

SERVICE DESK AUTOMATION AI™
PASSWORDLESS & PASSWORD GOVERNANCE PILLAR 5

AVATIER HYBRID PASSWORDLESS LOGIN™ (patent pending)

Closing the Gap Between Passwordless Vision and Password Reality

Even with Windows Hello and passkeys, passwords don't disappear—they just move deeper into your infrastructure.

Why It Matters

The industry push for "passwordless" creates a dangerous gap: modern authentication on the surface, with ungoverned passwords buried in Active Directory, Entra ID, and legacy systems beneath. This fractured reality undermines security and complicates compliance.

Avatier Hybrid Passwordless Login™ closes this gap. It delivers a true hybrid framework that merges passwordless convenience with enterprise password governance. Users get a frictionless login experience, while administrators maintain zero-trust policy enforcement across every system.

The result is more than just passwordless; it's a unified identity framework where innovation and control coexist.

"A passwordless future requires a governed present. This is that governance." — Nelson Cicchitto, Avatier CEO

How It Works

Avatier replaces the traditional Windows credential process with a browser-based, zero-trust authentication flow. A lightweight credential provider intercepts the login sequence, redirecting users to a secure portal where they verify their identity using any MFA method.

The system seamlessly synchronizes and validates all credentials through the Avatier Password Firewall™, ensuring continuous compliance. Users enroll automatically the first time they log in—no complex provisioning, TPM dependencies, or IT intervention required.

The Critical Need: Beyond Device-Bound Limitations

Limitation	Vendor Example	Business Impact
Hardware Dependency	Windows Hello for Business	Locks credentials to specific devices, failing for shared workstations, VDI, and Citrix environments.
Mobile-First Design	Okta FastPass, HYPR	Excludes high-security, manufacturing, or healthcare sites where personal mobile devices are prohibited.
No Password Governance	Most Passwordless Solutions	Creates unmanaged password sprawl in legacy systems, creating compliance gaps and audit failures.
Complex Deployment	PKI/Certificate Models	Requires months and significant budget for PKI infrastructure, delaying time-to-value.

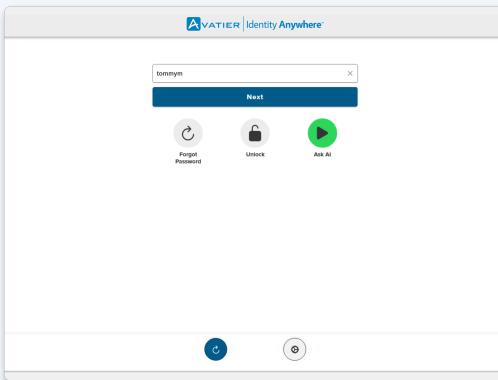
Traditional passwordless systems trade control for convenience, creating new security risks.

Avatier Hybrid Passwordless Login eliminates this compromise by providing a cloud-aware, hardware-agnostic gateway that unites passwordless access with proven password management controls.

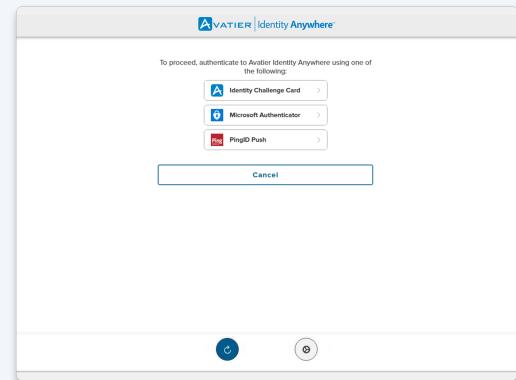
Avatier Hybrid Passwordless Login



Step 1



Step 2



Step 3

The Windows login screen, transformed. No password field. Just a secure, browser-based gateway

Key Advantages & Benefits

Transform the Windows login screen into a universal, zero-trust authentication gateway.

Advantage	Key Benefit	Why It Matters
★ Universal Access	Browser-based login for any Windows device	Works on shared workstations, VDI, and Citrix—no TPM or hardware lock-in.
★ True Hybrid Model	Unifies passwordless and password governance	Maintains compliance and control across both modern and legacy systems.
★ Seamless Enrollment	Automatic enrollment during first login	Eliminates complex provisioning and user training—rollout in hours, not months.
★ Policy Enforcement	Powered by Avatier Password Firewall™	Ensures every credential is breach-checked and policy-compliant in real time.
★ Deviceless MFA	Identity Challenge Card for restricted areas	Provides passwordless access in defense, healthcare, and manufacturing sites where phones are banned.
★ AI Call Center	SIP-aware, multilingual voice authentication	Enables 24/7 zero-trust recovery and verification with zero hold time.
★ Unified Recovery	Integrated Self-Service Reset	Maintains the same MFA and compliance policies for instant, secure account recovery.
★ Centralized Control	Single console for MFA, policy, and audit	Simplifies compliance and reduces risk with one control plane for all identity events.

Top 10 Use Cases

1. Passwordless Windows Login - Zero-trust, browser-based login for any Windows device.
2. Automated User Enrollment - Users enroll automatically during their first login.
3. AI Call Center Authentication - Voice-based verification and resets in 34 languages.
4. Hybrid Coexistence - Maintain legacy system support while enabling modern login.
5. Unified MFA Enforcement - Validate every login against live policy and breach databases.
6. Deviceless MFA Access - Passwordless login for secure, device-restricted environments.
7. Virtual Desktop (VDI) Login - Native support for Citrix and Azure Virtual Desktop.
8. Automated Compliance Auditing - Generate immutable logs for SOC 2, ISO 27001, and CMMC.
9. Unified Access Recovery - Self-service recovery using the same MFA and policies.
10. Simplified Global Deployment - Enterprise rollout via MSI, GPO, or Intune in hours.

Perfect For These Scenarios

Avatier Hybrid Passwordless Login™ is essential for any organization bridging modern authentication with legacy enterprise reality.

Scenario	Why It's Critical
Regulated Enterprises	Maintains continuous password compliance (NIST, CMMC) while adopting passwordless authentication.
Virtualized Environments	Provides native passwordless login for Citrix and AVD where TPM-based solutions fail.
High-Security & Industrial Sites	Supports deviceless MFA for environments where mobile devices are prohibited.
Global Organizations	AI call center integration provides 24/7 multilingual support across all time zones.
Cost-Conscious IT	Deploys at one-third the cost of competitors with faster ROI and broader coverage.

Frequently Asked Questions

1. What is Avatier Hybrid Passwordless Login?

Avatier Hybrid Passwordless Login is a browser-based Windows credential provider that unites passwordless convenience with enterprise password governance. It enables secure, MFA-driven login while synchronizing and validating all credentials through the Avatier Password Firewall™.

2. How is it different from Okta FastPass or Windows Hello?

Unlike device-bound solutions, Avatier is hardware-agnostic and works on any Windows device—including shared workstations and virtual desktops—without TPM, PKI, or mobile dependencies.

3. What does "Hybrid Passwordless" mean?

It means Avatier combines passwordless authentication with active password governance. Users log in with MFA, while the system enforces password policies and synchronizes credentials across all connected systems for full compliance.

4. How does user enrollment work?

Enrollment is automatic. Users simply log in once with their existing password; Avatier captures, encrypts, and syncs the credential. No manual provisioning, QR codes, or app downloads are required.



5. Does it require TPM chips or PKI infrastructure?

No. Avatier is entirely hardware- and PKI-independent, using a secure browser interface to deliver the same zero-trust assurance without the cost or complexity.

6. How does it integrate with existing MFA?

Avatier integrates with Microsoft MFA, Okta Verify, Duo, RSA, and its own Identity Challenge Card. All MFA interactions are policy-enforced through the Password Firewall.

7. What happens if a user loses their MFA device?

Integrated Self-Service Reset allows instant recovery through the same MFA methods and compliance policies, eliminating help desk calls.

8. Can it support virtualized environments like Citrix?

Yes. Avatier is one of the only passwordless solutions that works natively in VDI and thin-client environments without hardware passthrough.

9. What compliance standards does it support?

All authentication events are immutably logged for SOC 2, ISO 27001, CMMC, and other major frameworks, providing complete audit readiness.

10. What is the typical cost and deployment time?

Enterprises typically deploy in hours (not months) at approximately one-third the cost of competitors, achieving faster ROI with broader coverage.

Unifying Innovation and Control

Passwordless shouldn't mean password chaos. True transformation requires a foundation of governance.

Avatier Hybrid Passwordless Login™ provides the intelligent framework that merges zero-trust access with proven password management. It turns the login screen into a universal authentication gateway—one that works everywhere, enforces policy consistently, and adapts to your enterprise reality.

This is how you close the final chapter of the password problem—by making passwordless practical, secure, and governed.

You've secured the password—now transcend it.



[Contact Avatier to see Hybrid Passwordless Login in action](#)

www.avatier.com