ManageEngine

Mastering privileged access management 2.0

Human, non-human, everything in between and beyond

ManageEngine

Factors driving the identity landscape

Fragmented identity stack

Disconnected tools creating operational inefficiency

Machine identity explosion

APIs, service accounts, bots, agents, and certificates proliferating

Hybrid security silos

Consistent privileged governance nearly impossible across on-premises, cloud, and hybrid infrastructure

Compliance

Regulatory requirements shaping purchasing decisions

Third-party risk

Business continuity concerns mounting due to vendor access concerns

ManageEngine

When PAM was about control, not context

Traditional PAM

Privileged account governance

Remote password reset

Remote session management

Privilege elevation and delegation management

Certificate life cycle management

Auditing and reporting

ManageEngine

True PAM maturity goes beyond human identity governance

Human

- Employee user accounts
- Privileged admin accounts
- Developer accounts
- Third-party vendor user accounts
- Privileged user accounts
- Break-glass / emergency access accounts
- On-call / incident response accounts
- Shared admin accounts

Non-Human

- Applications
- Microservices APIs & API keys
- Service accounts
- Kubernetes service accounts
- Serverless functions
- Batch jobs / schedulers
- SSH keys
- TLS / SSL certificates and more.

ManageEngine

What constitutes modern privileged access management?

Modern PAM

 Least-privilege access	 Zero Trust privilege	 Endpoint privilege management
 Non-human identity management	 Cloud access security	 Vendor access management
 Privileged task automation	 Privilege threat detection and response	 GRC

ManageEngine

Let's enter the simulation

Case 1

Human

ManageEngine

A case of access overdosing

A global aerospace manufacturer supports production and maintenance systems using a mix of full-time engineers and contract specialists. These users routinely require privileged access to endpoints, application servers, and deployment tools for testing, patching, and release activities.

To avoid delays, privileged access was historically granted as standing administrative rights, with shared credentials and broad permissions across systems.

The problem

- No centralized onboarding or discovery of privileged users and assets
- Privileged credentials shared informally, increasing exposure
- Static roles with overprovisioned access
- No time-bound or task-bound access controls
- Full admin shells available even for routine operations

ManageEngine

Enforcing least-privilege and Zero Trust access with PAM360

To eliminate standing administrative access while maintaining operational efficiency, the aerospace manufacturer restructured its privileged access model across users, endpoints, and applications.

- Centralized onboarding and discovery of all privileged users and assets
- Vaulted credentials and brokered access to them only when necessary, to whom it was necessary
- Role- and policy-based access aligned to task and responsibility
- Just-in-time privilege with monitored sessions
- Ephemeral roles and time-bound elevated access
- Command-level and application-level restrictions → Removal of standing local administrator rights on endpoints

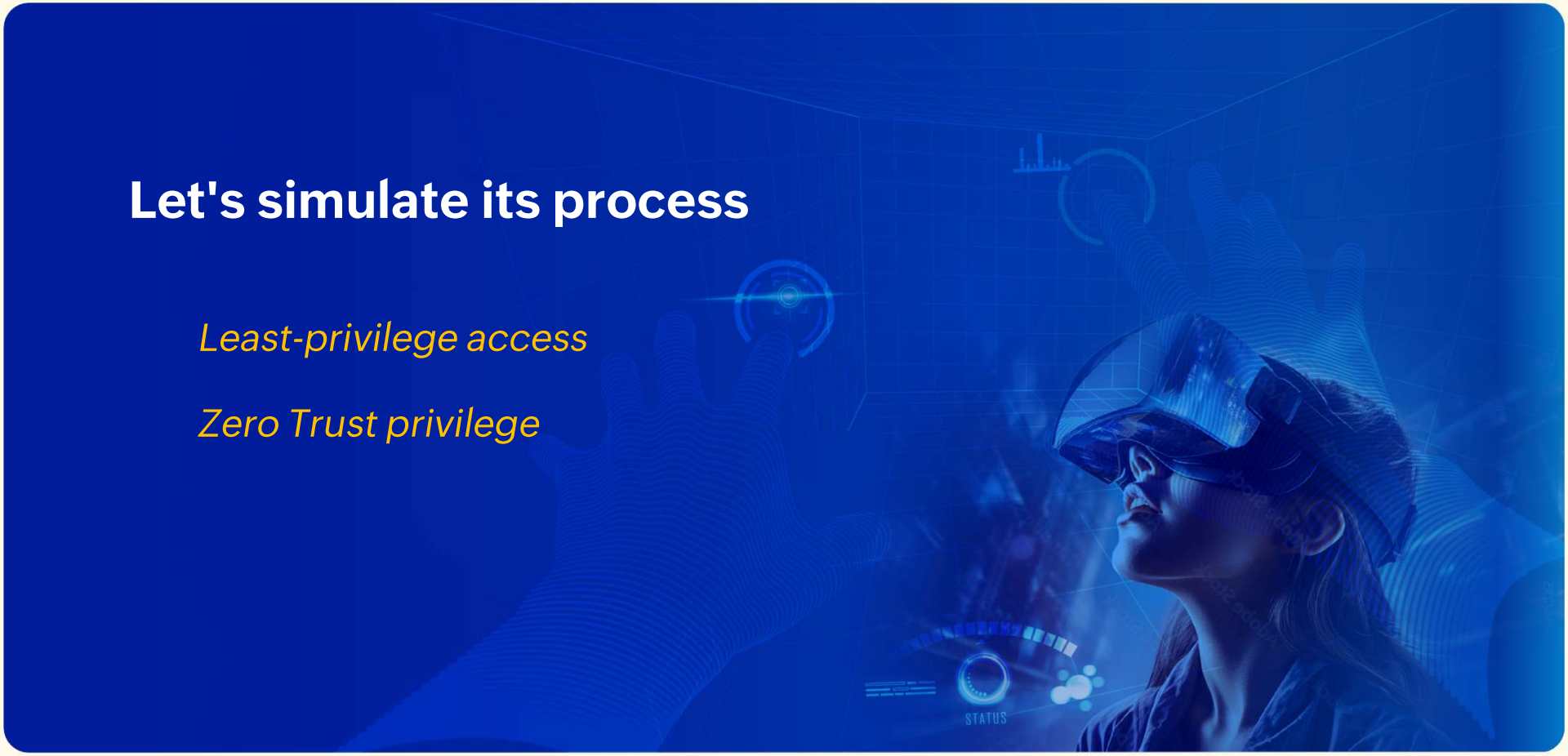
> *We stopped assuming access was safe just because the user was legitimate.*
>
> - Vice president of IT

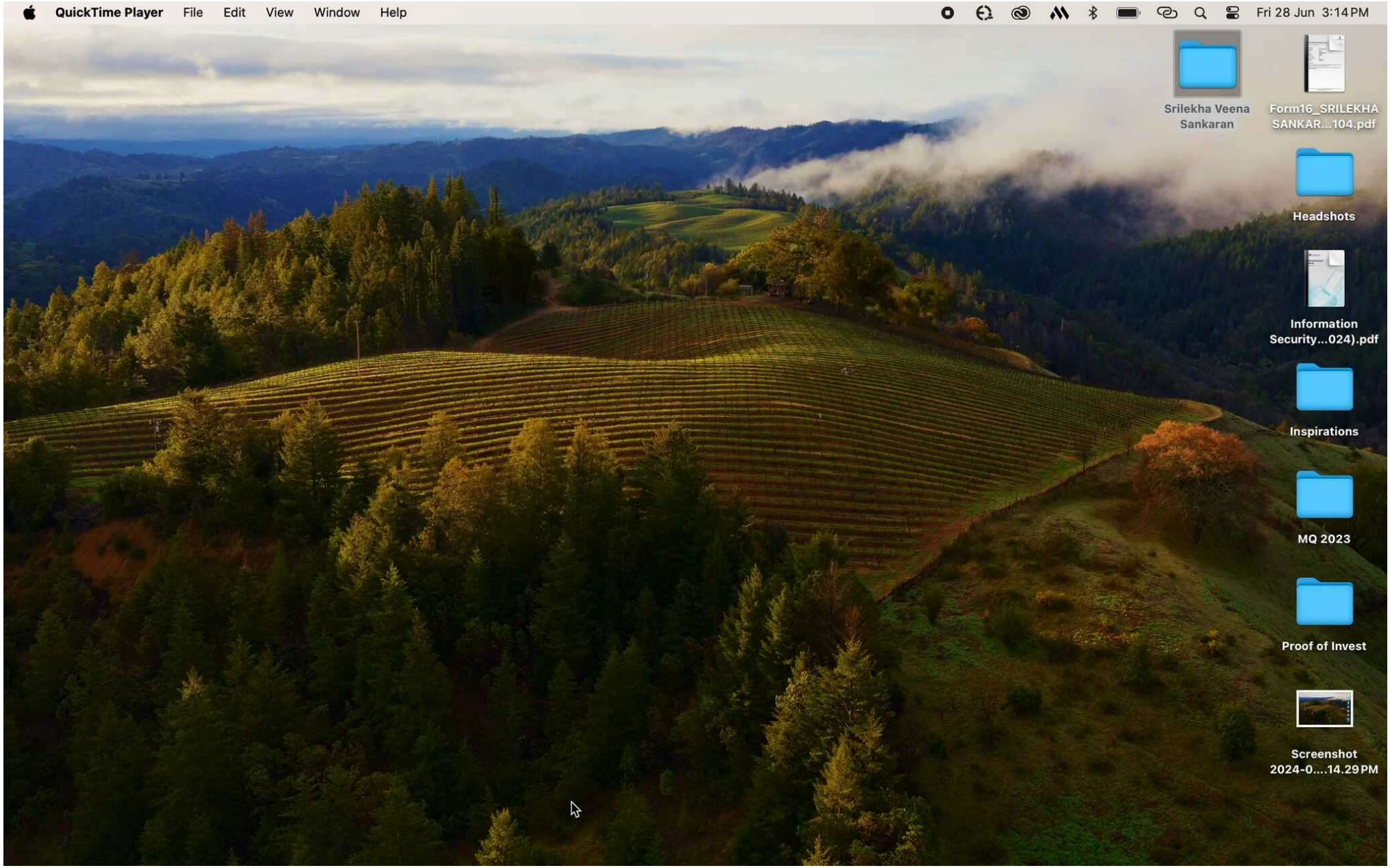
ManageEngine

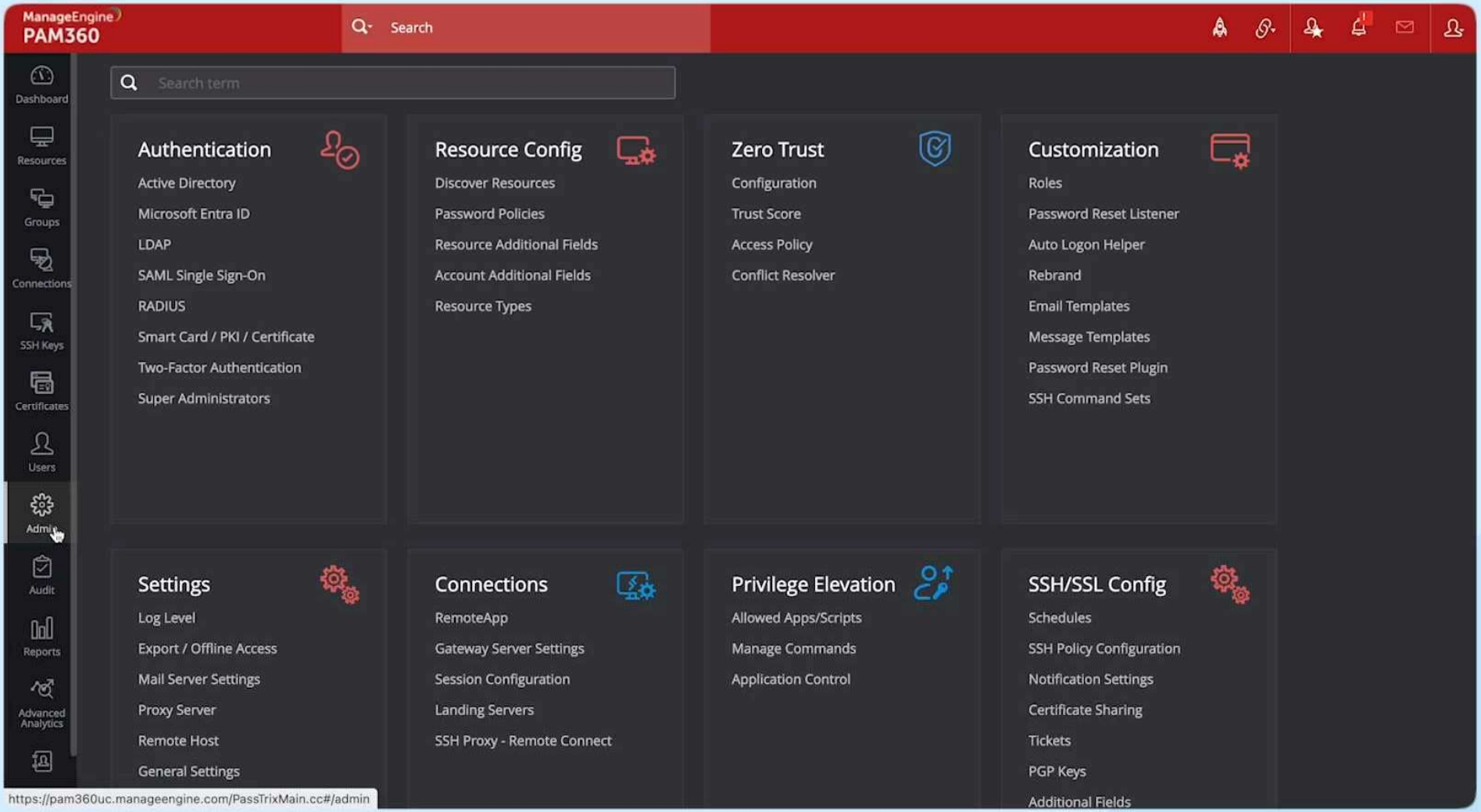
Let's simulate its process

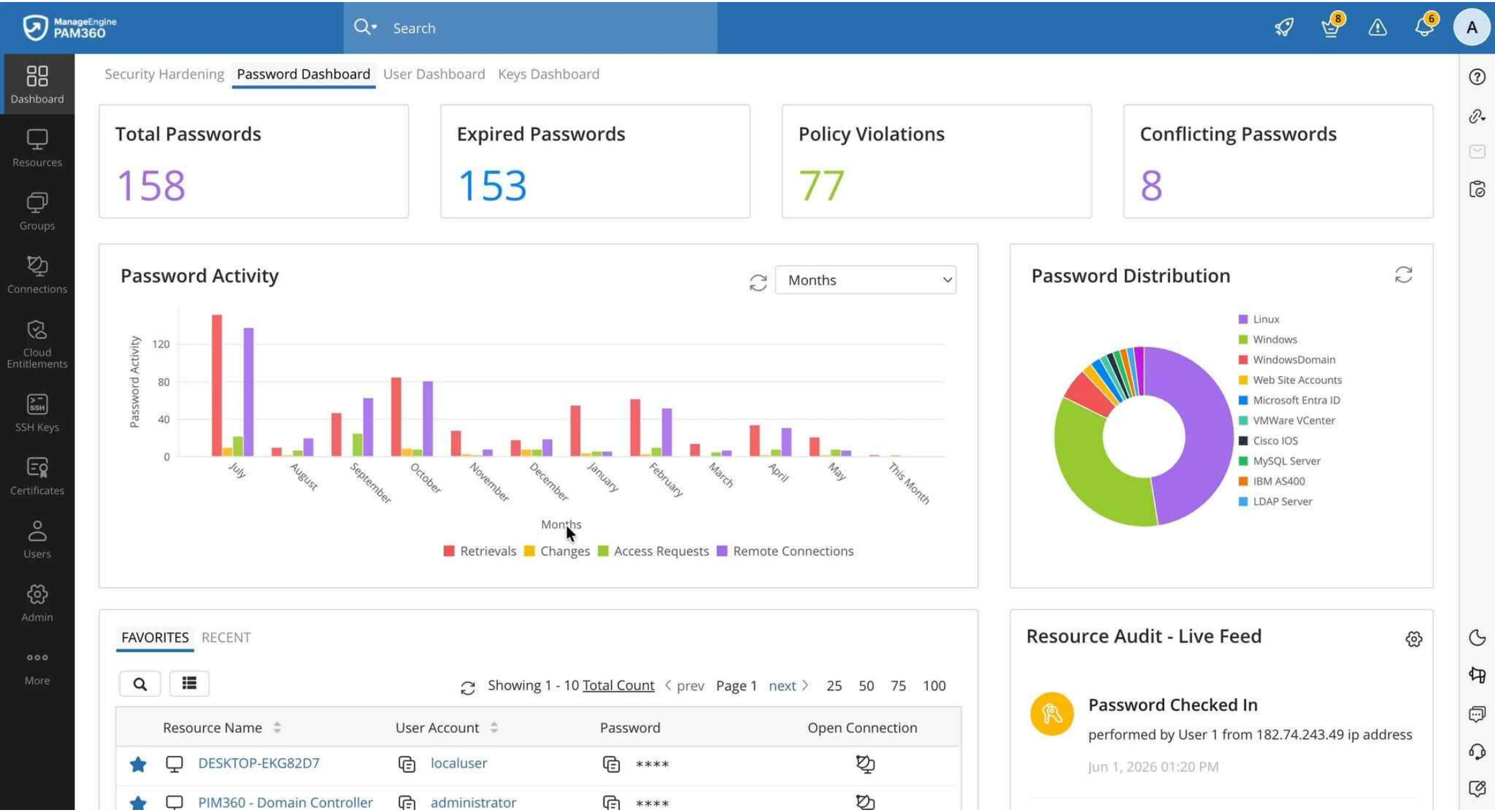
Least-privilege access

Zero Trust privilege




QuickTime Player File Edit View Window Help
Fri 28 Jun 3:14 PM
Srilekha Veena Sankaran
Form16_SRILEKHA SANKAR...104.pdf
Headshots
Information Security...024).pdf
Inspirations
MQ 2023
Proof of Invest
Screenshot 2024-0....14.29 PM


ManageEngine
PAM360
Search
Search term
Dashboard
Resources
Groups
Connections
SSH Keys
Certificates
Users
Admin
Audit
Reports
Advanced Analytics
Authentication
Active Directory
Microsoft Entra ID
LDAP
SAML Single Sign-On
RADIUS
Smart Card / PKI / Certificate
Two-Factor Authentication
Super Administrators
Resource Config
Discover Resources
Password Policies
Resource Additional Fields
Account Additional Fields
Resource Types
Zero Trust
Configuration
Trust Score
Access Policy
Conflict Resolver
Customization
Roles
Password Reset Listener
Auto Logon Helper
Rebrand
Email Templates
Message Templates
Password Reset Plugin
SSH Command Sets
Settings
Log Level
Export / Offline Access
Mail Server Settings
Proxy Server
Remote Host
General Settings
Connections
RemoteApp
Gateway Server Settings
Session Configuration
Landing Servers
SSH Proxy - Remote Connect
Privilege Elevation
Allowed Apps/Scripts
Manage Commands
Application Control
SSH/SSL Config
Schedules
SSH Policy Configuration
Notification Settings
Certificate Sharing
Tickets
PGP Keys
Additional Fields
https://pam360uc.manageengine.com/PassTrixMain.cc#/admin


ManageEngine PAM360
Search
Dashboard
Resources
Groups
Connections
Cloud Entitlements
SSH Keys
Certificates
Users
Admin
More
Security Hardening
Password Dashboard
User Dashboard
Keys Dashboard
Total Passwords
158
Expired Passwords
153
Policy Violations
77
Conflicting Passwords
8
Password Activity
Months
Password Activity
120
80
40
0
July
August
September
October
November
December
January
February
March
April
May
This Month
Months
Retrievals
Changes
Access Requests
Remote Connections
Password Distribution
Linux
Windows
WindowsDomain
Web Site Accounts
Microsoft Entra ID
VMWare VCenter
Cisco IOS
MySQL Server
IBM AS400
LDAP Server
FAVORITES
RECENT
Showing 1 - 10 Total Count
prev
Page 1
next
25
50
75
100
Resource Name
User Account
Password
Open Connection
DESKTOP-EKG82D7
localuser
****
PIM360 - Domain Controller
administrator
****
Resource Audit - Live Feed
Password Checked In
performed by User 1 from 182.74.243.49 ip address
Jun 1, 2026 01:20 PM

ManageEngine

Case 2

The vendor access puzzle

A case of uncontrolled third-party privileged access

The main strategic partner of the financial sector in Guatemala and the largest ATM network in Central America is responsible for overseeing a vast ATM infrastructure and managing the secure movement of cash across the country.

To support operations, the organization relies heavily on third-party vendors and external service providers for ATM maintenance, software updates, and incident response.

To reduce risk and maintain operational continuity, the organization sought to streamline third-party privileged access routines and establish centralized, controlled access to sensitive endpoints and critical systems, without disrupting vendor-led operations.

It also needed to monitor, record, and audit all vendor operations.

ManageEngine

Onboarding

- Practice complete governance over all onboarded privileged users
- Take an alternate, secure approach to VPN-based vendor remote access
- Prevent credential exposure and network infiltration
- Limit the visibility to simply the necessary endpoints without exposing other sensitive entities

Least-privilege access

- Least-privilege access across your enterprise
- Temporary, requisite access privileges to critical systems
- Access policies at a granular level
- Prevent lateral entry into the network
- Audits all privileged activity in the network

Offboarding

- Streamlined employee offboarding process
- Eliminate post contract credential exposure
- Deem standing privileges null and void
- Eliminate insider threats from ex-employees

ManageEngine

Let's simulate

Vendor access management

Privileged task automation

Two-Factor Authentication is not enabled yet! Turn it on to add an additional layer of security to PAM360.

ManageEngine PAM360

Search

Dashboard
Resources
Groups
Connections
New
Cloud Entitlements
SSH Keys
Certificates
Users
Admin
Audit
Reports

Security Hardening | Password Dashboard | User Dashboard | Keys Dashboard

Total Passwords
155

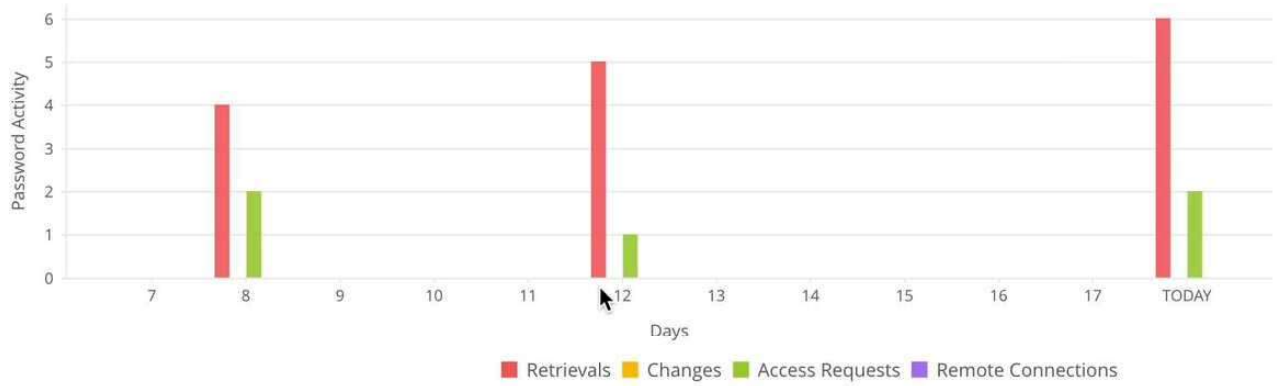
Expired Passwords
8

Policy Violations
38

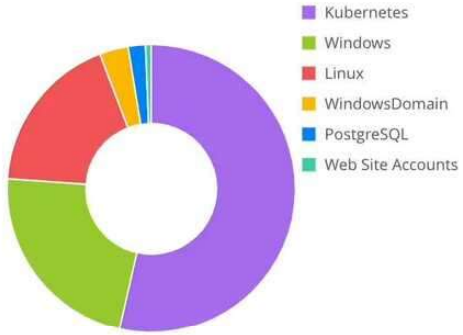
Conflicting Passwords
22

Password Activity

Days



Password Distribution



FAVORITES | RECENT

Showing 1 - 10 Total Count < prev Page 1 next > 25 50 75 100

Resource Name	User Account	Password	Open Connection
PAM-DC-SERVER2	pamadmin	****	
		****	

Resource Audit - Live Feed

Privileged Process Removed
performed by admin M from 106.51.175.60 ip address
Sep 18, 2025 10:19 AM

https://pam360demo.eastus.cloudapp.azure.com/PassTrixMain.cc#/PassTrixQuickView

Two-Factor Authentication is not enabled yet! Turn it on to add an additional layer of security to PAM360.

ManageEngine PAM360

Search

Dashboard
Resources
Groups
Connections
New
Cloud Entitlements
SSH Keys
Certificates
Users
Admin
Audit
Reports

Security Hardening | Password Dashboard | User Dashboard | Keys Dashboard

Total Passwords
155

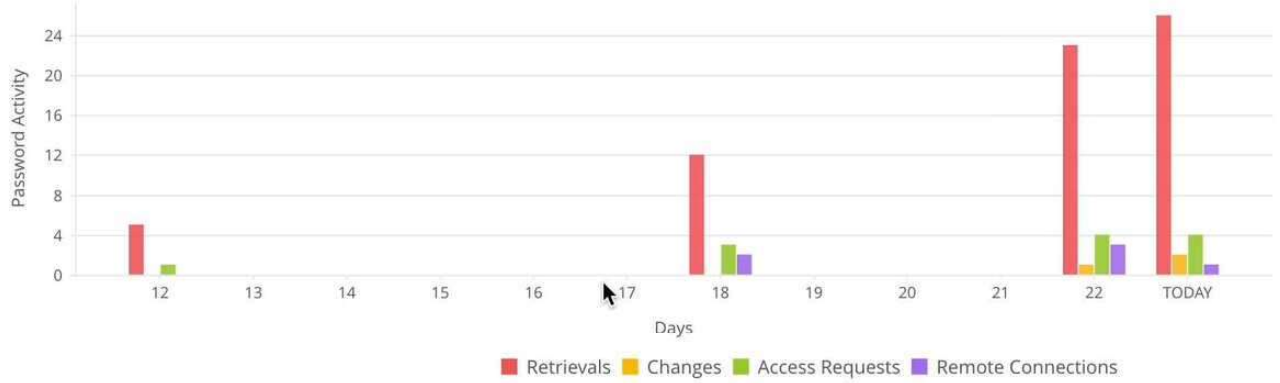
Expired Passwords
24

Policy Violations
36

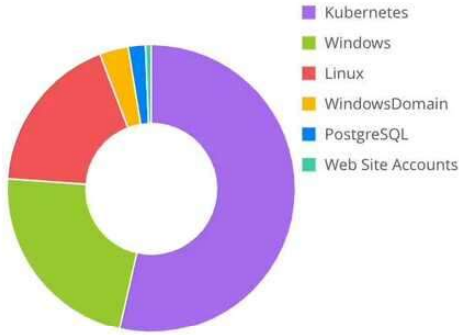
Conflicting Passwords
26

Password Activity

Days



Password Distribution



FAVORITES | RECENT

Showing 1 - 10 Total Count < prev Page 1 next > 25 50 75 100

Resource Name	User Account	Password	Open Connection
PAM-WINSERVER-2	Testuser2	****	
PAM-DC-SERVER2	pamadmin	****	

Resource Audit - Live Feed

Read Only Share Given

PTAResGroup1 (Group Name) operated by api admin from localhost

Sep 23, 2025 09:00 AM

ManageEngine

Case 3

Extended, hybrid environments

Hybrid privileged account management case

As the organization modernized its IT landscape, it adopted a hybrid operating model, running critical workloads across on-premises data centers and multiple public cloud platforms.

While privileged access controls were well established in the on-premises environment, cloud identities, roles, and permissions began to grow independently of existing PAM processes.

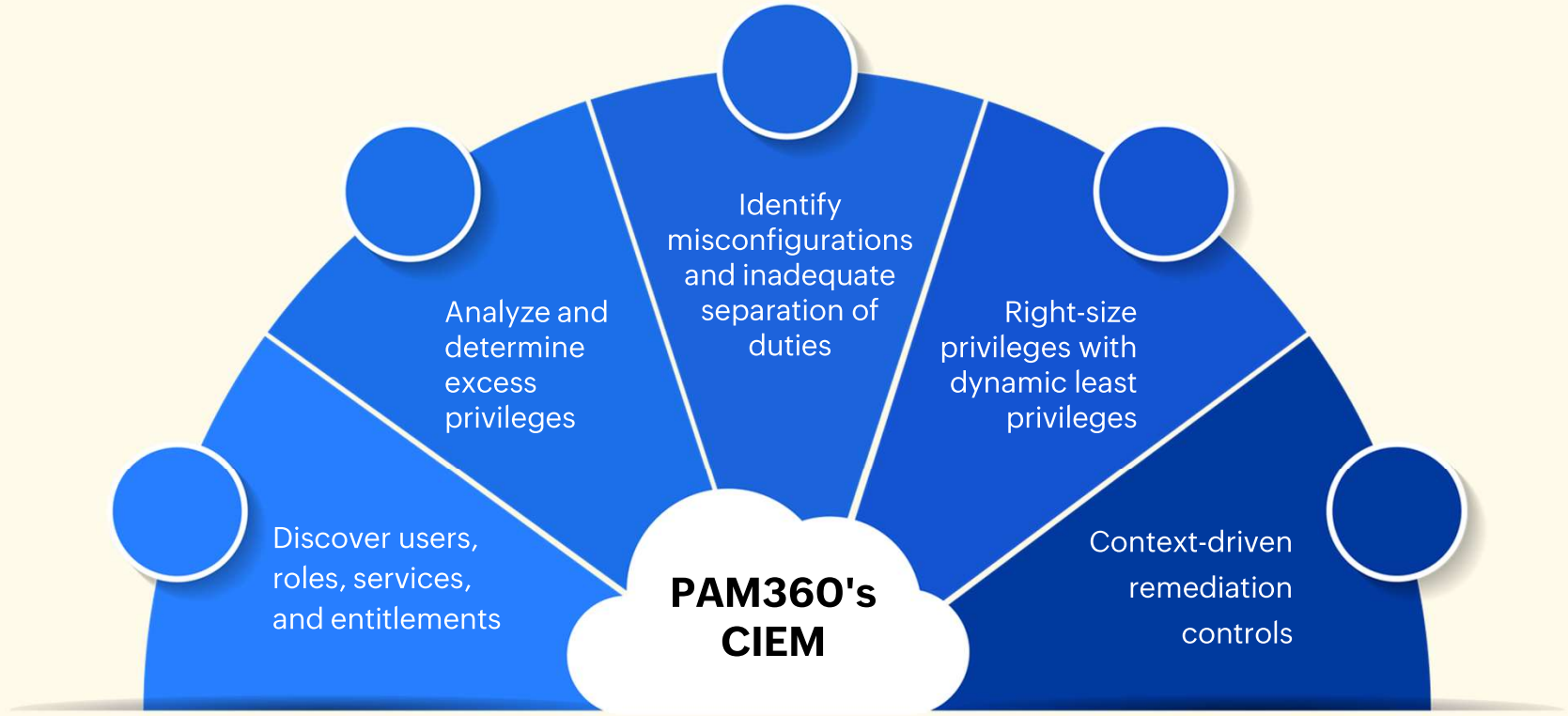
The problem

- Fragmented visibility into users, roles, services, and associated risks
- Cloud identities provisioned outside PAM, creating unmanaged privilege paths
- Excessive and persistent permissions with no continuous review
- Misaligned least-privilege enforcement between on-premises and cloud workloads
- Manual privilege management leading to configuration drift and errors
- Insufficient audit context for cloud privileged actions

ManageEngine

Extending PAM to multi-cloud environments

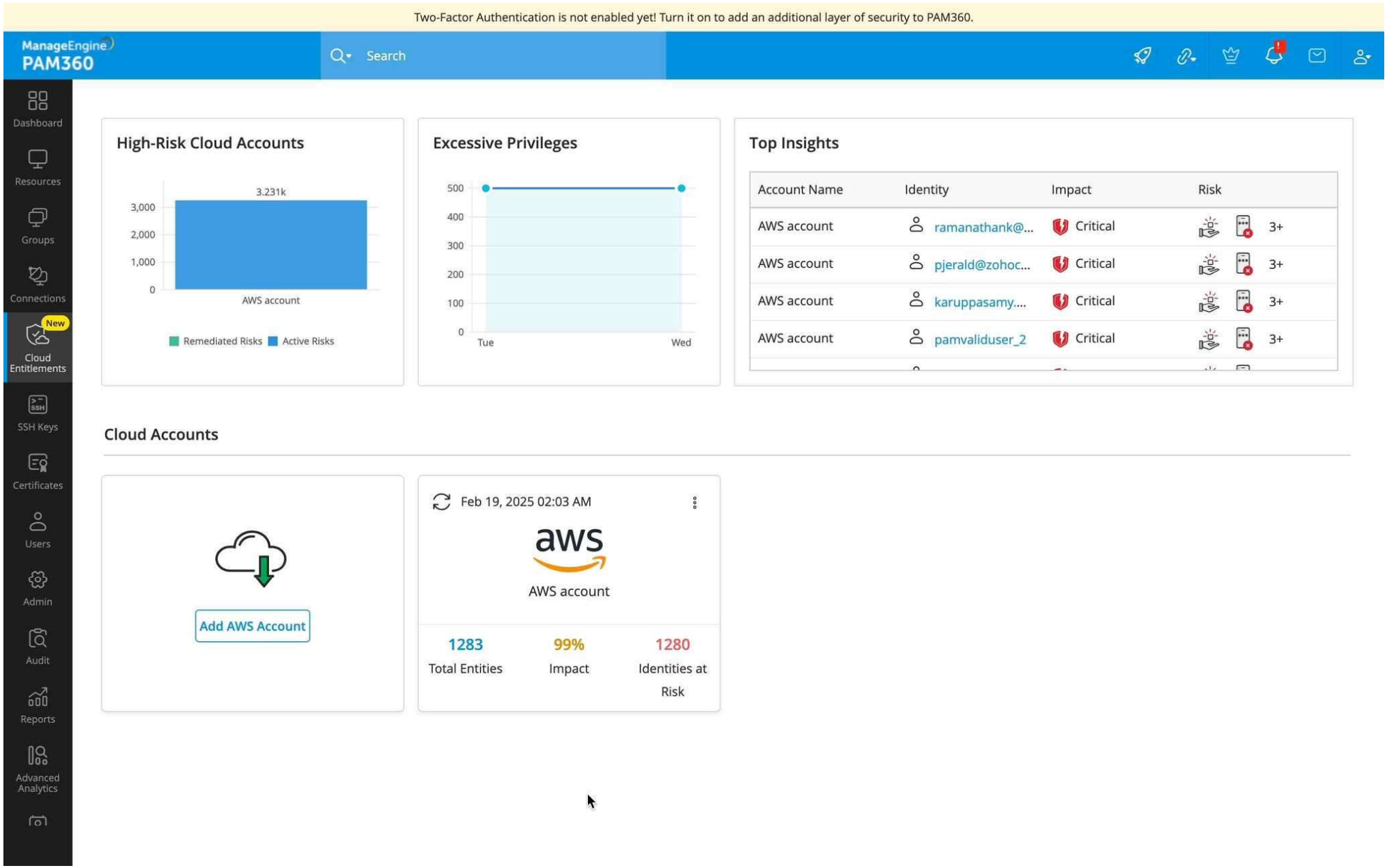
with PAM360's fully automated and native CIEM



ManageEngine

Let's simulate

Cloud access security


Two-Factor Authentication is not enabled yet! Turn it on to add an additional layer of security to PAM360.
ManageEngine
PAM360
Search
Dashboard
Resources
Groups
Connections
New
Cloud Entitlements
SSH Keys
Certificates
Users
Admin
Audit
Reports
Advanced Analytics
High-Risk Cloud Accounts
3.231k
3,000
2,000
1,000
0
AWS account
Remediated Risks
Active Risks
Excessive Privileges
500
400
300
200
100
0
Tue
Wed
Top Insights
Account Name
Identity
Impact
Risk
AWS account
ramanathank@...
Critical
3+
AWS account
pjerald@zohoc...
Critical
3+
AWS account
karuppasamy....
Critical
3+
AWS account
pamvaliduser_2
Critical
3+
Cloud Accounts
Add AWS Account
Feb 19, 2025 02:03 AM
aws
AWS account
1283
Total Entities
99%
Impact
1280
Identities at Risk

ManageEngine

Security leads to compliance, not the other way around

Checkbox approach

Security-first approach

> ***Instead of building to pass audits, organizations must build systems that can't help but be compliant because they're inherently secure, automated, and observable***

ManageEngine

ManageEngine's identity fabric

ManageEngine Identity360

ManageEngine AD360

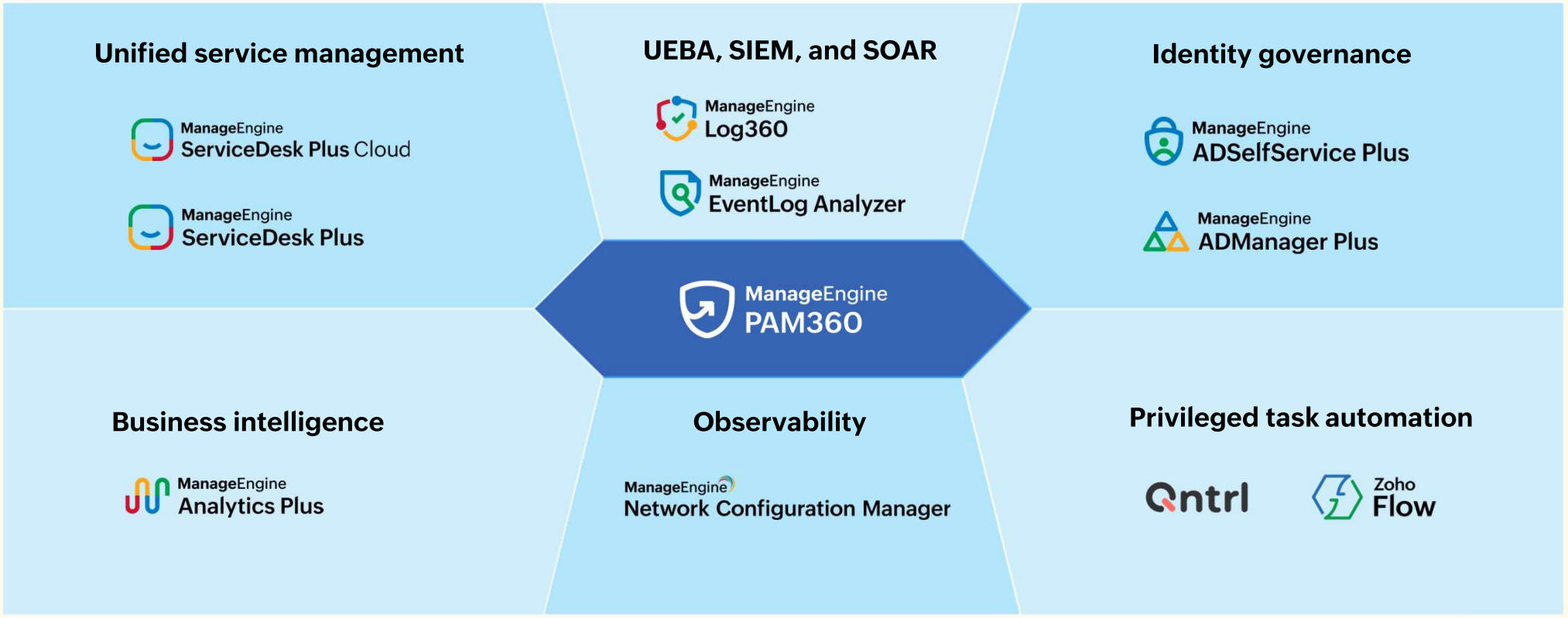
ManageEngine PAM360

- Workforce IAM
- Authentication
- Identity governance and administration
- Identity management
- Identity threat detection and response
- Access management

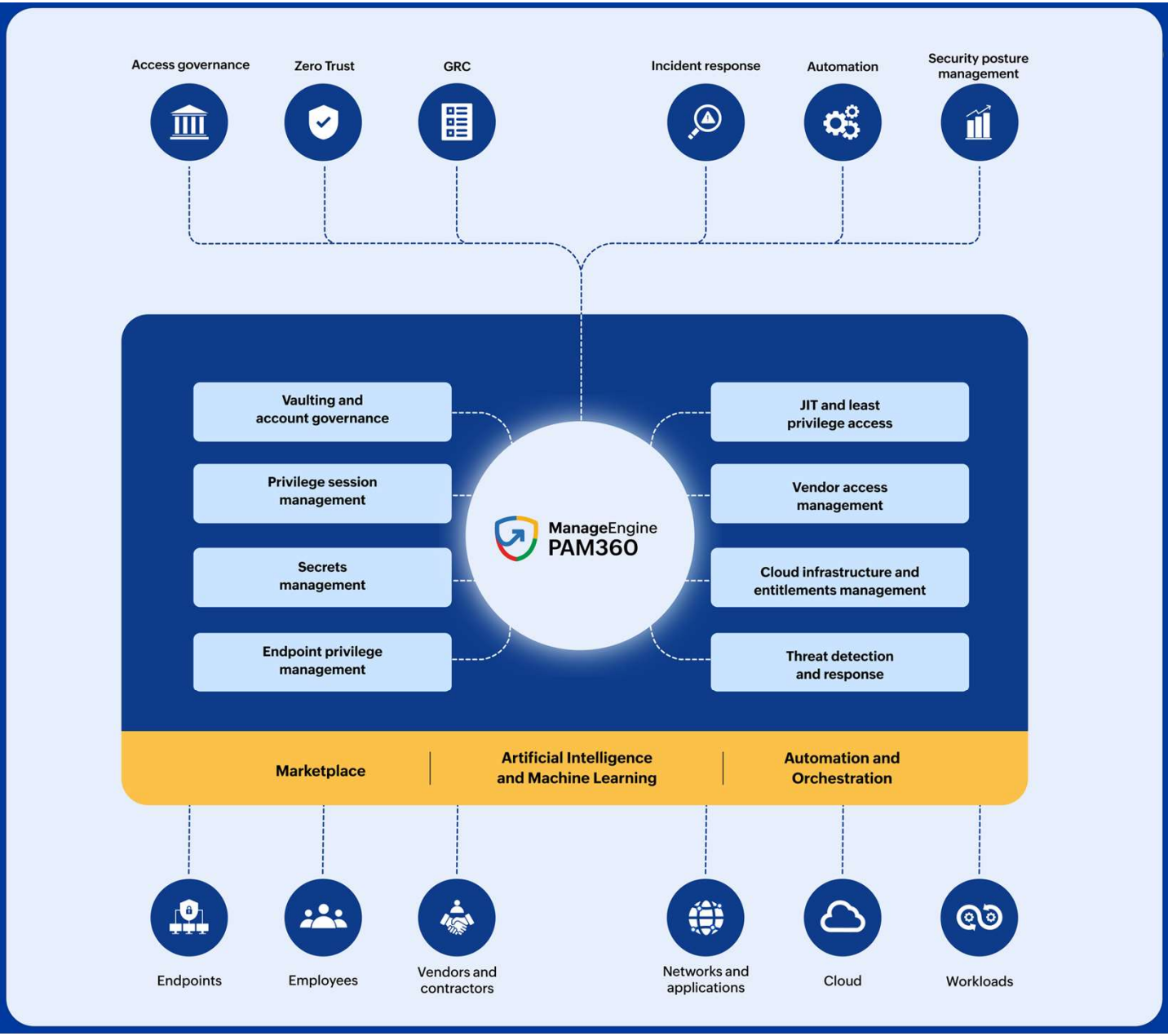
- Cloud
- Applications
- Endpoints
- Identity
- Network
- Third-party

ManageEngine

Complete your IT puzzle with PAM360



The unified PAM platform from ManageEngine



ManageEngine

Thank You.

sruthi.suresh@zohocorp.com