

ACCESS & GOVERNANCE AUTOMATION AI™ PILLAR 5

AVATIER ACCESS GOVERNANCE

AI-Powered Access Certification and Continuous Compliance

Turns slow, manual access reviews into automated, audit-ready certification across every system.

Why It Matters

Access reviews are where compliance goes to die. Manual certification campaigns are slow, spreadsheet-driven, and out of date the moment they finish, while orphaned accounts, rubber-stamped approvals, and unchecked access creep pile up between audits. Avatier replaces that scramble with AI-powered, continuous access governance that produces real, audit-ready evidence on demand.

By automating certification and attestation across every connected system, Avatier gives reviewers a clear snapshot of who has access to what and lets them approve or revoke in a click. For CISOs and auditors, that means provable least privilege, orphaned-account prevention, and continuous, audit-ready evidence for SOC 2 Type II and ISO 27001, plus the requirements associated with NIST, SOX, HIPAA, and GDPR.

"An access review that takes a quarter to finish is already out of date the day it's signed." (Sam Wertheim, Avatier CISO)

How It Works

Avatier captures Access Certification Snapshots across your environment and sends attestation tasks to 90+ enterprise systems and cloud services through a single unified integration, with no manual data gathering and no spreadsheets.

Reviewers certify access from any device, approving or revoking entitlements in real time through a mobile-first, conversational interface in Microsoft Teams, Slack, ServiceNow, and Outlook. A built-in Compliance Manager flags risk, tracks status, supports multi-level approvals, and captures evidence, while delta certification means each cycle reviews only what changed. Between campaigns, Avatier's patent-pending Continuous Governance™ keeps access aligned to role.

One Certification Layer. 90+ Systems & Cloud Services.

Avatier sends certification and attestation tasks to 90+ enterprise systems and cloud services through a single unified integration, with no point-to-point connectors to build or maintain and no spreadsheets to chase.

Enterprise Systems & Cloud



Where Users Self-Serve



Auditors don't ask whether you have a policy. They ask you to prove it, and the risk behind that question is real: 90% of organizations had an identity-related incident in the past year, and 84% said it directly affected the business (IDSA, 2024 Trends in Identity Security). The most expensive audit findings come from access nobody certified: orphaned accounts from departed employees, standing privilege from old roles, and approvals granted with no evidence behind them.

How It Happens: Manual, periodic reviews can't keep up. By the time a quarterly certification is complete, roles have changed, people have left, and new access has been granted, so the evidence is stale before it is filed. Rubber-stamped approvals and spreadsheet tracking leave gaps that surface as findings, fines, and breach exposure. Breaches that begin with stolen credentials take the longest to identify and contain, nearly 10 months (IBM, Cost of a Data Breach 2024).

The Business Imperative: Passing Audits and Stopping Access Creep

Root Cause	Solution
Orphaned Accounts: Accounts from departed or transferred users retain live access no one has reviewed.	Continuous Certification: Avatier detects orphaned and over-privileged access automatically and drives revocation in real time.
Rubber-Stamped Reviews: Manual campaigns encourage bulk approvals with no evidence and no accountability.	Risk-Aware Attestation: The Compliance Manager flags risk, requires evidence, and routes multi-level approvals to the right owners.
Stale, Manual Evidence: Spreadsheet-based reviews are out of date the moment they finish.	Patent-Pending Continuous Governance™: Access is continuously reconciled to role, with audit-ready evidence available on demand.

Manual, point-in-time reviews create immense risk and audit fatigue. Avatier Access Governance eliminates both with continuous, AI-powered certification that keeps least privilege provable and every audit ready.

Featured Capabilities

Access Certification Snapshots

Avatier captures a real-time snapshot of who has access to what across every connected system, then routes attestation tasks to reviewers who approve or revoke in a click, on any device and in the tools they already use. Delta certification means each cycle reviews only what changed.

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
Access Certification Snapshots	Faster Reviews	Real-time snapshots let reviewers approve or revoke access in a click, cutting campaigns from weeks to hours.
90+ System Attestation	Complete Coverage	Automated attestation reaches 90+ enterprise systems and cloud services through one integration.
Mobile-First Certification	Higher Completion	Reviewers certify from any device in Teams, Slack, ServiceNow, and Outlook, with no VPN and no spreadsheets.
Delta Certification	Less Fatigue	Each cycle reviews only what changed, eliminating rubber-stamping and reviewer burnout.
Compliance Manager	Audit Confidence	Real-time risk flags, evidence capture, and multi-level approvals produce provable compliance.
Orphaned-Account Prevention	Reduced Risk	Continuous detection surfaces orphaned and over-privileged access before it becomes a finding.
Patent-Pending Continuous Governance™	Always-Right Access	Access is continuously reconciled to role between campaigns, enforcing least privilege by default.
Conversational AI Approvals	Higher Adoption	A conversational assistant guides reviewers to fast, confident decisions.
Docker Deployment	Deploy Anywhere	Runs on-premise, in the cloud, or fully hosted, with isolation by design.

Patent-Pending Continuous Governance™

Between campaigns, Avatier's patent-pending Continuous Governance™ keeps access aligned to role. It detects orphaned accounts, revokes access that no longer fits, and maintains continuous, audit-ready evidence, so you are never scrambling before an audit.

Top Use Cases

1. Access Certification Campaigns: Launch and complete reviews across every connected system in a fraction of the time.	9. Mobile Approvals: Certify and approve from any device, anywhere, in familiar collaboration tools.
2. SOX, ISO & SOC 2 Audits: Produce audit-ready certification evidence on demand for regulators and auditors.	10. Evidence Collection: Attach evidence to every decision for a complete, defensible audit trail.
3. Orphaned-Account Detection: Surface and revoke access from departed or transferred users automatically.	11. Separation-of-Duties Review: Detect and remediate toxic combinations of access.
4. Delta Certification: Review only what changed since the last cycle to cut reviewer fatigue.	12. Risk-Based Prioritization: The Compliance Manager surfaces the riskiest access for review first.
5. Manager Attestation: Route access reviews to the business managers who actually know the users.	13. Continuous Governance™ Reconciliation: Keep access aligned to role between campaigns, automatically.
6. Privileged-Access Review: Focus certification on high-risk, high-privilege entitlements first.	14. Access Governance Warehouse: Maintain a graphical history of access and decisions over time.
7. Application-Owner Certification: App owners certify access to the systems they govern.	15. Multi-Level Approval Workflows: Route certifications through the approvals your policy requires.
8. Real-Time Revocation: Reviewers revoke access on the spot, with no tickets and no delay.	16. Compliance-Ready Reporting: Generate on-demand evidence reports for SOC 2, ISO 27001, NIST, SOX, HIPAA, and GDPR reviews.

Perfect For These Scenarios

Avatier Access Governance delivers critical value and rapid ROI for organizations facing these common challenges.

Scenario	Why It's Critical
Regulated Industries	Organizations requiring SOC 2, ISO 27001, NIST, SOX, HIPAA, FISMA, or GDPR certification evidence.
Audit Remediation	Companies remediating findings from orphaned accounts, access creep, or missing evidence.
Contractor & Partner Access	Organizations that must certify third-party access; third parties are now involved in 30% of breaches (Verizon 2025 DBIR).
Large, Distributed Workforces	Enterprises that need reviewers to certify access quickly from anywhere.
M&A or Reorganization	Businesses reconciling access across newly combined or restructured environments.
Cloud-First Enterprises	Organizations governing access across dozens of SaaS and cloud platforms.

Frequently Asked Questions

1. How is this different from a manual, spreadsheet-based access review?

Avatier automates the entire cycle: capturing real-time snapshots, routing attestation to 90+ systems, and letting reviewers approve or revoke in a click. There are no spreadsheets, and evidence is generated automatically.

2. Does Avatier provide AI-driven compliance reporting?

Yes. Avatier uses AI to turn certification decisions, access snapshots, and approval history into audit-ready reports on demand, mapped to the controls auditors expect. Instead of assembling evidence by hand before each audit, you generate plain-language, exportable reports covering SOC 2 Type II and ISO 27001, plus the evidence needs associated with NIST, SOX, HIPAA, and GDPR.

3. What is AI-driven configuration?

Rather than hand-building campaigns, rules, and connectors, administrators describe what they need in plain language, and Avatier recommends and sets up the configuration, then validates it before it goes live. Setup is faster, and every campaign stays consistent, auditable, and free of custom scripting.

4. Which systems can Avatier certify access for?

Avatier reaches 90+ enterprise systems and cloud services through a single unified integration, and delivers certification tasks in Teams, Slack, ServiceNow, and Outlook.

5. How does Avatier prevent orphaned accounts?

Continuous detection surfaces accounts from departed or transferred users and drives revocation automatically, so orphaned access never lingers between audits.

6. What is delta certification?

Delta certification reviews only the access that has changed since the last cycle, sharply reducing reviewer fatigue and the rubber-stamping that plagues full-list reviews.

7. Can business managers review access without IT help?

Yes. Reviews are routed to the managers and application owners who know the users, through a mobile-first, conversational interface that requires no training.

8. How does Access Governance support continuous compliance?

Avatier's patent-pending Continuous Governance™ keeps access aligned to role between campaigns and maintains audit-ready evidence on demand, so you are always prepared rather than scrambling.

9. Is Avatier secure and standards-aligned?

Yes. Avatier applies zero-trust controls, uses immutable audit logs, and holds SOC 2 Type II and ISO 27001 certifications. It also helps organizations support the requirements and evidence needs associated with NIST, SOX, HIPAA, FISMA, and GDPR. Every certification decision is policy-enforced and fully auditable.

10. Does it handle multi-level approvals and evidence?

Yes. The Compliance Manager supports multi-level approval workflows, real-time risk flags, and evidence attachment on every decision for a complete, defensible trail.

11. 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.

12. How fast can we go live?

Most customers deploy in weeks, not the 6–18 months typical of legacy IGA platforms, with minimal training required thanks to point-and-click configuration.

Continuous, Provable Access Governance

Automation can solve most IT tasks, but access certification remains a slow, manual risk that leaves orphaned accounts and access creep unchecked between audits. Avatier Access Governance secures the entire review lifecycle, turning access data into continuous, audit-ready evidence.

It turns periodic, spreadsheet-driven reviews into continuous, AI-powered governance, ensuring every user has the right access at the right time and proving it on demand. This is how you close the access-governance gap: with certification that never goes stale.

You've automated the access. Now govern and prove it.



[Contact Avatier to see Access Governance in action](#)

www.avatier.com

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