Securely Automating Sales & Service
Through Conversational AI Across
Voice, Phone, and Beyond

SERVICE DESK AUTOMATION AI™
PASSWORDLESS & PASSWORD GOVERNANCE PILLAR 1

# AVATIER PASSWORD FIREWALL

## Intercept. Validate. Enforce. Password Protection Reimagined.

The First Firewall Built for Passwords — and the Future Beyond Them.

## Why It Matters

In today's world, the network perimeter is no longer a firewall—it's your password policy. Inconsistent enforcement across systems like Active Directory, Entra ID, and legacy applications creates the very security gaps that attackers exploit.

Avatier Password Firewall™ closes these gaps by establishing a unified, zero-trust enforcement layer. It intercepts and validates every password change—from any source—against enterprise policies and breach databases before it reaches your directory, ensuring no weak or compromised credential is ever accepted.

The result is more than compliance; it's the foundational control that makes all other identity security—including passwordless—possible.

**"Zero-trust starts with zero exceptions. The Password Firewall ensures there are none." — Sam Wertheim, Avatier CISO**

### Control 1: Active Directory & Entra ID Password Filter Agent

| Component | Function | Outcome |
|---|---|---|
| **Lightweight Agent** | Installs on each domain controller to intercept password changes in real time. | Ensures every password event is captured at the source, before it is applied. |
| **Intelligent Rules Engine** | Validates passwords against enterprise-grade standards for strength, complexity, and policy. | Enforces consistent security, blocking weak or non-compliant credentials. |
| **Secure Synchronization** | Propagates approved passwords across all connected systems. | Guarantees credential consistency and control across the entire IT environment. |

### Control 2: Password Policy Deployment Engine (Patent Pending)

| Component | Function | Outcome |
|---|---|---|
| **★ Continuous Discovery** | Automatically scans for new or retired domain controllers. | Maintains complete visibility and protection as network infrastructure evolves. |
| **★ Automated Deployment** | Installs the Avatier agent on new controllers without manual effort. | Ensures continuous, hands-free protection and eliminates coverage gaps. |
| **★ Centralized Admin Console** | Provides remote management of reboots and deployment status. | Gives administrators full oversight and control, ensuring no credential is ever unprotected. |

### Control 3: Application Password Policies

| Component | Function | Outcome |
|---|---|---|
| **Connector-Specific Policies** | Applies unique password rules for different systems (AD, ERP, POS, HR, etc.). | Balances security with practicality, meeting the specific needs of each platform. |
| **Unified Workflow** | Manages all system-specific policies within a single, centralized engine. | Simplifies administration while providing granular control, ensuring a seamless user experience. |
| **★ Connector Groups** | Multiple connectors can appear as one to the end user. | Simplified resets and unlocks across many connectors. |

### Control 4: Password Policy Rules & Delegation Framework

| Component | Function | Outcome |
|---|---|---|
| **Role-Based Delegation** | Centralizes governance with policies assigned by source, division, or user group. | Enables local control and flexibility without sacrificing global oversight and compliance. |
| **Advanced Intelligence** | Integrates NIST lists, HIBP breach checks, Diceware, and custom dictionaries. | Provides enterprise-grade password hygiene, proactively blocking compromised and weak credentials. |
| **Advanced Rules** | Avoids Patterns, Select Special Chars, Password Generation Rules for Help Desk. | Increase security without end user complication by avoiding bad password practices. |

### The Result: Unified Control. Zero Exceptions. Total Assurance.

| Aspect | Description | Business Outcome |
|---|---|---|
| **Core Function** | Turns password management into a true security control layer. | **For CIOs & CISOs:** Every system and password is governed by one consistent security framework. |
| **Key Capabilities** | Enforces one policy everywhere, automates deployment, eliminates compliance gaps. | Establishes a secure, automated foundation that reduces risk and operational overhead. |
| **Strategic Value** | Prepares organizations for a passwordless future without sacrificing oversight, security, or speed. | Future-proofs the identity stack, enabling a seamless transition to modern authentication. |
| **Ultimate Vision** | The first firewall built for passwords — and the foundation for everything that comes after. | Provides the critical, non-negotiable security baseline upon which all future identity initiatives are built. |

## How It Works

Every identity system still relies on passwords somewhere — even in “passwordless” environments. The Avatier Password Firewall™ exists to control, validate, and secure every password event before it ever reaches a domain controller or connected system. It is the first and most critical defense tier in Avatier’s password and passwordless strategy.

1. **Core Purpose**

   The Password Firewall™ ensures that every password—no matter who changes it, where it’s changed, or what system it touches—is inspected and approved by one unified security engine.

   This closes the most common compliance and breach gap: inconsistent or unenforced password policies across multiple platforms, domains, and applications.

2. **How It Works**

   I. **Agent-Based Enforcement at the Source**
   - A lightweight Password Firewall Agent installs on each Microsoft Active Directory Domain Controller (and can extend to other authoritative sources).
   - The agent intercepts all password-change requests—whether initiated by an end user, administrator, API, or third-party system.

   II. **Centralized Validation via Rules Engine**
   - The intercepted password is securely transmitted to the Password Firewall Rules Engine inside Avatier’s platform.
   - The rules engine validates it against your enterprise’s configured policies, including:
     - Length, complexity, and pattern controls
     - Custom dictionaries and word filters
     - NIST Common Password List and Have I Been Pwned (HIBP) breach checks
     - Industry- or system-specific compliance policies (CMMC, NIST 800-63, ISO 27001)

   III. **Instant Decision & Synchronization**
   - If the password meets all requirements, the agent approves the change locally and synchronizes it through the Avatier framework to all linked systems (Active Directory, Entra ID, POS, ERP, mainframe, etc.).
   - If it fails, the change is rejected immediately with user feedback on why, ensuring policies are enforced in real time.

### 3. Automation and Resilience

- **Autonomous Deployment:** When new domain controllers are added, Avatier automatically detects them and installs the Password Firewall Agent—no manual tracking or change requests required.
- **Central Visibility:** Administrators can view deployment status, pending reboots, and synchronization health through the Avatier Admin Console.
- **Fault-Tolerant Design:** Even if network connectivity to the Avatier Cloud is lost, local agents continue enforcing cached policy rules until synchronization resumes.

### 4. Unified UX and Policy Delegation

- The Avatier UI provides a single place to define and test password policies.
- Policies can be assigned independently per system connector or synchronized globally, allowing password rules for a POS system, Unix server, or Entra ID to differ while still passing through the same enforcement engine.
- Delegation options enable policy control at the organization, OU, connector group, or user level—maintaining flexibility without losing central authority.

### 5. Security Architecture

| Environment | Why It's Ideal |
|---|---|
| **Isolation-by-Design** | Each customer runs inside a private Docker container with its own rules engine and database. |
| **Zero-Trust Control** | Every password event must pass MFA-bound validation before acceptance or sync. |
| **Outbound-Only Connectivity** | Password Firewall Agents initiate outbound TLS 1.3 channels; no inbound ports are exposed. |
| **Immutable Logging** | All validations, rejections, and synchronizations are timestamped and audit-ready for **SOC 2, ISO 27001, CMMC, and GDPR.** |

### 6. Business Impact

- **CFO:** Reduces costs by eliminating password-related tickets and compliance exceptions.
- **CIO:** Centralizes control and automates enforcement across hybrid and multi-domain environments. Delegation options enable policy control at the organization, OU, connector group, or user level—maintaining flexibility without losing central authority.
- **CISO:** Ensures every password meets enterprise, industry, and government-grade standards before it exists.
- **Engineers:** Gain a scalable, self-updating enforcement layer that works natively with Microsoft AD and Entra ID.

## Key Advantages & Benefits

Avatier Password Firewall provides unique advantages that differentiate it from other solutions.

| Advantage | Key Benefit | Why It Matters |
|---|---|---|
| **★ Enterprise-Wide Policy Enforcement** | Enforces one unified password policy across all systems—AD, Entra ID, ERP, POS, cloud, and legacy. | Ensures consistent compliance; eliminates audit gaps and policy drift. |
| **★ Zero-Trust Password Validation** | Intercepts every password event; validates with MFA, NIST, and breach checks before approval. | Blocks unverified credentials; stops insider error and social engineering attacks. |
| **★ Isolation-by-Design Architecture** | Runs in a dedicated, private Docker container with outbound-only TLS communication. | Guarantees data isolation; prevents cross-tenant or network exposure. |
| **Immutable Audit & Compliance Evidence** | Logs every event—approval, rejection, or sync—for SOC 2, ISO, and CMMC audits. | Simplifies compliance reviews and strengthens forensic accountability. |
| **★ Intelligent Automation & Self-Healing Deployment** | Detects new domain controllers and auto-installs the Password Firewall Agent. | Reduces admin overhead; ensures continuous protection as infrastructure evolves. |
| **System-Aware Synchronization & Delegation** | Synchronizes validated passwords across systems with connector-specific policy control. | Balances central control with local flexibility; improves governance efficiency. |
| **★ Accelerates Passwordless Transformation** | Establishes the control framework needed for secure MFA and passkey adoption. | Enables phased passwordless rollout without disrupting legacy systems. |

## Top 10 Use Cases

1. Unified Password Governance - One policy across all systems
2. Real-Time Breach Prevention - Block compromised passwords instantly
3. Zero-Trust Password Enforcement - Verify every change with MFA
4. Automated Domain Protection - Auto-deploy to domain controllers
5. System-Specific Policies - Different rules for different systems
6. Compliance Automation - Generate audit logs for all frameworks
7. Insider Threat Prevention - Stop admin bypass and shared credentials
8. Passwordless Foundation - Policy layer for FIDO2 and passkeys
9. Self-Service Integration - Extend protection to user resets
10. Centralized Global Management - One console for all domains

## Perfect For These Environments & Use Cases

Avatier Password Firewall is essential for any organization that needs to eliminate weak and compromised passwords, enforce consistent security policies across all systems, and prove compliance—all while reducing the risk of credential-based attacks.

| Environment | Why It’s Ideal |
|---|---|
| **Enterprises of All Sizes** | Eliminates the most frequent help desk tickets (password resets, account unlocks), significantly reducing support costs and user downtime. |
| **Remote & Hybrid Workforces** | Provides secure, consistent account recovery for distributed users who may not have immediate access to on-site IT support. |
| **High-Security & Regulated Organizations** | Enforces MFA, zero-trust principles, and complex password policies at the source, ensuring compliance with NIST, CMMC, SOC 2, and more. |
| **Citrix & VDI Environments** | Integrates seamlessly with virtual desktop infrastructures to maintain consistent password policy enforcement and recovery capabilities. |
| **High-Turnover Workplaces** | Simplifies and secures account onboarding and offboarding for contractors, temporary staff, and seasonal employees. |
| **Hybrid IT Infrastructures** | Governs password policy across a fragmented landscape—from Active Directory to Entra ID, SaaS apps, and legacy mainframes—from one console. |
| **Organizations Battling Credential Attacks** | Prevents the use of breached, weak, or common passwords in real-time by validating against threat intelligence feeds before a password is set. |

## Frequently Asked Questions

**1. What is the Avatier Password Firewall™?**

A real-time enforcement layer that inspects and validates every password change against your security policies before it's set.

**2. Why is it considered the first pillar of password and passwordless management?**

Because It creates the secure, unified foundation that all other identity management—including passwordless—relies on.

**3. How does it integrate with Microsoft?**

A lightweight agent on each domain controller intercepts and validates changes in real-time for both Active Directory and Entra ID.

**4. What if a new domain controller is added?**
The system auto-detects it and installs the agent instantly, ensuring continuous, hands-off protection.

**5. Can it enforce different policies for different systems?**
Yes, You can set unique rules for systems like POS or ERP while maintaining central control.

**6. How does it support compliance?**
It enforces standards like NIST and HIBP and generates immutable audit logs for frameworks like SOC 2 and ISO 27001.

**7. What makes Avatier different from traditional password policy tools?**
It's an active, cloud-aware security checkpoint, not a static policy tool. It works across all systems and users.

**8. How is it secured within the enterprise environment?**
It runs in a private, isolated container with outbound-only TLS encryption—no open inbound ports.

**9. How does the Password Firewall support passwordless transformation?**
It provides the essential governance layer to securely transition to passkeys and FIDO2.

**10. What are the business outcomes?**

- **CISO:** Stops password breaches
- **CIO:** Unified control
- **CFO:** Cuts costs
- **Engineers:** Zero maintenance.

## Transforming the Password Change into a Zero-Trust Checkpoint

The Avatier Password Firewall™ is not just a policy engine — it's a real-time security checkpoint that governs every password change across the enterprise.

It turns password management from an administrative task into an automated, auditable, zero-trust control system — the foundation of Avatier's password and passwordless security architecture.

AVATIER™ | Identity Anywhere™

**Eliminate weak and compromised passwords at the source. Transform your password system from a vulnerability into a verified, zero-trust control point.**

[Contact Avatier to see Password Firewall in action]

[www.avatier.com]