ManageEngine
AD360

Unified identity platform

One control plane for workforce identities and AI agents

ManageEngine

The challenge

Identity is the attack surface, and it now includes AI agents

$4.99M

Global average cost of a data breach, a record and up 12% year on year

IBM, Cost of a Data Breach Report 2026

92%

of organizations that had an AI-related breach lacked proper AI access controls

IBM, Cost of a Data Breach Report 2026

39%

of breaches involve credential abuse somewhere in the attack chain

Verizon 2026 Data Breach Investigations Report

$225,622

Average breach-cost reduction associated with identity and access management

IBM, Cost of a Data Breach Report 2026

The challenge

Where identity control breaks down

The framework is rarely the problem. Applying it to every identity is.

Identity sprawl

AD, Entra ID, Microsoft 365, file servers and SaaS, each managed differently, with no single view

Privilege creep

Access accumulates with every role change and is rarely removed

Agents nobody owns

AI agents are spun up across Copilot Studio, AI Foundry, Gemini and Zia, often without IT in the loop

Unmonitored at runtime

Agents call tools through MCP servers with standing credentials and no inspection

Audit pressure

DPDP Act, DORA, NIS2, HIPAA and PCI DSS demand access evidence, and AI frameworks now add their own

The challenge

Traditional IAM wasn't built for agents

Agents read from and write to ticketing, CRM, cloud and code repositories. They act, they don't just answer.

Built for people who sign in

Not for autonomous agents that reason and chain tool calls

No concept of what an agent is made of

No view of its model, instructions, knowledge sources or tools

Blind to agent-to-tool traffic

Nothing inspects the MCP layer where agents act on real systems

No AI-specific evidence

Compliance frameworks now expect AI controls legacy IAM was never designed to show

What AD360 covers

01

Manage

Automate every identity's life cycle, from new hires to newly discovered AI agents

02

Protect

MFA on every login, SSO to every app, and self-service password reset

03

Govern

Certify access for people and agents, and route approvals

04

Detect and audit

Track every change, flag anomalies, log every agent call

05

Recover

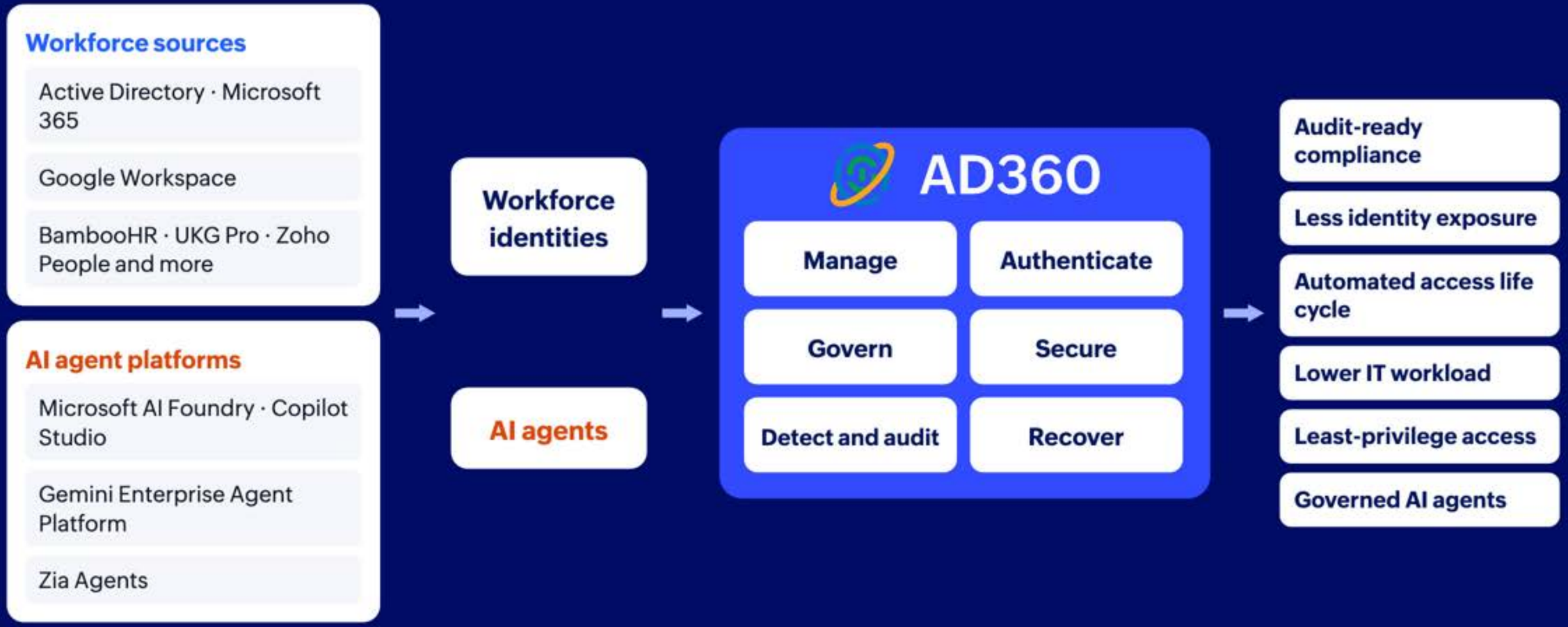
Back up and restore identity data at the attribute level

The approach

Same principles, applied to people and agents

Workforce identities	Principle	AI agents
One view of users, groups, entitlements and cloud accounts	Visibility	An inventory of every agent, model and MCP server
Resource owners certify who has access	Accountability	Every agent gets an accountable human owner
Role-based access, removed when roles change	Least privilege	Entitlements and access templates scope each agent
Context-aware MFA at every login	Runtime control	Every MCP tool call checked against policy
Audit trails and compliance reports	Evidence	A log of every agent call, mapped to AI frameworks

One control plane for workforce identities and AI agents



Risk assessment also covers Anthropic Claude, Gemini and GitHub Copilot accounts.

ManageEngine

The platform

Everything AD360 does for your people, and now for your AI agents

WHAT AD360 ALREADY DOES

Identity life cycle
HR-driven joiner, mover and leaver automation

Authentication
MFA, SSO and self-service passwords

Access governance
Certification campaigns and approval workflows

Risk and auditing
Attack paths, change auditing, UBA, compliance reports

Backup and recovery
Attribute-level restore to full domain recovery

NEW WITH SECUREAI

Discovery and ownership
Every agent, model and MCP server inventoried, each with an accountable owner

Agent access reviews
Agent entitlements certified in the same campaigns as employee access

Agent graph and AI risk
What each agent can reach, plus risk scores for AI platforms

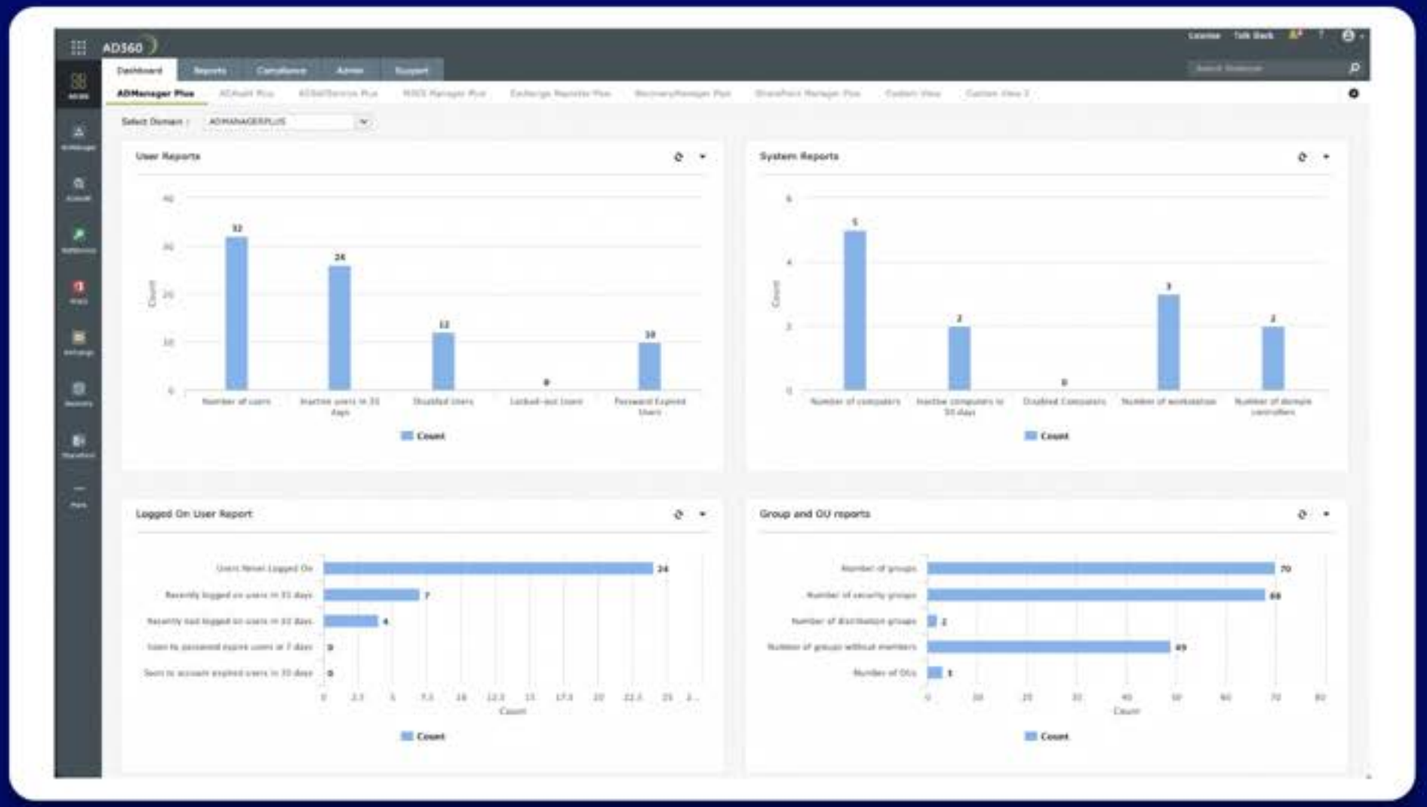
MCP gateway
Every agent tool call checked against access and DLP policies

Agent activity log
A record of every call: Agent, identity, tool, decision

Dashboard

Every identity system, one console

Dashboards and reports across directories, mail, collaboration and AI agents, without switching tools.



ManageEngine

AI agent dashboard

Your AI posture at a glance

The numbers a security lead needs about the AI estate, on one dashboard.

Agents and MCP servers

Totals, broken down by platform

Unmanaged and privileged agents

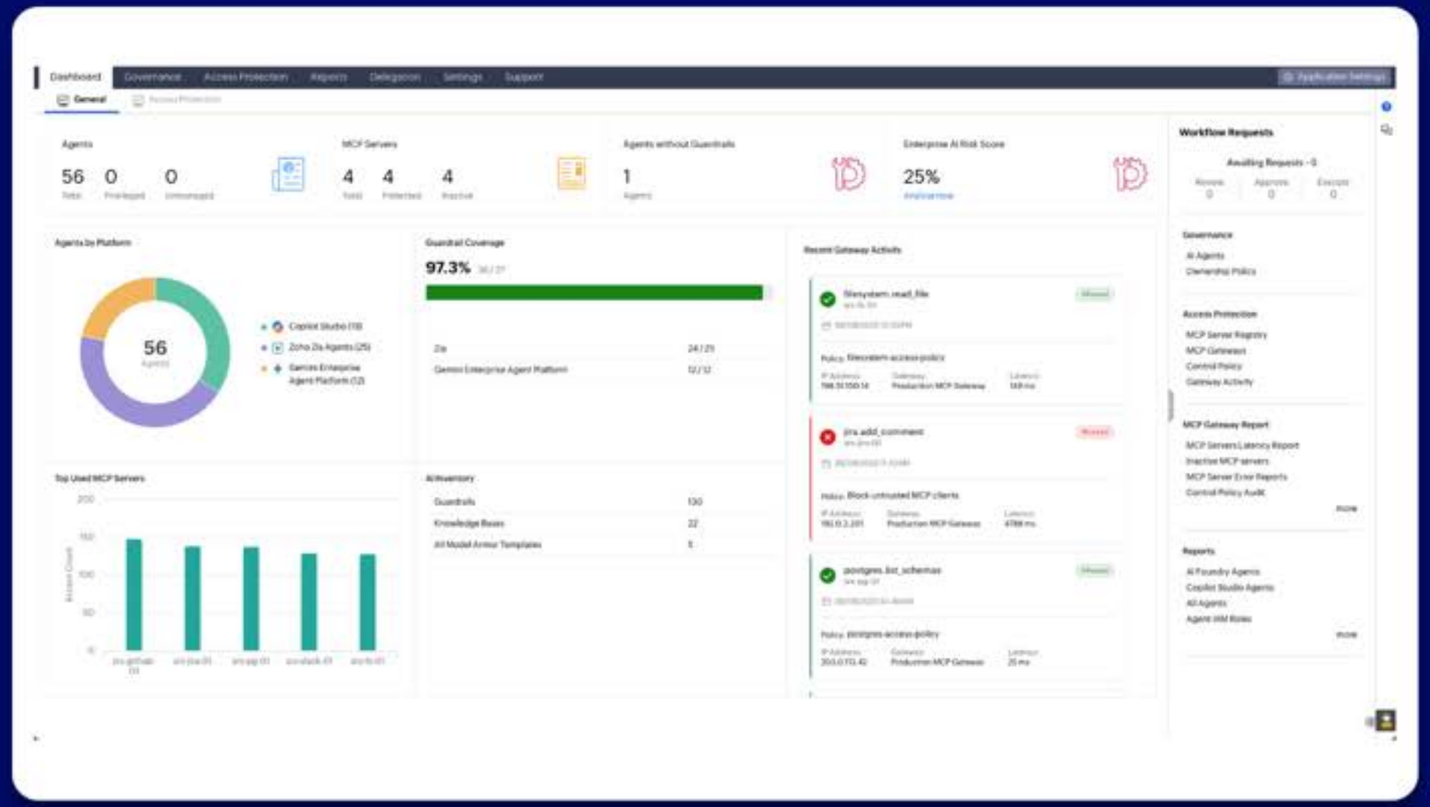
Agents with no owner or elevated access

Guardrail coverage

Agents without platform safeguards

AI risk score

Posture across connected AI platforms



ManageEngine

01

Manage

Create, change and retire identities across every connected system, without doing it by hand.

For AI agents: Discovered across platforms and assigned an accountable owner from day one.

Manage

HR is the trigger. AD360 does the rest.

Joiner

- Accounts created from the HR record
- Role-based access applied
- Set up in every app they need

Mover

- Access adjusted to the new role
- Old entitlements removed
- Manager approval where needed

Leaver

- Accounts disabled or deleted
- Access revoked from every app
- Backup retained, then deleted

Triggered from Workday, BambooHR, Zoho People, UKG and other HR systems, or from ServiceDesk Plus and ServiceNow tickets

Smart templates

One template. Every system a new hire needs.

User creation templates define every attribute once, across AD, Exchange, Microsoft 365 and more.

Naming formats built in

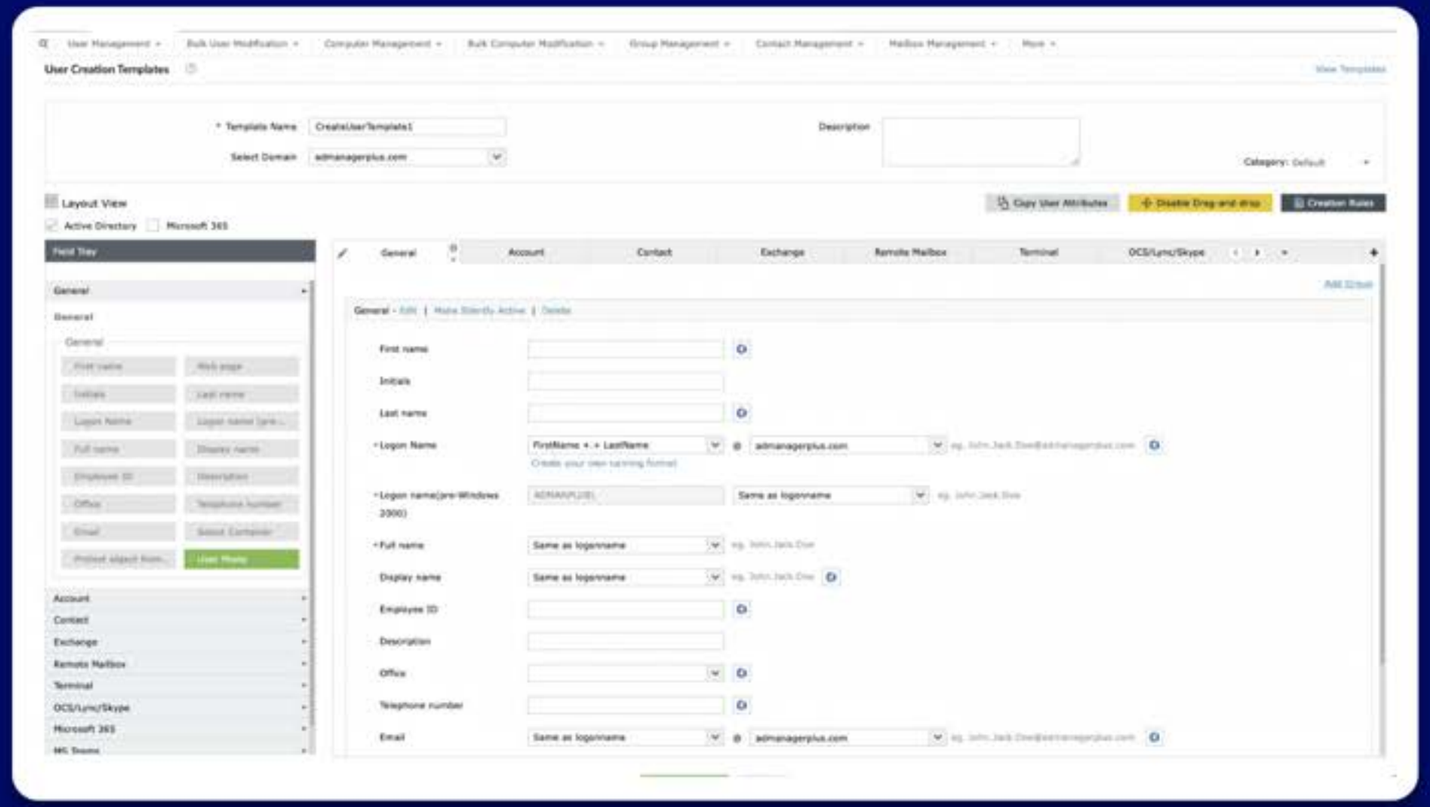
Logon name, display name and email generated consistently

AD, Exchange and Microsoft 365 in one form

Mailbox, licenses and groups set at creation

Reuse everywhere

Single users, CSV bulk creation and HR-driven provisioning



ManageEngine

Large scale management

One console, every directory

Active Directory, Entra ID, Microsoft 365 and Exchange objects, managed from one place.

Every object type

Users, groups, OUs, GPOs, contacts and computers

Bulk, from a CSV

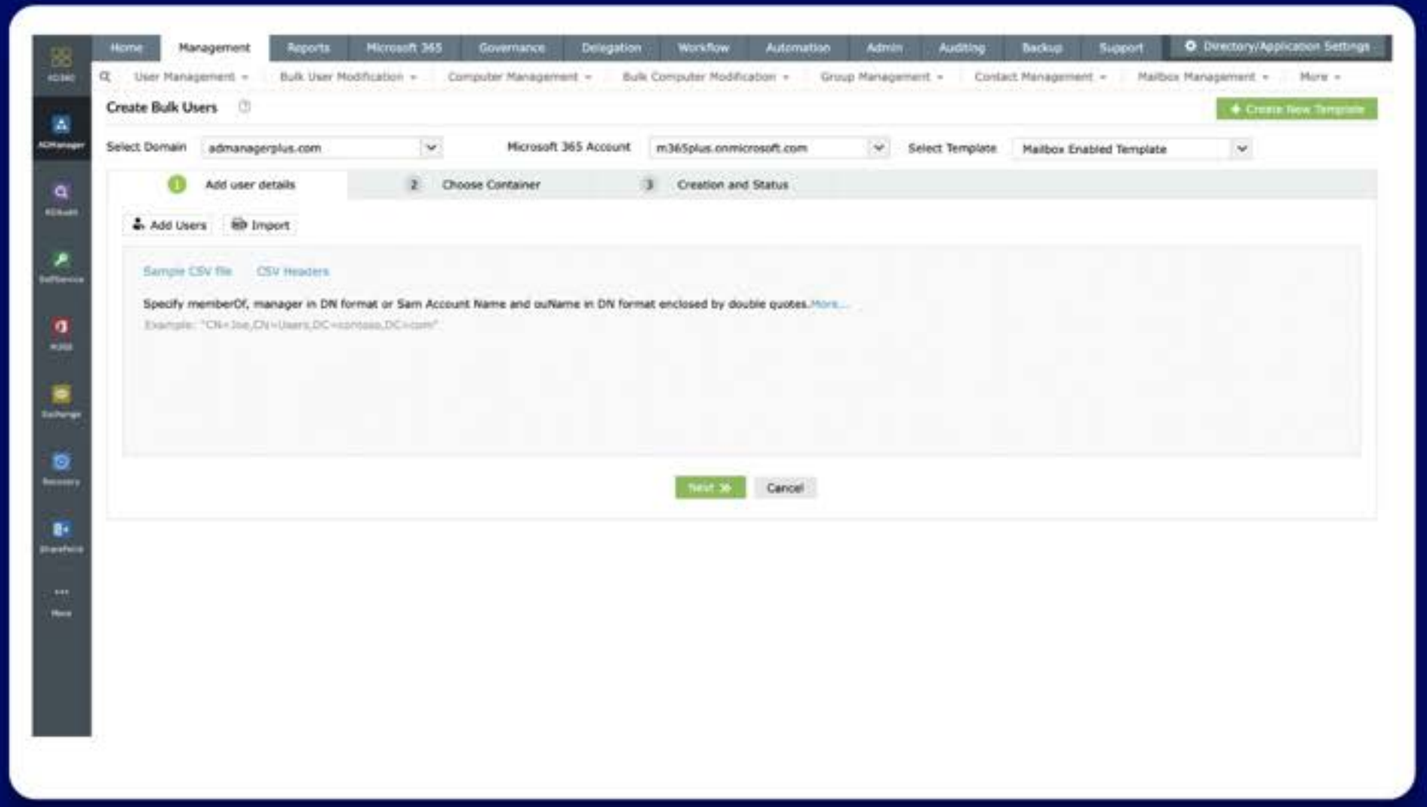
Create or modify accounts in bulk using a template and a file

AD and Microsoft 365 in one run

The AD account and the Microsoft 365 user created together

Migration and hygiene

Move objects between domains; clean up stale and inactive accounts



ManageEngine

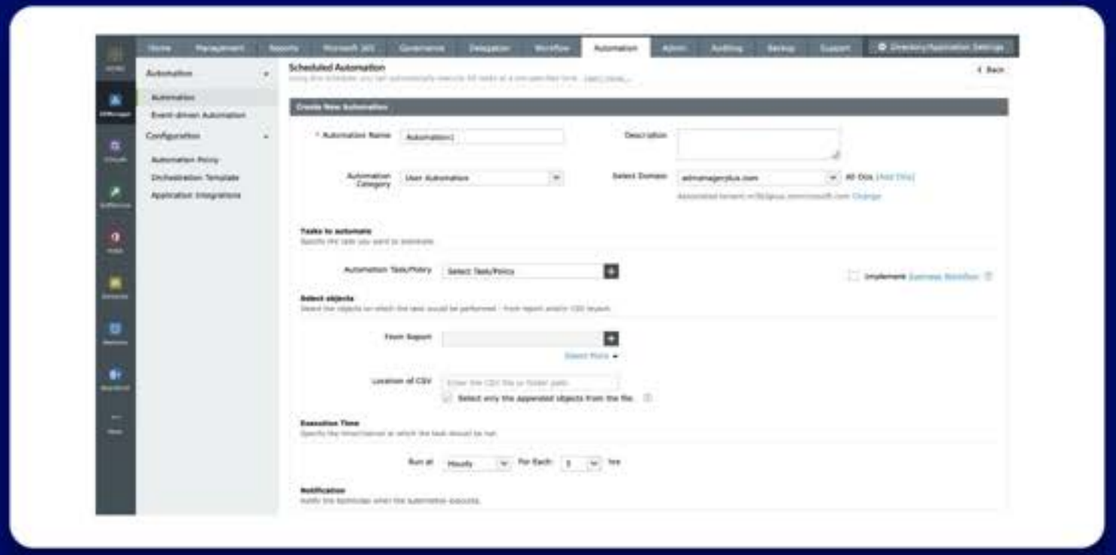
Identity automation

Automate it once, on your terms

Two ways to take routine identity work off the help desk, with no scripting.

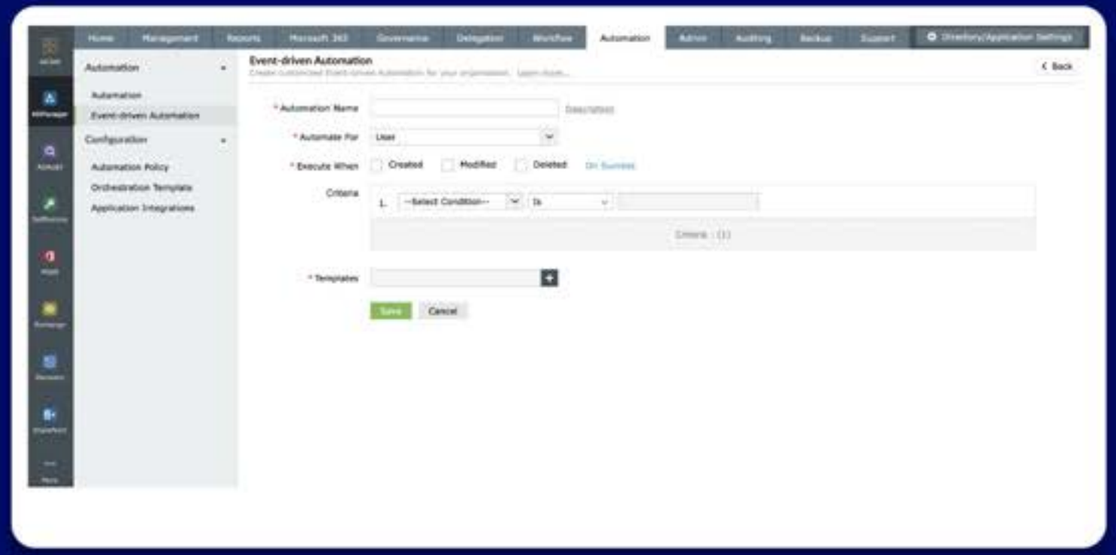
Scheduled automation

Run AD tasks at set times or intervals, on objects pulled from a report or a CSV file, with optional business workflow and technician notifications.



Event-driven automation

When a user or other object is created, modified or deleted and meets your criteria, run an orchestration template automatically.



Both run on automation policies and drag-and-drop orchestration templates, extended to enterprise apps through application integrations.

ManageEngine

Automation policy

One task, and everything that should follow

Automation policies chain an instant task with follow-up tasks on a timeline you set.

Instant tasks

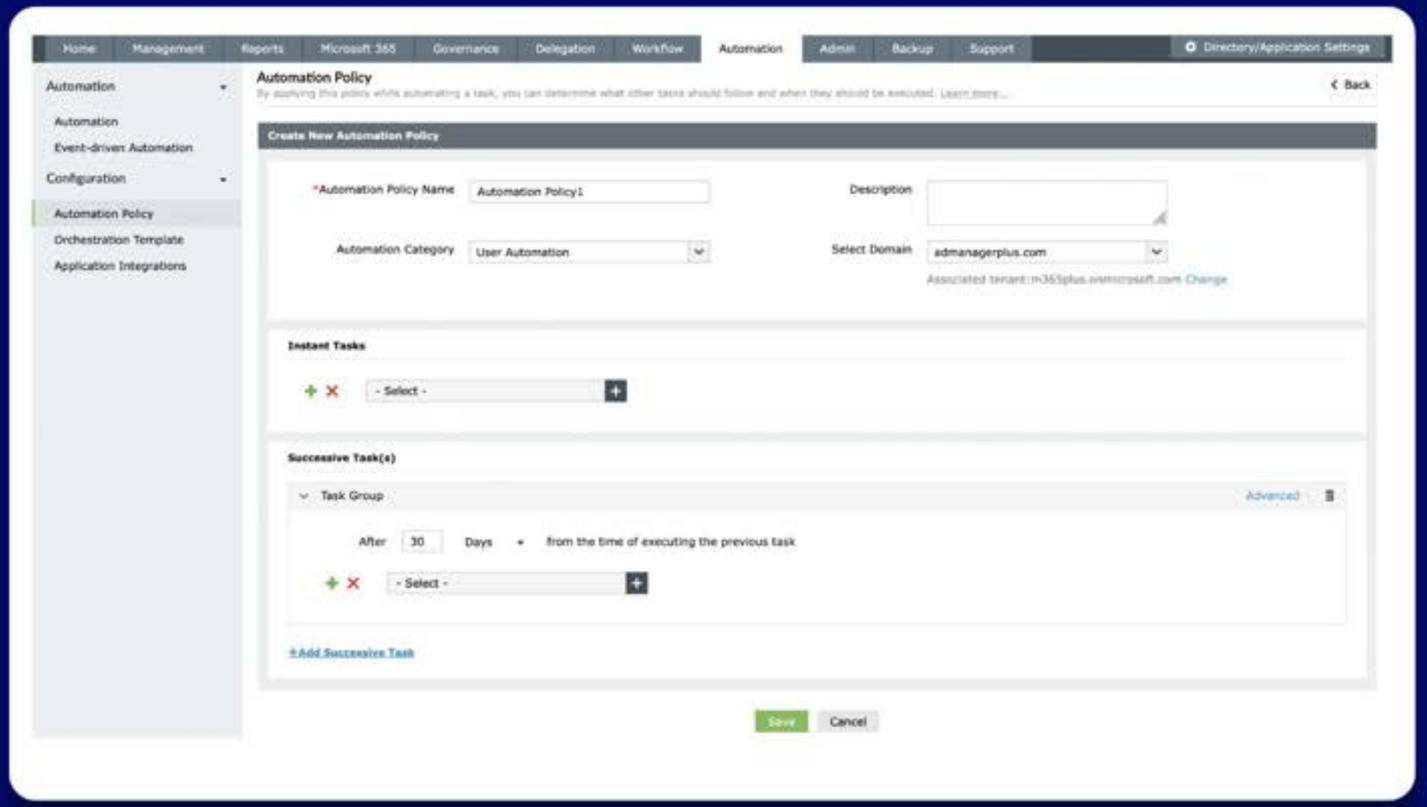
Run the moment the automation fires

Successive task groups

Run after the delay you set, such as 30 days later

Applied everywhere

Used by scheduled and event-driven automation alike



ManageEngine

Identity orchestration

Chain actions across AD, Microsoft 365 and connected apps

Build a workflow once. Every leaver after that is handled the same way, in the same order.

Drag and drop builder

AD, Exchange, cloud and custom actions in one flow

Logic and time delays

Add conditions, and wait before the final step

One trigger, every system

Account, groups, mailbox and Microsoft 365 access, in sequence



ManageEngine

Zia, AI assistant

Ask, don’t navigate

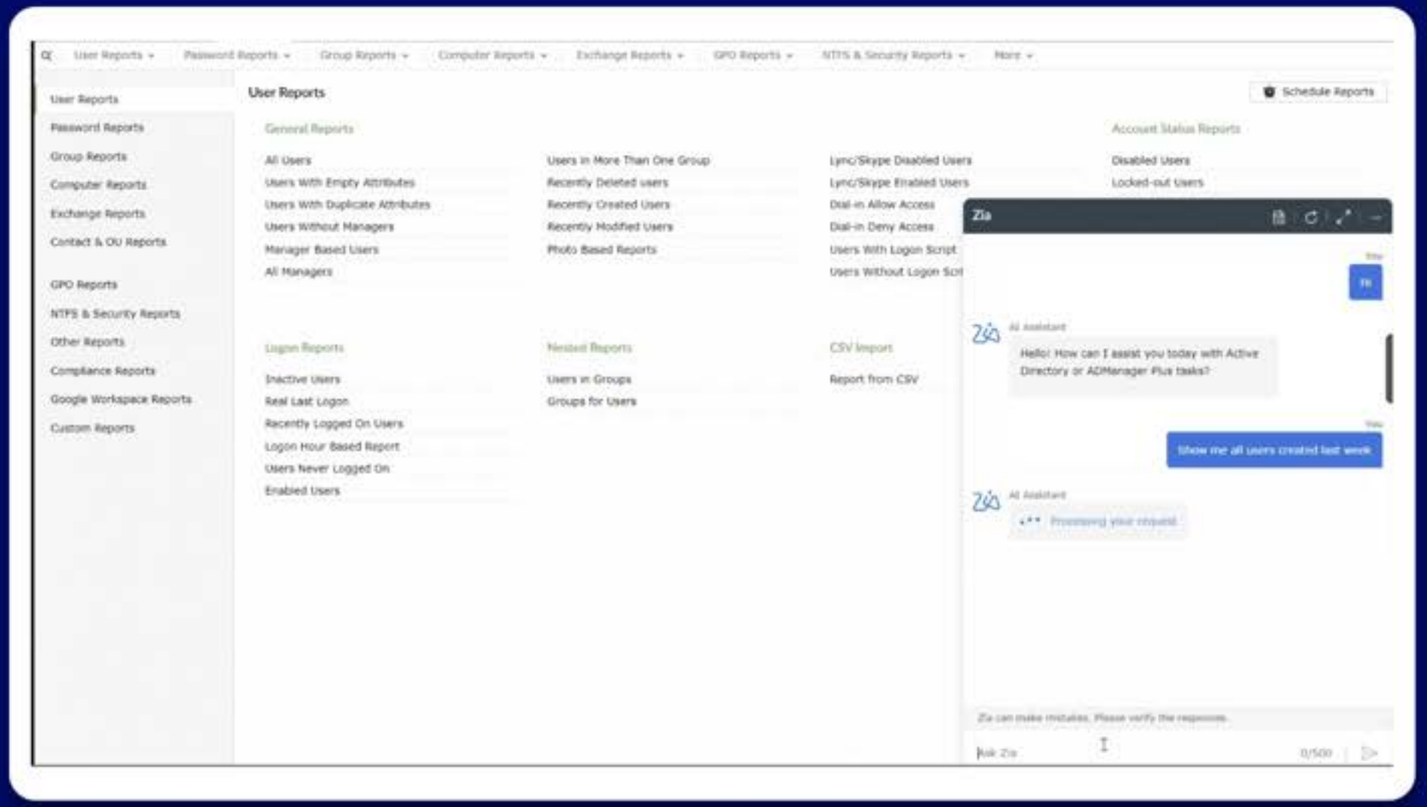
Zia performs AD tasks and pulls reports from a chat window, in plain language.

Perform actions

Enable or disable users, unlock accounts, reset passwords

Pull reports

Users, groups, contacts, and computers



ManageEngine

Help desk delegation

Delegate without handing over admin rights

Help desk technicians get exactly the tasks they need, and nothing more.

Scoped by role and OU

Assign help desk roles to users or groups, per domain and OU

AD privileges unchanged

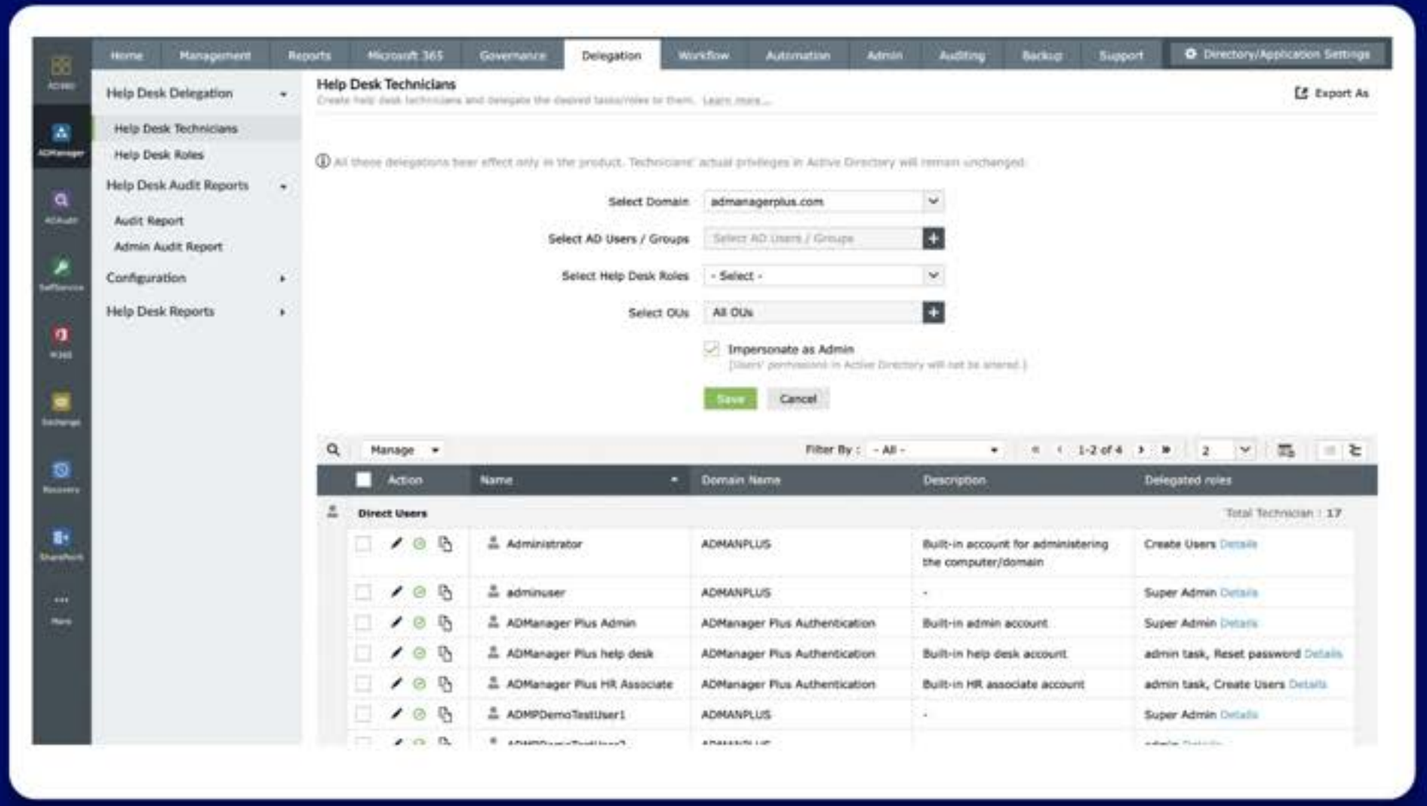
Delegations take effect only in the product

Every action audited

Help desk audit and admin audit reports

Same model for AI agents

SecureAI help desk roles, scoped to platforms and resources



ManageEngine

Manage AI agents

Bring every agent in

Connect the platforms your teams build on. Every agent, model and MCP server lands in one inventory.

Agent platforms

Discover, govern and protect at runtime

Microsoft AI Foundry · Copilot Studio · Gemini Enterprise Agent Platform · Zia Agents

Enterprise AI platforms

Risk assessment

Anthropic Claude · Gemini · GitHub Copilot

Identity providers

Agent identities and permissions

Microsoft Entra ID · Google Workspace

ManageEngine

AI agent discovery

Every agent, accounted for

One inventory of the agents your teams built, with the platform, model and owner of each.

Unmanaged agents

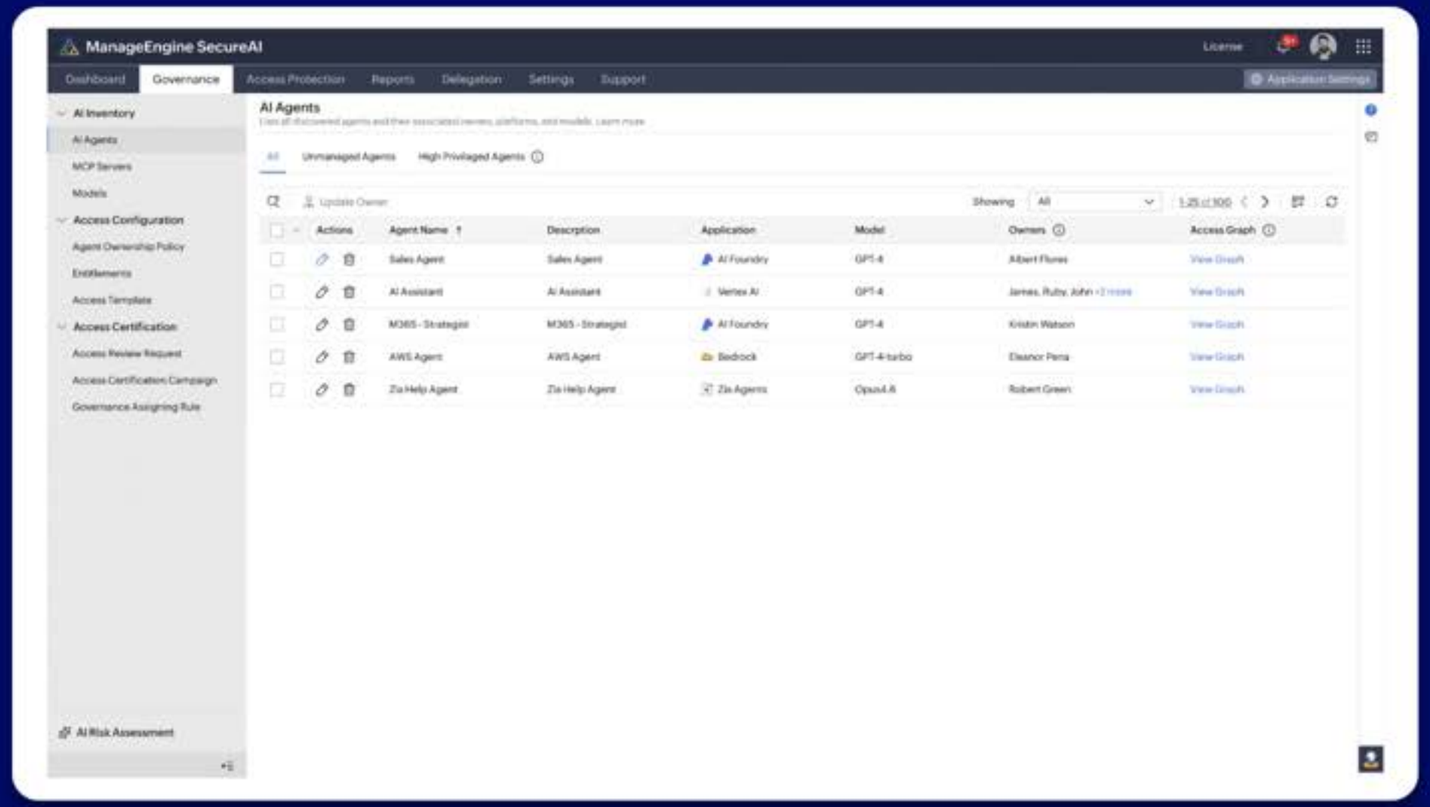
No owner on record; assign one from the list

High-privileged agents

Elevated access, flagged for closer oversight

Access graph per agent

One click to see what it can reach



ManageEngine

MCP server management

What your agents run on: MCP servers and models

The inventory goes beyond agents to the servers and models behind them.

MCP servers

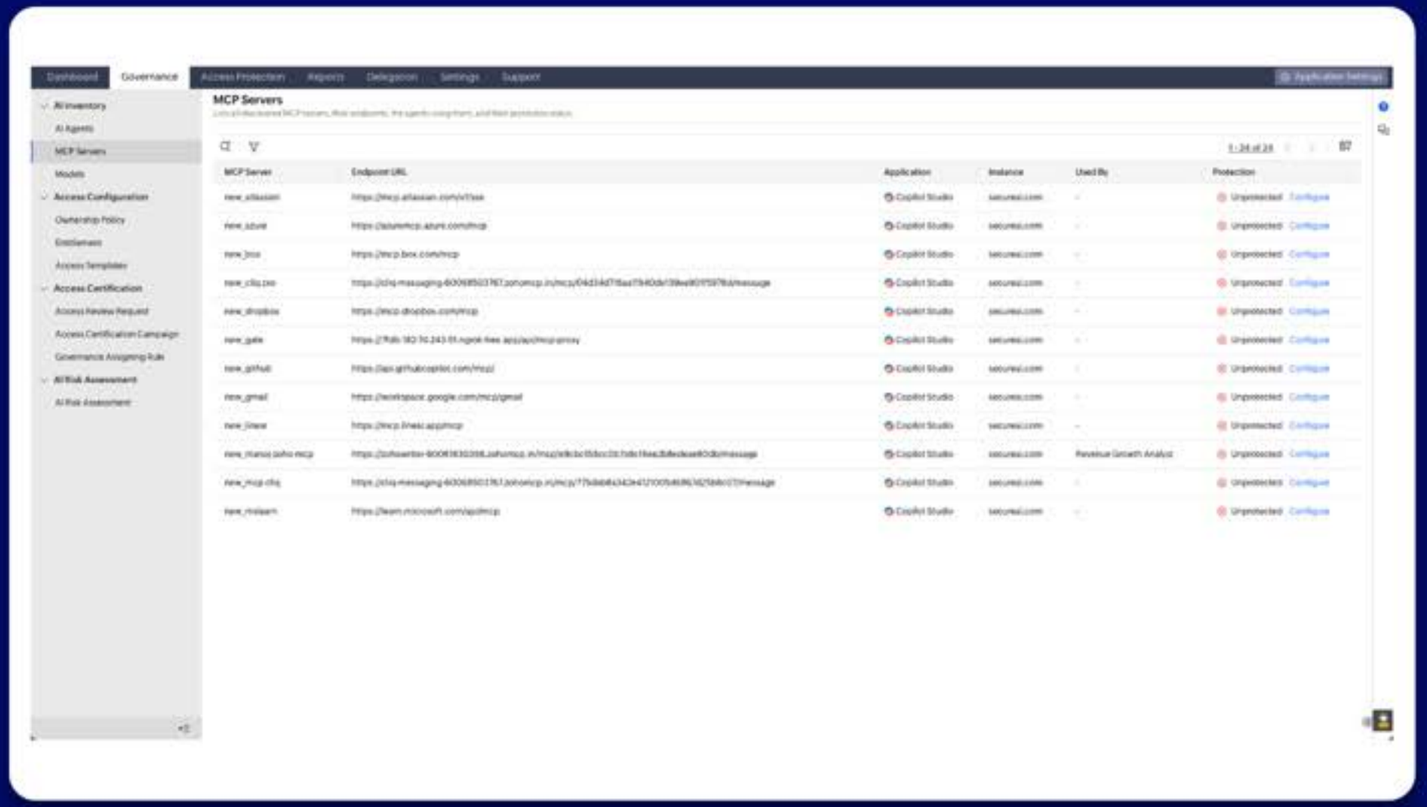
Endpoint, application, agents using it, protection status

Unprotected servers flagged

Secure them by registering and binding to a gateway

Models

Name, model ID, provider and the agents using each



AI agent ownership policy

Every agent gets an accountable human

An agent with no owner is an agent nobody answers for.

Assigned at discovery

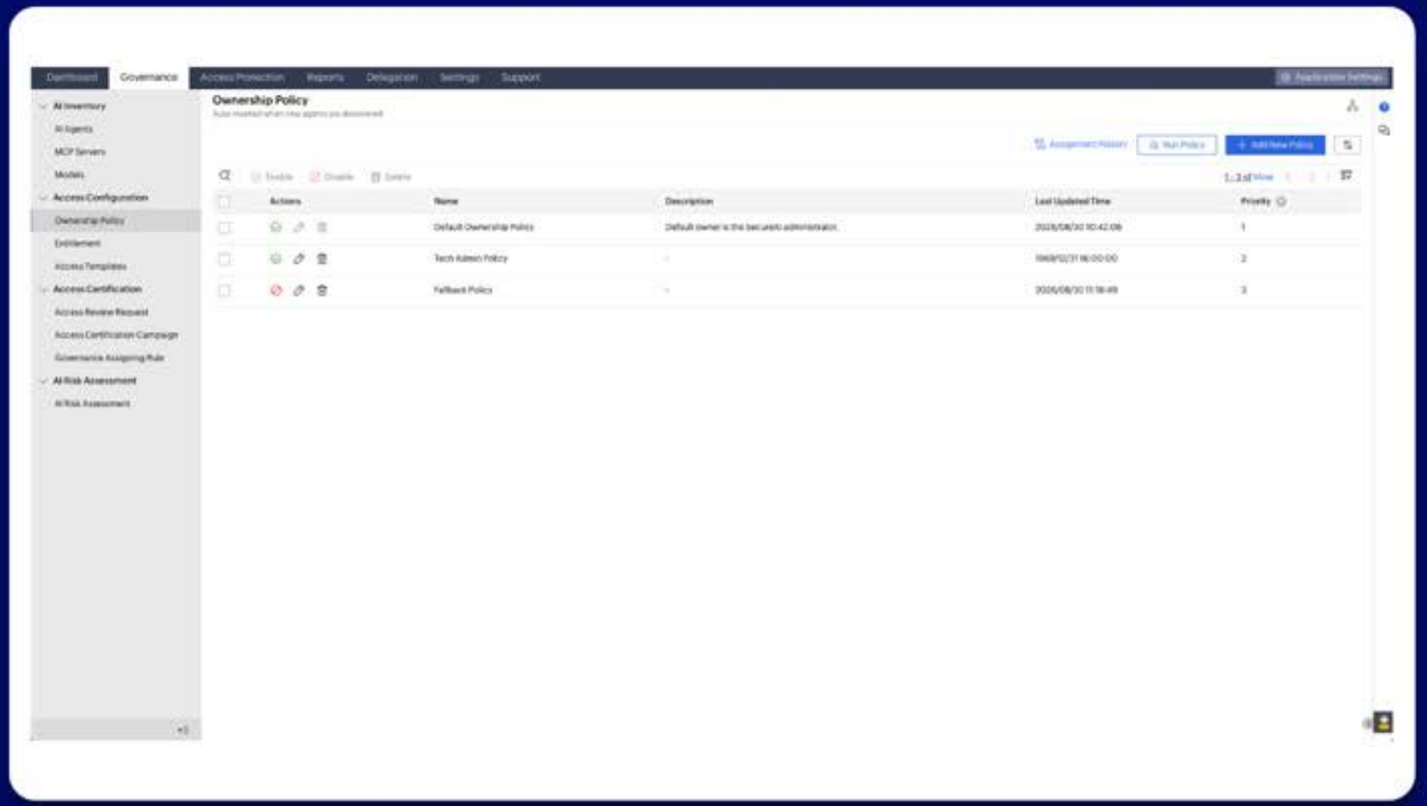
Ownership policy runs automatically, by role and agent name conditions

Owners from your directory

Owner pools sourced from Microsoft Entra ID and Google Workspace

Mandatory, not optional

No agent enters the governed environment without a responsible human



ManageEngine

Use case

New hire ready, access not given

A new hire joins. IT is waiting for a ticket, a manager's email, or someone to remember.

The problem

Provisioning waits days for manual tickets. MFA enrollment is missed on day one. AD, Microsoft 365 and apps are handled separately.

With AD360

An HR record starts the workflow

AD account, MFA dependency and app assignment, with notifications at each step

Location-aware branching

The right resources for US and UK employees

Ready before day one

Provisioned and productive on the first morning

ManageEngine

02

Protect

Verify who's asking at every login, on every system, not just the cloud ones.

For AI agents: AI agents are not routed through MFA; their runtime checks happen at the MCP gateway.

MFA

MFA on every login, not just the cloud ones

Most MFA stops at cloud apps. AD360 extends it to machine logins and remote access.

Endpoint logins

Windows, macOS and Linux, including local accounts

Remote access

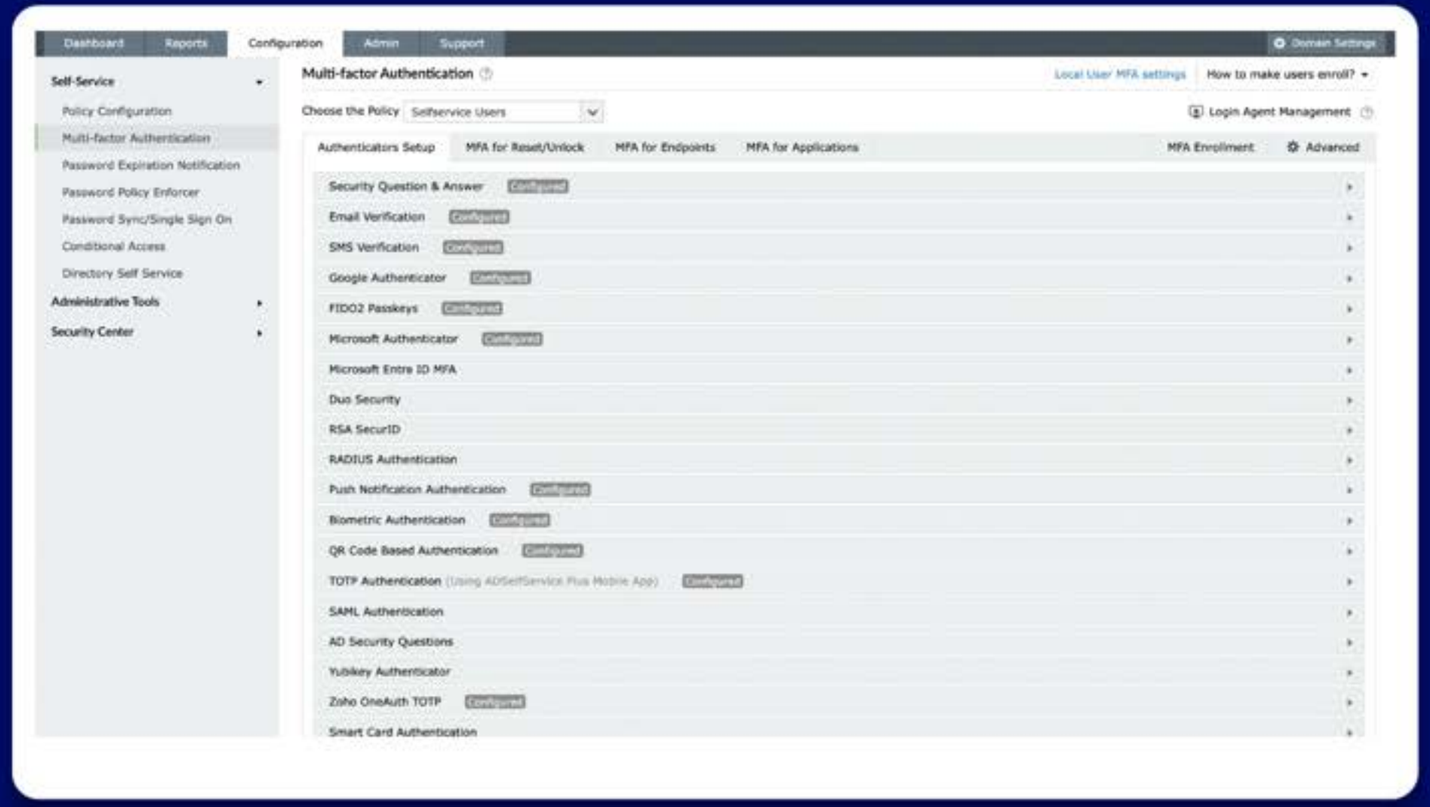
VPN, RDP, Outlook on the web and enterprise apps

20 authenticators

FIDO2 passkeys, biometrics, YubiKey, Duo, RSA SecurID, smart cards and more

Context-aware

Step up or skip by IP, device, time and location



ManageEngine

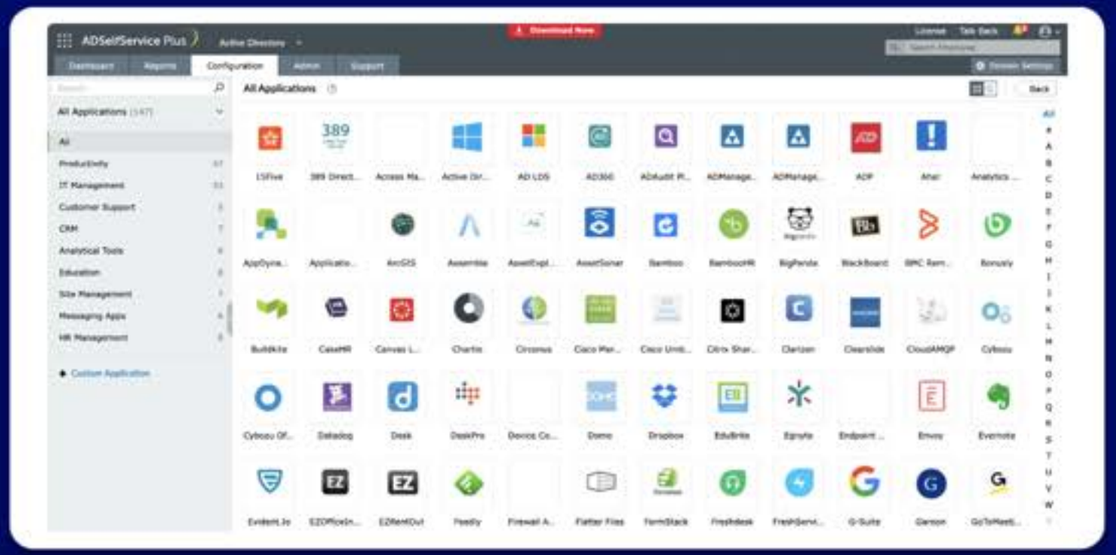
SSO

One click into every app, on your terms

Single sign-on with one set of Active Directory credentials, gated by the policies you set.

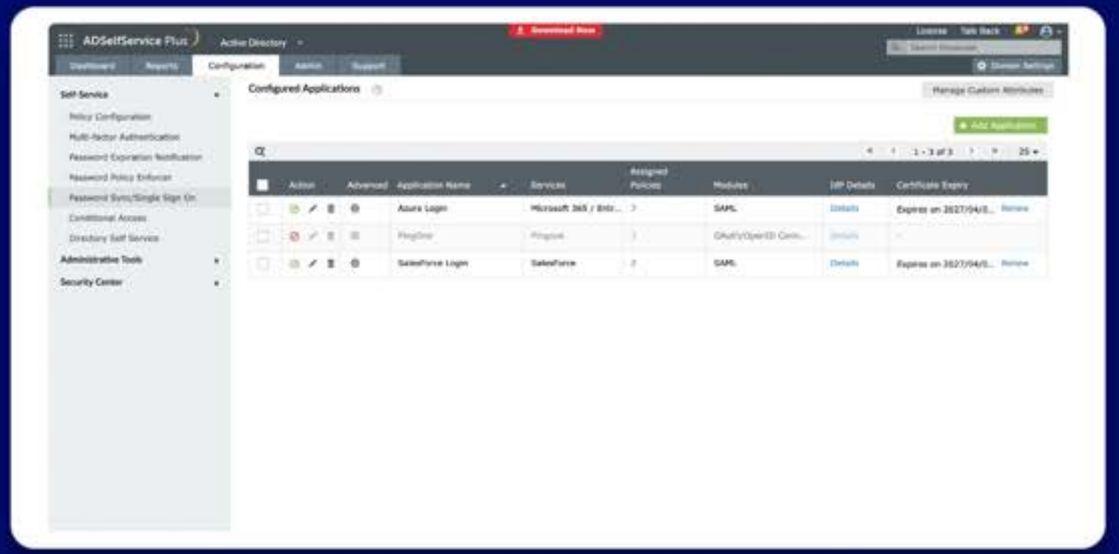
A ready-made app catalog

Hundreds of preconfigured applications, plus custom applications for anything else.



Standard protocols

Apps connect over SAML or OAuth and OpenID Connect, with policies assigned per app.



Passwordless sign-in with passkeys, biometrics or push, and policies scoped to specific OUs and groups.

ManageEngine

Password policy enforcer

Fewer resets, stronger rules

Self-service where it's safe, enforcement where it matters.

Reset and unlock, self-service

From the Windows, macOS or Linux logon screen

Real policy rules

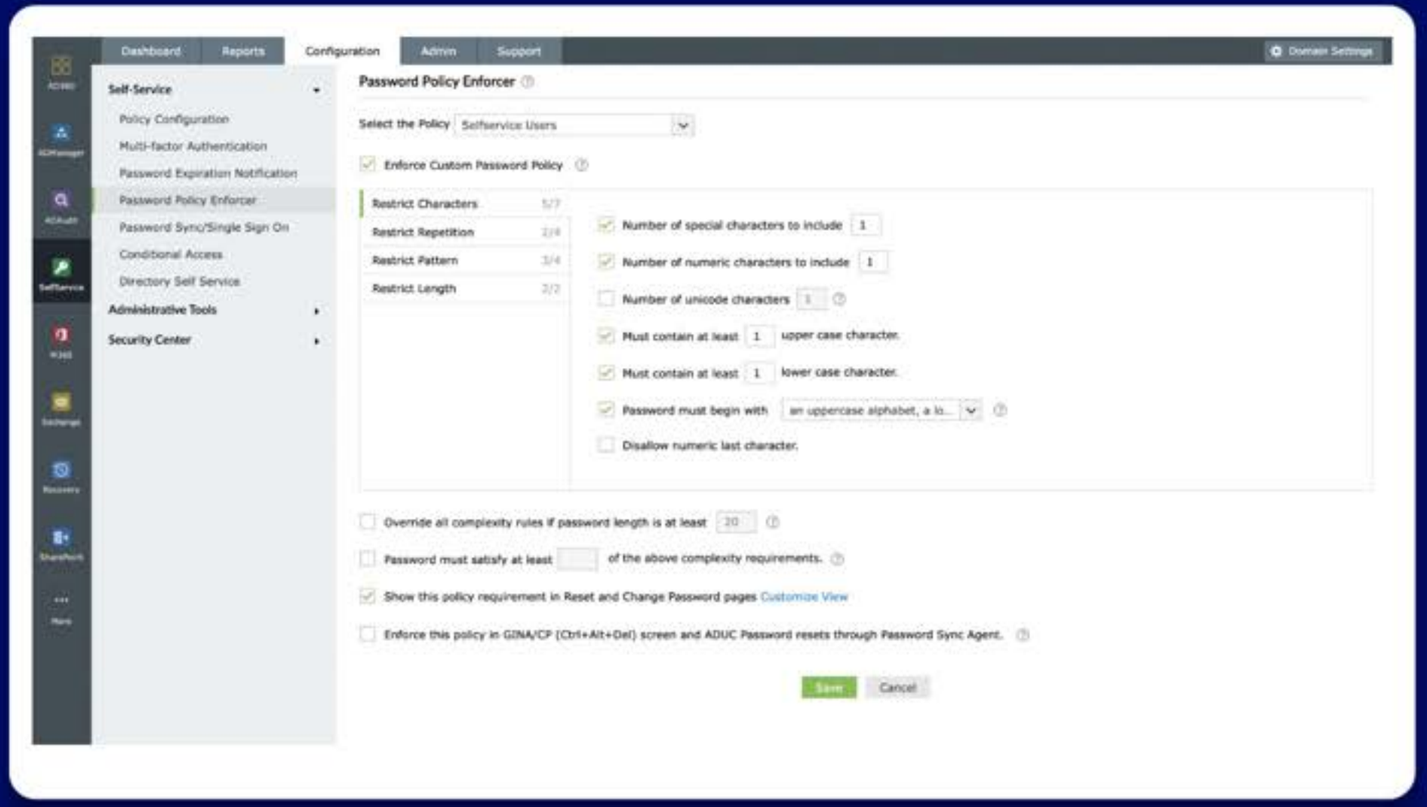
Characters, repetition, patterns and length, shown on reset pages

Enforced everywhere

Including Ctrl+Alt+Del and ADUC resets through the sync agent

Breach checks and reminders

Have I Been Pwned check; expiry alerts by email, SMS and push



ManageEngine

Self-service password reset

A locked-out user, back in, without the help desk

Self-service password reset and account unlock, in three steps.

Identify

The user enters their username and domain, from the logon screen, a browser or the mobile app.



Verify

Identity is confirmed with security questions or any enrolled factor: biometrics, push, TOTP, YubiKey and more.



Reset

A new password is set against your policy, with every rule shown to the user as they type it.



Remote workers too: Cached credentials update and offline MFA for Windows and macOS logins.

ManageEngine

03

Govern

Prove the right people have the right access, and find the access nobody should have.

For AI agents: Entitlements reviewed in the same certification campaigns, with requests routed to the right approver.

Identity risk assessment

Know your identity risk before an auditor does

Continuous risk assessment across Active Directory and Microsoft 365.

Score and trend

One risk score out of 100, tracked over time

Every object type

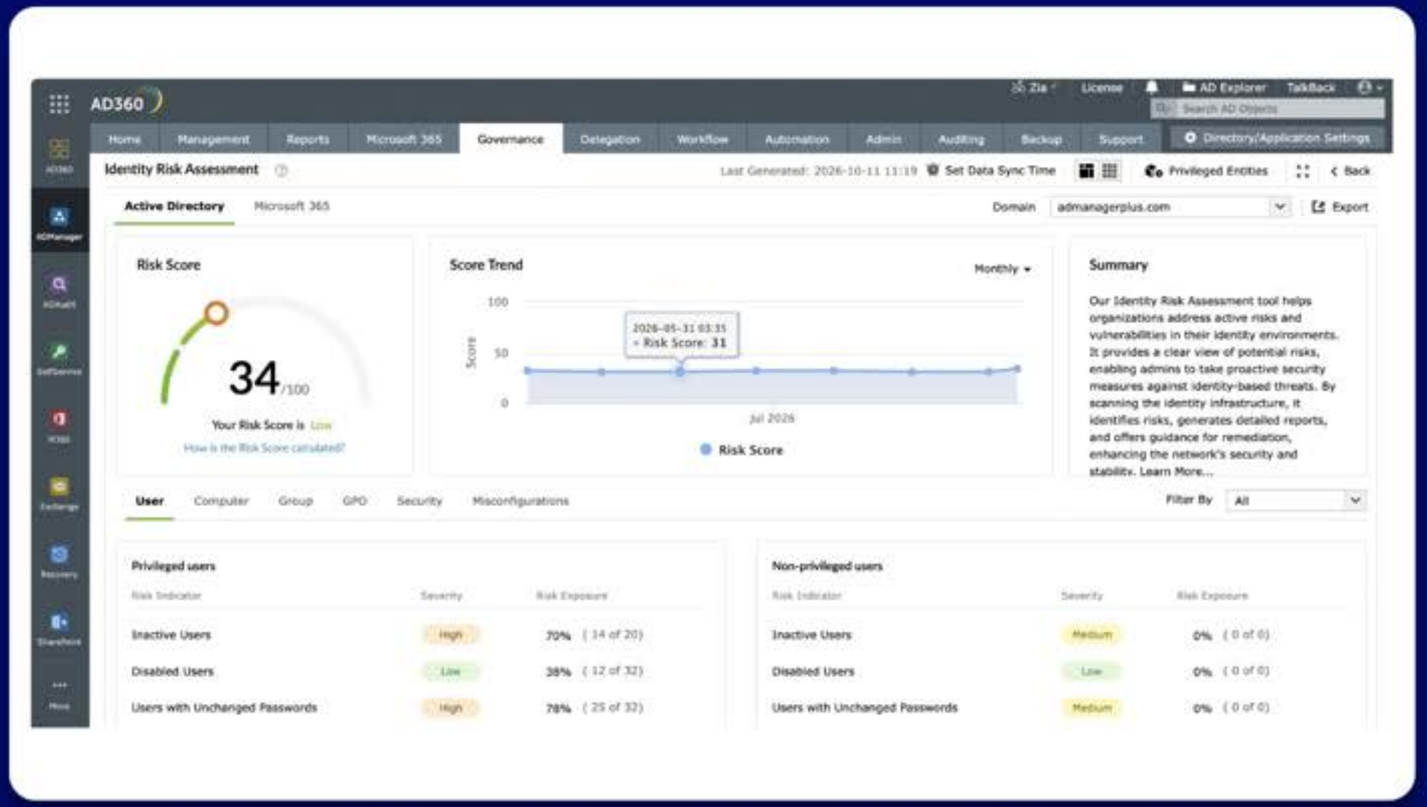
Users, computers, groups, GPOs, security settings and misconfigurations

Severity and exposure

Each risk indicator rated and sized, with privileged accounts separated out

Fix it on the spot

Remediate a finding right from the assessment, no separate tool or ticket



ManageEngine

AI agent identity risk assessment

Know your AI risk, by platform

A risk view for Anthropic Claude, Gemini and GitHub Copilot accounts, whether or not their agents are managed.

Risk score and trend

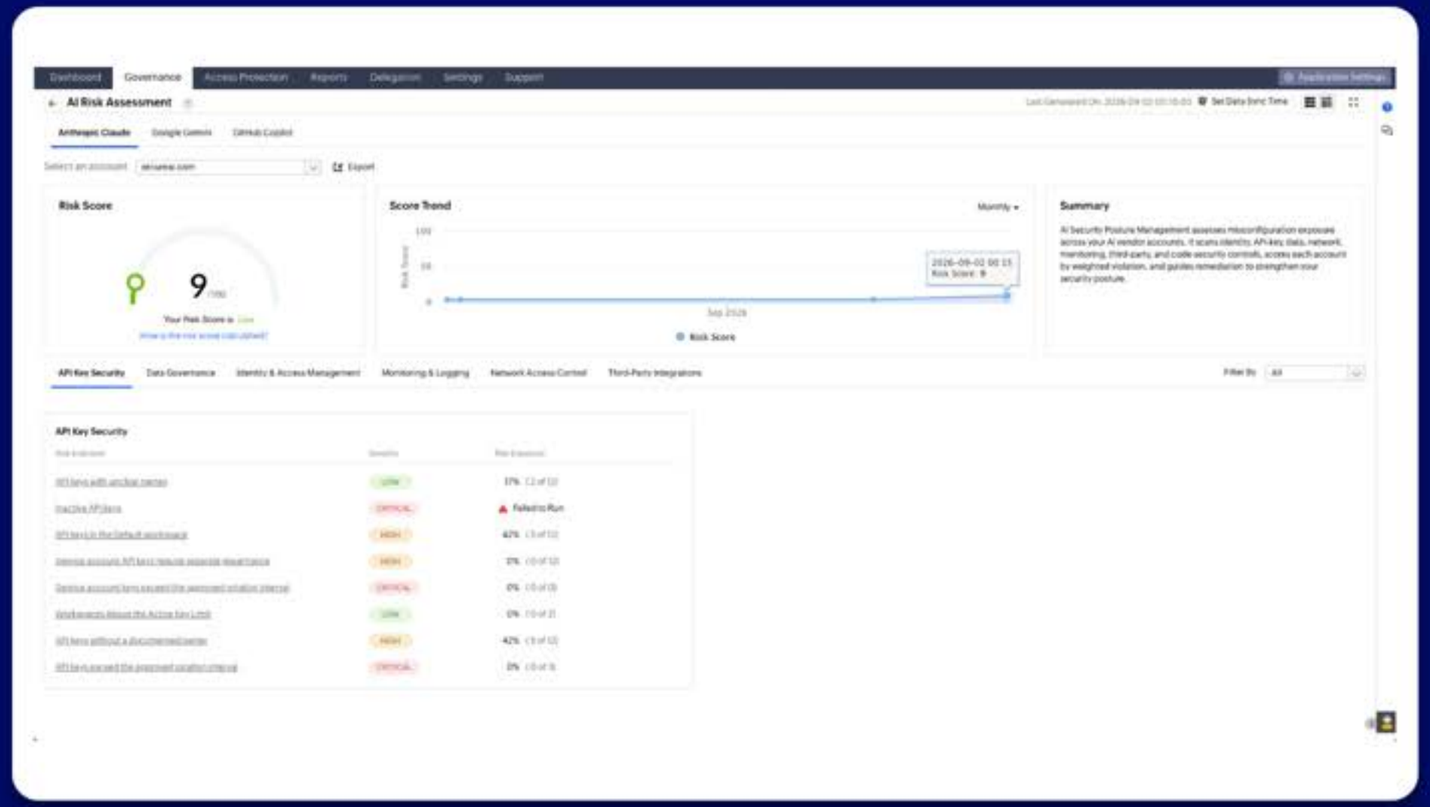
From detected misconfigurations

Findings with fixes

Evidence and step-by-step remediation

Compliance mapping

EU AI Act, ISO/IEC 42001, NIST AI RMF, Gartner AI TRiSM, NCSC

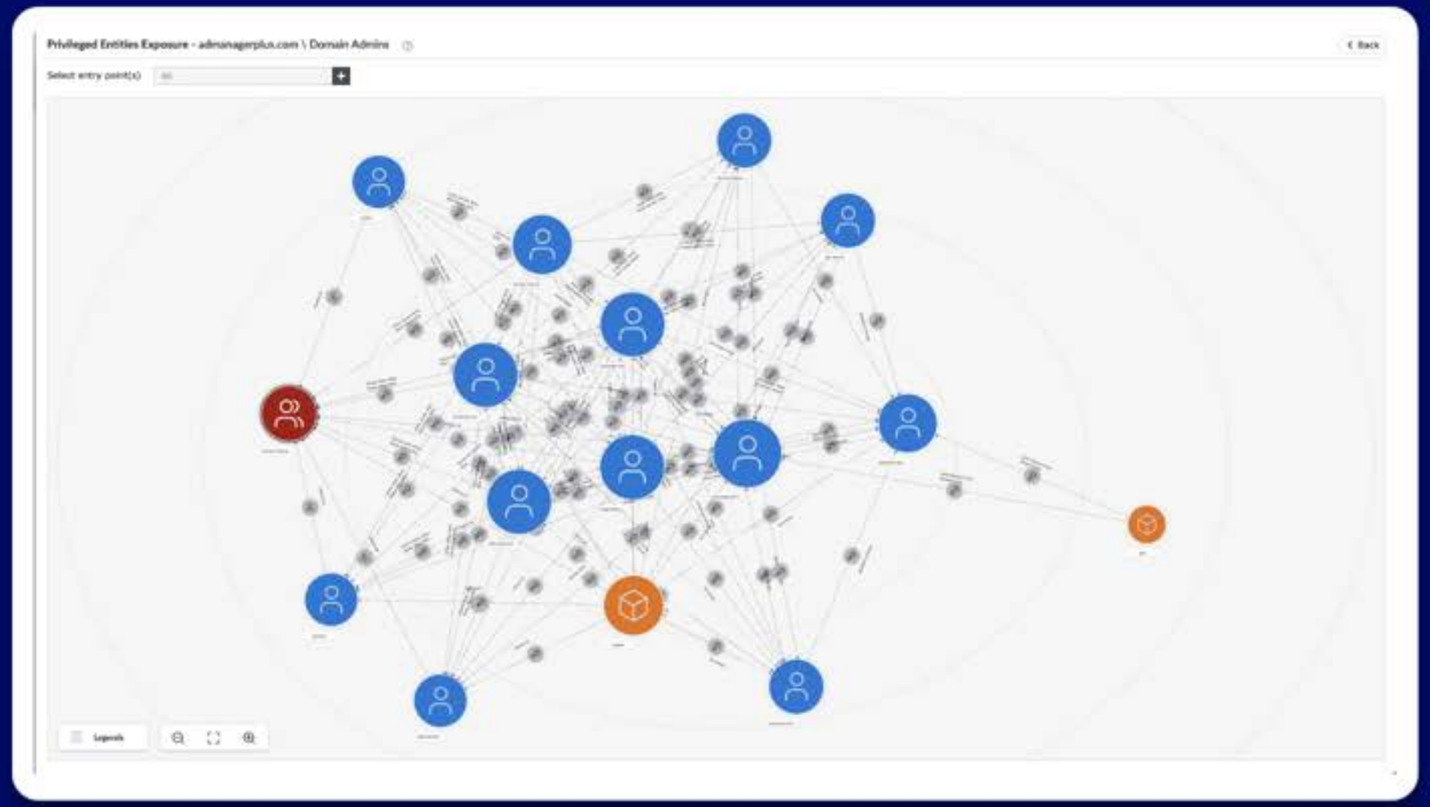


ManageEngine

Risk exposure management

See how an attacker could reach privilege

Risk exposure management maps every route to your privileged entities, and what it takes to close each one.



Beyond default admin groups

Exposure around nested and custom privileged groups, not just built-in roles

Close the path from the graph

Click any link to see the exact permission behind it, then remove it right there

Predefined queries

Paths from Domain Users or Kerberoastable users to privileged entities

Prioritized by real risk

Ranked by likelihood, impact and exposure context

ManageEngine

AI agent risk exposure management

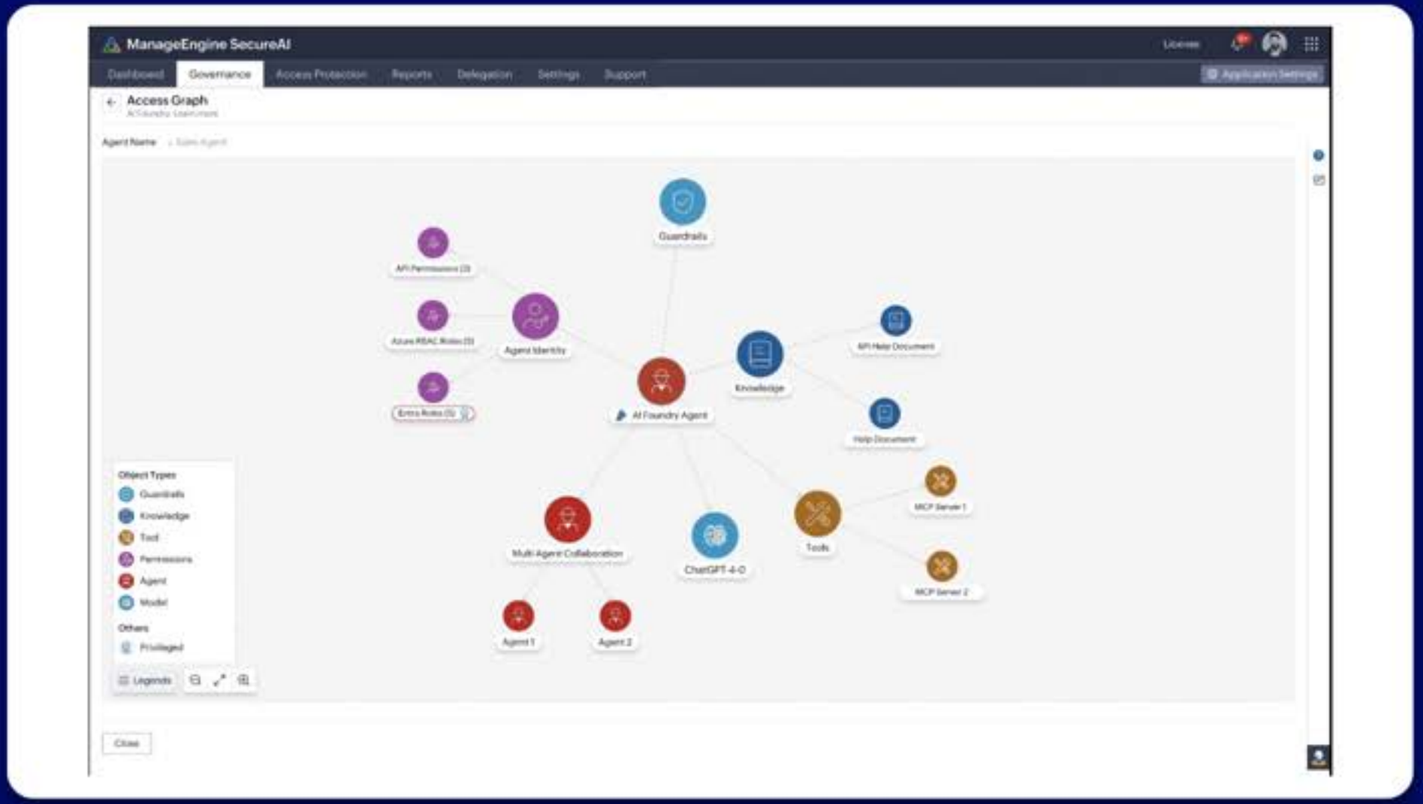
See everything an agent can reach

For any agent, generate a visual map of its access.

Identity and permissions
API permissions, Entra roles, Azure RBAC roles

Knowledge sources and tools
What the agent reads and calls

MCP servers, model, guardrails
What it runs on and what limits it



ManageEngine

Access review

Access reviews that don’t stall

Certification campaigns that route themselves, for employees and AI agents alike.

Workforce access

Groups, Entra ID roles, Microsoft 365 licenses, Teams and mailbox rights

ML recommendations suggest the right groups from similar users

Rejected access revoked

AI agent access

Entitlements fetched from every agent platform, each with an owner

Access templates bundle Entra roles, API permissions, Azure RBAC roles, model, MCP servers and knowledge

Templates scope exactly what a campaign reviews

Both: Certifiers assigned by rule, separate reviewer, approver and executor, custom notifications per campaign stage.

ManageEngine

Business workflow

Right request, right approver

Administrative tasks and AI agent access requests follow a business workflow you define.

Four stages

Requester, reviewer, approver and executor

Configurable per stage

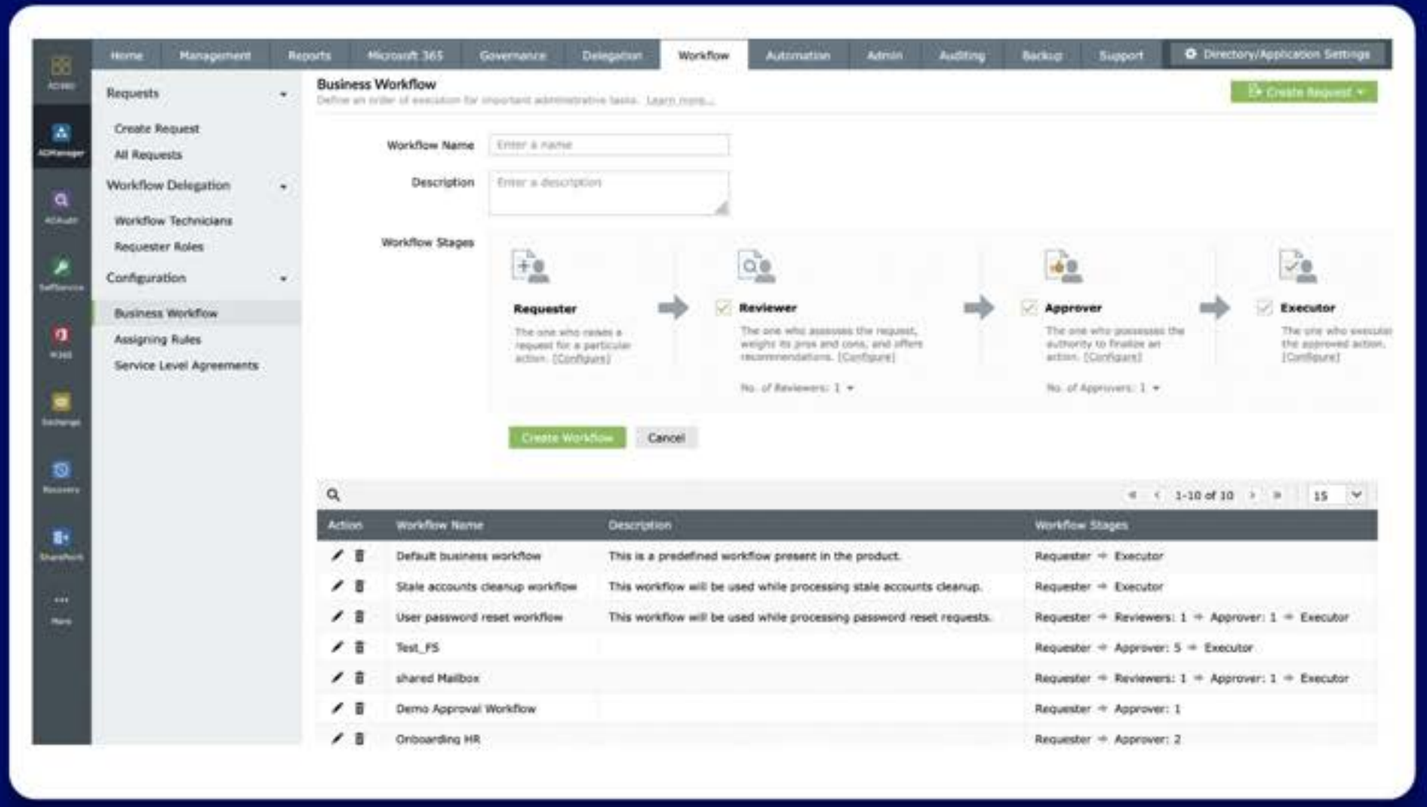
Number of reviewers and approvers

Routed and tracked

Assigning rules route requests; SLAs track pending ones

Agents too

AI agent access requests follow the same workflow

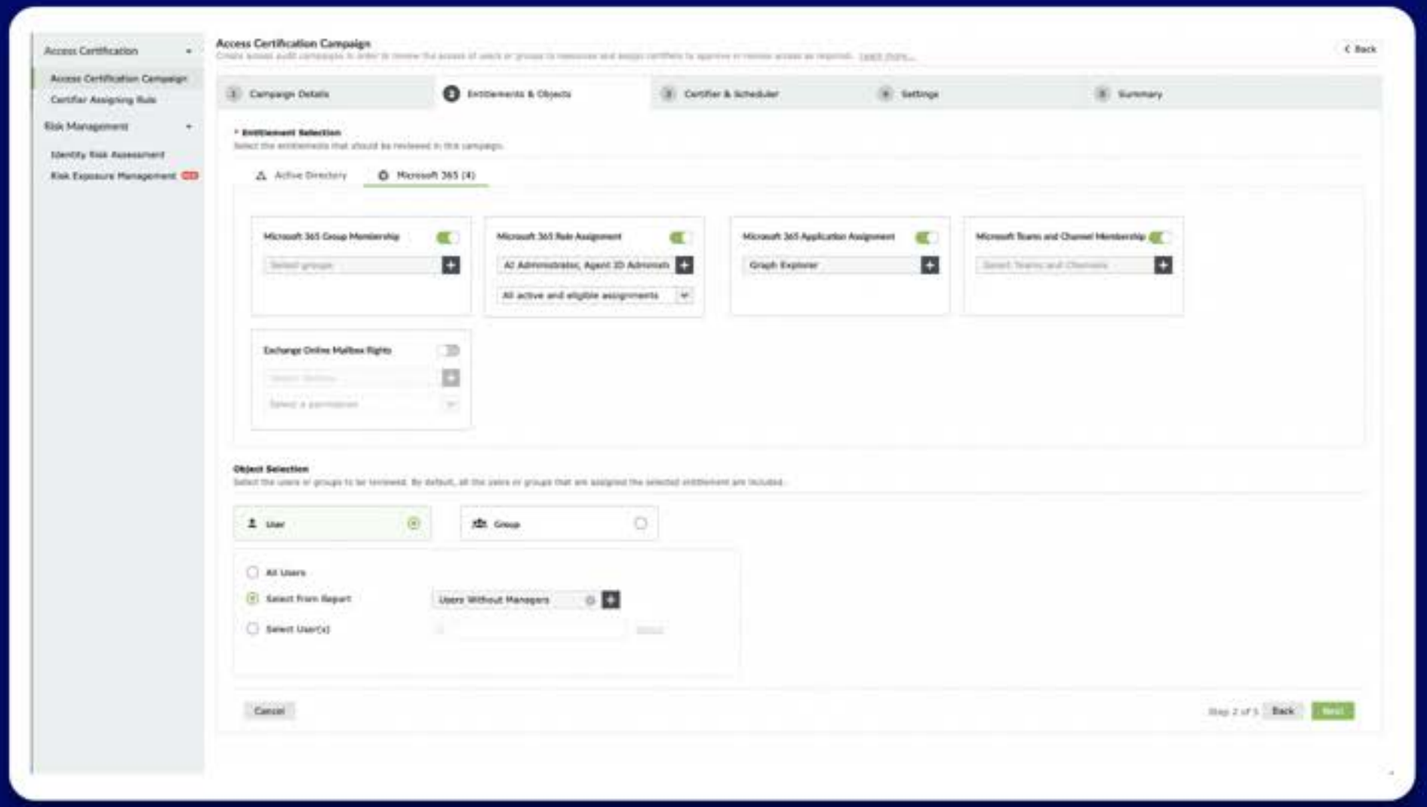


ManageEngine

Access certification campaign

Every entitlement type, one review

Pick Active Directory or Microsoft 365 entitlements, choose the users or groups, and assign certifiers by rule.



ManageEngine

Entitlement management

Every agent entitlement, in one view

Entitlements are fetched from every configured agent platform and bundled into access templates for review.

Entitlements, normalized

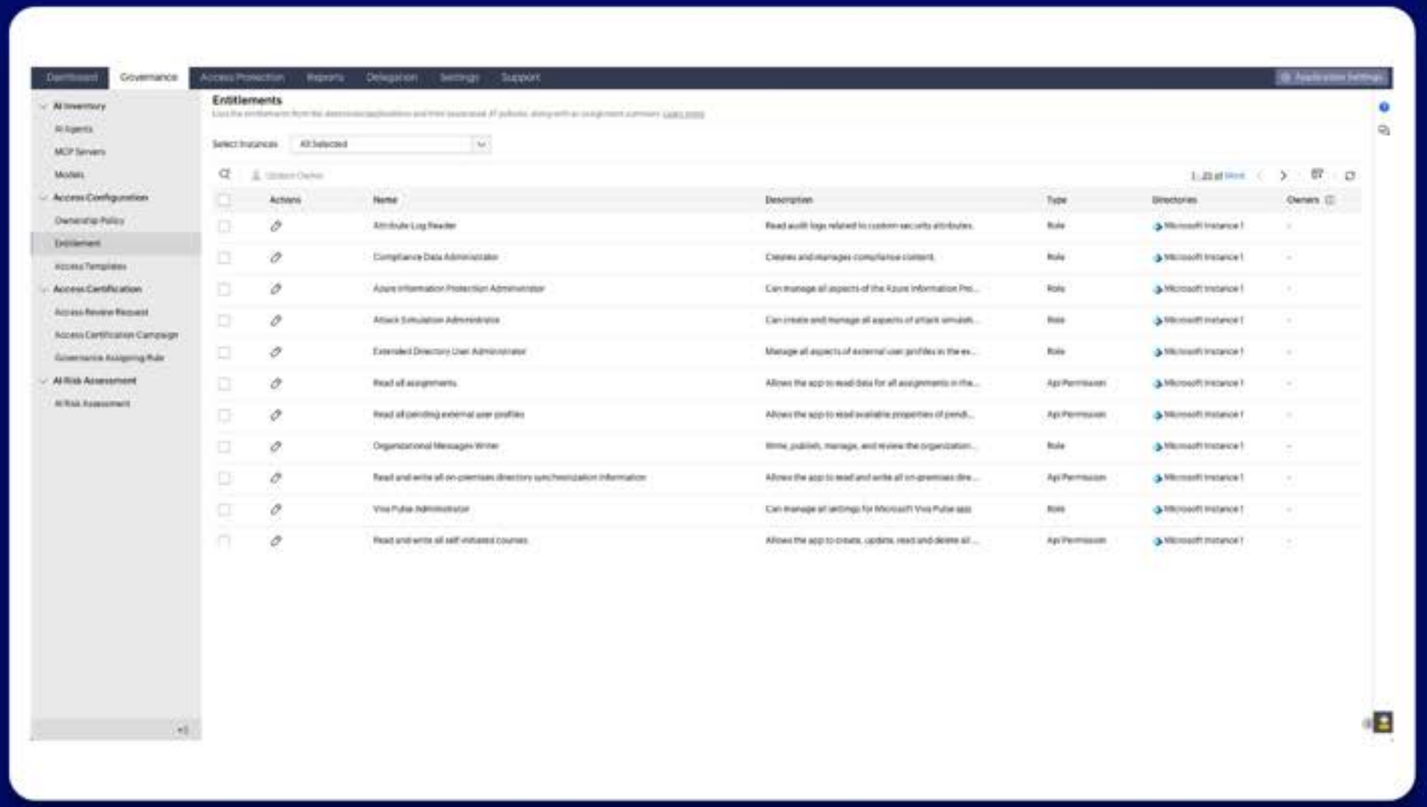
Name, description, type, application and owner

Owners reassigned in bulk

Or one at a time

Access templates

Identity permissions plus model, MCP servers and knowledge, bundled for review



ManageEngine

AI agent access certification campaign

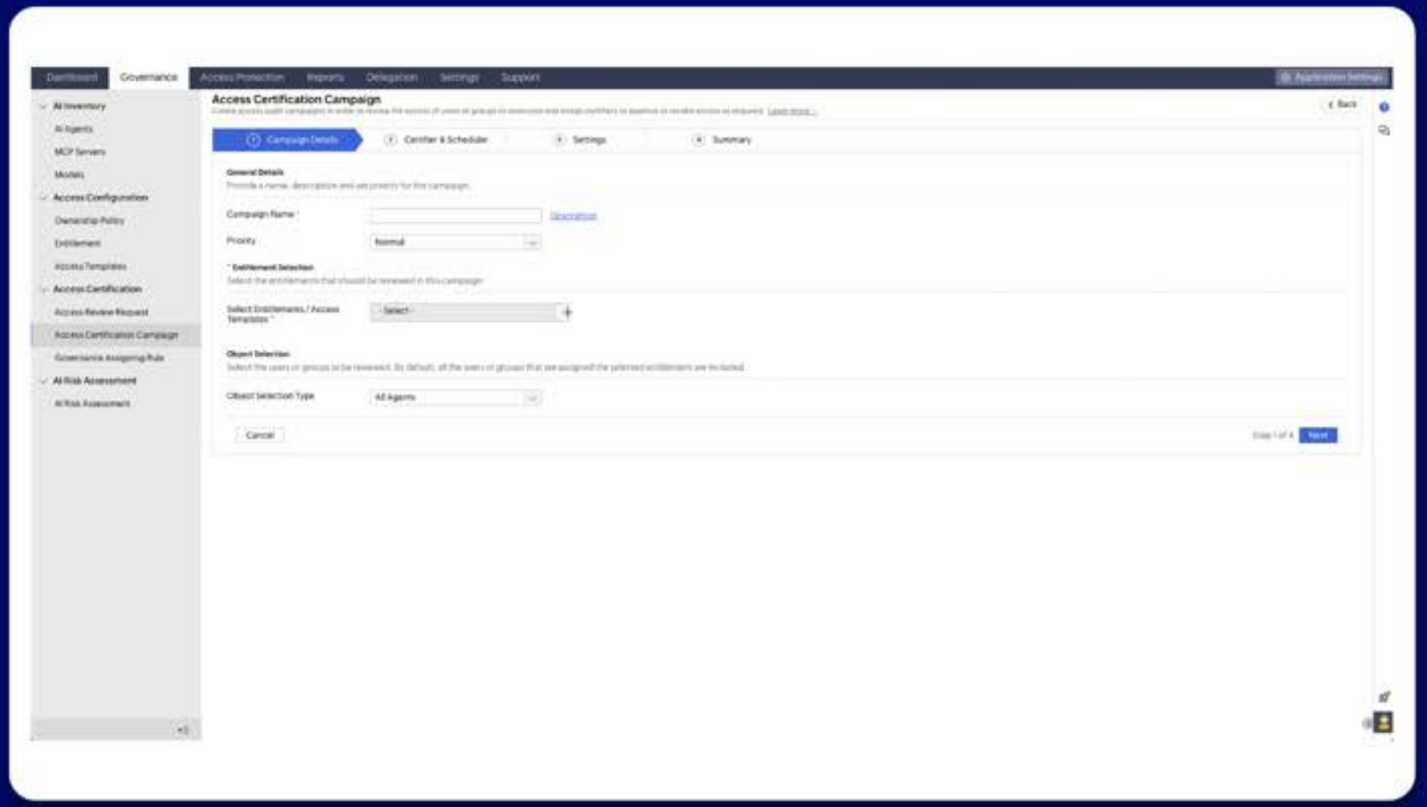
Agent access, reviewed the same way

The same campaign model as employee access, applied to AI agents.

Pick what gets reviewed
Agent entitlements or access templates

Pick which agents
All agents, or a chosen set

Routed and decided
Assigning rules route reviews, and owners certify or revoke



ManageEngine

Zia access insights

Is this access normal for this role?

Zia analyzes group memberships and tells you what doesn't fit.

Peer comparison

Benchmarks a user's memberships against direct peers

High-risk findings

Flags dangerous combinations of memberships

Pattern recognition

Deviations from the norm for a job title or department

Actionable recommendations

Which permissions to certify, monitor or modify

MCP gateway

Knowing what an agent can reach isn’t enough

Risk happens at runtime

Governance decides what an agent should do. Live tool calls to real systems are where the risk is realized.

Uninspected calls

A prompt-injected or misbehaving agent can issue destructive or sensitive calls.

Standing credentials

An agent often has more reach than any single task needs.

AD360 inserts an **MCP gateway** between agents and tools, so every call is identity-bound and policy-checked.

MCP gateway

One gateway, every call inspected

Three steps bring a tool under control.

1. Register the MCP server

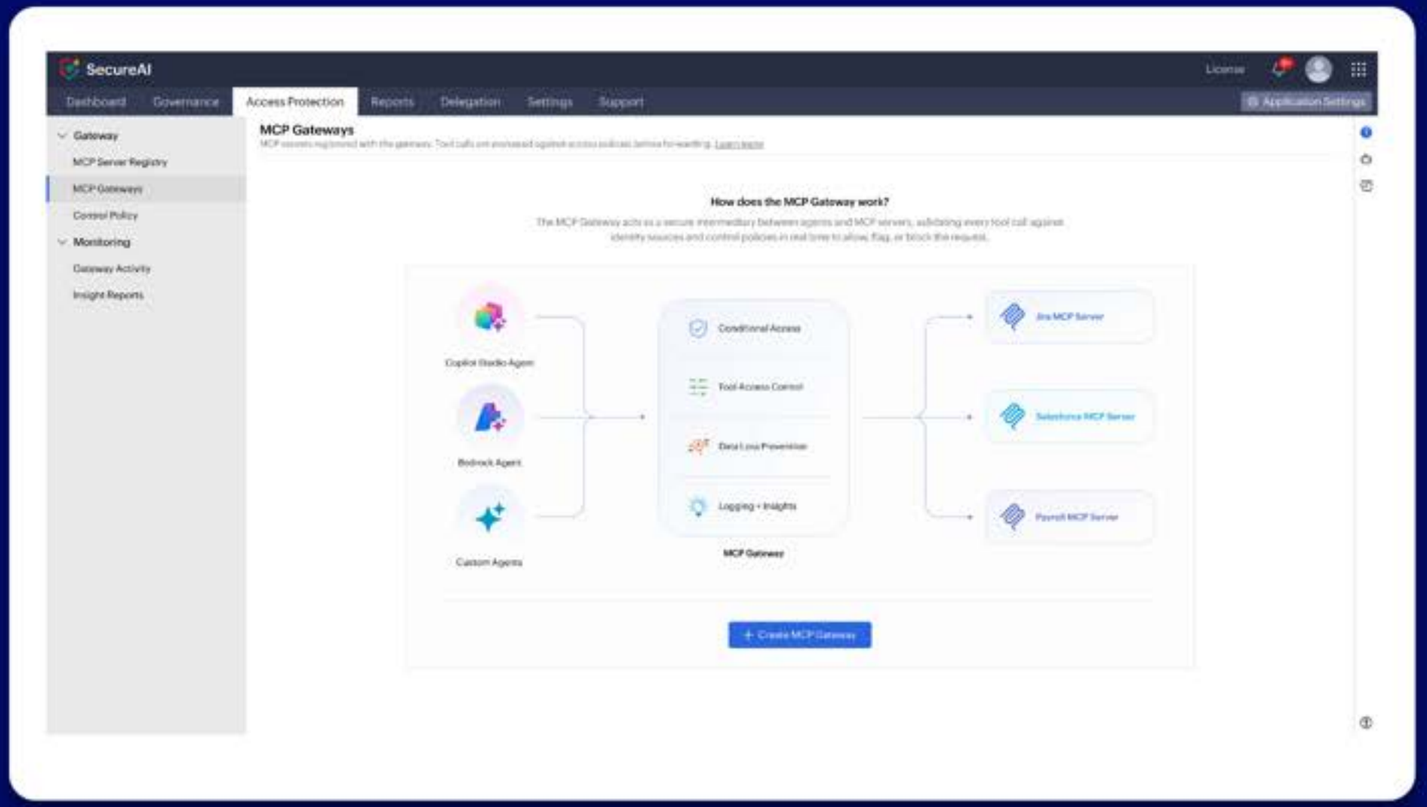
Add the upstream URL and authentication

2. Create a gateway

Group servers under one signed URL with shared rules

3. Connect the client

Point Copilot Studio, AI Foundry or custom agents at it



ManageEngine

Control policy

Block the dangerous call, allow the rest

Two policy types, evaluated on every tool call at runtime.

Access policy

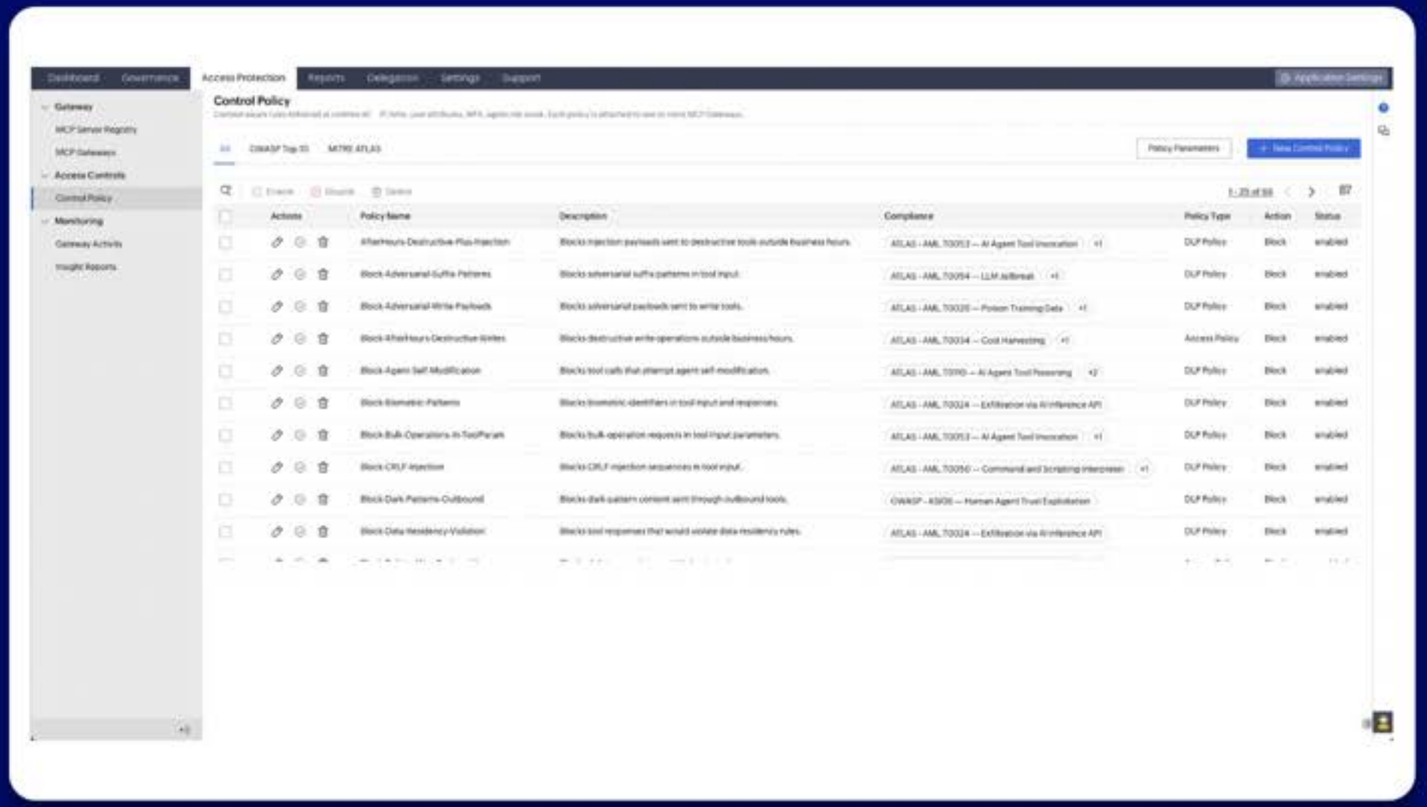
Allow or block. For example, block bulk deletes outside business hours

DLP policy

Redact or block sensitive data before it reaches the tool

Built from context

IP, time, location, tool, role, MFA and agent risk score



ManageEngine

AI agent access protection

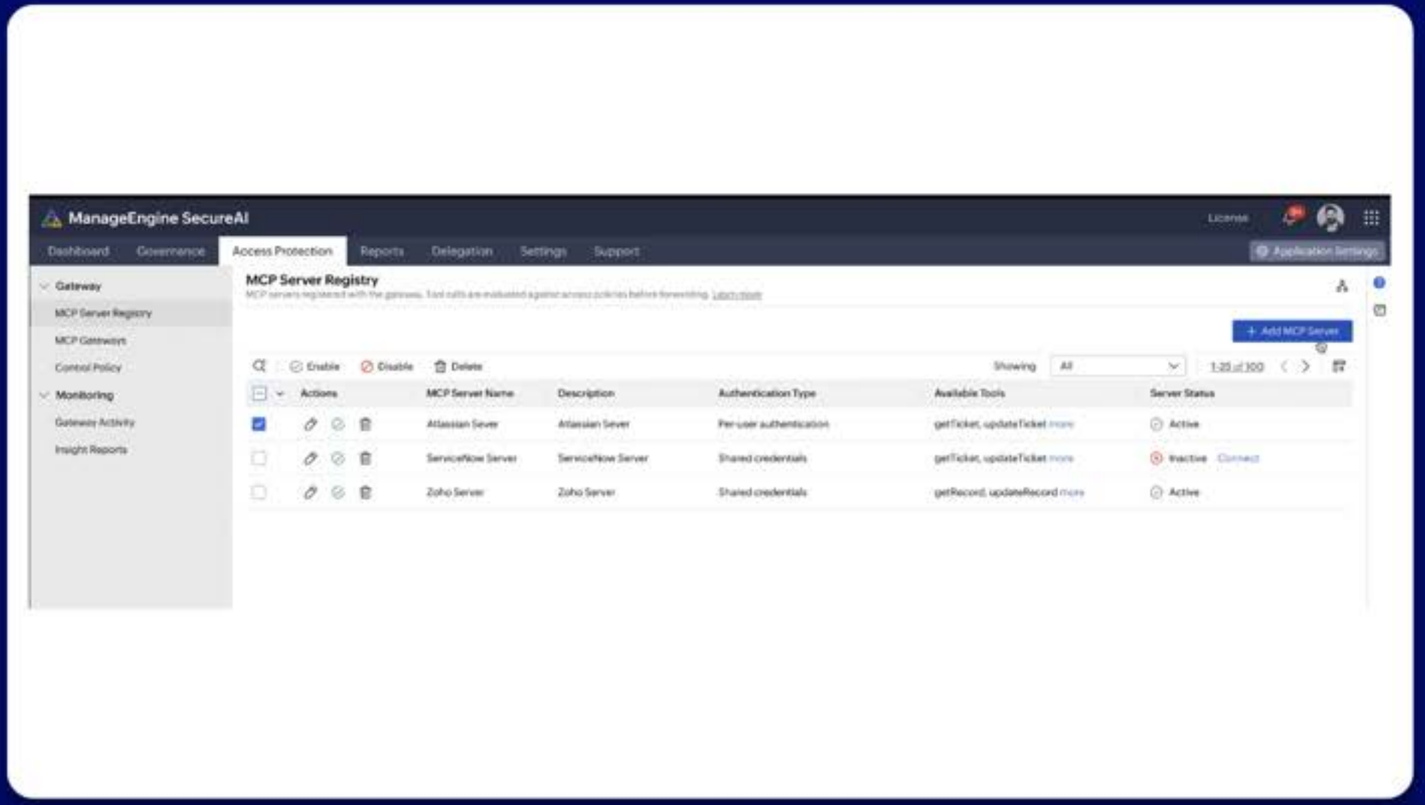
From what exists to what's happening

The Access Protection view shows the gateway at work.

Active and inactive MCP servers
Which servers agents actually use

Live tool-call outcomes
Allowed versus blocked

Policy activity and latency
Access and DLP policy hits, gateway latency percentiles



ManageEngine

Use case

An agent with more reach than its job

Built in an afternoon to help the support team. Nobody registered it. Nobody owns it.

The problem

A team builds a Copilot Studio agent to triage support tickets. Its connected tools can also delete records, and no one in IT knows it exists.

With AD360

01 Discovered and owned
The agent appears in the inventory and is assigned an owner from Entra ID

02 Its reach made visible
The agent graph shows tools and permissions far beyond ticket triage

03 Risky calls blocked
A gateway access policy blocks bulk and wildcard delete operations

04 Every call on record
Each tool call is logged against the agent's identity and the policy decision

ManageEngine

04

Detect and audit

See what changed, who changed it, and what looks wrong across on-premises and cloud.

For AI agents: A real-time record of every MCP call, with the agent, identity, tool and policy decision.

Compliance reports

Compliance reports, ready for the audit

Report sets mapped to the regulations you report against.

Regulation report sets

SOX, HIPAA, PCI DSS, FISMA, GLBA and GDPR

Schedule any of them

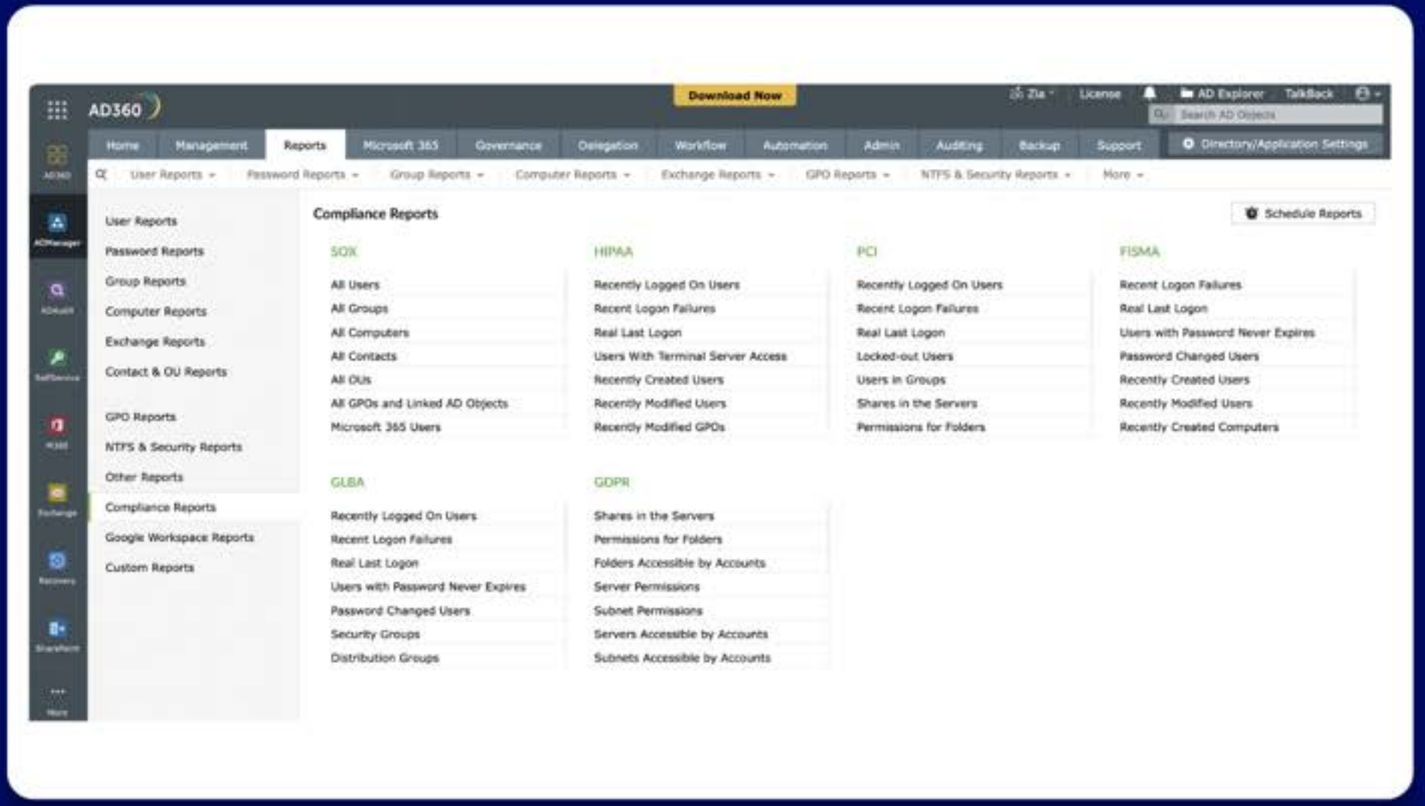
Delivered to auditors without anyone running them

AI frameworks too

EU AI Act, ISO/IEC 42001 and NIST AI RMF through SecureAI

Predefined reports

Stale accounts, weak passwords, privileged accounts and more



ManageEngine

Audit

Auditing beyond Active Directory

Who did what, when and from where, across servers, workstations and file storage.

Windows Server and workstations

Logons, local accounts, PowerShell, processes and policy changes

File servers and NAS

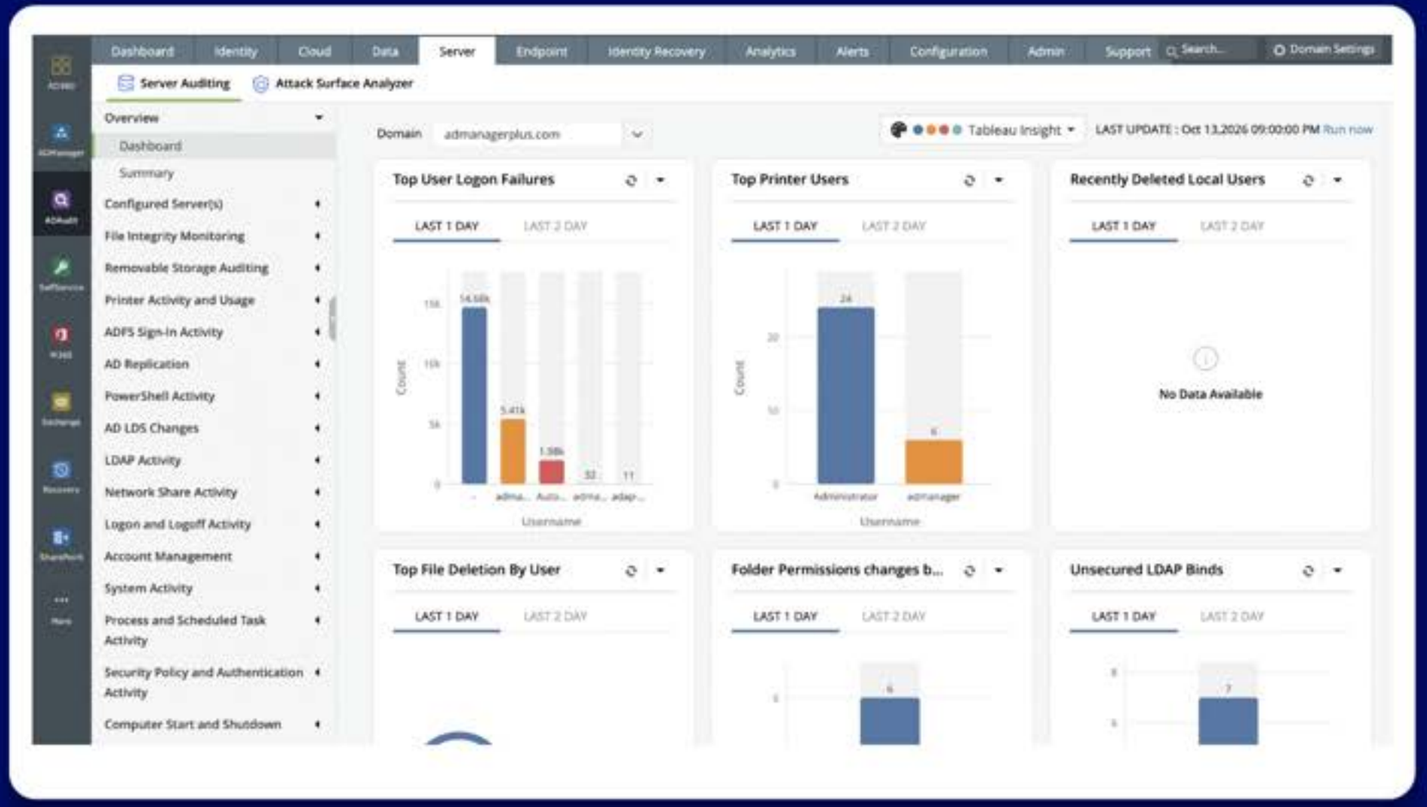
Windows, NetApp, EMC, Synology, Hitachi, Huawei, QNAP, Amazon FSx, Azure Files

Integrity and removable storage

File integrity monitoring and USB activity

Identity infrastructure

ADFS sign-ins, LDAP activity and AD replication



ManageEngine

UBA

Five failed logons at 2AM. The usual is two.

Real-time detection across logons, file activity and privileged accounts.

UBA baselining

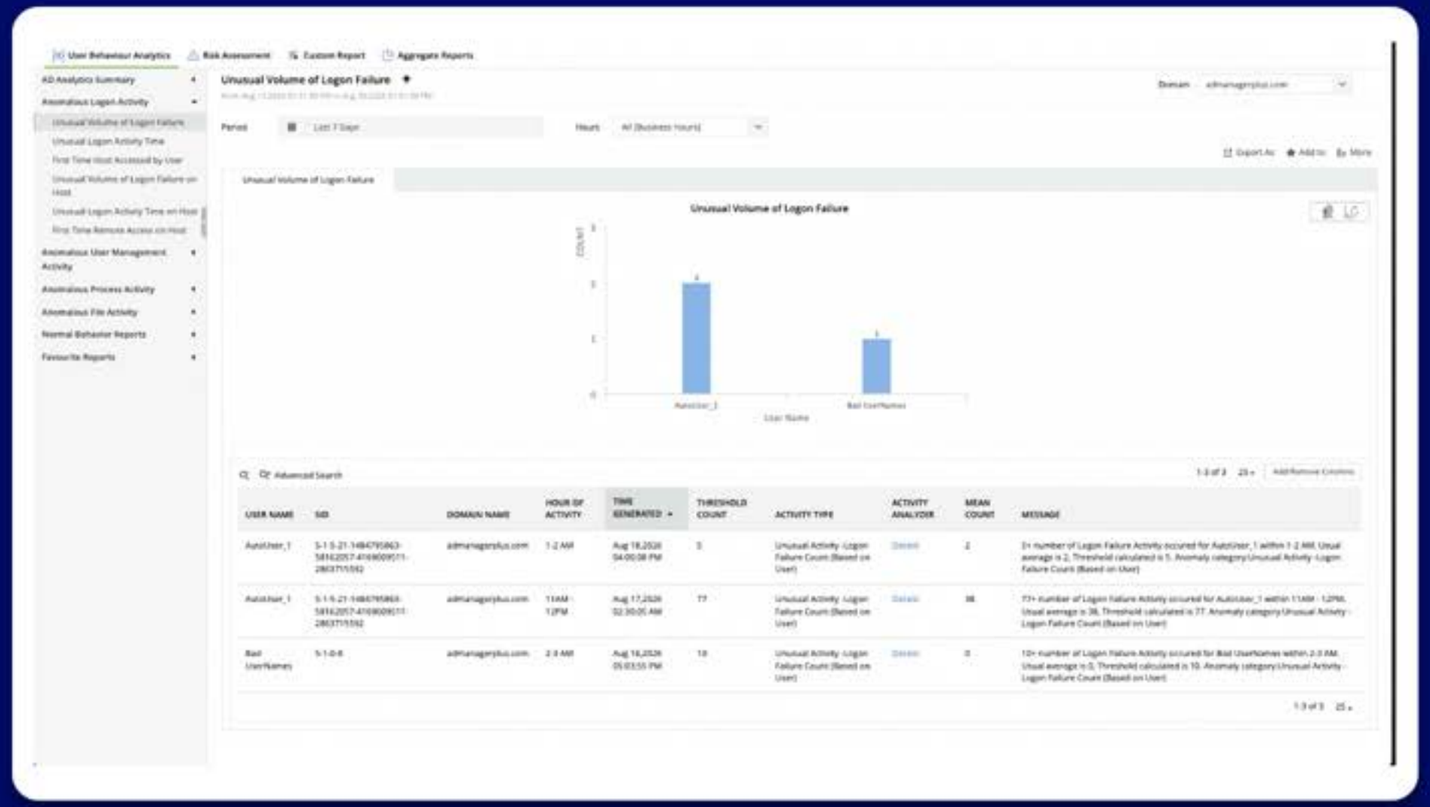
Activity outside a user's normal pattern

Insider threat monitoring

Unusual access volumes, off-hours activity

Alert plus ticket

Notifies the team and opens an ITSM ticket



ManageEngine

Attack surface analyzer

Find the weakness, catch the attack, respond

From a misconfigured server to a live attack, find the cause and act on it.

Misconfiguration scans

Servers checked against CIS benchmarks, grouped by exposure

Attack detection

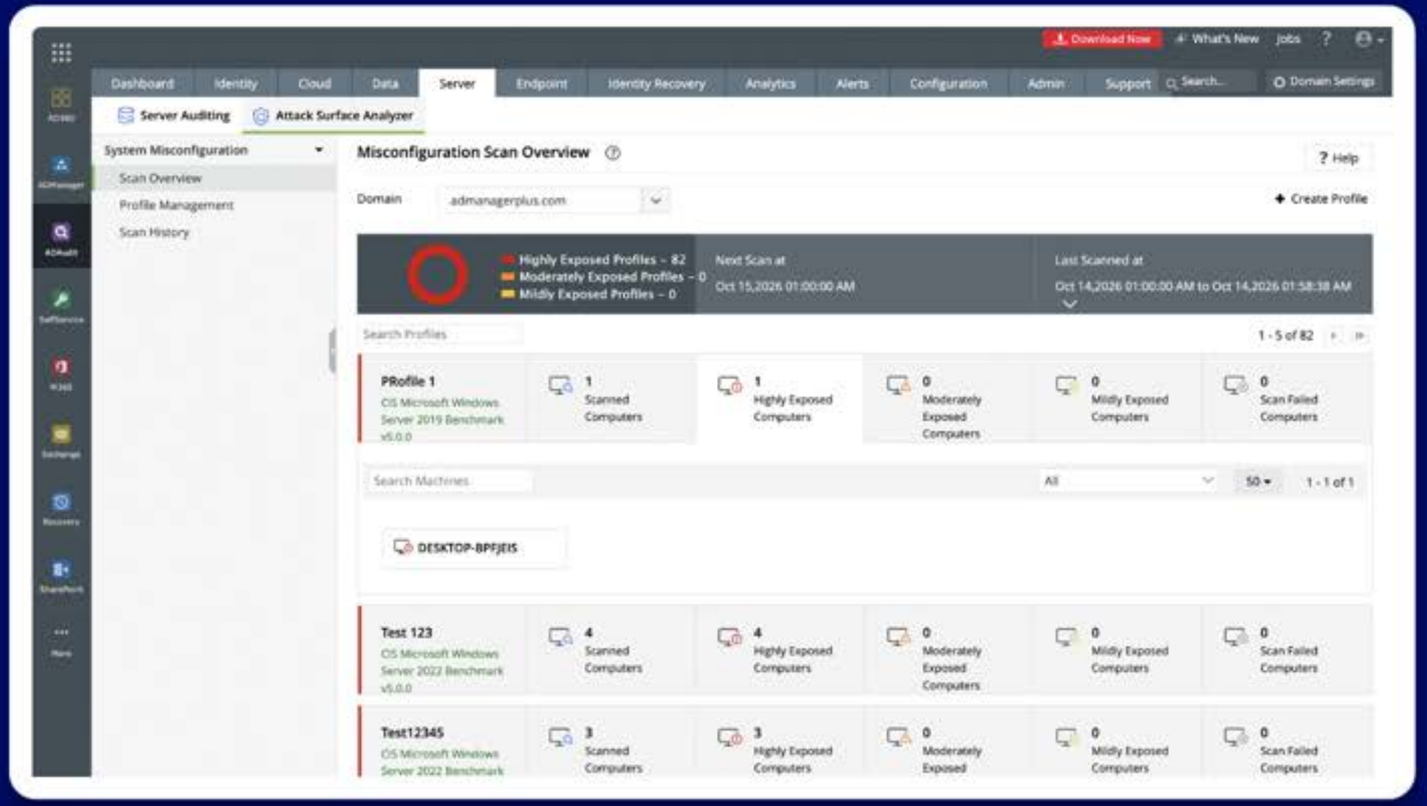
25+ Active Directory attacks and risky Azure configurations

Account lockout analysis

Pinpoints the source of repeated lockouts

Automated response

Run scripts on alerts, such as disabling an account



ManageEngine

MCP gateway activity

A receipt for every agent action

A real-time log of every MCP call through the gateway.

Every call on record

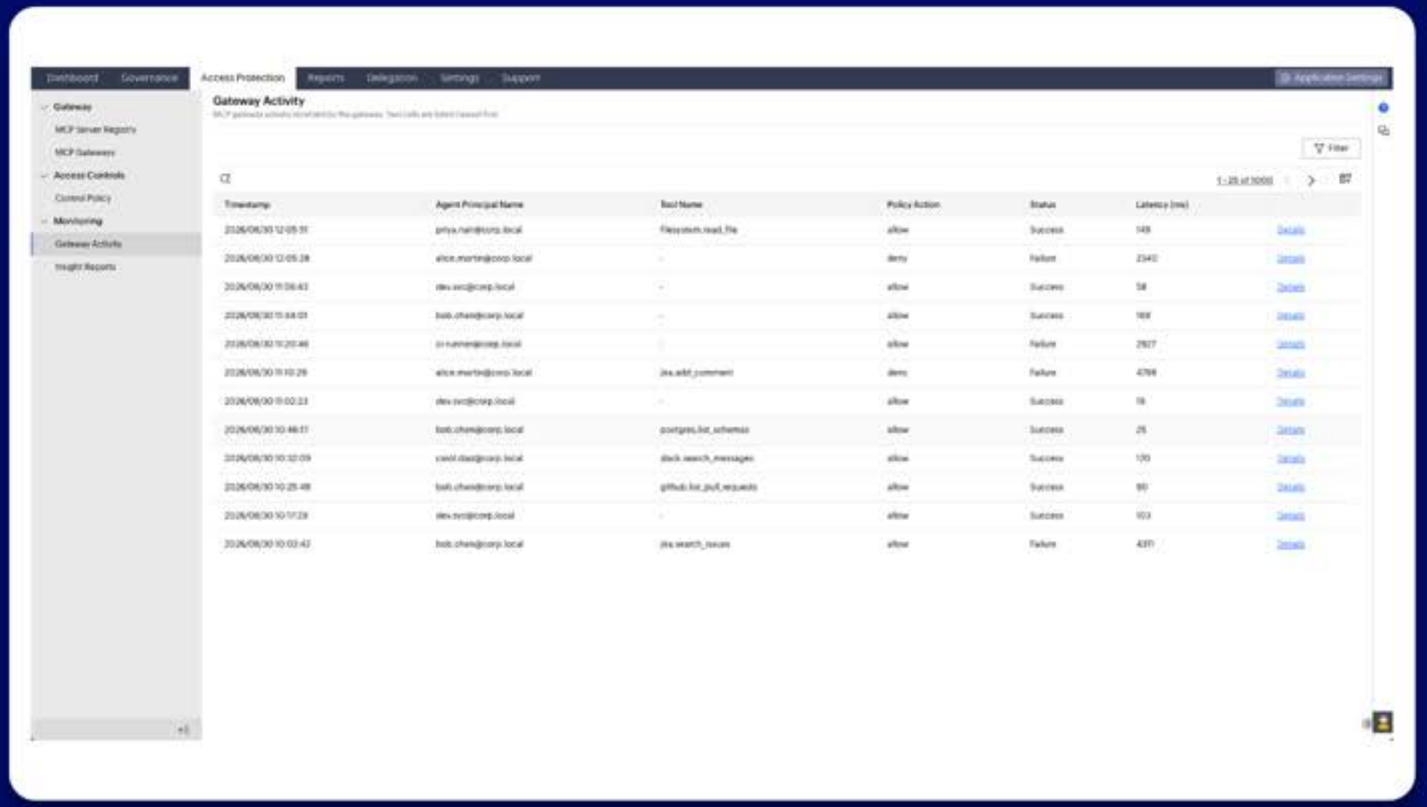
Agent, identity, tool, policy action, status

Drill into any request

Exact arguments and response

Insight reports

Tool usage, latency, errors, policy audits



ManageEngine

Microsoft 365 health monitoring

Microsoft 365, Exchange and SharePoint, covered

Monitoring, auditing and content search for the collaboration stack.

Service health monitoring

Features and endpoints of every Microsoft 365 service

Auditing and alerts

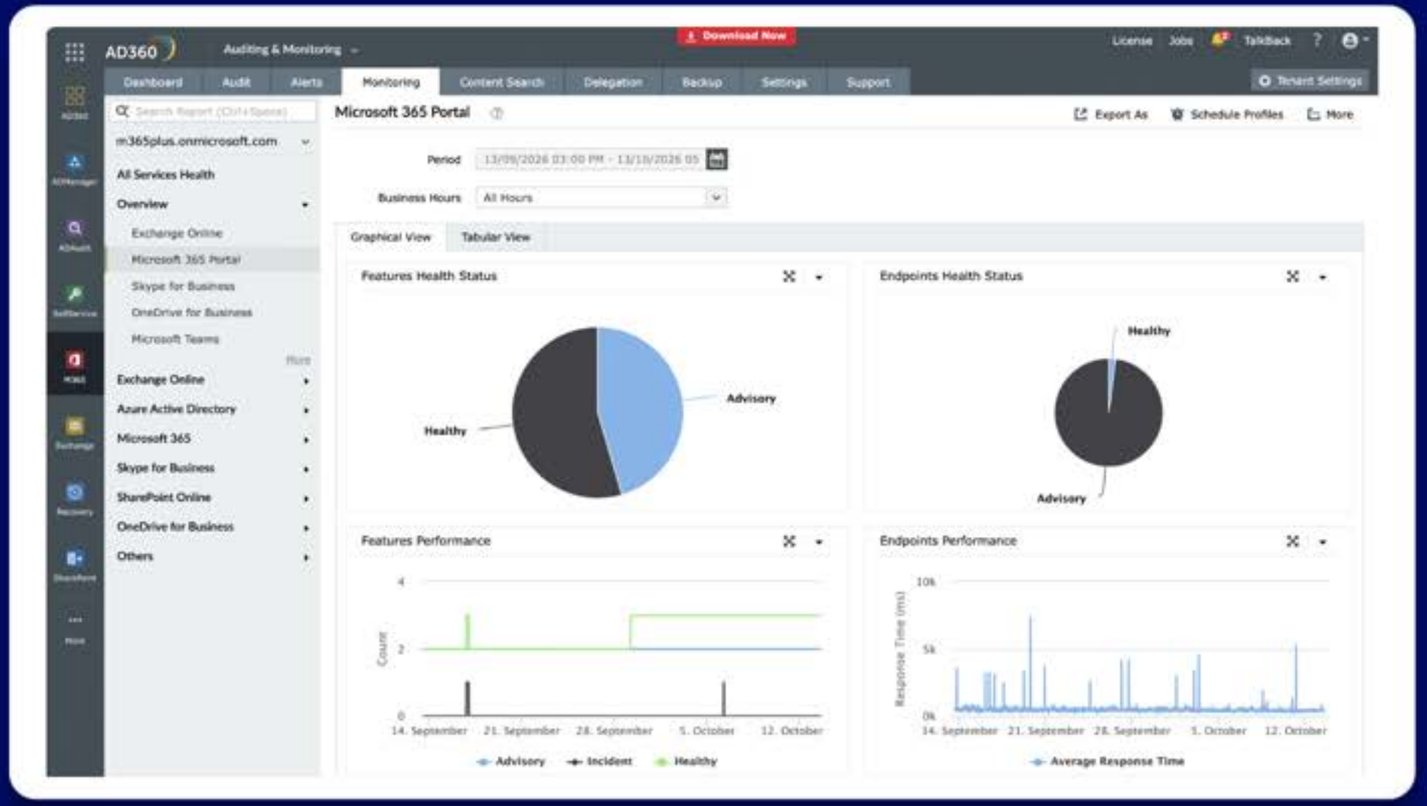
Custom audit profiles with instant alerts

Content search

Find emails with PII, insider information or malicious content

Exchange and SharePoint

Reporting and auditing, across multiple tenants



ManageEngine

Reports

1,000+ reports, scheduled and delivered

The answer to most audit questions already exists as a report.

Every category

Users, passwords, groups, computers, Exchange, GPOs, NTFS and more

On a schedule

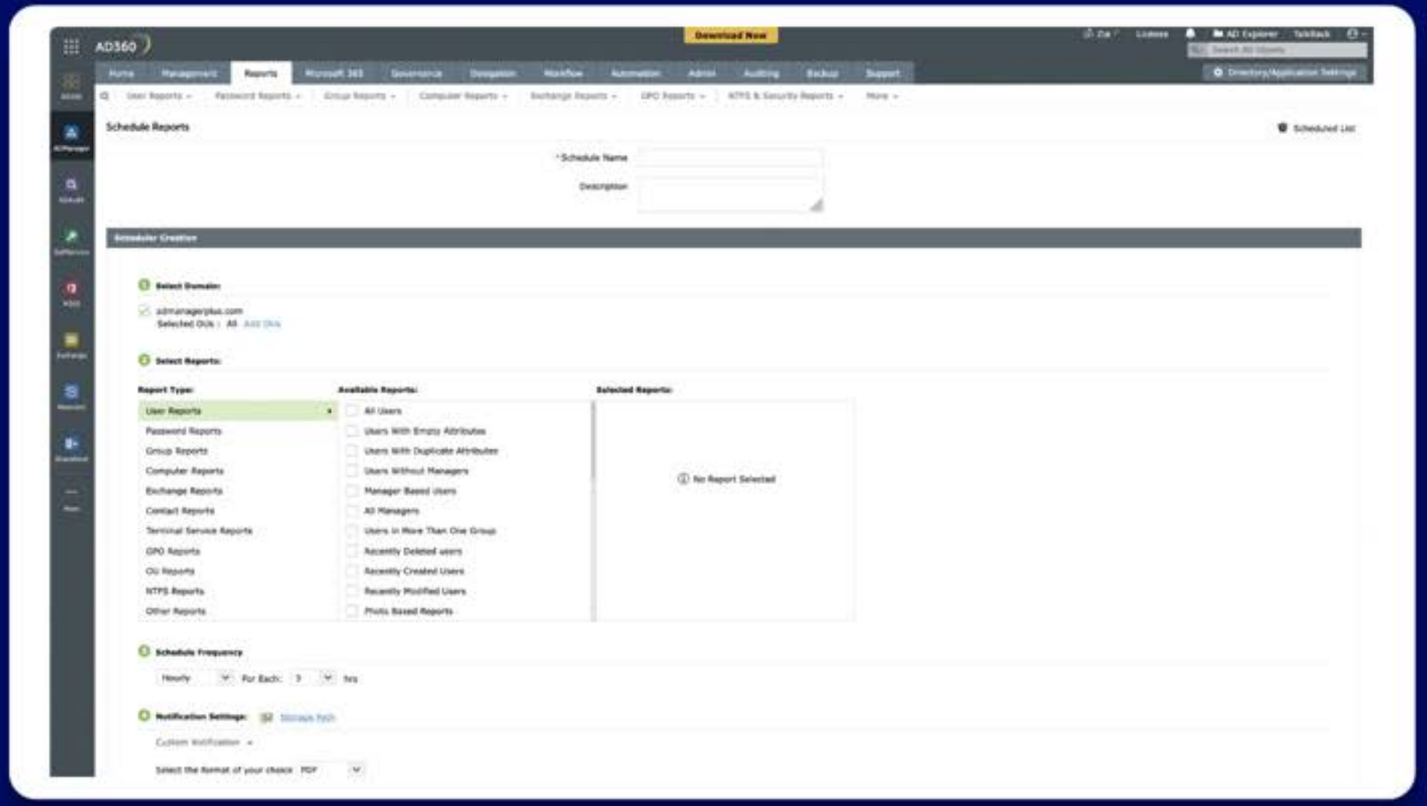
At the frequency you set, for the domains and OUs you pick

Delivered your way

By email or to a storage path, in the format you choose

AI agents too

Per-platform agent reports in SecureAI, next slide



ManageEngine

AI agent reports

Reporting for every agent platform

Pre-built reports per platform, plus insight reports from the gateway.

Per-platform packs

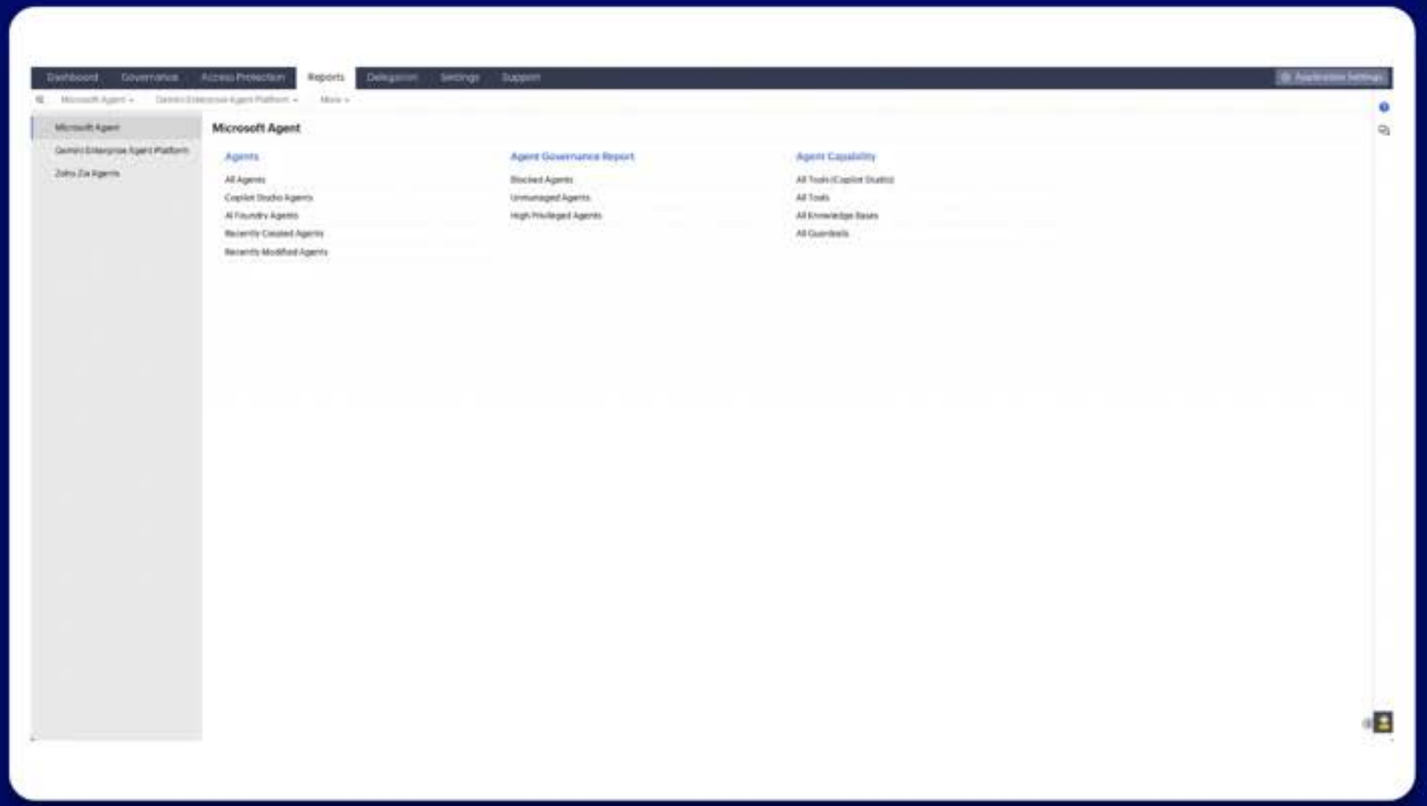
Microsoft, Gemini Enterprise Agent Platform, Zia Agents

Unmanaged and high-privilege cuts

Plus permissions and capabilities

Blocked agents

Microsoft agents blocked on the platform



ManageEngine

05

Recover

Undo the change, restore the object, rebuild the domain, without restoring everything.

For AI agents: Recovery applies to identity data in your directories and cloud apps; agent configuration lives on the agent platforms.

Backup and restore

Restore what broke, not the whole domain

Granular recovery, backed by immutable storage for ransomware defense.

Back up

AD · Entra ID · Microsoft 365 · Exchange · Google Workspace · Zoho WorkDrive

Full and incremental backups

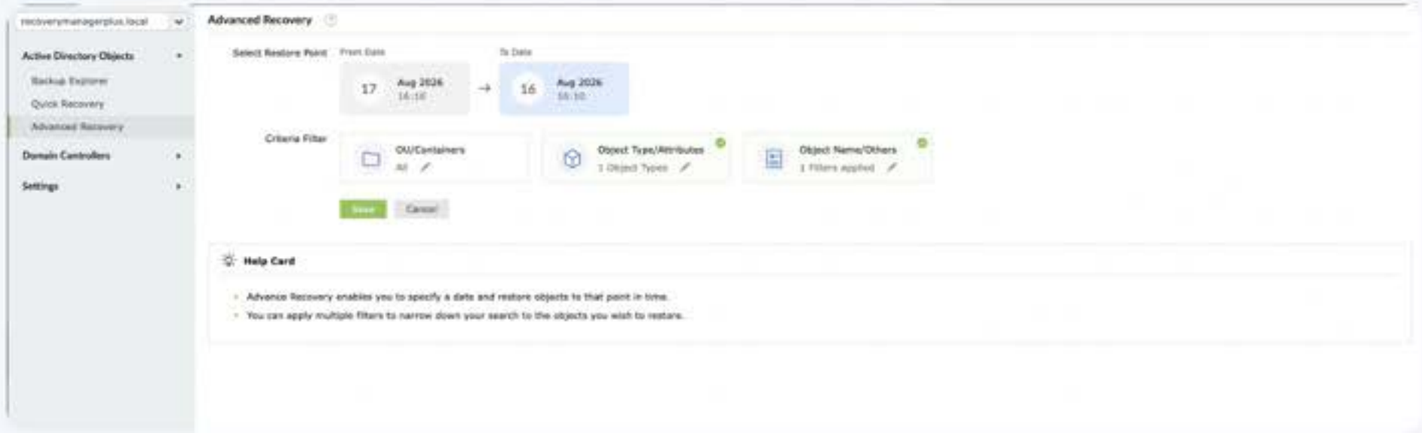
Immutable, WORM-locked storage in Azure Blob, S3 or Wasabi

Restore

Attribute-level rollback: undo one value

Object-level restore with memberships intact

Point-in-time and full domain controller recovery



ManageEngine

Integration

Extends the stack you already run

HR systems, ITSM, SIEM and AI platforms, connected.

Your service desk stays the front door

ServiceDesk Plus or ServiceNow tickets trigger provisioning

Your SIEM stays the system of record

Identity events forward to Log360 or whatever you run

Your AI platforms stay where they are

Microsoft, Google and Zia agent platforms connect with scoped authorization

Your ManageEngine and Zoho licenses compound

Native integrations with Endpoint Central, Zoho Flow, Zoho Desk and more

Everything else

REST API and webhooks

ManageEngine

Customer case study

$375,000 saved a year across 300,000 identities

A US government agency with 300,000+ users and 250,000+ groups

	Before	With AD360
Time from hire to live access	72 hours	1 hour
Provisioning errors	12%	0.5%
Help desk tickets per month	150	15

Recognition

Recognized by industry analysts

2026

Cyber Defense Magazine, Global Infosec Awards

AD360 named a Market Innovator in identity and access management

2025

KuppingerCole Leadership Compass, Identity Threat Detection and Response

AD360 recognized as a Market Leader

2025

IDC MarketScape: Worldwide Integrated Solutions for Identity Security

ManageEngine recognized as a Major Player

2025

Gartner® Market Guide for Identity Governance and Administration

ManageEngine included as a Representative Vendor

See AD360 in your own environment

IN A LIVE DEMO

01 Provision a new hire from an HR record across AD, Microsoft 365 and apps

02 Discover your AI agents and assign each one an owner

03 Watch the MCP gateway block a risky tool call in real time

Book a demo

Start a free trial

https://www.manageengine.com/active-directory-360/

ManageEngine

Thank you

Questions?

ManageEngine