Whitepaper

See clearly and build better with identity-based control

okta

Contents

See clearly and build better with identity-based control

Nobody likes to waste their time. And yet, the average workday is loaded with unproductive activity — from excessive meetings and training to administrative tasks. Not surprisingly, managers are frustrated when their team is too often distracted from critical business objectives. Employees become exasperated, too, if it looks like their skills aren't always being put to good use. Of course, exactly what counts as unproductive can depend on your perspective. In some organizations, coffee breaks and visits to the water cooler are now being seen as opportunities for serendipitous connections. One thing that's often overlooked, though, is the time it takes to access mission-critical software, harness key data, and generate insights needed to get the real work done.

In their quest to optimize each day with more productive work, organizations have loaded up the workplace with tools that promise efficiency and better collaboration. Digital transformation strategies lean heavily on the promise of more agile innovation through the adoption of the latest SaaS and cloud applications. The resulting challenge, unfortunately, is that users — including employees, contractors, and partners — are spending more time navigating a maze of tools to find the information they need to do their jobs. Modern organizations have become a sprawling mix of cloud platforms, on-premises systems, and third-party applications, each with its own set of access controls and security policies. On the journey to evolve the external customer's digital experience, many companies have lost sight of the internal user experience.

Preventing unauthorized access is paramount, but it often comes at a cost — slower, more cumbersome business operations caused by access friction. One study[1] showed that employees spend up to 12 hours a week struggling to locate information. This hunt is often stymied by security protocols that slow or block access, causing people to look for workarounds or simply give up. In fact, 68% of respondents to a data connectivity study[2] said they've knowingly disregarded certain data inputs because of accessibility issues. Nearly half (49%) said they were unable to access information in time for it to be useful.

342

Different SaaS apps the average business subscribes to.[3]

2.5

endpoints per day
Employees use about 2.5 different endpoints per day.[4]

With all these systems and applications, a workday can feel like a long hallway of digital doors, each unlocked with a different key from an overstuffed key ring. Some employees may be tempted to kick down a door or slip through when nobody's looking. When they encounter persistent authentication hurdles, permission delays, and siloed systems, their work is slowed and frustration builds. Blanket security protection almost always runs counter to business priorities, stifling innovation that's needed for a competitive edge.

When you can streamline access management without sacrificing a strong security posture, your organization is liberated to focus on core business objectives — resulting in better collaboration, faster decision-making, and more growth opportunities.

> It's hard to get away from the belief that convoluted access makes an environment more secure. In fact, that can be an illusion. Or, more accurately, a delusion.

When identity is the center of your business strategy

A traditional security model that focuses on locking down endpoints and fortifying the perimeter is becoming obsolete for a growing number of reasons. For one thing, the perimeter has become much more difficult to define. Customers, vendors, and contractors are being invited in, which highlights the need to control access at a granular level. This is vital if you're going to develop true workflow integration, automate processes end to end, and make every task as efficient as it can be across internal and external teams. The paradigm has shifted: You can now create a system of access that's frictionless for legitimate users as well as impenetrable to bad actors. It's a fundamental rethinking of how businesses operate, deep into the digital era.

Every workday, minutes and hours are lost to access friction. When teams are blocked from contributing at their full capacity, frustration saps their energy, productivity, and creativity. When you reduce access friction, workers can maximize their time and tap into all the resources that will help them contribute at the highest level. No more struggling with layers of authentication, permission requests, and password resets in order to navigate the disparate systems and tools needed to get through the day.

> "Okta was able to consolidate all our authentication and authorization requirements into a single location and establish a standard for all our applications."
>
> **Emnet Gossaye,**
> Security Software Engineer, Kensho

An identity-first approach structures trust around each individual, enabling secure access from anywhere — but only for the right people. In an evolving digital landscape, with accelerated cloud adoption and less-defined perimeters, identity has emerged as the most reliable control point for organizations to automate processes and securely integrate systems. Identity has gone from being a technical security component to a strategic business capability that provides tangible competitive advantages.

Use Case: Kensho

Kensho is a S&P Global subsidiary that uses data to develop AI and machine learning solutions. Security and customer trust are among the company's highest priorities. After implementing multiple Okta identity solutions, Kensho is able to launch new apps, services, and features six to nine months faster because its engineers are free to focus on business priorities and meeting client needs. Kensho estimates it has saved about two years of senior developer time by not having to build their own authentication system.

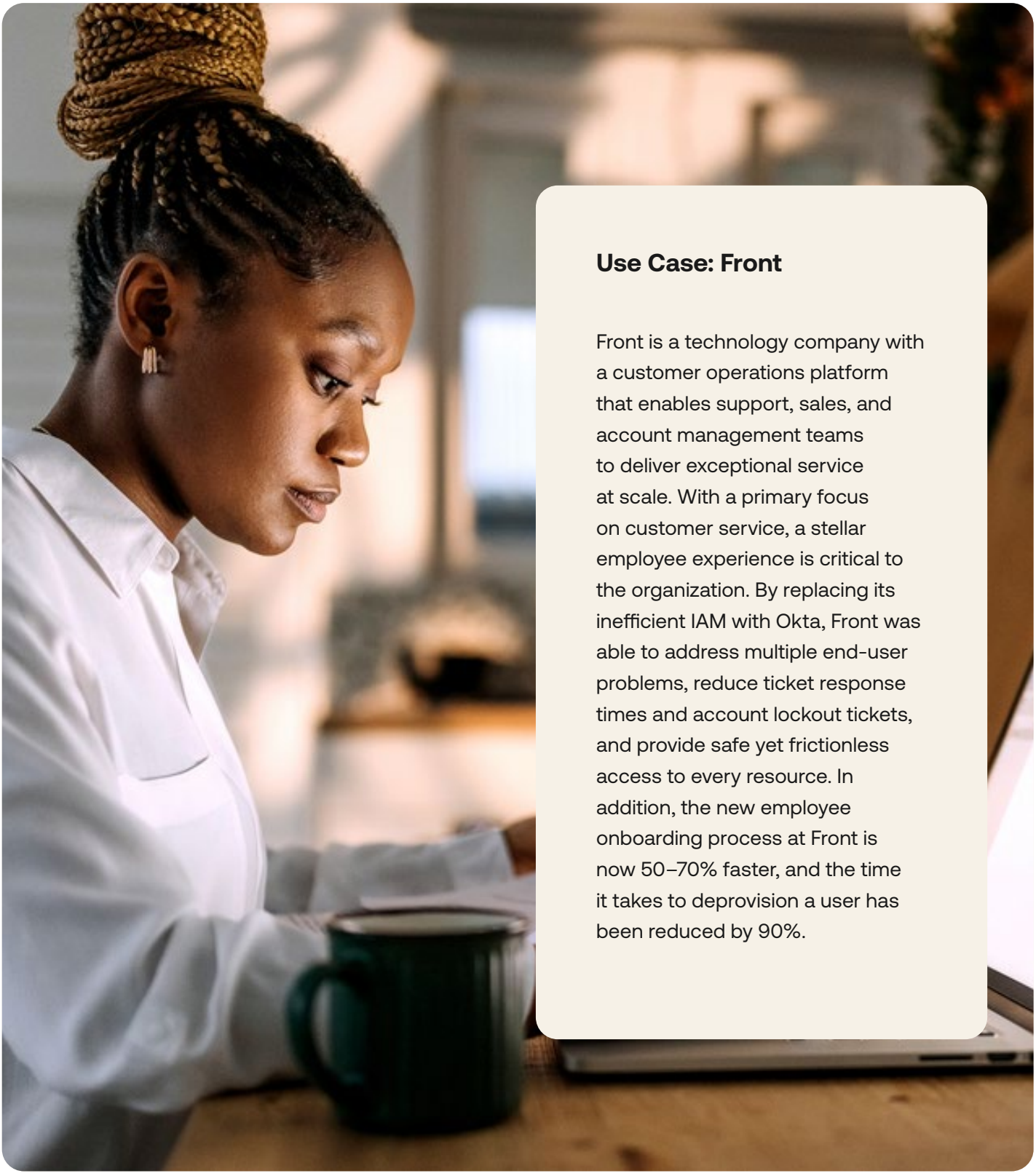
Remove bottlenecks to growth

Organizations add applications to fulfill specific needs, anticipating performance gains from automation and digitalization. But the resulting layers of access controls often make it harder to get the most out of this proliferation of tools. An identity-centric approach removes technological barriers, transforming the employee experience. One thing employees and their managers can agree on, after all, is that they should be spending their time on business objectives, not trying to find their way around disjointed systems to retrieve some stashed-away piece of information. It shouldn't matter what kind of network, system, or server they need to access. Employees should be freed up to work the way they work best, connecting from any location or device, whether at home or the office, or on their mobile device or PC.

> "Okta helps us have a highly efficient IT organization and avoid panicking when we grow."
>
> **Greg Karp-Neufeld,**
> Director of Corporate IT, Front

A modern identity solution provides streamlined authentication, automated provisioning, and contextual access controls, fulfilling the promise of barrier-free productivity. Teams can move faster and collaborate better. Leaders may have to completely rethink project schedules when they find their people delivering more in less time because life has simply gotten easier.

IT teams also get to focus on strategic initiatives that drive real business outcomes. They'll be spending considerably less energy on administrative tasks like granting routine access, manual provisioning, and resetting those pesky passwords while double-checking every task to avoid errors. No more frustrated users, only extremely frustrated bad guys.



Use Case: Front

Front is a technology company with a customer operations platform that enables support, sales, and account management teams to deliver exceptional service at scale. With a primary focus on customer service, a stellar employee experience is critical to the organization. By replacing its inefficient IAM with Okta, Front was able to address multiple end-user problems, reduce ticket response times and account lockout tickets, and provide safe yet frictionless access to every resource. In addition, the new employee onboarding process at Front is now 50–70% faster, and the time it takes to deprovision a user has been reduced by 90%.

Unlock agility and growth

The era is long past when companies would simply invest more resources in order to stay ahead. Throwing more money and people at an idea doesn't necessarily bear fruit sooner. Smart teams are now successful with less rather than more — with fewer obstacles in the way so they can adapt to market changes by shortening product development cycles, improving service, and speeding up customer response times. This ability to move quicker creates an operational velocity that's hard for slower-moving competitors to match. With access barriers removed, the entire organization can accelerate. Increased agility clears the way for growth at a pace your people have been asking for.

Here's how identity unlocks agility and growth:

- **The data advantage.** Your people and organizational data are your two most valuable assets. Protecting sensitive data with a risk-informed cybersecurity model needs to be coupled with seamless access. Effective identity management ensures the right people can source the right information when they need it, unlocking real insights that might otherwise remain hidden in organizational silos. No one wants to spend valuable time begging for a report or trying to figure out who has the rights to extract some bit of vital information. Democratization of data — properly secured through identity controls — supports informed decisions at every level, resulting in company-wide intelligence that drives superior outcomes.
- **Cross-functional innovation.** Modern business innovation isn't an isolated endeavor. It requires seamless collaboration across disciplines, from research and product development to marketing and customer service. Identity facilitates the free flow of tools, data, and expertise to ignite the flame of productive collaboration. With a modern identity platform, innovation is a team event, and strong controls keep resources protected from nefarious as well as accidental access, even between internal teams and contingent workers.
- **Accelerate AI innovation.** The only way to get the most out of enterprise AI is with access to all appropriate data. Despite all that AI can bring to your organization — automation, enhanced digital experiences, accelerated innovation — access friction can be a major barrier to AI implementation. With a modern identity platform, you can streamline access across multiple locations, from data centers to public and private clouds to the edge.

- **Always keep the lights on.** The ultimate productivity-stopper is a breach or ransomware attack that results in an operational shutdown. Innovation, production, customer service, transactions — they all stop until after you safely recover your systems. A cybersecurity attack will not only stop progress, but also cause long-term legal issues, mitigation costs, reputational damage, and, probably, a hit to your stock price. That's why an identity-centric solution must be leakproof. It's not enough to simply monitor, track, and report threats, because once an incident is detected, malicious actors are already inside causing disruptions. With individual-based access, the right ones get in and the wrong ones stay out.

IT security can finally shrug off its reputation as a burdensome roadblock. When your security is identity-centric, it does more than get out of the way. Identity becomes a business accelerator, fueling expansion, differentiation, and new revenue streams.

Identity advancements that enable growth with security

You get the idea. Remove the friction and you'll have more opportunities to unlock agility, speed, and growth, while enhancing security at the same time. Identity-first strategies make this possible. Let's take a look at the key innovations that power this inside-out approach to securing your business and enabling your teams:

- **Passwordless authentication.** It's finally here. At the same time hackers are figuring out more creative ways to crack passwords — unfortunately with the assistance of AI — you can move past that threat by doing away with passwords altogether. This is nothing short of a revolution in identity management. You can simultaneously strengthen security and improve user experiences by replacing knowledge-based authentication with possession-based factors (devices) and biometrics. Advanced passwordless solutions combine device trust, biometric verification, and behavioral analytics to swiftly authenticate legitimate users while making the environment more resistant to compromise.

> "What took a thousand lines of code to do before, we could now put together in 10 minutes with Okta."
>
> **Bob Durfee,**
> Head of Digital Engagement and DevSecOps, Takeda, a biopharmaceutical company

- **No-code, identity-based automation.** Even if you've got skilled developers on your IT team, you'd probably prefer they spend their time on more meaningful bottom-line projects. A modern identity management platform will make it easy for you to automate identity and access processes with a no-code interface. Administrators can design and implement workflows that make user onboarding, access provisioning, and compliance reporting a snap. IT teams using no-code automation are deploying and managing their identity tools five times faster than they had been with an in-house solution. That translates into significant cost savings both up front and on an ongoing basis. Because when business requirements change, the team can move quickly without having to hire a consultant or pull a specialist off business-critical work.
- **Adaptive, risk-based, just-in-time access.** There's a lot going on behind the scenes when you deploy a modern identity platform. Static rules have been replaced by dynamic, context-aware decisions. The right level of access can be granted quickly and with confidence because the platform is analyzing interrelated signals, including device health, location anomalies, time patterns, and behavior. Multiple inputs are used to calculate a real-time risk score that seamlessly approves routine access while flagging suspicious activity for verification. Just-in-time privileges grant temporary, time-bound access instead of standing privileges. This gives users the access they need when they need it. Access is then automatically revoked when the task is complete.
- **Centralized identity governance.** The promise of increased organizational agility only works if you've got unified visibility and control — even in the most sprawling hybrid environment. Modern identity solutions centralize management across cloud and on-premises resources and provide insights into who has access to what, how that access is being used, and whether it complies with policy. Compliance that used to be a periodic, time-consuming pain can turn into ongoing governance that continually strengthens your security posture and provides the assurance that business can keep moving full steam ahead.

Identity as a competitive advantage

The old mindset is that data and systems security had to be as tough on honest employees as it was on bad guys in order to be effective. Jumping through hoops seemed to enhance the perception of a strong security posture. Unfortunately, employees often became adept at working around the system — always in the name of productivity, of course. Meanwhile, those who should never be roaming around your systems have made it their full-time job to seek out and exploit every weakness.

The threat is all too real. Ninety percent of organizations in a 2024 study[5] by the Identity Defined Security Alliance (IDSA) had experienced an identity-related incident in the past year. Of those, 84% reported direct business impacts, including operational disruptions and reputational damage. The headline of Red Canary's 2025 Threat Detection Report[6] announced this chilling news: "Threat researchers detect 4x more identity-enabled attacks as infostealers continue to surge." Before the advent of identity-centric security, the only solution was to lock everything down tightly and wait until somebody hollered for a key.

Easy access and tighter control can now work hand in hand. Okta makes that possible, freeing up your organization to operate at its full potential with identity-based solutions. You may not even realize how much productivity is consumed logging in to multiple tools and juggling credentials because it tends to happen a few minutes at a time. It turns out that about 7 in 10 people (69%)[7] report that finding the information they need to do their job is too time-consuming. Identity-based solutions mean no more pleading for report access or searching for hidden data. Instead, teams can contribute more value with open and productive collaboration, internally and with external partners.

Moving forward with identity

Identity has moved beyond being a technical function to become a strategic capability that can transform the way people leverage data and technology to achieve business outcomes. But it's not something you simply install. Here are three tips for turning identity into a competitive advantage by first understanding your current state and then defining a clear path forward:

1. Any change in strategy should start with your business objectives. Assess your existing identity capabilities to pinpoint the highest-impact opportunities for improvement.
2. Develop a strategic roadmap that balances quick wins with long-term transformation goals, always checking alignment with overall business strategy.
3. Position identity at the center of your digital initiatives rather than as a supporting function. This perspective shift alone will create significant value.

---

[1] https://venturebeat.com/data-infrastructure/report-data-silos-cause-employees-to-lose-12-hours-a-week-chasing-data/.
[2] https://www.cdata.com/lp/data-connectivity-report-2024/.
[3] https://productiv.com/state-of-saas/2024-saas-trends-growth/.
[4] http://zippia.com/advice/byod-statistics/.
[5] https://www.prnewswire.com/news-releases/new-study-reveals-90-of-organizations-experienced-an-identity-related-incident-in-the-last-year-84-reported-a-direct-business-impact-302156769.html.
[6] https://redcanary.com/news/2025-threat-detection-report/.
[7] https://assets.qatalog.com/language.work/qatalog-2021-workgeist-report.pdf.

It's time to rethink how your company manages access, security, and growth.
You can do that by putting identity at the core. Contact Okta today — we can help.

- Learn more about Okta - https://www.okta.com/
- Learn about securing with identity - https://www.okta.com/solutions/secure-identity/
- Reach out to learn more - https://okta.com/contact-sales/