

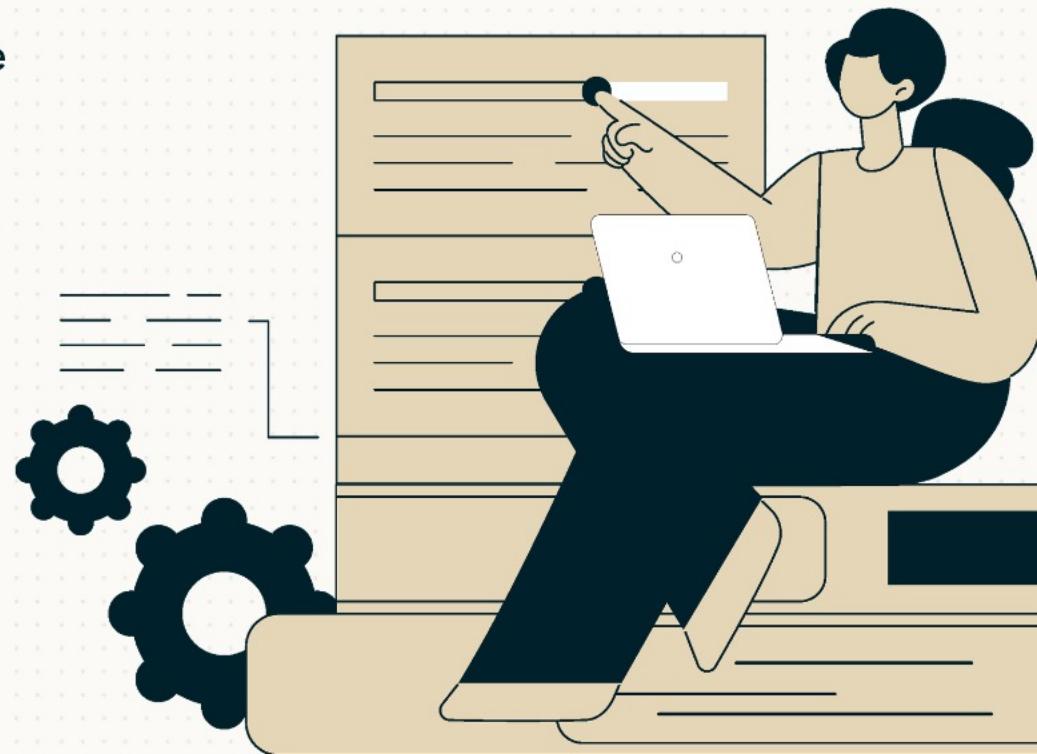
Boost your organization's security and centralize management with Identity360

A cloud-native identity platform for workforce IAM



Outline

- Identity360's vision
- Critical IAM challenges for enterprises
- Identity360 solutions
- Universal Directory
- Integrations
- Life cycle management
- Single sign-on (SSO)
- Multi-factor authentication (MFA)
- Access management
- Delegation
- Reports and identity analytics
- Identity360 architecture
- Identity360 licensing



Identity360's vision

Unify identity silos, streamline
identity management, and secure
resources with centralized access
management

Critical IAM challenges for enterprises



Identity fragmentation

Enterprises often struggle with managing multiple user identities across various platforms, leading to inefficiencies and security risks



Complex identity life cycle management

Managing the entire identity life cycle, from onboarding to offboarding, can be challenging and error-prone for enterprises.



Increased IT costs

The lack of scalability and flexibility in managing access requirements can result in higher infrastructure costs as organizations struggle to adapt to changing business needs

Identity360 solutions



Universal Directory



Life cycle management



Single sign-on (SSO)



Multi-factor authentication (MFA)



Access management



Delegation



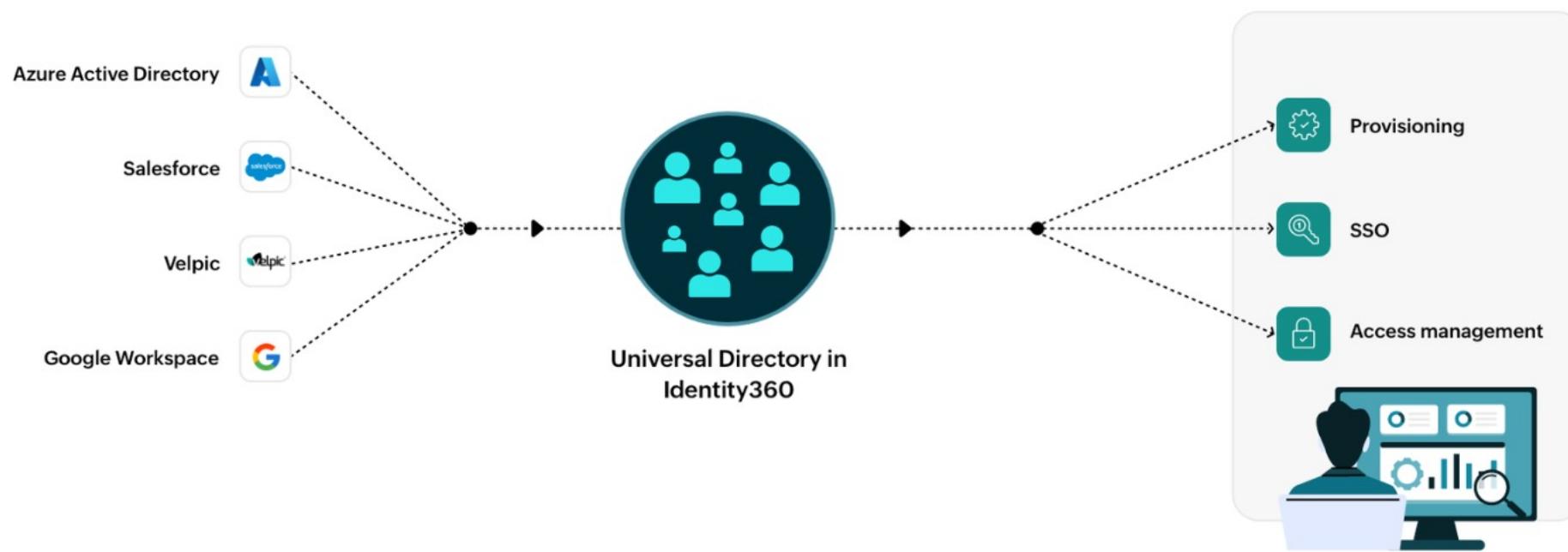
Reports and identity analytics

Identity360 solutions

Universal Directory

Consolidate identity silos into a single source of truth and enable centralized identity management with our cloud directory

How does Universal Directory work?



Unlock efficient directory services with Universal Directory

Unified solution

Leverage Universal Directory to consolidate identities from multiple platforms

Cost saving

Centralize identity management and streamline access control to achieve significant cost savings by reducing manual processes and errors

Efficiency gains

Effortlessly gather precise information from all your integrated directories with preconfigured reports

Unify users from multiple directories and applications, providing a single point of access management

Universal Directory

- All Users
- All Groups

Orchestration

User Creation Templates

Directory Integration

Manage Directory

Directory Sync Settings

Azure Directory

Azure Active Directory is Microsoft's cloud-based identity and access management service, allowing organizations to securely manage user identities and enable single sign-on to various applications and resources.

Salesforce

Salesforce is a leading customer relationship management (CRM) platform that helps businesses manage customer interactions, streamline processes, and drive growth through cloud-based applications and services.

Configure

Configure

Integrate with our roster of applications including Slack, Zendesk, Google Workspace, Jira, Zoho People, and more

Service Desk Plus

Jira

GSuite

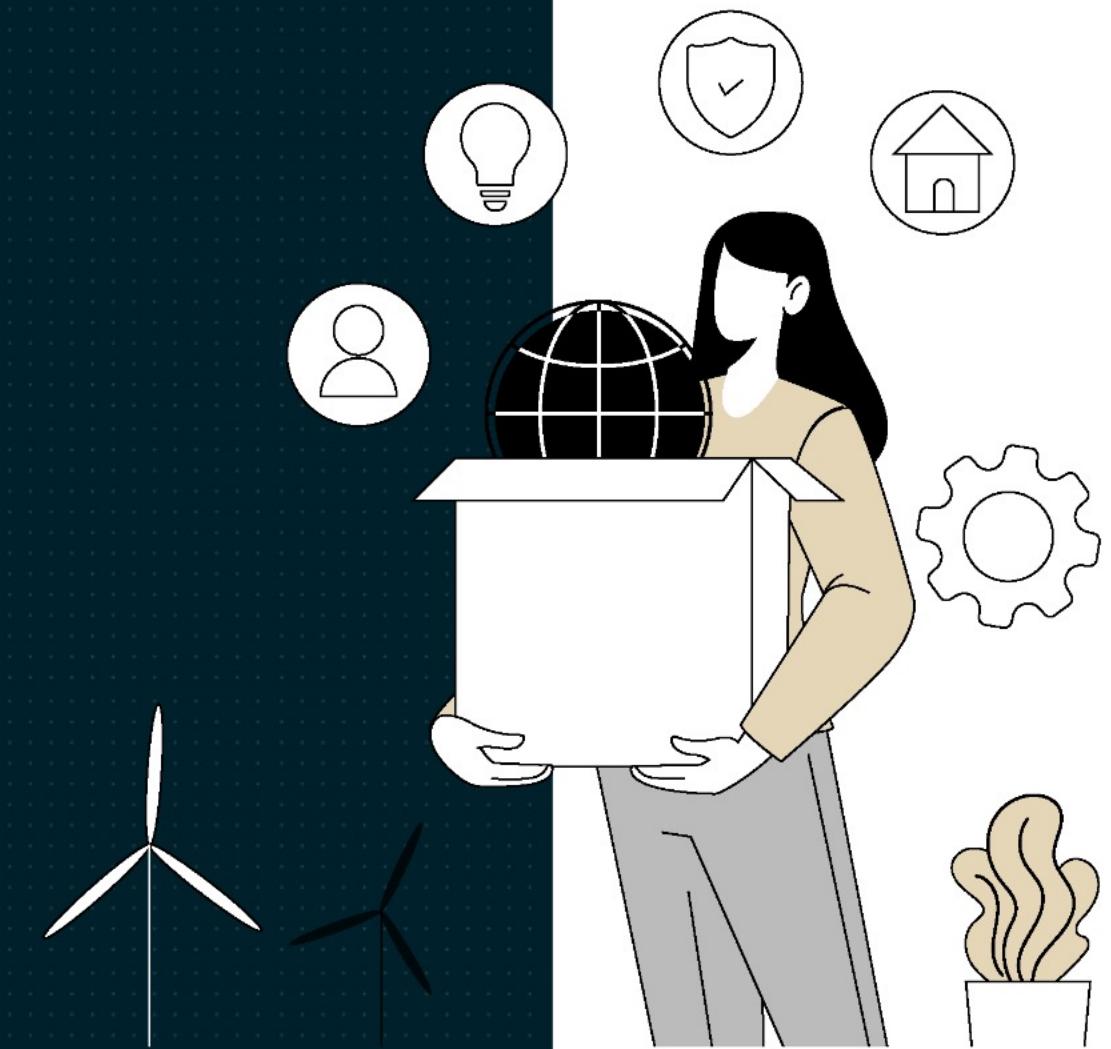
Universal Directory use case

Problem

Organization faces identity management challenges due to fragmented sources across directories and applications, causing operational inefficiencies.

Solution

Implement Universal Directory to centralize identity management and consolidate sources into a single, cloud-based directory. Gain a unified view of identities for streamlined access control.



Identity360 solutions

Life cycle management

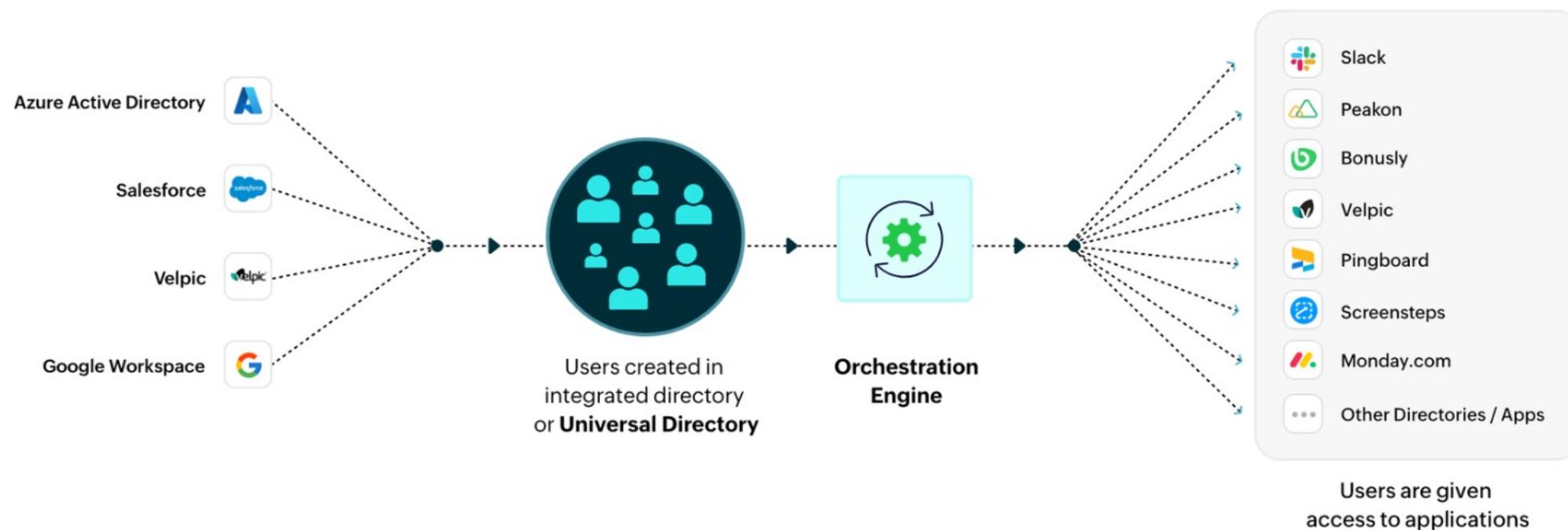
Enhance workforce productivity by
seamlessly managing the complete
life cycle of digital identities

Identity life cycle management breakdown



Orchestration

Streamline IAM processes with centralized cloud orchestration



Universal Directory

- All Users
- All Groups

Orchestration

- User Creation Templates
- Directory Integration
- Manage Directory
- Directory Sync Settings

Create New Profiles

Profile Name: User Onboarding Profile

Action executed/synced in Universal Directory

Choose Action: User Created

Profile Criteria

1. Member Of In User Onboarding Group
2. AND Office Is not Empty

OR

3. Created Date On 2024/01/01 12:00:00 AM
4. AND IsActive Is True
5. AND Title Contains Employee

Criteria Pattern: (1 & 2) || (3 & 4 & 5)

Action to be performed in other directories/applications

Choose Action: Create User

Action will be performed in the below selected directories/applications

- ✓ GSuite: Google User Creation Template
- ✓ id360.onmicrosoft.com: AAD Onboarding Template
- ✓ Salesforce: Salesforce Onboarding Template
- ✓ Velpic: Velpic User Creation Template

Enable Notification

Select Template: Employee Onboarding Notification

Receive notifications when the orchestration occurs

Orchestrate events across external applications from a single interface

Add conditions based on which tasks should be executed

Smart templates

Speed up your onboarding process with smart templates



Generate common
templates



Automate
management with
Orchestration



Utilize customized
templates in orchestration
profiles



Successful user

The screenshot displays the ManageEngine Identity360 web interface. At the top, a navigation bar lists several identity providers: Active Directory (admanagerplus.com), Microsoft 365 (adselfservice.onmicrosoft.com), Azure Active Directory (gcp.google.com), and Ultipro (ultipro.com). There are buttons for '10 more', '+ Add More', 'Copy User Attributes', 'Disable Drag-n-Drop' (which is highlighted in yellow), and 'Creation Rules'. A dark callout box on the right side of the interface contains the text: 'Set up rules that assign values to fields when they match a specified criteria'.

The main interface shows a 'General' tab for a user profile. The profile fields include: First Name, Last Name, Email, Role, Profile, Alias, Date Of Birth, Phone, Mobile, Website, and Fax. Below these, there are tabs for Account, Contact, Exchange, Custom Attributes, Microsoft 365, and Applications. A dark callout box on the left side contains the text: 'Effortlessly craft customizable templates tailored to various departments using the drag-and-drop interface'.

The Microsoft 365 tab is currently selected, showing a detailed configuration for a user account. The fields include: First Name, Initials, Logon Name* (set to 'First Name + Last Name' and '@ admanagerplus.com' with an example 'eg. johnsmith@admanagerplus.com'), Logon Name* (Pre-Windows 2000) (set to 'admanagerplus\'), Full Name* (set to 'Same as Logon Name'), Display Name, Employee ID, Description, Telephone number, Email, Web page, and Select container (set to 'OU=ZOHO,OU=Users,OU=All...'). There is also a '+3' button next to the Display Name field.

Reap the benefits of managing your identities throughout their entire life cycle with life cycle management



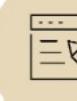
Operational efficiency

Automate the entire identity life cycle process by streamlining administrative tasks, thereby reducing the burden on IT administrators, minimizing the risk of errors, and improving overall operational efficiency



Reduced risk of errors

Reduce the likelihood of manual errors that can occur during user onboarding, offboarding, and role changes, ensuring data accuracy and consistency across all integrated platforms.



Customizable templates

Utilize predefined templates with intuitive creation rules for quick and easy user onboarding

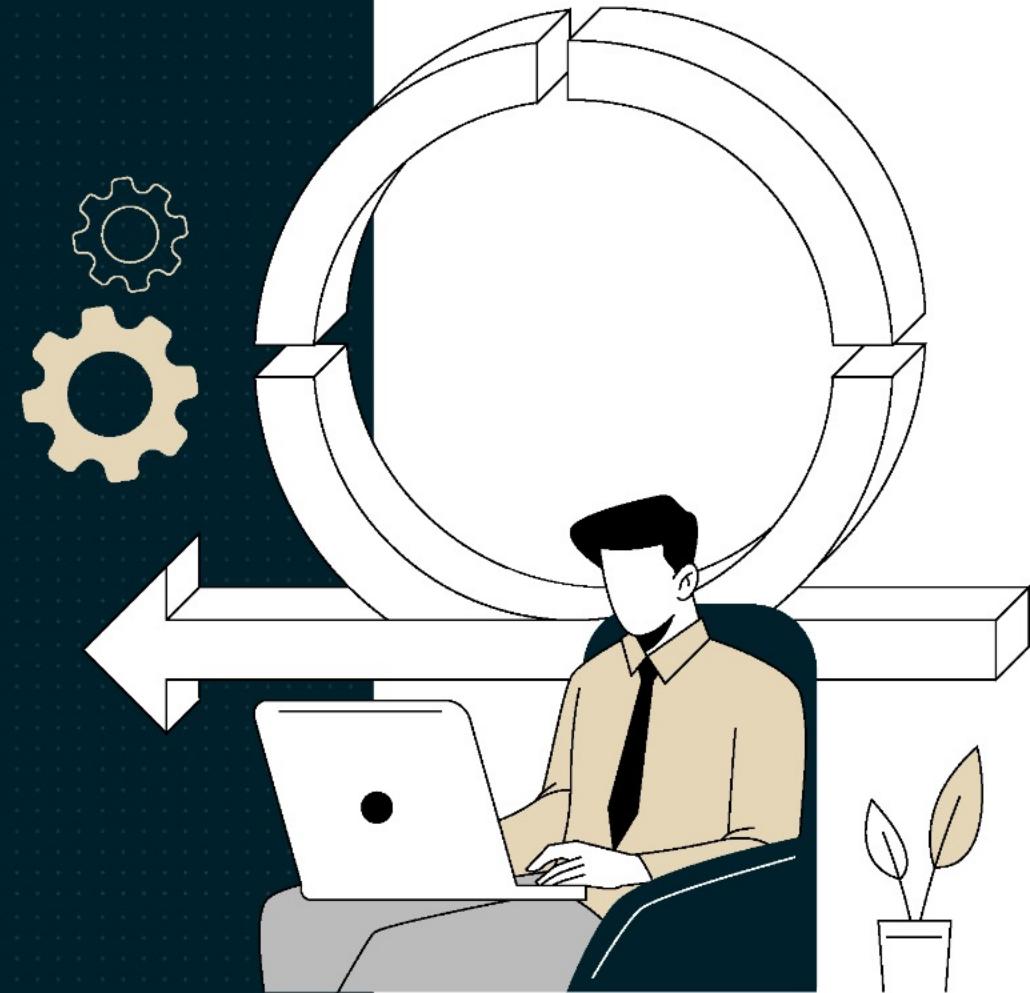
Life cycle management use case

Problem

An organization is managing the identity life cycle for a diverse workforce. Traditional processes don't keep up with employee turnover and profile changes. These challenges result in time-consuming, error-prone onboarding and offboarding, leading to security gaps and compliance concerns

Solution

Implementing identity life cycle management enhances agility and security, ensuring regulatory compliance and aligning employee engagements with legal standards. This fosters sustainable growth in today's dynamic business landscape

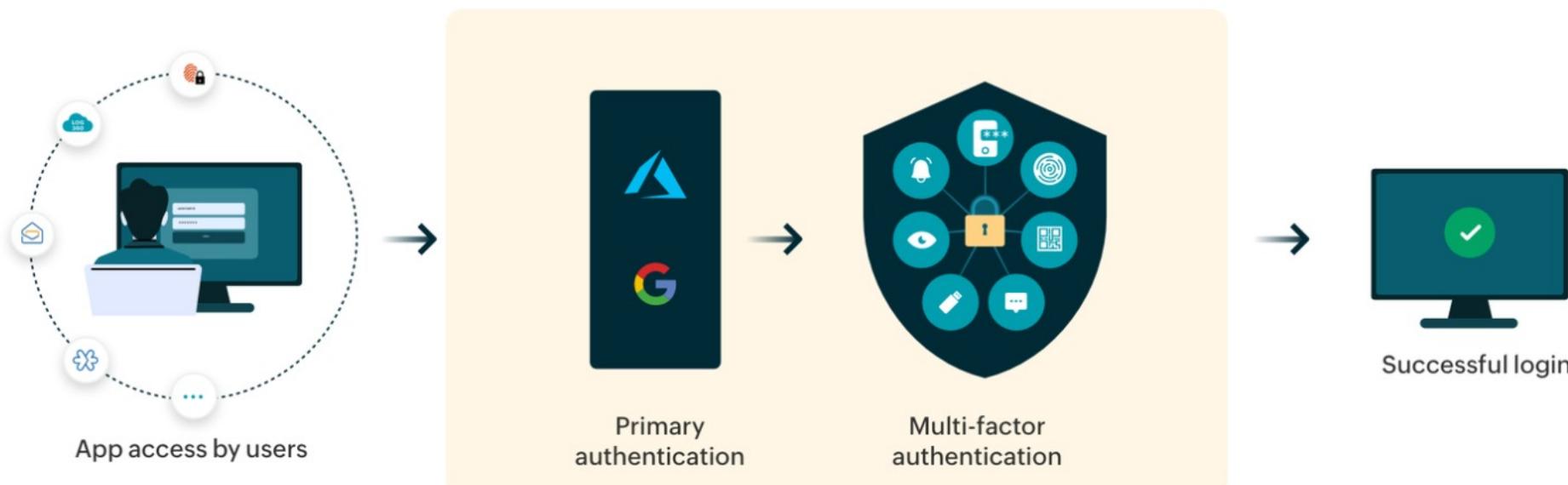


Identity360 solutions

Single sign-on (SSO)

Streamline access to enterprise
resources with secure SSO

How does SSO work?



Elevate user experience with secure passwordless login and seamless SSO



Increase employee productivity

Provide one-click access to enterprise apps and reduce password fatigue by eliminating traditional passwords and time-consuming login processes.



Broad spectrum of supported apps

Enable SSO to over 450 pre-integrated enterprise applications, or any custom application that supports federation standards, in a few steps



Secure user access

Mitigate security threats by empowering IT teams to promptly disable access to accounts in the event of theft or unauthorized access

The screenshot displays the ManageEngine Identity360 application integration interface. At the top, a navigation bar includes 'Application Integration', a search bar, and buttons for 'Custom Application', 'Application Connection', and 'Back'. Below the navigation is a grid of application cards, each with a thumbnail, name, category, and integration status indicators (Import/Sync, SSO, Access Management, Provisioning).

SSO can be enabled easily for a myriad of pre-integrated applications

Easily integrate your own custom applications for end-user SSO

Application	Category	Integration Status
Azure Active Directory	Directory	Import/Sync, SSO, Provisioning
Slack Directory	IT Management	SSO
Salesforce	Directory	Import/Sync, SSO, Access Management, Provisioning
Zendesk	CRM	SSO
Google Workspace	Messaging Apps	Import/Sync, SSO, Access Management, Provisioning
Dropbox	Messaging Apps	SSO
PagerDuty	Messaging Apps	SSO
PlanMyLeave	Messaging Apps	SSO
Sumo Logic Code	Analytical Tools	SSO
JitBit	Collaboration	SSO
AppDynamics	Messaging Apps	SSO
Panorama9	HR Management	SSO
Velpic	Customer Support	Import/Sync, SSO, Access Management, Provisioning
Egnyte	Messaging Apps	SSO
Canvas LMS by Instructure	Customer Support	SSO
Flatter Files	Messaging Apps	SSO

SSO use case

Problem

A large enterprise faces challenges managing access to numerous applications. Employees waste time navigating multiple login screens, causing inefficiencies and frustration

Solution

Implementing SSO improves efficiency, granting employees one-click entry to multiple enterprise apps, cutting login friction, and enhancing productivity

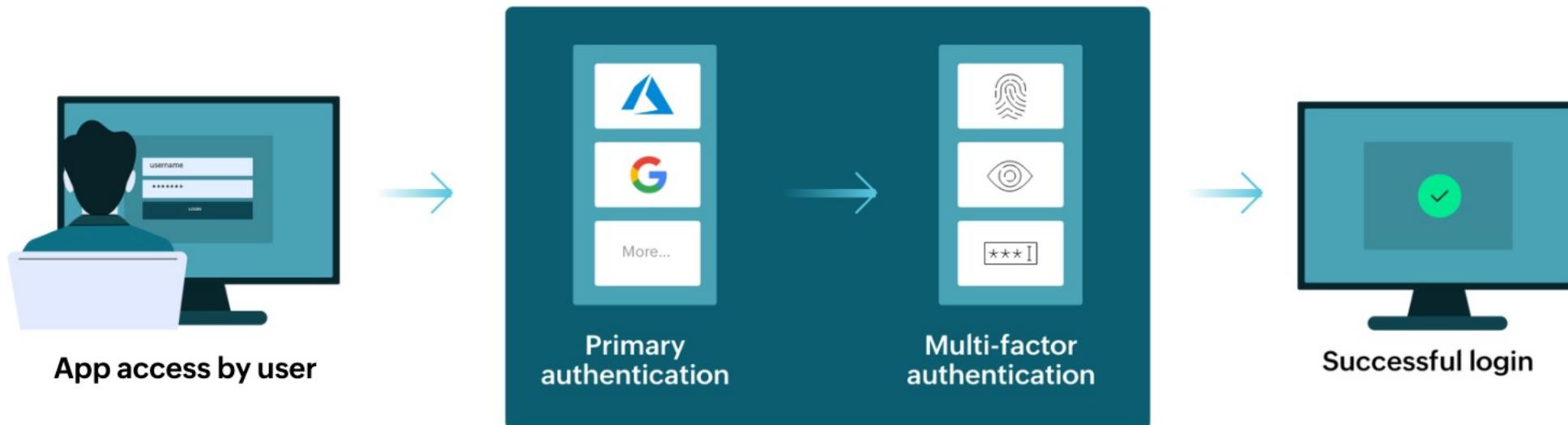


Identity360 solutions

Multi-factor authentication

Secures access to enterprise
applications with MFA

How MFA works



Advanced Settings

Customize MFA for your organization with fine-grained controls

MFA for Windows machines

Enable MFA for

Enable MFA for Remote Desktop access during RDP Server Authentication RDP Client Authentication

Users must complete the MFA process for machine login within

Allow users to trust their machines for to skip MFA.

Keep the 'Trust this machine' option selected by default.

Deny machine login for partially enrolled users.

Skip MFA verification when the device is offline.

Multi-factor Authentication

Authenticators Setup MFA for Endpoints

Configured Authenticators

Authenticator	Status
Email Verification	Enabled
Salesforce	Enabled
Google Authenticator	Enabled
Microsoft Authenticator	Enabled
Zoho OneAuth TOTP	Enabled
totp1	Enabled

FIDO2 Passkeys SMS Verification

Non-Configured Authenticators

Authenticator
Azure Active Directory
Custom TOTP Authenticator
Duo

Choose from a variety of MFA authenticators to verify users' identities

Advanced Settings

MFA Settings

MFA for Identity360 & enterprise applications

Users must complete MFA within

Allow users to trust browser for to skip MFA.

Keep the 'Trust this browser' option selected by default.

Deny login for users who have not enrolled for all the required MFA factors.

Secure identities with multi-factor authentication



Compatible with multiple directories

Choose your preferred directory for primary authentication—like Azure AD, Google, and Salesforce—which your users may already be a part of



An interactive, user-friendly UI

Makes MFA configuration and enrollment easy for admins and end users respectively, with a simple and easy-to-understand UI



Security against cyberthreats

Defend against various credential-based attacks, including those targeting UAC, Windows login, RDP, VPN and RADIUS-supporting endpoints while ensuring seamless application access to employees

MFA use case

Problem

A corporation in diverse sectors faces growing cybersecurity threats to sensitive data. Traditional password-based authentication methods used for Windows login are vulnerable to phishing and breaches, posing significant security risks

Solution

Implementing MFA for Windows login strengthens the organization's security by enhancing security during logins to Windows machines, RDP sessions, and UAC prompts. This multi-layered authentication adds robust protection against unauthorized access



Identity360 solutions

Access management

Secure and ensure that the right users have the right access consistently across resources

How does access management work?



Cross-platform access management capabilities



Improved compliance

Ensure compliance with regulatory requirements and industry standards related to data protection and privacy



Enhanced user experience

Users experience seamless and convenient access to the resources they need, leading to higher satisfaction and improved user experience



Security against cyberthreats

Safeguard against unauthorized access attempts and mitigate the risk of various cyberthreats, while also providing easy application access to employees

Within each app, you can fine-tune users' access rights by assigning them relevant roles and permissions in bulk

The screenshots illustrate the 'Application Access Management' interface for the Salesforce application. The top screenshot shows a list of users with checkboxes for selecting multiple users. The middle screenshot shows the 'Access Management' tab where users can assign profiles and permission sets to accounts. The bottom screenshot shows the 'Status' tab, which displays a consolidated table of users and their provisioning statuses.

Provides enhanced tracking capabilities for admins using consolidated tables showing users' access assignment statuses for each application

First Name	Last Name	Full Name	Username	Email	Provisioning Status
Regina	Peters	Regina Peters	reginapeters@testmail.com	reginapeters@testmail.com	Assignment is pending
Wilona	Nelson	Wilona Nelson	wilonanelson@testmail.com	wilonanelson@testmail.com	Assignment is pending

Access management use case

Problem

An organization handles extensive customer data, including personal information and payment details. With rising cyberthreats, securing access to this sensitive data is vital to preserving customer privacy and trust in the brand

Solution

Implementing access management provides robust control over data access while adhering to regulatory requirements such as the GDPR and the PCI DSS. This is achieved through tailored access controls that align with the organization's structure and operational needs



Delegation

Entrust routine tasks to non-admin users without altering their inherit permissions, allowing admins to focus on critical tasks

How does help desk delegation work?



Predefined and custom roles



Admin assigns the role to technician



Task delegated successfully

Adopt delegation to transform your IT support environment



Reduced workload

Decrease the workload for IT admins by delegating management tasks to technicians, mitigating burnout and boosting job satisfaction



Improved responsiveness

Enable quicker response times to user inquiries and technical issues by assigning specific tasks to designated team members



Scalability and flexibility

Adapt to changing workload demands and scale operations as needed, ensuring continued efficiency and effectiveness in providing support services

The screenshot illustrates the Help Desk Delegation feature in the Identity360 console. The main interface shows a table of technicians with columns for Action, User Name, Email, Primary Source, Added Time, and Invitation Status. A callout box highlights the central console's capability to manage technicians and roles. Below, a modal dialog titled 'Add New Technician(s)' shows a 'Select User(s)' input field and a 'Select Role' dropdown menu with options like Admin, Operator, HR, and Lead.

Enable or disable technicians and modify the delegated roles from the central console

Choose predefined technician roles like the Admin or Operator, or create custom roles to be assigned to non-admin users

Action	User Name	Email	Primary Source	Added Time	Invitation Status
<input type="checkbox"/>	Nick	nick@test.com	Zoho	2023/10/16 22:32:50	Unverified
<input type="checkbox"/>	John	john@test.com	Zoho	2024/09/03 16:31:28	Unverified
<input type="checkbox"/>	Bravo	bravo@test.com	Zoho	2024/09/03 16:31:28	Unverified

Add New Technician(s)

Select User(s)

Select Role

- Select -

- Admin
- Operator
- HR
- Lead

The screenshot displays two main sections of the Identity360 interface. The top section shows the 'Untitled Role' creation screen, which includes tabs for 'Universal Directory', 'Applications', 'Reports', and 'Settings'. The 'Universal Directory' tab is selected, showing four main categories: 'User Management', 'Group Management', 'Directory Management', and 'Others'. Each category has a 'Deselect All' checkbox and a list of specific permissions. The 'User Management' section includes 'All Users', 'Single User management', 'Create User', 'Modify User', 'Bulk User Management', 'Delete Users', 'Enable/Disable Users', 'Modify UD Group Members', 'Change Primary Source', and 'Create Users In Apps'. The 'Group Management' section includes 'All Groups', 'Single Group Management', 'Create Group', 'Modify Group', 'Bulk Group Management', and 'Delete Groups'. The 'Directory Management' section includes 'Directory Integration', 'Manage Directory', and 'Directory Sync Settings'. The 'Others' section includes 'Orchestration Profile', 'Templates', and 'User Creation Templates'. The bottom section shows the 'Help Desk Delegation' interface, featuring a navigation bar with 'Identity360', 'Dashboard', 'Universal Directory', 'Applications', 'Reports', 'Settings', and 'Support'. The 'Help Desk Delegation' tab is selected, showing two tabs: 'Help Desk Technicians' and 'Help Desk Roles'. The 'Help Desk Roles' tab is active, displaying a table with columns for 'Action', 'Role Name', 'Role Description', and 'Associated Technicians'. The table contains five rows: 'Super Admin' (Default Organization's Super Admin, Nick), 'Operator' (Is capable of auditing the operations within the application, John), 'Admin' (Holds full control, except for the ability to modify the product's subscription, Bravo), 'Lead' (- , -), and 'HR' (- , -). A 'Create New Role' button is located at the top right of the table.

Create custom technician roles to suit your organization's needs and manage the permissions required to carry out specific tasks

Action	Role Name	Role Description	Associated Technicians
	Super Admin	Default Organization's Super Admin	Nick
	Operator	Is capable of auditing the operations within the application.	John
	Admin	Holds full control, except for the ability to modify the product's subscription.	Bravo
	Lead	-	-
	HR	-	-

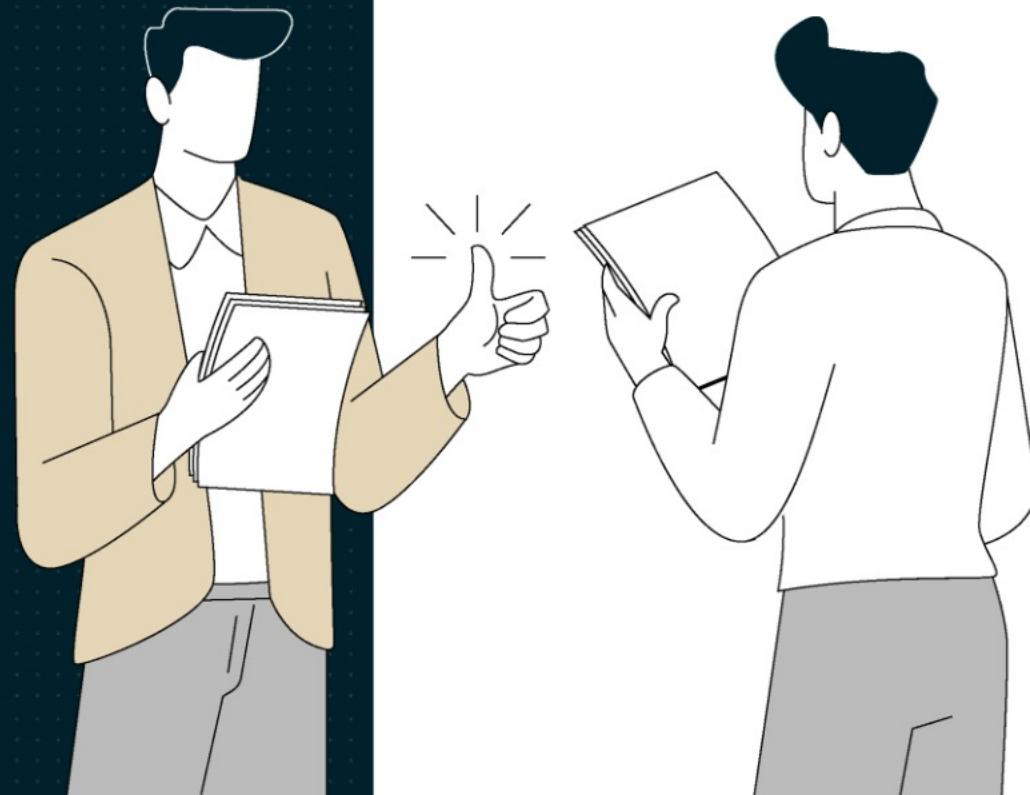
Help desk delegation use case

Problem

A large corporation heavily relies on its IT support team for user inquiries, technical issues, and service requests. However, a surge in support tickets and limited resources strain the IT department's efficiency and responsiveness.

Solution

Implementing a help desk delegation system streamlines operations and boosts service delivery. Technicians are assigned specific tasks, with access easily managed and revocable, ensuring efficient handling for timely issue resolution.

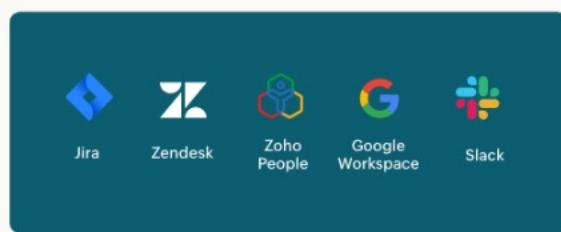


Identity360 solutions

Reports and identity analytics

Gain insights into application access, user activities, account status, and more to make informed decisions

How do reports and identity analytics work?



Administrators assign specific applications to user based on their roles and responsibilities within the organization



Users gain access to assigned applications.



Unlock superior access insights to boost your organization's security and efficiency



Enhanced visibility

Gain enhanced visibility into user activities and behaviors through comprehensive reports



Informed decisions

Enable admins to make informed decisions based on real-time data and user interactions



Prebuilt reports

Access prebuilt reports to help admins identify security risks and understand end-user application and service consumption patterns

Identity360

Subscription | Jobs | ? | -

Dashboard Universal Directory Applications Reports Settings Support

Universal Directory Azure AD Salesforce Directory

Universal Directory

235 Users 184 Groups

License

10 Consumed 0 Remaining

Configuration

3 Directory 2 Application

Inside Identity360

An identity platform with workforce IAM for digital enterprises.

All Users

468 Total Users

vexor.com (234)
vexorenterprises.com (214)
vexorports.com (1)
vexorpower.com (19)

All Groups

184 Total Groups

vexorenterprises.com (145)
vexorports.com (39)

Application Access

Access Count

vexorelectricity.com: 5
vexorenterprises.com: 2
vexorpower.com: 2

Gain insights into various aspects, such as user activities and access patterns, from a single console of various directories and applications

Active Users

Users count

2024/02/12, 2024/02/14, 2024/02/16, 2024/02/18, 2024/02/20, 2024/02/22, 2024/02/24, 2024/02/26, 2024/02/28, 2024/03/01, 2024/03/03, 2024/03/05, 2024/03/07, 2024/03/09, 2024/03/11

User Management

User Provisioning
User Deprovisioning
Enable/Disable Users
Reset Password
Unlock Users

Application Management

Application Access Management

User Reports

Universal Directory Reports
Azure Active Directory Reports
Salesforce Reports

Integrations

Directory Integration
Application Integration

The screenshot displays two reports from the ManageEngine Identity360 interface:

Soon To Expire Passwords

Filter settings: Azure AD Tenant (tester1695outlook.onmicrosoft.com), Filter By (-Select Domain(s)-), Account expiry within (2024/03/08 12:00:00 AM - 2024/04/01). The table shows 10 users with their display names, user principal names, and days since last password change.

Display Name	User Principal Name	Days Since Last Password Change
John	johnitor@tester1695outlook.onmicrosoft.com	63
Jack	jackdaniels@tester1695outlook.onmicrosoft.com	84
Patricia	patriciacorner@tester1695outlook.onmicrosoft.com	84
Jade	jadesmith@tester1695outlook.onmicrosoft.com	84
Kumar	kokkikumar@tester1695outlook.onmicrosoft.com	64
Samuel	samuelingaa@tester1695outlook.onmicrosoft.com	63
Jerry	samueljack@tester1695outlook.onmicrosoft.com	85
Mathew	mathewthompson@tester1695outlook.onmicrosoft.com	85
Lucy	lucypeach@tester1695outlook.onmicrosoft.com	85
Luna	lunaprince@tester1695outlook.onmicrosoft.com	63

Inactive Users/Technicians

Select the desired time period (Last 30 Days). The table shows 14 users with their email addresses, display names, directory types, directory names, days since last logon, created times, and last activity dates.

Email Address	Display Name	Directory Type	Directory Name	Days Since Last Logon	Created Time	Last Activity
chesterpink@chatter.sale...	Chester	Salesforce	salesforce	160	29/09/23 17:57:42	29/09/23 17:57:42
hankmint@gmail.com	HM	Salesforce	salesforce	160	29/09/23 17:57:42	29/09/23 17:57:42
daniel@prod.com	Daniel	Universal Directory	Hozo	79	20/12/23 15:05:21	-
diana@hacker.com	Diana	Salesforce	salesforce	160	29/09/23 17:57:42	29/09/23 17:57:42
llena@tester1695outlook....	llena	Azure Active Directory	tester1695outlook.onmicrosoft.com	113	16/11/23 00:54:04	16/11/23 00:54:04
cleopatra@slajs.com	Cleopatra	Universal Directory	Hozo	115	14/11/23 13:19:29	-
penguin@kind.com	Penguin	Salesforce	salesforce	160	29/09/23 17:57:42	29/09/23 17:57:42
lunapeach@kind.com	Luna	Salesforce	salesforce	160	29/09/23 17:57:42	29/09/23 17:57:42
lucypink@thangara1998....	Lucy	Universal Directory	Hozo	158	02/10/23 15:06:03	-
tonysmith@thangara1998....	Tony	Azure Active Directory	thangara1998.onmicrosoft.com	159	01/10/23 00:02:28	01/10/23 00:02:28
samuelthompsonking@z...	Samuel	Salesforce	ChanSales	77	21/12/23 17:47:43	21/12/23 17:47:43

Explore built-in reports that offer insights into user-related data across various directories like Universal Directory, Azure AD, and Salesforce

Explore various export options for your reports to further analyze identity data and gain insights

Reports and identity analytics use case

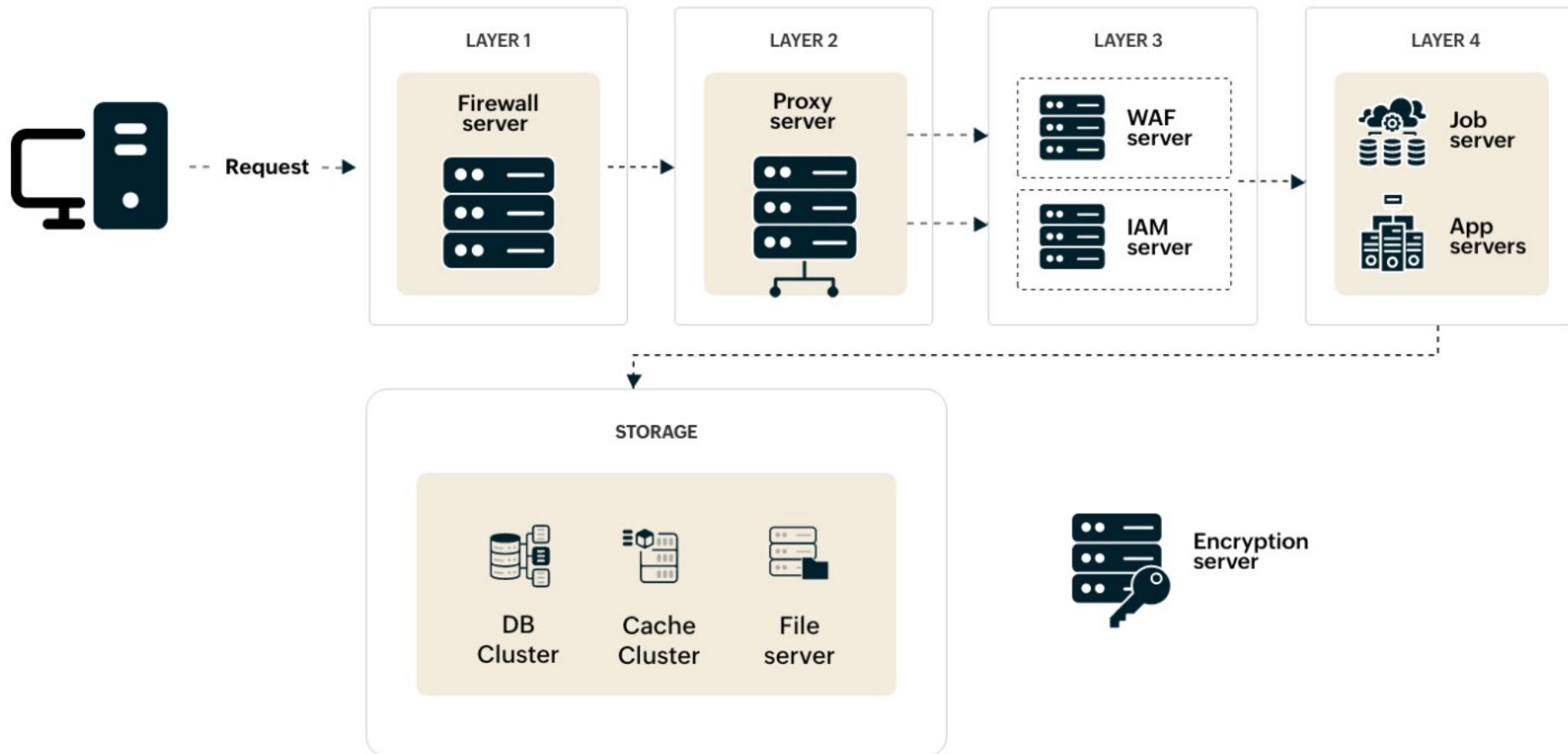
Problem

In an organization with a diverse workforce and extensive system access, ensuring security and compliance is paramount. With rising cybersecurity threats and regulatory standards like the GDPR and SOC 2, the challenge lies in effectively monitoring and managing user identities and access.

Solution

Identity360 enables the organization to extract actionable insights from user access patterns and behavior, swiftly identifying anomalies, unauthorized access, and compliance issues.





Security and compliance

Identity360 showcases its dedication to maintaining a secure and compliant environment by adhering to various industry-standard certifications:

- ISO/IEC 27001
- ISO/IEC 27701
- ISO/IEC 27017
- ISO/IEC 27018
- SOC 2 Type II
- Cyber Essentials
- ESQUEMA NACIONAL DE SEGURIDAD (ENS) - Spain
- CSA STAR Self-Assessment
- GDPR
- CCPA
- Signal spam

Identity360 licensing

Life cycle
management

Starts at **\$295** per
100 users,
per year

MFA and SSO

Starts at **\$195** per
100 users,
per year

All inclusive (life cycle
management with
MFA and SSO)

Starts at **\$415** per
100 users,
per year



Thank you!

www.manageengine.com/identity-360

identity360-support@manageengine.com

START FREE TRIAL →

