fido ALLIANCE | simpler stronger authentication

Inside RSA: Deploying FIDO and Passwordless Solutions at Scale

The Challenge

When an organization sells authentication solutions, there's no hiding from the hard question: **Does it actually use what it builds?**

In 2024, RSA leadership set a goal: 100% passwordless for its workforce. RSA is a global security company with employees distributed across offices worldwide—a deployment footprint that mirrors what many enterprise customers face. The motivation to go passwordless was twofold: to reduce credential risk and strengthen RSA's security posture, and to stop speaking about passwordless deployment from a distance. RSA put itself in its customers' shoes—to experience every integration challenge, every policy decision, every change management hurdle that enterprises face deploying passwordless and FIDO at scale.

This is what RSA learned when theory met reality.

RSA's Starting Position

For RSA, that gap had a specific shape. RSA® ID Plus is an identity and access management (IAM) security platform that supports passwordless multi-factor authentication, access, SSO, and other capabilities across cloud, hybrid, and on-premises environments.

The ID Plus platform team was actively building the capabilities enterprises need for passwordless deployment—enrollment flows, recovery paths, and access policies—while RSA's own workforce was still using passwords. RSA's security and R&D teams had run early experiments with FIDO hardware security keys, and those experiments confirmed the technology's security properties. What those reviews also surfaced were the operational realities of deploying FIDO passwordless: cross-platform friction, global distribution complexity, the gap between a working proof of concept and an enterprise-wide rollout. The decision to deploy RSA ID Plus and support passwordless across RSA's own organization wasn't a marketing exercise. It was the only honest way to validate its solution's efficacy in supporting passwordless for all users, in all environments, and for every use case.

Case Study Authors:
Shauna Pettit-Brown, Robert Hughes, Jean-Christophe Laurent, Kenn Chong, and Philip J Corriveau

RSA®

About RSA Security

RSA provides the identity intelligence, authentication, access, governance, and lifecycle capabilities needed to prevent threats, secure access, and enable compliance. More than 9,000 security-first organizations trust RSA to manage more than 60 million identities across on-premises, hybrid, and multi-cloud environments. For additional information, visit RSA.com.

What Internal Deployment Exposed

In deploying its own platform, RSA learned something critical: ID Plus worked as expected. The complexity was in how it interacted with the broader RSA identity ecosystem.

In implementing enterprise-wide passwordless, RSA discovered assumptions and dependencies that defaulted to password-based authentication. In the process to implement 100% passwordless, RSA resolved those dependencies and cleared the way for true passwordless. The following details the use cases where RSA uncovered passwordless-based authentication, and how RSA removed them to support passwordless for every user, in every environment, throughout the identity lifecycle.

The Architecture Catch-22

One of the first use cases RSA discovered was how new users register for their first authenticator.

The RSA self-service portal required an authenticator for passwordless authentication—but new employees needed a password to access the portal to register their first authenticator. This wasn't a product limitation; it was a previous architectural dependency that assumed users would need passwords.

What RSA fixed (Late 2024):

- New user enrollment ⟶ Dedicated entry point requiring no password
- Account recovery ⟶ Separate flow bypassing password reset
- Daily authentication ⟶ Policies making passwordless the default

What RSA learned: Having implemented these changes itself, RSA now asks customers different questions during planning—not "what authenticators do you want" but "where are passwords still required?"

Securing Help Desk Interactions

As RSA deployed passwordless authentication and resolved new user onboarding, RSA addressed an adjacent security concern: help desk verification. Traditional knowledge-based verification (employee ID, manager name) can be researched by attackers, who then socially engineer support staff into resetting credentials, or social engineer employees into handing over credentials.

The RSA approach: RSA implemented bi-directional live verification for help desk interactions. When an employee contacts support, the agent initiates a verification session. The employee authenticates using any registered method (passkey, QR code, biometric), and the system generates a single-use code that the employee provides to the agent. This can verify both parties, confirming the user is legitimate, and the agent is an authorized representative.

What RSA learned: Passwordless infrastructure made this solution feasible. RSA could leverage the same methods employees already used for daily authentication, eliminating shared secrets at the help desk touchpoint where social engineering attacks often succeed.

Policy and Group Management Complexity

The ID Plus platform had robust policy capabilities. What internal deployment exposed was the organizational complexity of deciding those policies and implementing them in a coordinated way. RSA had to address the following questions in rolling out passwordless:

- Who are the first groups to get the new policies?
- How should it phase policies across departments with different risk profiles?
- What's the fallback for the unforeseen edge cases?

What RSA learned: This isn't a technology problem customers can solve with software. It's organizational decision-making that requires time, stakeholder alignment, and iteration. RSA couldn't shortcut it for itself, and RSA can't shortcut it for customers either—but RSA can share what worked and what didn't.

The Mobile Passkey Breakthrough

With platform architecture in place, RSA tackled the hardware distribution challenge its R&D teams encountered.

In early 2025, RSA integrated FIDO-based device-bound passkeys support into its mobile authenticator app, which is now a FIDO2 certified authenticator. This ensured RSA could distribute passkeys in a way that fit how its workforce already worked.

The adoption advantage: RSA employees were already using the mobile app for authentication. Adding passkey support to it required no new app, no separate enrollment, and no user-initiated setup.

Outcome: Passkey adoption wasn't an uphill climb—it was a natural extension of existing behavior. RSA eliminated the hardware distribution challenges faced in R&D while maintaining FIDO phishing resistance.

Why this matters for enterprises: Organizations evaluating "software-based synced passkeys vs. hardware-based (device-bound passkeys)" often miss this third option: software-based device-bound passkeys in an existing enterprise mobile authenticator app. It gives organizations the control and security of device-bound passkeys with better UX and no hardware distribution overhead.

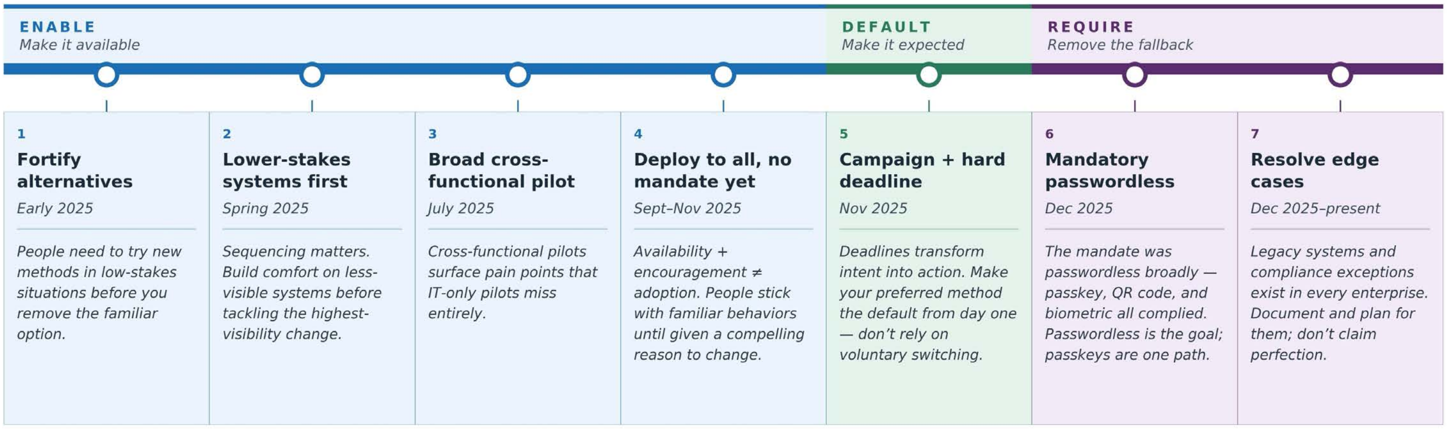
The Deployment Journey: Where Technology Met Human Behavior

With the platform ready and mobile passkeys easing distribution and onboarding, RSA began workforce rollout. **This is where the company learned that technical readiness ≠ organizational readiness.**

The technology was deployed in weeks. Changing employee habits took longer, up to a year for some. The journey moved through three meaningful shifts: making passwordless available **(Enable)**, making it the expected path **(Default)**, and removing the fallback entirely **(Require)**. The steps below map to that arc.

FIGURE

The Passwordless Journey: Enable → Default → Require



ENABLE
Make it available

DEFAULT
Make it expected

REQUIRE
Remove the fallback

1 **Fortify alternatives**
Early 2025
People need to try new methods in low-stakes situations before you remove the familiar option.

2 **Lower-stakes systems first**
Spring 2025
Sequencing matters. Build comfort on less-visible systems before tackling the highest-visibility change.

3 **Broad cross-functional pilot**
July 2025
Cross-functional pilots surface pain points that IT-only pilots miss entirely.

4 **Deploy to all, no mandate yet**
Sept–Nov 2025
Availability + encouragement ≠ adoption. People stick with familiar behaviors until given a compelling reason to change.

5 **Campaign + hard deadline**
Nov 2025
Deadlines transform intent into action. Make your preferred method the default from day one — don't rely on voluntary switching.

6 **Mandatory passwordless**
Dec 2025
The mandate was passwordless broadly — passkey, QR code, and biometric all complied. Passwordless is the goal; passkeys are one path.

7 **Resolve edge cases**
Dec 2025–present
Legacy systems and compliance exceptions exist in every enterprise. Document and plan for them; don't claim perfection.

ENABLE

Steps 1–4: Make Passwordless Available

Before organizations can ask people to change, they have to make change feel safe to try. The 'Enable' stage is about removing the psychological cost of experimenting with something new—not by pushing adoption, but by ensuring the familiar fallback still exists while employees build confidence. Change management research consistently shows that people need low-stakes exposure to a new behavior before they'll voluntarily substitute it for an established one.

The goal here isn't momentum; it's readiness.

STEP 1:
Fortify Alternatives Before Removing Passwords (Early 2025)

Passwordless options were available. Passwords still worked. Goal: familiarization, not adoption.

What RSA learned: People need to try new methods in low-stakes situations before organizations remove the familiar option.

STEP 2:
Remove Passwords from Lower-Stakes Systems First (Spring 2025)

VPN and SSO went passwordless before desktop login. This normalized “passwords aren’t always available” before the highest-visibility change.

What RSA learned: Sequencing matters. Build comfort on less visible systems before tackling what employees use more frequently.

STEP 3:
Pilot Desktop Agent Broadly (July 2025)

50 employees across the company—not just IT—tested desktop passkey authentication with passwords as fallback.

Key decision: Diverse roles, not just technical users, build credibility.

What RSA learned: Cross-functional pilots surface different pain points than IT-only pilots. RSA found UX issues and communication gaps that would have been missed otherwise.

STEP 4:
Deploy to All, Don’t Mandate Yet (Sept-Nov 2025)

Workstation passkey authentication available to everyone. Passwords still worked.

Result: Adoption was very modest. Despite availability and encouragement, most employees continued using passwords.

What RSA learned: Availability and encouragement don’t lead to adoption. Experiencing this first-hand gave RSA deeper empathy for what its customers face. People stick with familiar behaviors unless they are given a compelling reason to change. People may fear being unable to access their systems and get their job done when their authentication methods change.

DEFAULT
Step 5: Make Passwordless the Expected Path

Availability is not the same as adoption. When people have a choice between a familiar path and a new one, they take the familiar path—almost every time. Behavioral research on default effects makes this plain: the option that requires the least effort wins, regardless of which option is objectively better. The default stage is where an organization stops relying on voluntary switching and starts designing the system so that passwordless is simply what happens. A deadline makes that design decision visible and real.

STEP 5:
Campaign + Clear Deadline (November 2025)

Intensive 3-week push combining:

- Gamification (scavenger hunts, prizes, leaderboards)
- Social proof (executive participation, peer champions)
- Clear deadline: “Passwordless becomes mandatory December 1”

Result: Usage increased 3x in three weeks.

What RSA learned: Deadlines transform “I should try this eventually” into “I need to do this now.” Voluntary adoption plateaus, but campaigns with deadlines drive real behavior change—a pattern RSA expects customers will encounter as well.

One further lesson: if organizations want employees to adopt a particular authentication method, make it the default from day one. Asking users to actively switch on their own is an uphill battle—most will stay on whichever path requires the least effort. Design the default toward the preferred authenticator; don’t rely on voluntary switching to deliver results.

REQUIRE
Steps 6–7: Remove the Fallback

Behavior change sticks when the old behavior is no longer an option. Removing the password fallback is what transformed this campaign into a permanent shift—it’s the difference between a temporary experiment and a new organizational norm.

This is also where the distinction between “passwordless” and “passkeys” becomes operationally important: employees could comply via passkey, QR code, or biometric. From the outset, RSA had been working to fulfill the mandate for passwordless authentication, not the method. Prioritizing that mandate reduced friction and avoided the perception of a forced technology choice.

STEP 6:
Mandatory Desktop Passwordless (December 2025)

Passwords disabled for workstation authentication. Because most employees had already switched in November, the mandate minimized disruption.

What RSA learned: With an expanded testing group, the implementation team had already identified and resolved problems. Help desk volume increased but was manageable.

One important distinction worth making explicit: the mandate was for **passwordless authentication**, not specifically passkeys. Employees who authenticated via QR code, biometric, or other FIDO-based methods were fully compliant. RSA’s desire was to use FIDO wherever possible, however at this point in the journey something is better than nothing and phishing risk was reduced in these specific use cases relative to password-based authentication. “Passwordless” is the outcome; passkeys are one path to get there. This distinction matters for customer conversations—enterprises often conflate the two, and setting expectations correctly up front reduces confusion during rollout. The added advantage here was RSA had all these options in the same application, so the right method could be offered at the right moment with virtually the same user experience, hence not causing added friction to the authentication process.

STEP 7:
Finding the Edge Cases (Dec 2025-Present)

RSA is continuing to find and resolve edge cases that still require some degree of password-based authentication. Examples include third-party integrations that need reconfiguration; legacy systems where the FIDO authentication flow is not yet supported; and systems where FIDO authentication cannot be used because of compliance requirements. RSA is also identifying other identity silos that may need dedicated attention.

What RSA learned: Even with careful planning, organizations discover exceptions in production. RSA is addressing these through workarounds, action plans, and documented exceptions. This is normal—other organizations working toward similar passwordless mandates face it too.

What RSA Now Knows—From Experience, Not Theory

The results have been directionally clear across every dimension RSA tracked. Password-related help desk tickets dropped significantly once the mandate took effect—the volume spike during transition was temporary and manageable. RSA reached near complete passwordless adoption across managed endpoints within twelve months of starting workforce rollout, a timeline that included the slow voluntary phase and the campaign requiring passwordless that broke the plateau. Phishing and credential-based attack surface on managed systems has measurably narrowed. And the deployment itself—from platform readiness through full mandate—was achievable within a single fiscal year, even accounting for the organizational change work that technology timelines rarely budget for.

What Worked: RSA's Recommendations for Enterprise Passwordless

RSA recommends the following best practices for implementing enterprise-wide passwordless:

Technology Best Practices

Platform architecture comes first. Remove password dependencies from enrollment, recovery, and policies before deploying authenticators. Otherwise, FIDO becomes an add-on, not a replacement, leaving weak links in an organization's identity chain.

Passwordless enables adjacent security improvements. Help desk verification was a longstanding vulnerability. Passwordless infrastructure made bi-directional live verification feasible, eliminating shared secrets at a critical touchpoint.

Device-bound passkeys in mobile apps offer a third option. Beyond "synced passkeys vs. security keys," this approach enhances enterprise control, improves UX, and eliminates hardware distribution overhead.

Deployment Best Practices

Leverage existing user behavior. RSA progressed faster because employees already had the mobile app. Organizations should find and prioritize their existing authentication foothold.

Sequence deliberately: alternatives ⟶ lower-stakes ⟶ high-stakes. Don't start with the most visible system. Build comfort first.

Deploy broadly, mandate later. Give employees time to adopt on their timeline. Learn what confuses people. Build a network of interested testers across the business and champions.

Campaigns and deadlines outperform either alone. Voluntary adoption will plateau regardless of how good the UX is — plan for it. Social proof matters, but so does urgency. RSA saw a 3x usage increase when it combined them with a clear deadline.

Redundancy Best Practices

Plan for when a method fails or a device goes missing — because it will happen. Passwordless authentication requires deliberate redundancy, both in methods and devices. The FIDO Alliance recommends each user register at least two passkeys when possible for this reason. In the RSA deployment, certain user groups received both a software-based device-bound passkey via the RSA mobile app and a hardware-based device-bound passkey, so that losing access to either one never meant losing access entirely.

RSA's Organizational Change Best Practices

Budget enough time to drive behavior change. Technology deployment takes weeks. Organizational habit change takes months.

Set ambitious goals, then be transparent about scope. The RSA leadership team mandated 100% passwordless—and that bold target drove the organization much further than a softer goal like "improve authentication" would have. RSA eliminated passwords from all managed endpoints and primary authentication flows. Legacy systems and edge cases exist; RSA documents them and is developing plans to resolve them rather than claiming perfection. Every enterprise will face this reality.

"What's a passkey?" is a real question. Outside engineering, employees needed education. RSA developed clear analogies and updated documentation to connect the technology to familiar mental models.

Consolidate authenticator methods in a single application. When employees can authenticate via passkey, QR code, or biometric from the same app they already use, compliance doesn't require behavior change — it just requires a different tap. RSA's ability to offer the right method at the right moment, without switching apps or adding friction, materially reduced resistance during the mandate rollout.

What This Proved to RSA (and Customers)

Going passwordless internally gave RSA something it couldn't get from customer pilots or lab testing: **live experience with the full complexity** of implementing passwordless for everyone.

RSA experienced:

- Executive buy-in was critical to getting started
- Platform integration with existing infrastructure
- Cross-platform complexity, offline scenarios, heterogeneous devices
- Ongoing policy refinement as deployment realities emerged
- Change management that takes months, not weeks
- Help desk volume during transition
- The gap between voluntary adoption and mandate
- Edge cases organizations can't predict in planning

When customers ask, "how long will this really take?" or "what about employees who resist?" or "what do we do about legacy systems?"—RSA answers from experience, not theory.

RSA moved from passkeys as an R&D experiment to passwordless as its default for managed environments. The organization has validated its platform in production under real enterprise conditions—including the year-long organizational journey most case studies compress into a single paragraph.

That authenticity is what no demo environment can provide.

This process has shaped how RSA contributes to the FIDO Alliance community. RSA will continue working with other members to develop deployment playbooks, implementation guides, and share learnings that help enterprises navigate the same journey. Because the more organizations succeed with passkeys, the more secure all organizations become.

The technical standards are established.
Now it's about helping enterprises deploy them successfully—together.