

ACCESS & GOVERNANCE AUTOMATION AI™ PILLAR 2

AVATIER GROUP AUTOMATION

Rule-Based Group & Distribution-List Governance That Runs Itself

Eliminates manual group management by enforcing membership from your authoritative HR data automatically.

Why It Matters

Group membership is where access quietly goes wrong. Manual group and distribution-list management is slow, error-prone, and impossible to audit at scale — and stale, over-permissioned groups are exactly how privilege creep and insider risk take hold. Avatier replaces manual administration with rule-based, policy-enforced group automation that keeps every security group and email distribution list continuously accurate, secure by design.

By driving membership directly from authoritative HR attributes — title, department, location, and manager — Avatier places users in exactly the right groups the moment they are hired, moved, or termed, and removes them from the ones they should no longer be in. For CISOs, that means least privilege enforced automatically, continuous audit evidence, and no unauthorized members hiding in privileged groups.

"Most breaches don't start with a cracked password — they start with a group nobody was watching."
— Sam Wertheim, Avatier CISO

How It Works

Avatier connects to your directories — Active Directory and Entra ID — and to 70+ HR and payroll systems through a single unified integration, turning authoritative attributes into live group-membership rules.

A wizard-driven rules engine lets business owners define membership by job attributes with no scripting. Avatier enforces those rules on the schedule you choose — daily, weekly, or monthly — continuously reconciling security groups and email distribution lists. You can test any rule before it goes live, handle exceptions with controlled manual overrides, and every change is captured for audit.

Continuous monitoring flags unauthorized members and membership drift the moment they appear. Avatier's patent-pending Continuous Governance™ automatically removes access that no longer fits and restores what a user's role requires — enforcing least privilege without IT effort. Deploy as Docker containers on-premise, in the cloud, or fully hosted.

One Unified Integration. Directories, HR & 70+ Systems.

Avatier enforces group membership from your authoritative sources through a single unified integration — no point-to-point connectors to build or maintain, and no scripts to break when a vendor changes an API.

Directories & HR Sources



Mid-Market & Global Payroll



A single over-permissioned group can hand an attacker the keys to your network. When ransomware crews land a foothold, they look for one thing first: broad, poorly governed group memberships that let them move laterally and escalate to domain-wide control.

How It Happens: Manual group management guarantees this exposure. Memberships are added for a project and never removed, employees change roles but keep old group access, and privileged groups quietly accumulate members no one is reviewing. Without automated enforcement, there is no reliable way to prove who belongs in a group — or to keep them out.

The Business Imperative: Stopping Access Creep and Group Sprawl

Root Cause	Solution
Membership Creep: Users keep old group access after transfers and projects end, accumulating standing privilege.	HR-Driven Enforcement: Membership is derived from live HR attributes, so access is added and removed automatically as roles change.
Unwatched Privileged Groups: No automated process reviews who belongs in high-privilege security groups.	Unauthorized-Member Detection: Continuous monitoring flags and removes members who don't match policy, with real-time alerts.
Manual, Unauditable Changes: Ad-hoc group edits leave no reliable trail for auditors.	Patent-Pending Continuous Governance™: Every membership change is policy-enforced and logged, with automatic reconciliation to each user's current role.

Manual processes and disconnected directories create immense risk. Avatier Group Automation eliminates it by enforcing least privilege at the group level — continuously, automatically, and with full audit evidence.

Featured Capabilities

No-Code Rules Engine

Business owners define group membership by job attributes through a guided wizard — no scripting and no PowerShell. Test any rule against production data before you enable it, so you see exactly who will be added or removed before a single change is made.

Patent-Pending Continuous Governance™

Avatier's patent-pending Continuous Governance™ continuously reconciles every group — removing unauthorized members, restoring access aligned to each user's role, and alerting on drift the moment it appears. The result is least privilege enforced by default, with zero group sprawl.

Key Advantages & Benefits

Avatier delivers a modern, AI-driven identity and workforce automation platform designed for speed, security, and simplicity.

Advantage	Key Benefit	Why It Matters
No-Code Rules Engine	Faster Deployment	Wizard-driven, attribute-based rules eliminate scripting and cut rollout time from months to days.
HR-Driven Membership	Zero-Touch Group Management	Groups and distribution lists follow authoritative HR data automatically as roles change.
Scheduled Enforcement	Always-Accurate Groups	Daily, weekly, or monthly reconciliation keeps every group continuously correct.
Unauthorized-Member Detection	Reduced Risk	Continuous monitoring flags and removes members who don't match policy, with real-time alerts.
Patent-Pending Continuous Governance™	Always-Right Access	Automatic role reconciliation removes or restores membership to match each user's role, eliminating access creep.
Test-Before-Production	Safe Changes	Validate any rule against live data before enabling it — no surprises.
Distribution-List Automation	Higher Productivity	Email distribution lists are built and maintained automatically from HR attributes.
Compliance-Ready Audit Trails	Audit Confidence	Every membership change is logged and policy-enforced for SOC 2, ISO 27001, NIST, SOX, and more.
Docker Deployment	Deploy Anywhere	Runs on-premise, in the cloud, or fully hosted with isolation by design.

Top Use Cases	
1. Security Group Automation — Membership for AD and Entra ID security groups is enforced from authoritative attributes.	9. Contractor, Supplier & Partner Groups — Non-employee populations are governed by the same attribute-based rules.
2. Email Distribution List Automation — Distribution lists are built and maintained automatically — no manual edits.	10. Scheduled Enforcement — Rules run on a daily, weekly, or monthly cadence you control.
3. HR-Driven Membership — Title, department, location, and manager drive attribute-based group assignment.	11. Test Rule Before Production — Preview exactly who a rule will add or remove before enabling it.
4. New-Hire Group Assignment — New employees land in exactly the right groups on day one.	12. Exception Handling — Controlled manual overrides cover the edge cases policy can't.
5. Transfer / Role-Change Re-Grouping — Role changes add new group access and remove what no longer fits.	13. Application Access via Groups — Group-based application entitlements stay aligned to role.
6. Offboarding Group Cleanup — Departures are removed from every group instantly, eliminating stale access.	14. Compliance-Ready Audit Reporting — Every change is logged for SOC 2, ISO 27001, NIST, and SOX evidence.
7. Unauthorized-Member Detection — Continuous monitoring flags and removes members who don't match policy.	15. Continuous Governance™ Reconciliation — Automatic role reconciliation keeps membership matched to each user's current role.
8. Nested & Dynamic Group Governance — Complex nested and dynamic group structures stay accurate automatically.	16. Separation-of-Duties Enforcement — Rules prevent toxic combinations of group access from ever accumulating.

Perfect For These Scenarios

Avatier Group Automation delivers critical value and rapid ROI for organizations facing these common challenges.

Scenario	Why It's Critical
Large Active Directory Estates	Organizations with sprawling AD/Entra ID groups that are impossible to govern by hand.
Regulated Industries	Organizations requiring SOC 2, ISO 27001, NIST, SOX, HIPAA, or GDPR access evidence.
M&A or Reorganization	Businesses where roles and structures change fast and group access must keep up.
HR-Driven Enterprises	Companies seeking to govern group membership from a single source of truth.
Previous Audit Findings	Organizations remediating over-permissioned groups, stale membership, or access creep.

Frequently Asked Questions

1. How does Avatier decide who belongs in a group?

Membership is derived from authoritative attributes — title, department, location, manager, and more — using a wizard-driven rules engine. When HR data changes, Avatier automatically adds and removes members to keep every group accurate.

2. Do we need to write scripts or PowerShell?

No. Avatier's no-code rules engine lets business owners define and manage membership without scripting. Even complex, nested, and dynamic groups are handled through the wizard.

3. Can we test a rule before it changes production?

Yes. Every rule can be tested against live data first, so you see exactly who will be added or removed before a single change is made.

4. How does Avatier catch unauthorized group members?

Continuous monitoring compares actual membership against policy and flags unauthorized members in real time, automatically removing them and alerting the right owners.

5. Does it manage email distribution lists too?

Yes. Security groups and email distribution lists are both built and maintained automatically from HR attributes, eliminating manual list upkeep.

6. How does Group Automation prevent access creep?

Avatier's patent-pending Continuous Governance™ continuously reconciles membership to each user's current role — removing standing access that no longer fits and enforcing least privilege by default.

7. How does it handle transfers and terminations?

The moment HR marks a transfer or termination, Avatier updates group membership automatically — granting the new role's access and removing everything the user should no longer have, within seconds.

8. Where does Avatier deploy?

Avatier deploys as Docker containers on-premise, in the cloud, or fully hosted, with a private cloud instance and isolation by design.

9. Is every change auditable?

Yes. Every membership change is policy-enforced and logged with immutable audit trails, giving you continuous evidence for SOC 2, ISO 27001, NIST, SOX, HIPAA, and GDPR.

10. How fast can we go live?

Most customers go live in days to weeks. Point-and-click configuration, a Quick-Start Guide, and a dedicated onboarding team dramatically shorten deployment.

Governed Groups, Enforced Automatically

Automation can solve most IT tasks — but group membership remains a critical, manual risk that quietly drives access creep and insider exposure. Avatier Group Automation enforces the right membership everywhere, transforming authoritative HR data into the single source of truth for group access.

It turns your directories into a governed, least-privilege environment where every user has exactly the group access their role requires — and none they don't. This is how you close the access-creep gap at the group level: by automating governance continuously, from hire to retire.

You've automated the accounts — now govern the groups.



Contact Avatier to see Group Automation in action

www.avatier.com

Continuous Governance™, Password Firewall™, and Identity Anywhere™ are trademarks of Avatier Corporation. Patent pending.