Special Report

Fast Track to Passwordless: How to Implement Passkeys and Passwordless Authentication in Your Organization

SECFENSE

secfense.com

Table of contents

1. Introduction

The transition to passwordless authentication using **passkey** technology is no longer a question of if, but how. Traditional passwords have proven ineffective against modern cybersecurity threats, and weak or stolen credentials remain one of the leading causes of data breaches and significant financial losses.

Passwordless solutions—such as **passkeys**—are widely recognized for delivering stronger security, lower costs, and improved user convenience. However, many organizations still face uncertainty around how to effectively implement these technologies.

This guide provides **practical steps** for selecting the right provider and deploying passkeys in the most efficient and secure way.

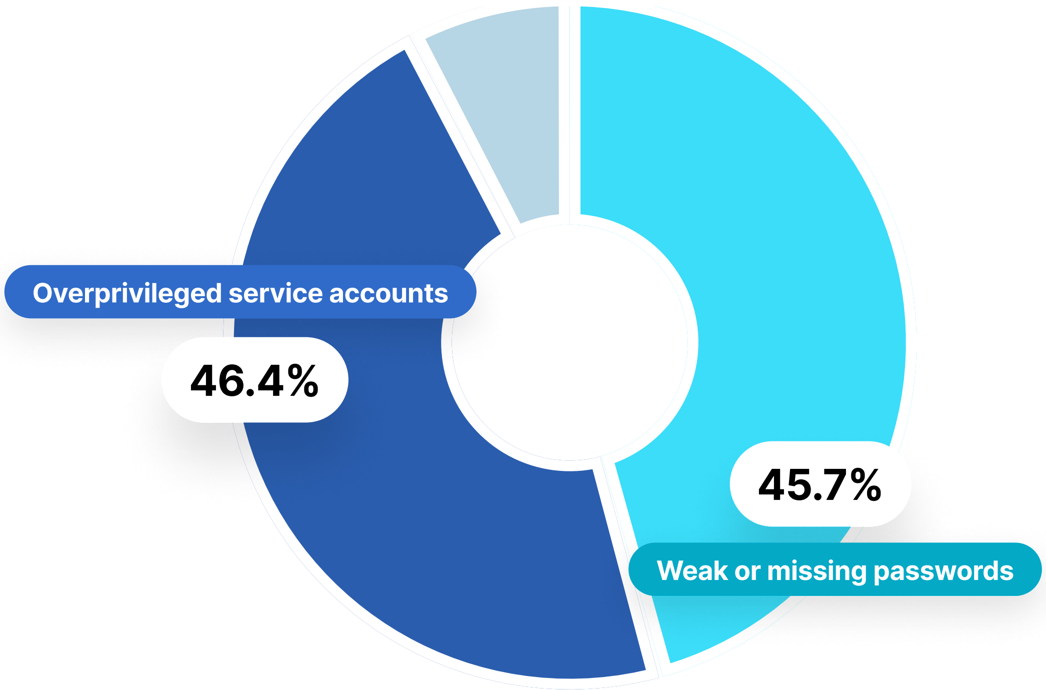
2. Why Passwordless Authentication is Inevitable and Necessary

Passwords are becoming increasingly ineffective. Over **80% of data breaches** are linked to compromised credentials (according to the Verizon DBIR report). Password management is costly and inefficient—Gartner estimates that **20% to 50%** of all IT helpdesk requests involve password resets.

Passkeys, based on the **FIDO2 standard**, replace passwords with secure, user-friendly methods such as biometric or hardware keys. This eliminates inherent weaknesses of passwords, such as susceptibility to phishing or data leaks. Industry leaders like **Google** and **Microsoft** have already adopted passkeys, and regulations like **GDPR** and **NIS2** are encouraging the use of stronger authentication methods.

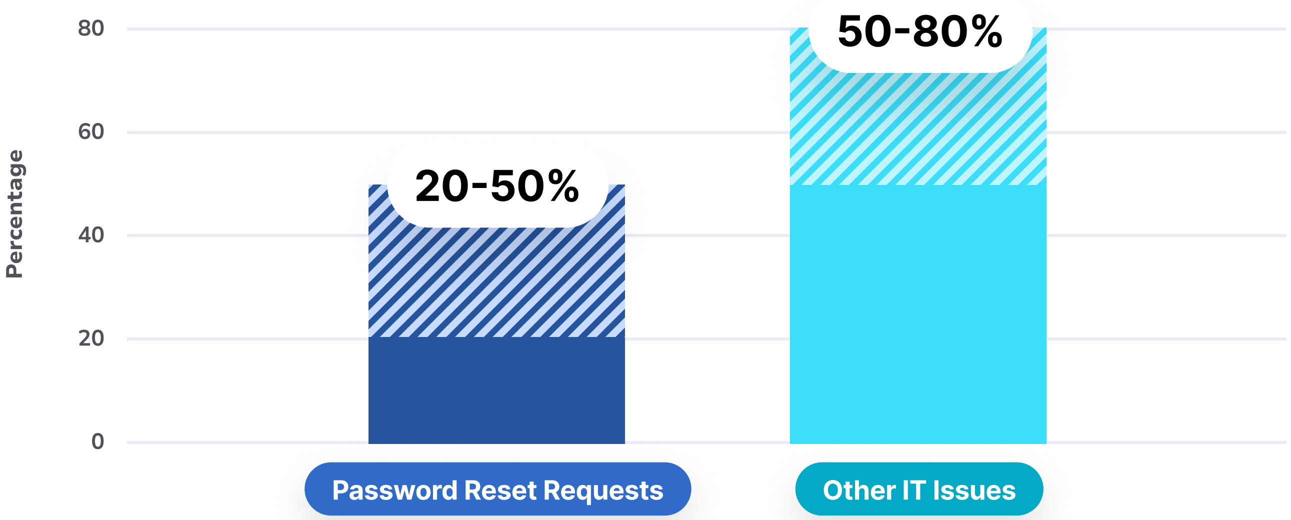
Moving to passwordless authentication is **no longer optional**—it's a necessity for ensuring both security and regulatory compliance.

Common Identity and Authentication Gaps



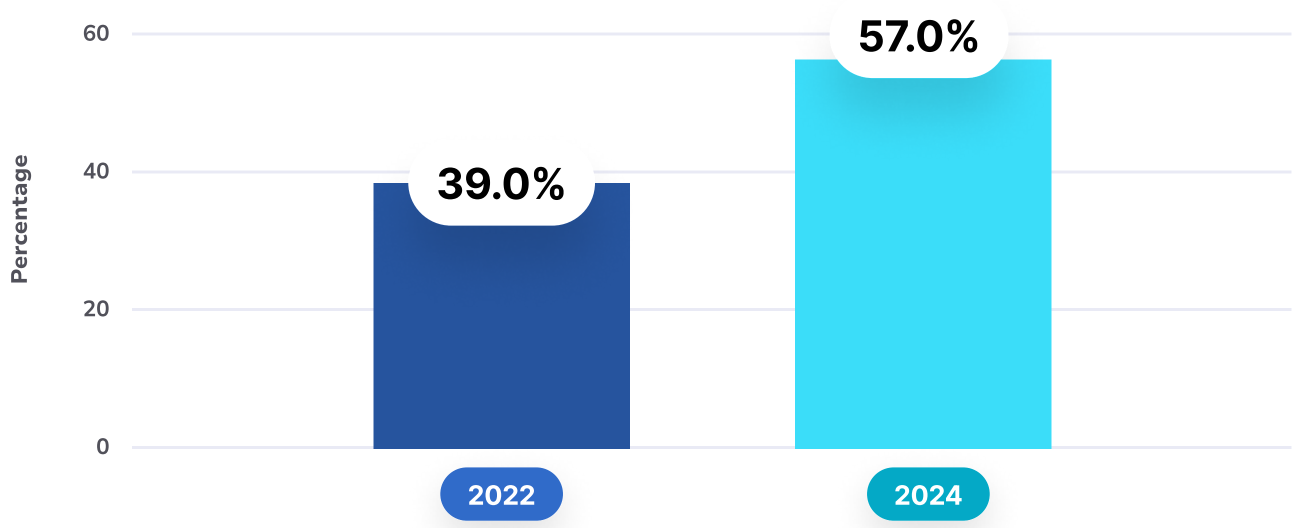
Source: Google Cloud Threat Horizons H1 2025 Report

IT Helpdesk Calls: Password Resets vs. Other Issues



Source: BleepingComputer

Global Awareness of Passkeys



A 50% increase in global awareness of passkeys between 2022 and 2024

Source: FIDO Alliance 2024 Online Authentication Barometer
Among those aware of passkeys, **62%** already use them to protect online accounts.

Key Regulations Emphasizing Strong Authentication & Identity Management

Regulation	Sector
General Data Protection Regulation (GDPR)	All sectors processing personal data in the EU
NIST Cybersecurity Framework (CSF) 2.0	All sectors, especially critical infrastructure in the US
Payment Card Industry Data Security Standard (PCI DSS) 4.0	Organizations globally that handle payment card data
NIS2 Directive	Critical infrastructure in the EU (energy, transport, banking, healthcare, digital infrastructure)
Digital Operational Resilience Act (DORA)	EU financial entities, including banks, insurers, and investment firms

3. Costs and Benefits of Transitioning to Passkeys and Passwordless Authentication

This chapter compares the costs of traditional passwords and passwordless authentication over a five-year period. Moving to passwordless authentication requires an upfront investment but offers significant long-term financial and security benefits. By analyzing costs over a five-year horizon, we can better understand the potential return on investment (ROI) and the long-term advantages of adopting passkeys.

To provide specific context, we focus on a mid-sized enterprise with approximately 5,000 employees. This profile is typical for organizations in sectors like financial services, technology, healthcare, and retail. Companies of this size face challenges in balancing security practices with operational efficiency, making them ideal candidates for passwordless solutions.

3.1 Breakdown of Password Costs

Passwords pose both security risks and considerable financial burdens. For a company with 5,000 employees, these costs add up as follows:

Password reset costs:

- Each employee requests an average of two password resets per year, and each reset costs $70 in IT helpdesk resources. Annual reset cost:

5,000 employees × 2 resets × $70 = $700,000

(Forrester Research estimates each password reset costs approximately $70.)

Security breach costs:

- Password-related breaches are common and expensive. According to IBM's 2024 Cost of a Data Breach Report, the average global cost of a data breach is $4.88 million. With an estimated 60% likelihood of a breach per year:

$4,880,000 × 0.60 = $2,928,000 annually

(The 60% attack probability estimate was derived using Perplexity AI, an AI search engine combining language models with real-time web results.)

Time lost entering passwords:

- Employees enter passwords an average of 154 times per month, each taking about 10 seconds. That amounts to:

154 entries × 10 seconds × 12 months = 18,480 seconds/year ≈ 5 hours/employee/year

- Assuming a labor cost of $40/hour, the annual cost of wasted time per employee is:

5 hours × $40 = $200

- For 5,000 employees:

$200 × 5,000 = $1,000,000

(According to a report by LastPass, employees enter credentials 154 times per month on average.)

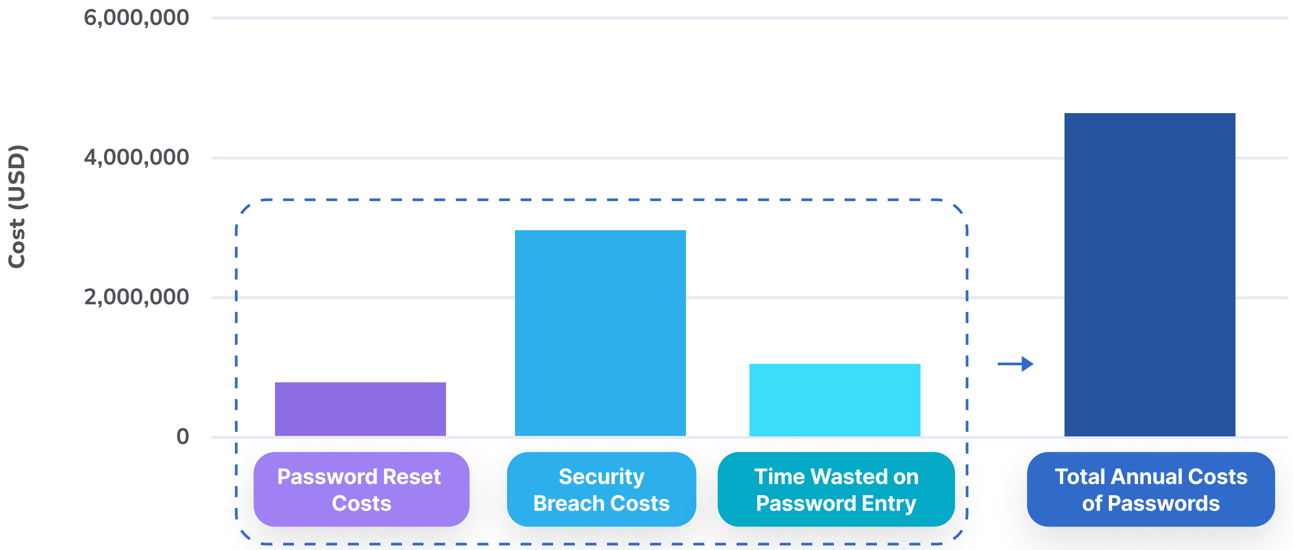
Total annual cost of passwords:

$700,000 + $2,928,000 + $1,000,000 = $4,628,000

Assuming a 4% annual increase in costs due to inflation, labor cost growth, and security policy changes, the cost progression over five years looks like:

- **Year 1:** $4,628,000
- **Year 2:** $4,813,120
- **Year 3:** $5,005,645
- **Year 4:** $5,205,871
- **Year 5:** $5,414,106

Costs related to passwords



This chart visualizes the breakdown of password-related costs, illustrating the expenses on resets, breaches, and time wasted.

3.2 Understanding the Cost of Implementing Passkeys

Passwordless authentication requires an initial investment, but ongoing costs are significantly lower than those associated with traditional password management.

For the same 5,000-employee company, costs include:

- **Software licenses:**
  - $35 per user annually = $175,000/year
- **Hardware security keys:**
  - $30 per user one-time = $165,000 (includes 10% extra for backup keys)
- **Integration and deployment:**
  - $70,000 (initial setup and training)

Total Year 1 cost (with hardware keys):

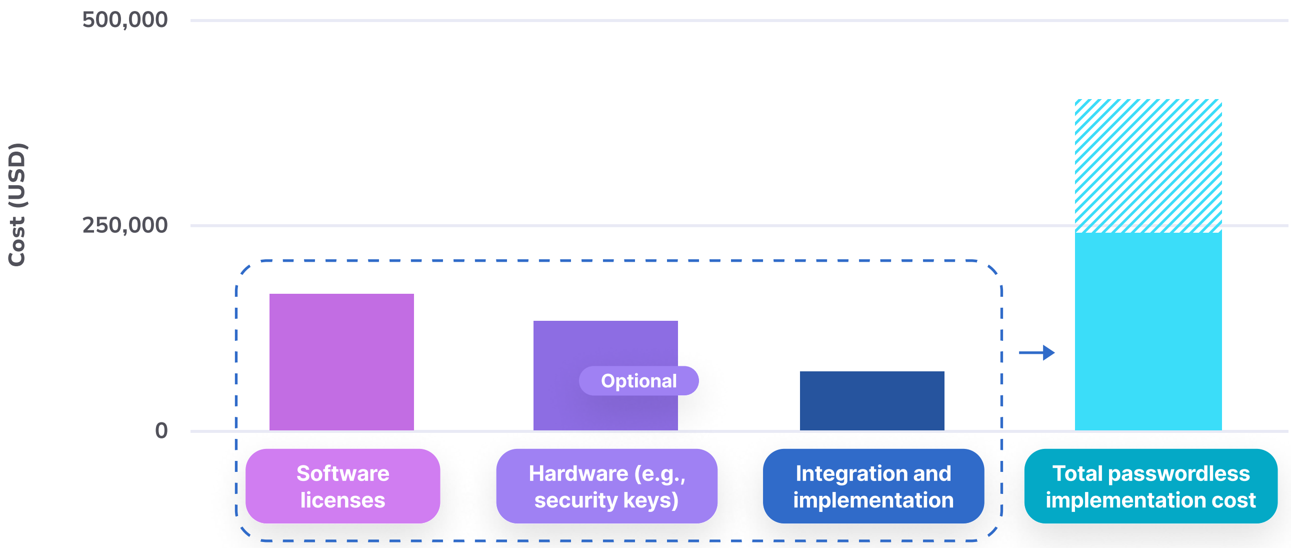
$175,000 + $165,000 + $70,000 = $410,000

Total Year 1 cost (without hardware keys):

If the organization uses existing devices (e.g., mobile phones) as FIDO authenticators, hardware key costs can be eliminated:

$175,000 + $70,000 = $245,000

Costs of passwordless implementation



This chart illustrates the costs of passwordless implementation, including software, with and without hardware keys, and integration expenses.

3.3 Passkey Implementation Costs Over Five Years

Assuming software licensing costs increase 10% annually due to product enhancements and new features:

- **Year 1:** $410,000 (with hardware keys)
- **Year 2:** $192,500
- **Year 3:** $211,750
- **Year 4:** $232,925
- **Year 5:** $256,218

3.4 Cost Comparison and Savings: Passwords vs. Passkeys

The transition to passkeys delivers significant financial benefits by reducing helpdesk dependency, limiting security breaches, and eliminating inefficiencies. Based on the data:

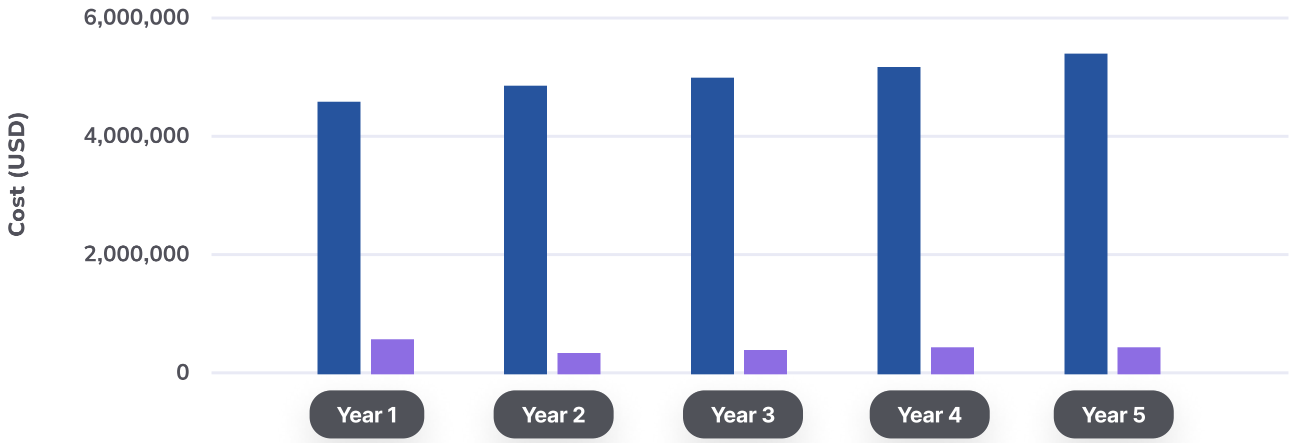
Year	Password Costs	Passkey Costs
Year 1	$4,628,000	$410,000
Year 2	$4,813,120	$192,500
Year 3	$5,005,645	$211,750
Year 4	$5,205,871	$232,925
Year 5	$5,414,106	$256,218

Five-year total:

- Passwords: $25,066,742
- Passkeys: $1,233,392

Total savings over 5 years:

$25,066,742 - $1,233,392 = $23,833,350



This chart compares the total costs of passwords and passwordless solutions over five years, clearly highlighting the dramatic reduction in expenses and ROI.

4. Passkey Implementation Plan

To successfully transition to passkeys, an effective implementation plan is essential. This action plan offers a structured step-by-step process designed to minimize disruptions and maximize the effectiveness of the rollout across the organization. It serves as a guide to assess readiness, conduct pilot testing, roll out the solution gradually, and optimize performance over time. The ultimate goal is to replace traditional passwords with a seamless, secure, and efficient authentication system—while maintaining business continuity and user satisfaction.

To visualize the implementation plan, we present three approaches for representing the deployment process. Each method provides a different perspective tailored to various stakeholders or organizational needs:

- **Option 1: Gantt Chart** – A timeline-based approach for tracking phases and their duration
- **Option 2: Flowchart** – A process-oriented representation focusing on task sequences and dependencies
- **Option 3: Layered Timeline Chart** – A high-level overview showing overlapping phases and milestones over time

4.1 Option 1: Gantt Chart

The Gantt chart organizes the action plan into phases and tasks with specific start and end dates. It provides a clear picture of task durations, enabling teams to allocate resources efficiently and identify dependencies.

Example:
The action plan begins with an **Organizational Readiness Assessment** (Weeks 1–3), followed by a **Proof of Concept (PoC)** (Weeks 4–6). **Phased Rollout** covers Weeks 7–10, while **Transition and Training** occur during Weeks 11–13. **Ongoing Optimization** continues beyond Week 13.

This structure is ideal for project managers who need to monitor progress and coordinate tasks across teams.

Phase	Subtask	Duration (days)
Organizational Readiness	Assess current authentication methods, analyze technical infrastructure	7
Proof of Concept	Identify high-risk systems and users, select pilot group and applications	7
	Test user experience and integration, collect feedback, refine strategy	7
Phased Rollout	Plan the phased deployment schedule	7
	Start with non-critical systems	7
	Expand to business-critical environments	7
Transition & Training	Provide training and clear instructions	7
	Implement self-service registration	7
	Monitor adoption and address issues	7
Ongoing Optimization	Review and improve security policies	7
	Update according to FIDO2 standards	7

4.2 Option 2: Flowchart

The flowchart emphasizes the logical sequence of steps, highlighting dependencies between tasks. It’s especially useful for presenting the process to stakeholders or teams unfamiliar with technical details, as it simplifies complex procedures into accessible stages.

Example:
The roadmap begins with **Readiness Assessment** tasks (e.g., infrastructure analysis), moves on to **Proof of Concept**, which tests user experience and integration. After gathering feedback, the solution enters **Phased Rollout**, followed by **Transition and Training**, and ends with **Ongoing Optimization** for continuous improvement.

Step	Details
Step 1: Readiness	Assess systems, infrastructure, and prioritize high-risk areas
Step 2: PoC	Test the solution on a small group to refine the strategy
Step 3: Rollout	Gradual implementation starting with non-critical systems
Step 4: Transition	Train users and monitor adoption
Step 5: Optimization	Regularly review and enhance policies, update to align with standards

4.3 Option 3: Layered Timeline Chart

The layered timeline chart presents overlapping phases and milestones in a compact, visual format. It's ideal for communicating a high-level overview of the action plan to executives or large teams.

Example:
Each phase is represented as a horizontal bar spanning its duration, with key milestones marked at relevant points. For instance, the **Proof of Concept** phase may partially overlap with early **Rollout** activities, demonstrating how parts of the project progress simultaneously.

Phase	Week 1	Week 2	Week 3	Week 4	Week 5	Week 6	Week 7	Week 8
Readiness	▬	▬						
Proof of Concept			▬	▬				
Rollout					▬	▬	▬	
Transition							▬	▬

Each visualization option offers unique advantages. The **Gantt chart** is precise and supports detailed planning, the **flowchart** is intuitive and user-friendly, and the **layered timeline** provides a concise high-level summary. The choice depends on the target audience and the level of detail needed to effectively communicate the implementation strategy.

5. Vendor Selection Checklist

Choosing the right passkey provider is a crucial step toward secure and efficient implementation. To make an informed decision, solutions should be evaluated based on technical compatibility, user experience, cost transparency, and support services. This chapter outlines key factors to consider and provides a practical checklist to assist in the selection process.

5.1 Steps to Achieve Vendor Selection Goals

To confidently select a provider, follow these steps:

1. **Identify your organization's unique authentication needs and technical environment**
2. **Use the checklist provided** to evaluate potential solutions based on essential criteria
3. **Refer to independent analyses and comparisons,** such as the KuppingerCole Leadership Compass, for objective insight

As a vendor, we recognize that our recommendations may be seen as subjective. Our goal, however, is to equip you with tools and an evaluation framework that enable you to make a well-informed decision based on reliable information.

Criteria	Details	Yes/No
Support for FIDO2 and Passkeys	Is the solution compliant with FIDO2 standards?	□
	Does it support various types of authenticators, including passkeys, cryptographic keys, and third-party solutions already in use?	□
Device and Platform Compatibility	Is the solution compatible with legacy systems, cloud applications, and modern devices?	□
	Does it work with commonly used hardware like security keys, laptops, and mobile devices?	□
User Onboarding Process	Is the onboarding process intuitive, such as through self-service registration?	□
	Does it integrate seamlessly with existing user directories (e.g., Active Directory)?	□
	Does it support bulk user registration to reduce administrative overhead?	□
Pricing Transparency	Are the pricing models clear, with no hidden fees?	□
	Are there extra charges for scaling, integrations, or advanced features?	□
Technical Support and Availability Guarantees	Does the provider offer 24/7 support and SLAs with 99.99% uptime guarantees?	□
	Are onboarding support resources and training materials available?	□

5.2 Why Refer to Independent Analyses?

Selecting the right vendor can be challenging without an objective point of reference. We recommend using third-party reports like the KuppingerCole Leadership Compass, which provides independent evaluations of leading passwordless authentication solutions. These analyses cover various criteria, including technical capabilities, market position, and vendor innovation.

By combining the checklist above with independent evaluations, your organization can confidently choose the solution that best meets its needs—balancing security, user convenience, and cost-effectiveness.

6. Call to Action

Transitioning to passwordless authentication is a critical step for organizations aiming to strengthen security and increase operational efficiency. Implementing passkeys eliminates password-related vulnerabilities, enhances the user experience, and reduces the burden on IT departments.

6.1 What to Do Next?

To start your journey toward passwordless authentication, we recommend the following actions:

- **Approve a Proof of Concept (PoC) Deployment**
  Test the solution in a controlled environment.
- **Evaluate Passkeys for Your Environment**
  Assess if passkeys are appropriate for your systems and users.
- **Check Compatibility and Collect Feedback**
  Verify technical compatibility with existing systems and gather input from a selected user group.
- **Engage Trusted Providers**
  Analyze available passwordless solutions tailored to your organization’s needs.
- **Use Independent Reports**
  Leverage evaluations like the KuppingerCole Leadership Compass to compare providers based on their technical capabilities, innovation, and market position.

- **Establish a Rollout Schedule**
  Create a migration plan to eliminate passwords.
- **Prioritize High-Risk Systems and Key Users**
  Focus on critical systems and individuals first.
- **Adopt a Phased Rollout Approach**
  Reduce disruptions by introducing changes gradually across the organization.

By taking these steps, your organization can make a smooth transition to a more secure and efficient authentication model.

6.2 Start Your Journey with Experts and Trusted Resources

To make informed decisions about passwordless authentication, begin with the following resources:

- **FIDO Alliance**
  The FIDO Alliance is a leading organization focused on passwordless authentication standards. Technologies such as FIDO2 and passkeys are the foundation of secure and interoperable solutions.Visit fidoalliance.org to explore technical documentation, best practices, and resources to support your organization's authentication transformation.
- **KuppingerCole Leadership Compass**
  KuppingerCole provides in-depth vendor comparisons and independent analysis of the strengths and weaknesses of leading passwordless solutions. Review the report at kuppingercole.com to select solutions that best fit your needs.

6.3 Let’s Talk – Book a Consultation with Our Experts

At Secfense, we understand that moving to passwordless authentication is a major undertaking. Our consultants are ready to help.

- **Free Consultation (30 minutes)**
  Schedule a session with one of our experts to discuss your organization’s needs and learn how passkeys and passwordless authentication can enhance your security strategy.
- **Tailored Roadmap Support**
  Our team will help design a custom implementation plan—from proof of concept to full deployment—ensuring a smooth and effective transformation.

Book your consultation today and begin your journey to a password-free future!

SECFENSE

www.secfense.com