

SERVICE DESK AUTOMATION AI™ PASSWORDLESS & PASSWORD GOVERNANCE PILLAR 3 AVATIER ASSISTED RESET

Guided, Secure Help Desk Verification

Most password-reset systems stop where the real risk begins — the human at the help desk.

Why It Matters

Every breach tells the same story: attackers don't hack systems first — they hack people. The help desk has become the new front line of identity compromise, where a single unverified reset can unravel millions in security investment.

Avatier Assisted Reset closes that gap. Its patent-pending, human-assisted MFA transforms every service-desk call into a verified, zero-trust workflow — extending your existing authentication stack directly to the people who handle access.

Every interaction is identity-proofed, auditable, and policy-enforced. The result is more than security; it's engineered trust at human speed.

"Security isn't just software. It's human trust, engineered." — Nelson Cicchitto, Avatier CEO

How It Works

Avatier Assisted Reset brings MFA verification directly into every help desk interaction. Agents follow guided prompts to confirm identity using existing MFA methods before performing unlocks, password resets, or enrollment tasks.

Once validated, changes are applied instantly and fully logged for compliance and audit proof.

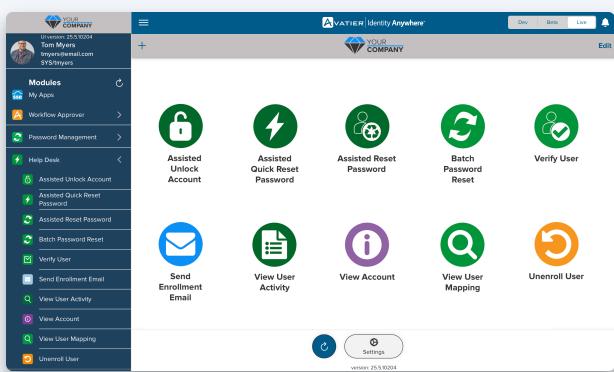
The Critical Need: Stopping Modern Social Engineering Attacks

Financial Impact	Organization (Year)	Attack Details
\$100M	MGM Resorts (2023)	Social engineering attack on IT support led to systemwide outage and >\$100M loss.
\$15M	Caesars Entertainment (2023)	Vendor help desk compromise resulted in ~\$15M ransom payment.
\$380M	Clorox (2023)	Avatier enables new users to securely provision accounts before ever logging in by leveraging the Forgot Password option.
\$22M	Change Healthcare (2024)	Help desk-based credential theft caused a nationwide medical billing outage, impacting hospitals and pharmacies.
\$500M+	Octo Tempest (2022–2024)	Coordinated campaigns exploiting service-desk resets across tech, telecom, and finance sectors.

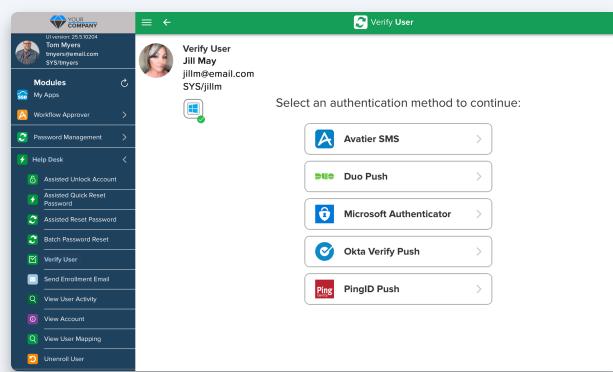
Traditional password-reset systems fail where attackers succeed — by convincing help-desk staff to bypass MFA or reset credentials without proof.

Avatier Assisted Reset eliminates that weakness by turning the service desk into a zero-trust enforcement layer — not an exception path. Every reset is MFA-verified, logged, and identity-proofed, ensuring the human link becomes the strongest link in your security chain.

Avatier Help Desk



Avatier Verify User (Patent Pending)



Attackers can fool people — but not Avatier. Every help desk request is verified before assistance.

Key Advantages & Benefits

Every Help Desk interaction becomes MFA-enforced, auditable, and compliant — stopping social engineering where it starts.

Advantage	Key Benefit	Why It Matters
★ Verify User	Guided identity proofing	Stops social engineering before accounts are touched
★ Assisted Unlock Account	MFA-verified identity confirmation	Secure identity verification + eliminates impersonation
★ Assisted Quick Reset Password	Rapid, compliant password reset	Fast resolution + enforced MFA + consistent compliance
★ View Account	Instant user status insight	Faster triage + prevents unnecessary resets
★ Assisted Reset Password	Zero-trust identity enforcement	Zero-trust controls + breach-resistant password handling
★ View User Activity	Transparent, auditable actions	Real-time accountability + audit-ready data
★ Send Enrollment Email	Drives full MFA adoption	Drives MFA coverage + improves user success
★ Unenroll User	Lifecycle access removal	Instant access revocation + lifecycle hygiene
★ View User Mapping	Accurate access validation	Role clarity + reduced provisioning errors
★ Batch Password Reset	High-volume reset automation	Massive efficiency gains + no compliance shortcuts

Top 10 Use Cases

1. Secure Account Unlock - Agents verify identity before unlocking accounts
2. Assisted Password Reset - Human-supervised password changes with breach protection
3. Identity Verification - Confirm user identity for sensitive requests
4. Temporary Access Granting - Secure temporary credentials with forced reset
5. Account Status Checking - Real-time visibility into account conditions
6. Compliant Credential Changes - Ensure all password changes meet security policies
7. Emergency Access Recovery - Secure protocols for urgent access needs
8. Third-Party Verification - Verify contractors and external users properly
9. Audit Trail Generation - Create immutable records for compliance
10. Consistent User Experience - Standardized verification across all service desk interactions

Perfect For These Scenarios

Avatier Assisted Reset is essential for any organization where help desk interactions represent a security risk.

Scenario	Why It's Critical
High-Risk Industries	Financial services, healthcare, and critical infrastructure where social engineering threats are most prevalent.
Regulated Organizations	Companies requiring SOC 2, ISO 27001, NIST 800-63-3, or GDPR compliance evidence.
Large Service Desks	Organizations with multiple agents where consistent verification processes are challenging.
MFA-Enabled Enterprises	Companies that have invested in MFA but lack help desk integration for verification.
Previous Breach Victims	Organizations rebuilding security after social engineering incidents.

Frequently Asked Questions

1. What is Avatier Assisted Reset?

Avatier Assisted Reset is a human-assisted password reset and account unlock solution that integrates with your existing MFA systems. It enables service desk agents to securely verify user identity before performing any reset, closing the security gap exploited by social engineering attacks.

2. How does it protect against Scattered Spider-style attacks?

Groups like Scattered Spider target help desks to reset MFA or accounts. Avatier Assisted Reset removes this vulnerability by enforcing MFA challenges through your existing identity provider, ensuring no reset occurs without verified multi-factor authentication.

3. What MFA methods are supported?

Avatier integrates with your existing MFA providers including Avatier Identity Challenge Card, Microsoft Authenticator, Okta Verify, Duo, Google Authenticator, SMS/email OTPs, and more.

4. What compliance standards does it support?

The solution aligns with NIST 800-63-3, SOC 2, ISO 27001, GDPR, and HIPAA requirements. Every assisted event is logged for full audit traceability.

5. How does the Have I Been Pwned integration work?

During password reset, Avatier checks new passwords against the Have I Been Pwned breach database. If a match is found, the password is rejected, protecting against compromised credentials.

6. Does it work with existing ticketing systems?

Yes. It integrates seamlessly with ServiceNow, Zendesk, Jira Service Management, Freshservice, and other leading help desk platforms.

7. What measurable value does it provide?

- Up to 70% reduction in help desk password tickets
- 100% MFA enforcement for human-assisted resets
- Zero successful impersonation resets after implementation
- Immediate improvement in audit readiness

8. How are help desk agents authenticated and monitored?

Agents must securely log into the Avatier platform, and all their actions are logged and audited to enforce zero-trust principles.

9. Can policies be customized for different user risks?

Yes, granular policies can enforce stricter verification for high-privilege accounts while streamlining the process for standard users.

10. What if a user cannot access their MFA method?

Configurable fallback methods are available, such as alternate devices or security questions, without bypassing identity proofing.

Service Desk Workforce Assurance Automation

Automation can solve most password resets — but not the human problem.

Avatier Assisted Reset secures the last 30% of interactions where 100% of social-engineering breaches begin.

It transforms your help desk from the weakest link into your **strongest zero-trust defense**, turning every agent into a verified gatekeeper of your digital perimeter.

This is how you close the final gap in enterprise security — by engineering human trust into every access decision.



You've automated the system — now secure the human.

[Contact Avatier to see Assisted Reset in action](#)

www.avatier.com