, becoming harder than ever to detect.

Pressure from regulators, pressure from within

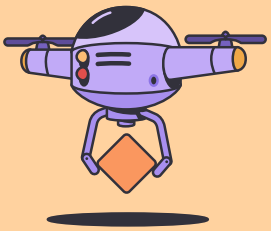
Auditors demand clear proof of who has access, why they have it, and when it was last reviewed. Frameworks like SOC 2, ISO 27001, and GDPR* all mandate strict enforcement of the principle of least privilege. But the pressure isn't only external. Executives expect flawless audits, security teams expect zero exposure, and business units expect IT to deliver without delay. When access reviews are handled manually, IT ends up chasing logs and approvals; burning valuable time, straining internal relationships, and still leaving behind gaps that can trigger findings or fines.

**Note:* While GDPR does not explicitly use the phrase "principle of least privilege", it effectively mandates it through its security requirements.

By 2026, 70% of identity-first security strategies will fail unless organizations adopt continuous, consistent access policies.

GARTNER

The new standard



IAM designed for speed, consistency, and compliance from day one.

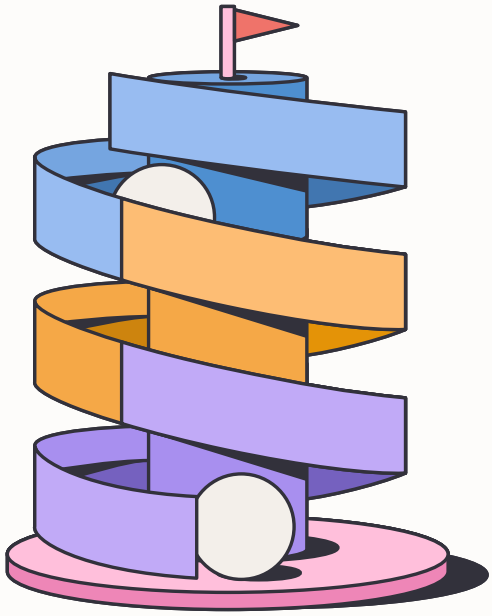
Imagine every employee receiving the right access in minutes, no matter the system. Imagine app owners and security/IT teams aligned by default, with governance built into every decision. Imagine compliance reviews that never derail projects, because evidence is always complete, and permission changes are transparent across the enterprise.

This new standard of IAM is possible by:

Increased operational efficiency

- Orchestrating identity workflows end to end, instead of stitching them together.
- Embedding visibility into every step, keeping IT, security, and app owners aligned.
- Capturing compliance evidence as part of daily operations, not last-minute scrambles.
- Meeting security expectations without slowing down the business.
- Empowering employees with self-service access requests and updates that are approved in minutes.

IAM is efficient when access requests flow seamlessly; fast to approve, consistent to enforce, and compliant at every step.



The proven impact

Faster access, stronger control.

Stronger identity isn't just control. It's a catalyst for speed, security, and trust across the enterprise:

Agility employees notice

- Access is delivered in minutes, outages resolve automatically, and provisioning runs without tickets. IT gains efficiency while employees stay productive.
- Example: A global workforce of 20,000 employees requests and tracks access in the same place, while lockouts resolve automatically across regions, reducing helpdesk volumes by thousands of tickets each month.

Security and compliance by design

- Privileges stay right-sized, approvals are logged, and evidence is captured automatically. Governance runs in the background, audits become routine, and least privilege is enforced without friction.
- Example: Role changes across multiple business units automatically trigger access revocation, while scheduled reviews generate audit-ready reports for SOC 2, ISO 27001, and GDPR without additional effort.

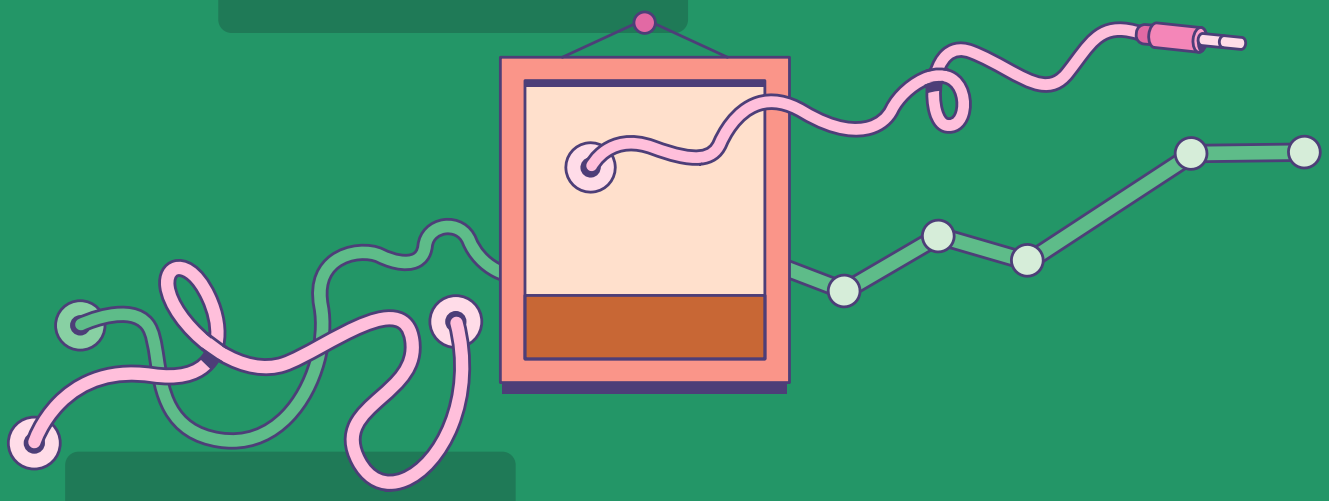
Confidence at scale

- IT, security, and compliance operate from a single source of truth, with visibility across hundreds of apps. Workflows adapt as fast as the business – new applications, new regulations, new models, without adding risk.
- Example: A multinational enterprise integrates identity workflows across 300+ SaaS and on-prem systems, while every request and decision remains searchable in Slack or Teams, reducing cross-team friction and shadow IT exposure.

Cutting down on manual processes can help organizations reduce onboarding time by 66%, process access requests at least 45 minutes faster, and eliminate hours of manual effort each week.

CRYPTO EXCHANGE RESULTS

What *great* looks like



It's one thing to talk about identity; it's another to put it into practice. See how leading teams use orchestration to reduce manual effort, strengthen controls, and simplify access management; proving IAM can be both secure and seamless at scale.

bitpanda

Case study Bitpanda

"With Tines, we're capable of building more complex detection rules, based on our organization's needs."

MARTIN SCHLATZER, CORPORATE IT SECURITY LEAD

THE GOAL

Give a fast-growing fintech team visibility into inactive accounts and assets across their environment, without adding manual overhead.

THE SOLUTION

Orchestrated identity and access workflows that provisioned and deprovisioned accounts consistently, all while integrated seamlessly across systems. This delivered full auditability without increasing IT workload.

Bitpanda strengthens threat resilience with intelligent workflow orchestration

Facing mounting identity checks and repetitive manual reviews, Bitpanda's security team needed a way to scale without adding risk. By orchestrating processes end to end, they eliminated time-consuming manual effort, reduced the chance of errors, and gained real-time visibility across their environment. The result: stronger security oversight and more time to focus on strategic initiatives that drive business value.

→ Read the full case study: tines.com/case-studies/bitpanda/

KnowBe4
Human error. Conquered.

Case study KnowBe4

"I was able to build a Tines story that reduced the time spent by 50 to 75%, which was a good and easy win."

DYLAN WHITE, INFORMATION SECURITY ENGINEER

THE GOAL

Reduce insider risk by ensuring employee offboarding is handled quickly and consistently, without relying on manual steps that leave accounts exposed.

THE SOLUTION

Orchestrated offboarding workflows which revoked access instantly, all while integrated with identity and HR systems. This established a standardized, auditable process that removed manual risk.

How KnowBe4 transformed internal processes with Tines

By replacing manual offboarding with orchestrated workflows, KnowBe4 closed insider risk gaps and accelerated execution. Access was removed in real time, oversight became continuous, and compliance teams gained immediate, audit-ready documentation, turning a once-fragmented process into a resilient, scalable control.

→ Read the full case study: tines.com/case-studies/knowbe4/

Case study PathAI

"Before, no matter what, something would go wrong and break. Now, it's all automated... We just get to enter a form, and it's done!"

IT TEAM MEMBER, PATHAI

THE GOAL

Reduce manual errors, improve repeatability, and gain audit visibility for onboarding processes that used to rely on complex, hard-to-maintain scripts.

THE SOLUTION

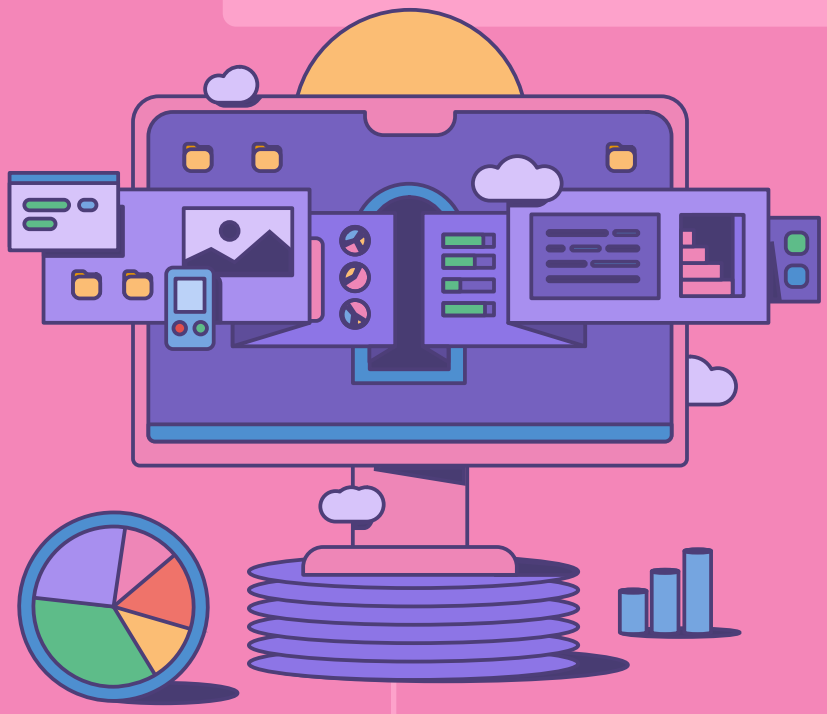
Orchestrated onboarding workflows that replaced custom scripts, automated repeatable steps, all while providing full audit visibility. This ensured consistency and eliminated manual errors.

PathAI ensures compliance and auditability with Tines

PathAI replaced custom scripts with a resilient, form-based workflow that delivered consistent onboarding, complete audit trails, and a significant reduction in errors. Each request saved up to 45 minutes, freeing the team to focus on high-impact work that strengthened the company's overall security posture.

→ Read the full case study: tines.com/case-studies/pathai/

Pre-built workflows



The Story Library provides a catalog of more than 1,000 workflows, covering everything from joiner/mover/leaver processes to access reviews. Each workflow is built for orchestration at scale and can be tailored to fit the unique requirements of your environment, helping IT and security teams move faster with confidence.

Monitor and deactivate long-lasting AWS IAM keys

Ensure your AWS access keys are rotated regularly. This workflow checks for any active AWS IAM keys older than 30 days and automatically deactivates them. Users receive notifications when their keys are scheduled for deactivation, keeping your environment compliant and secure without manual effort.

TOOLS

AWS

USE THIS FLOW

tines.com/tprlc

How SSF creates a common language for security tools

BY SCOTT BEAN, MONGO DB

Zero Trust remains a hot topic in the IAM space. One way the industry is streamlining adoption is through a universal standard for systems to share security-related signals: the Shared Signals Framework (SSF). SSF helps different security systems talk to each other directly, exchanging security signals and user status changes. Think of it as a direct line of communication between your security tools.

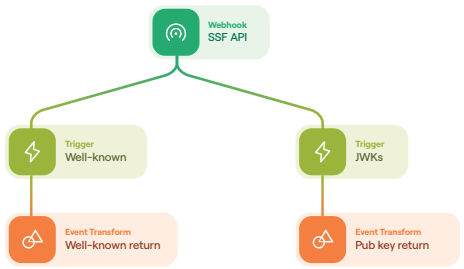
While SSF adoption is growing, gaps are inevitable. That's where Tines comes in. Since it's an OpenID standard built on HTTPS requests, SSF works perfectly with Tines' HTTP Action.

In this story, we integrate 1Passwords Kolide Device Trust product with Tines to allow it to generate and send SSF signals to Okta. If a device falls out of compliance, Kolide informs our Tines story through a webhook. Tines enriches the signal, ensures it can be tied to a user, builds a Security Event Token, and delivers it to Okta.

The SSF standard also requires hosting specific information for receivers to decrypt tokens. For this, we use my favorite Tines feature: API path prefixes. This lets us create a REST-style API that our receivers can interact with directly.

Integrate Kolide Device Trust with Okta using the Shared Signals Framework

The Shared Signals Framework is an OpenID standard designed to make an easy and standard way for vendors to share security events. This is a proof of concept SSF Transmitter capable of being registered with Okta and sending device compliance change CAEP events based off of issues generated in Kolide. Events are sent as Security Event Tokens.



TOOLS

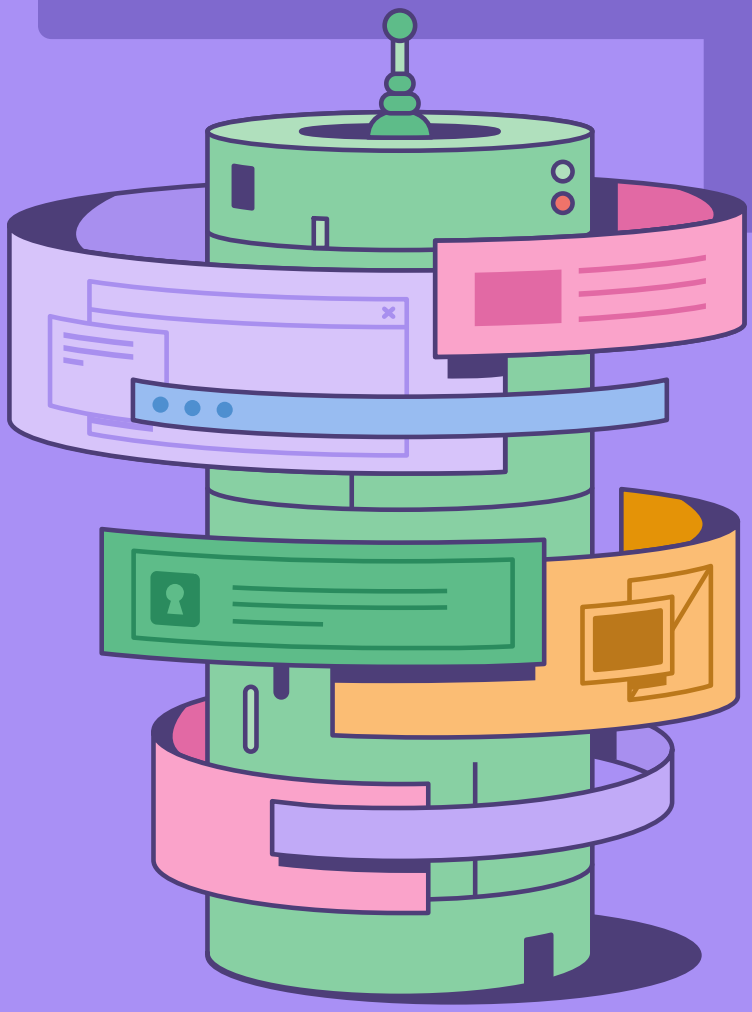
Kolide, Okta, Slack

USE THIS FLOW

tines.com/irlpq

→ Sign up for the always-free Community Edition: tines.com/community-edition

Orchestrating IAM



Your IAM readiness checklist

Modern identity spans SaaS, cloud services, and on-prem systems. True readiness means consistency across them all:

Access visibility and control

Vision: Every system, every account, fully accounted for.

- Do you know who has access to every system, cloud and on-prem, and why?
- Do orphaned accounts linger in directories or applications, creating unnecessary risk?
- Are permissions updated automatically when roles change, or do privileges quietly accumulate?

Efficiency and experience

Vision: Employees productive from day one, IT shifting left

- How quickly do new hires get the access they need; minutes, hours, or days, regardless of platform?
- Can all of a former employee's access be revoked in one step, across every application and environment?
- Is there a clear, logged approval process for access requests, consistent across SaaS and legacy systems?

Alignment and oversight

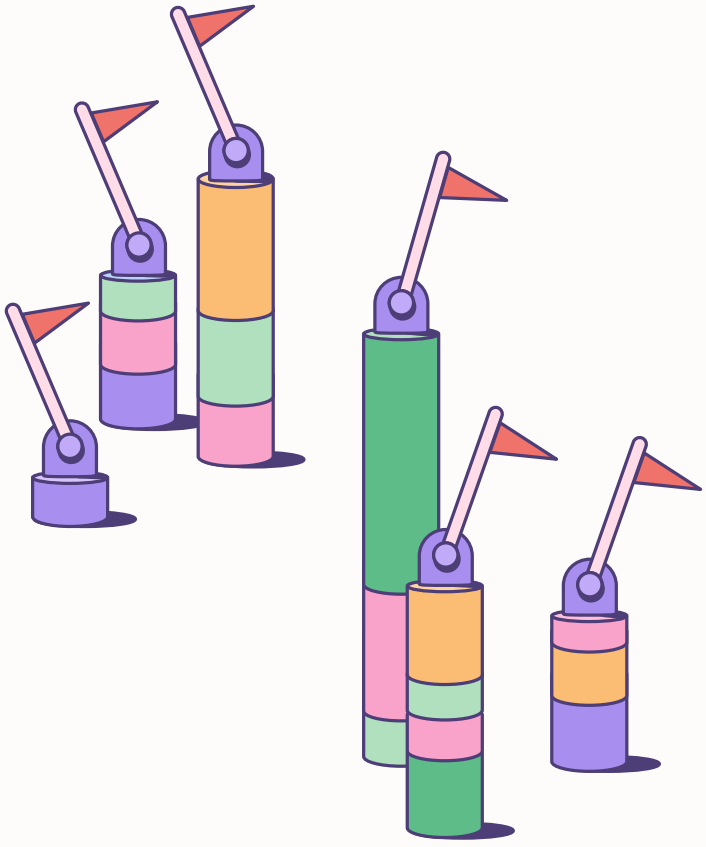
Vision: IT and security working from the same source of truth.

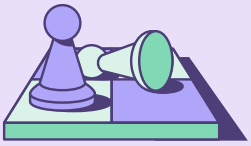
- Do IT and security teams share a unified view of logs and audit trails, or are they piecing together records from multiple tools?
- Could you pass a SOC 2, ISO 27001, or GDPR audit without scrambling for evidence across environments?
- Are periodic access reviews automated and reliable for both cloud services and on-prem infrastructure?

Scalability and adaptability

Vision: Identity processes that grow as fast as the business.

- When new applications or services are introduced, whether SaaS or self-hosted, can your identity workflows adapt without custom fixes?





Answering these questions with clarity and confidence is the first step towards creating an identity strategy without compromise. It's how IT and security move fast, stay secure, and operate as one; delivering consistent access, stronger governance, and seamless experiences across every system, from SaaS to on-prem.

Building your IAM strategy

Identity and access management is no longer just a back-office function - it sits at the heart of how businesses scale securely. The right strategy empowers employees to be productive from day one, gives security teams confidence that least privilege is enforced, and provides IT with processes that adapt as fast as the business. Orchestrated well, IAM balances speed with security, turning a potential point of friction into a foundation for growth.

Identify

- Define your sources of truth (HR system, directory, identity provider) and the access requirements for each role.
- Map key user journeys, such as onboarding, role changes, and offboarding, and clarify how authentication will be enforced across apps (SSO, MFA, biometrics).
- Pinpoint high-volume requests like SaaS access or password resets where manual work creates risk.

Structure

- Design role-based models so common job functions map to clear permissions.
- Establish clear authorization rules so users only receive the access they need, nothing more.
- Set up approval workflows and document exception paths. Use templates for one-time and unique access requests to reduce one-off decisions and bring consistency.

Implement

- Connect your identity provider and target systems, ensuring consistent governance across cloud and on-prem.
- Automate provisioning and deprovisioning so access is granted or revoked immediately.
- Add self-service access requests for routine needs to reduce ticket volume and improve visibility.

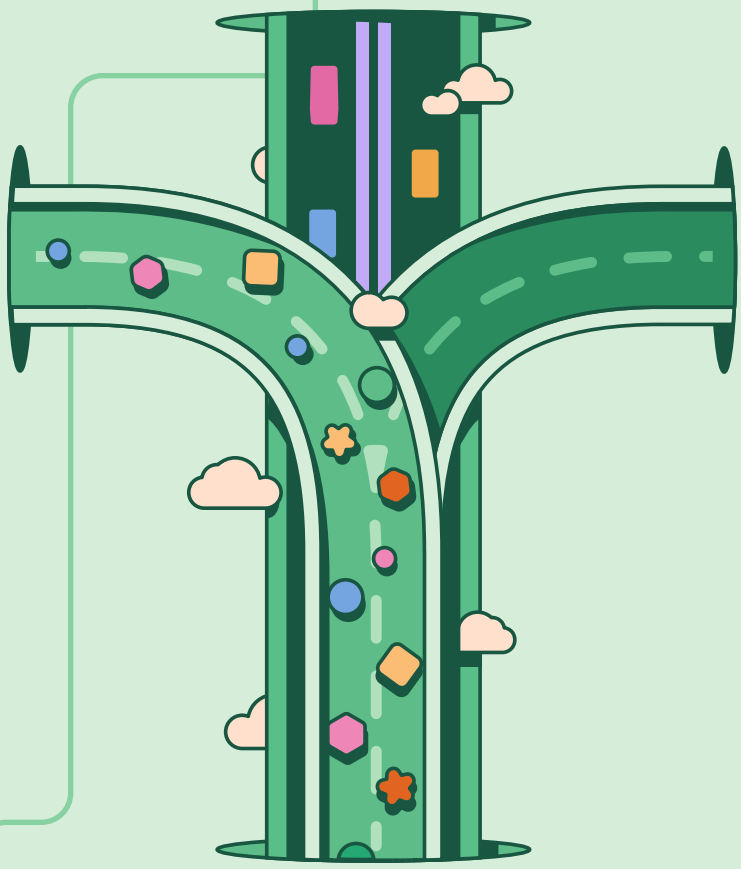
Monitor

- Track key metrics (request volumes, resolution times, review completion rates) to measure effectiveness.
- Confirm every workflow executes correctly, every approval is logged, and every change leaves an auditable record.
- Create shared dashboards so IT, security, and compliance all operate from the same data and insights.

Iterate

- Refine access models based on usage patterns and business needs.
- Add enhancements like just-in-time access or expiration dates where needed.
- Expand workflows to new applications, cloud services, and legacy systems to keep pace with growth and regulatory demands.

The Tines advantage



With Tines, IT and security teams can move faster and enforce stronger controls by shifting left, embedding governance earlier in the process and closer to the teams who use it. IAM becomes part of daily operations, not a bottleneck, connecting seamlessly into the broader stack without adding manual overhead, all while strengthening the security posture of the business.

End-to-end identity orchestration

From onboarding to offboarding, workflows link HR events directly to provisioning and deprovisioning. Access is applied or revoked immediately and consistently, closing gaps that manual processes leave behind.

Interoperability without limits

Identity providers, directories, and business applications connect effortlessly, while integrations extend into SIEM and security tools. Tines bridges cloud and on-prem environments with flexible, customizable workflows that adapt to enterprise needs.

Secure access, without friction

Approvals adapt to business context, and role-based provisioning removes repetitive steps. By shifting left, responsibility moves closer to app owners and team leads, ensuring least privilege is enforced naturally, with verification steps built into the flow.

Unified oversight

Real-time dashboards and complete audit trails give IT, security, and compliance a single view of activity. Every request, review, and approval is logged automatically, making audits routine and oversight continuous.

Getting started

Managing the identity lifecycle is about more than provisioning accounts. Done right, it empowers IT and security teams to enforce least privilege, reduce delays, and stay audit-ready, all while giving employees seamless access to the tools they need. It's not a trade-off between speed and security; it's both, working together.

With orchestration, this future is achievable without a full overhaul. Start small – offboard leavers in real time, streamline approvals, or schedule access reviews automatically. Each workflow you add builds consistency, strengthens security, and simplifies compliance, all while helping IT and security operate as one, with confidence.

"The reality is that these inherent gaps will always exist. However, by automating and augmenting IAM, we can achieve a truly seamless experience across our entire application ecosystem."

SCOTT BEAN, SENIOR IAM & SECURITY ENGINEER, MONGODB

→ **View the webinar:** Orchestrating IAM across teams and systems with AWS

→ **Learn more about Tines for IT Operations:** tines.com/solutions/it-operations

→ **Sign up for the always-free Community Edition of Tines**

→ **Book a demo**

RESOURCES:

Midnight Blizzard breach: https://www.mitiga.io/blog/microsoft-breach-by-midnight-blizzard-apt29-what-happened-and-what-now

Mailchimp breach: https://www.computerweekly.com/news/252529368/Mailchimp-suffers-third-breach-in-12-months

JP Morgan chase breach: https://en.wikipedia.org/wiki/2014_JPMorgan_Chase_data_breach

https://goteleport.com/api/files/identity-security-at-a-crossroads-balancing-stability-agility-and-security/

https://msrc.microsoft.com/blog/2024/01/microsoft-actions-following-attack-by-nation-state-actor-midnight-blizzard/

https://en.wikipedia.org/wiki/Principle_of_least_privilege

tines