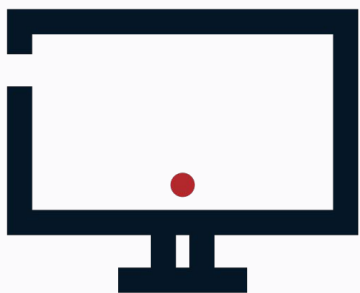




UX is an IT Issue (Whether You Know It or Not)

The IAM & security pros' guide
to why UX must be an IT priority



EBOOK



Table of Contents

- 03** **Why UX Should Be an IT Priority**
- 04** **UX Expectations Are Changing**
- 05** **Great UX = Strong Security**
- 06** **Start Small: Identify, Segment, Prioritize**
- 07** **Set Your IT Team Up for Success**
- 08** **From Reactive to Proactive Identity**



Why UX Should Be an IT Priority

User experience (UX) is often seen as a design problem, but for IT professionals; it's a foundational part of performance, productivity, and security. Many UX issues originate when IT teams fail to fully understand and accommodate the range of user needs across their organization, customer base, and business-to-business (B2B) relationships. These needs vary widely based on remote access requirements and use of personal devices amongst your workforce, users' temporary or permanent disabilities, customer demographics, industry, and more..

Often, accessibility and usability concerns are tacked on at the end of an implementation, if they're considered at all. The result are systems that users struggle with, leading to abandoned sessions, increased support tickets, and security workarounds. Poor UX isn't a superficial problem; it undercuts the effectiveness of IT systems and creates measurable costs. Fortunately, a modern identity and access management (IAM) approach can help IT pros navigate UX with seamlessness and security at the forefront.

Is Your Identity Strategy UX-Ready?

- ✓ Do you apply multi-factor authentication (MFA) only when risk is detected?
- ✓ Have you implemented self-service recovery for users?
- ✓ Are login, registration, onboarding, and recovery flows consistent across channels and apps?
- ✓ Do you support social login or passwordless authentication for ease of use?
- ✓ Can users easily update their profile and preferences without calling support?

If you answered “no” to any of these, it's time to re-evaluate your IAM.



UX Expectations Are Changing

Consumer technology has raised the bar for enterprise and B2B UX. Employees and partners expect the same convenience and immediacy at work that they experience in ecommerce or mobile apps. Waiting for access or calling IT for help is no longer acceptable.

However, friction isn't inherently bad. For sensitive transactions or access to critical systems, a second authentication step can provide assurance and build trust. The challenge is to find the right balance and apply friction intelligently, in ways that make users feel secure rather than frustrated.

Organizations that calibrate security with thoughtful UX are better positioned to meet these rising expectations while still managing risk.

Key Considerations

- Consider UX both emotionally and functionally
- Password resets are the most hated, and most common, IT support tickets
- Persistent sessions + invisible risk checks = seamless *and* secure

76% of consumers globally say ease of use is important when interacting with brands online.¹

70% are not satisfied with the password recovery process on the websites and apps they frequently use.¹

54% have stopped using an online account or service due to login frustrations.¹



Great UX = Strong Security

A common misconception in IT is that better security must come at the cost of usability, but the opposite is often true.

- When UX is intentionally designed, it can strengthen security.
- Access journeys designed to reflect real-world usage reduce friction while supporting secure behavior.

In bring-your-own-device (BYOD) environments or among hybrid and mobile workers, traditional network-based signals are no longer reliable. Additionally, today's consumer is more mobile than ever, and may attempt to make purchases in different countries within the same week. That's where capabilities like user and entity behavior analytics (UEBA) come in, enabling seamless, risk-aware access decisions. In large enterprises, device loss and replacement are frequent, so recovery must be fast and intuitive to avoid insecure workarounds. By applying friction only when necessary, and clearly communicating why it's needed, organizations can build trust with their customers, employees, and the businesses they work with day in and day out.

Ultimately, strong security and great UX aren't competing priorities; they're mutually reinforcing when designed with all users in mind.

Real Results from Ping Customers

Multi-National Payment Provider



Reduced MFA prompts from multiple times daily to once per week after working Ping Identity. The change led to a measurable drop in abandonment and **30% fewer help desk tickets** for login issues.

Leading U.S. Freight & Logistics Company



Implemented passwordless and identity verification, and in just a few months, onboarded 200,000 users with **100% MFA adoption**, generating less than 2% of support call volumes.²

Global Pharmaceutical Enterprise



By offering multiple MFA options (biometrics, apps, SMS), **98% of users** now opt for Ping Identity's mobile app, improving both security and UX.²



Start Small: Identify, Segment, Prioritize

The most effective IT teams begin by deeply understanding their user base and identifying where friction creates real problems. A one-size-fits-all approach rarely works. Different user segments need different identity strategies, and not every app is ready for a full modernization.

Rather than tackling the entire stack, teams should start with a low-risk application and test a modernized user journey. This makes it easier to gather feedback, refine the approach, and earn support from stakeholders across the business.

IT leaders also face the challenge of coordination. App owners, security leads, and compliance officers may all have conflicting priorities. Starting small helps build momentum and alignment.



Tips for Getting Started

1. Align on the top 10 identity-related issues before implementing solution
2. Focus on improving UX on one channel before overhauling everything
3. A "crawl, walk, run" approach wins stakeholder trust and long-term success

Ready to Fix Your UX Pain Points?

Pinpoint friction with our UX checklist.

[Get the Checklist](#)



Set Your IT Team Up for Success

Improving user journeys isn't a one-and-done project. In fact, it's almost guaranteed that the first version won't be optimal. That's why monitoring and adaptability are essential.

Capabilities like orchestration let teams test different flows, make changes quickly, and personalize experiences for different user types or risk levels. An IAM platform's ability to integrate with third-party analytics tools and provide orchestration-enabled A/B testing helps pinpoint exactly where users are getting stuck or dropping off.

Support teams are also a valuable source of insight—frequent password reset requests or recovery failures are signs of deeper UX flaws that need to be addressed.

A leading home improvement retailer saw **83% growth** in new online accounts in the 2 years since implementing Ping Identity's solution to streamline and simplify registration.

The IT UX Toolkit

- ✓ **Orchestration** for adapting flows in real time
- ✓ **Monitoring and analytics** to find and fix excessive friction
- ✓ **SDKs** that enable dynamic journey updates without app-store redeployments
- ✓ **Support team input** to surface pain points fast



From Reactive to Proactive Identity

Today's IT teams aren't just infrastructure maintainers; they're valuable UX contributors. Identity is the first and last touchpoint for most digital interactions, and when access flows are smooth and secure, sales, productivity, and overall user satisfaction rises.

Rather than reacting to complaints or security issues, proactive teams embed experience thinking into every part of their identity strategy. They understand that better UX leads to fewer support issues, higher engagement, stronger customer loyalty, and productive B2B relationships.

The opportunity is clear: IT professionals who lead on UX will shape more agile, secure, and business-aligned organizations.

Walk in Your Users' Shoes

Uncover UX issues with our identity checklist.

Get the Checklist

#4180 | 06.25 | v01



EBOOK | The IT Pro's Survival Guide to UX

Hear From the Experts

Gartner®

- [2024 Gartner® Magic Quadrant™ for Access Management](#)
- [2025 Gartner® Critical Capabilities for Access Management](#)

FORRESTER®

- [The Forrester Wave™: Customer Identity and Access Management Solutions, Q4 2024](#)



- [2024 KuppingerCole Leadership Compass: Passwordless for Enterprise](#)
- [2024 KuppingerCole Leadership Compass: CIAM](#)

¹ [Ping Identity Consumer Survey - October 2024](#)

At Ping Identity, we believe in making digital experiences both secure and seamless for all users, without compromise. That's digital freedom. Ping enables enterprises to combine our best-in-class identity solutions with third-party services they already use to remove passwords, prevent fraud, enable Zero Trust, or anything in between. And they can do it all with a simple drag-and-drop canvas. That's why more than half of the Fortune 100 choose Ping Identity to protect every single digital interaction for their users, while making experiences frictionless. Learn more at www.pingidentity.com.