



miniOrange

# Secure Identity, Access & Data Everywhere

# 14+ YEARS OF INNOVATION

25,000+ CUSTOMERS

6,000+ INTEGRATIONS

24/7 ENGINEER FIRST SUPPORT

▲ ATLISSIAN

4.8 ★

WordPress

4.5 ★

shopify

4.6 ★

Drupal

4.2 ★

## Accolades

Recognized as  
**“Strong Performer”**  
In Gartner VOTC 2025



*“Our mission is simple: to create a safer digital world by providing identity solutions that balance security, efficiency, and trust”*

**ANIRBAN MUKHERJI**

CEO & Founder  
miniOrange



# miniOrange Suite of Products

## Identity and Access Management (IAM)

For your employees and customers to seamlessly access and securely authenticate to any applications.



Single Sign-On (SSO)



Multi-Factor Authentication (MFA)



User Lifecycle Management (ULM)



Adaptive/Risk Based Authentication



Role Based Access Control (RBAC)



JML Workflows



Privileged Access Management (PAM)



Identity Governance & Administration (IGA)

## Unified Endpoint Management (UEM)



Data Loss Prevention (DLP)



Mobile Device Management (MDM)



Cloud Access Security Broker (CASB)



AD Management & Auditing



Data Privacy & Protection



AI Integrated Solutions

## Security Solutions for Marketplaces



# Identity & Access Management (IAM)

For Employees

For Customers

## Single Sign-On (SSO)

Secure access to all applications with our unified SSO solution. Leverage identity federation, customizable branding and URLs, passwordless authentication, and local language support. Strengthen security and compliance with user activity logs and SIEM integration.

SaaS Apps

Legacy Apps

In-House Apps

Directory Integration

SIEM Integration

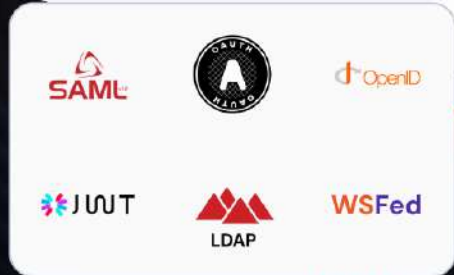
On-Premise Apps



Database



Active Directory



## Adaptive / Risk-Based Authentication

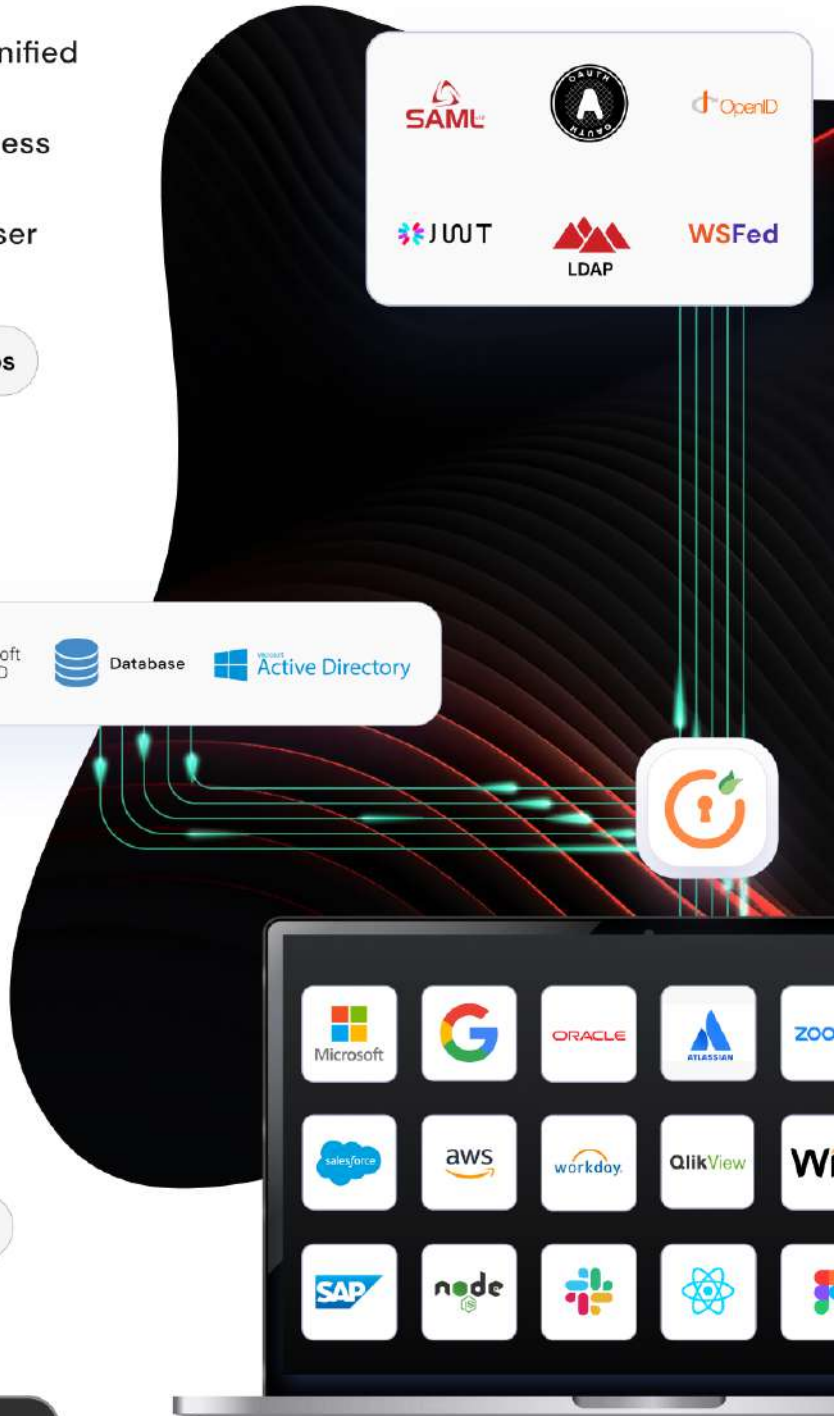
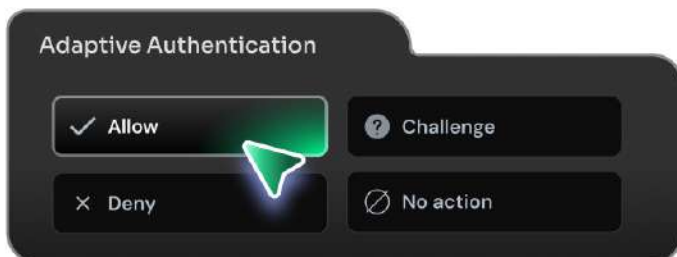
Deploy a behavioral adaptive module that continuously monitors user activity to detect and challenge risky access attempts with customizable response actions.

IP Address

Device

Time

Location

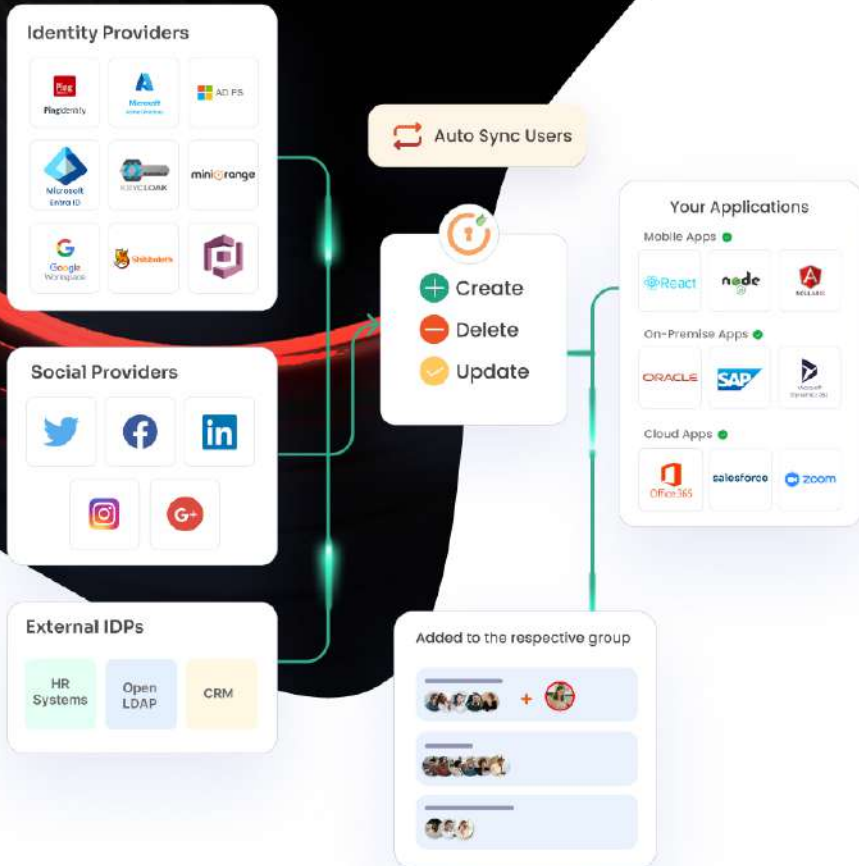


## Multi – Factor Authentication (MFA)

Enhance your security with additional layer of protection

Supports 15+ authentication methods such as OTP, Push notifications, Authenticator apps, Biometrics & FIDO 2 Keys

- VPNs
- Windows
- Linux
- Mac
- Network Device
- Radius & TACACS



## User Lifecycle Management (ULM)

Automate employee onboarding, offboarding, and user management tasks including joiners, movers, and leavers to reduce manual effort. Define automated workflows for provisioning, deprovisioning, and access control, with custom rules for role-based access, approvals, and time-based account actions.

- Workflow Automation
- SCIM
- HR Driven
- API & Webhook

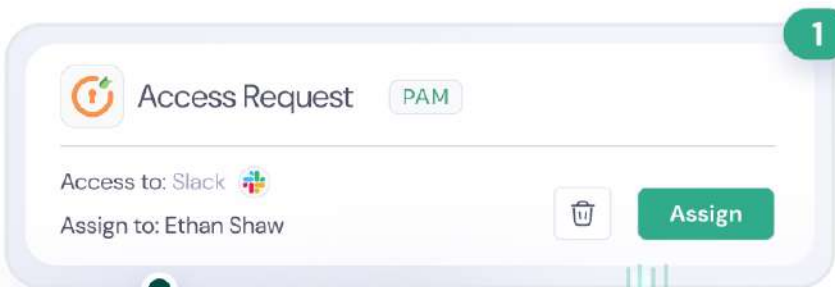
# ★ Privileged Access Management (PAM)

Privileged Access Management (PAM) safeguards sensitive accounts by managing and monitoring access to critical systems. It enforces the least privilege, secures credentials, controls sessions, and ensures compliance. PAM reduces insider threats and protects against external attacks.

- RDP & SSH
- Databases
- FTP & SFTP
- VDI & VNCs
- Web & Desktop Apps
- OT & Telecom Devices
- Anomaly and Behavior Based Detection

## Privilege Elevation & Delegation

Grant just-in-time elevated access for specific tasks. Delegate privileges without compromising control or system integrity.



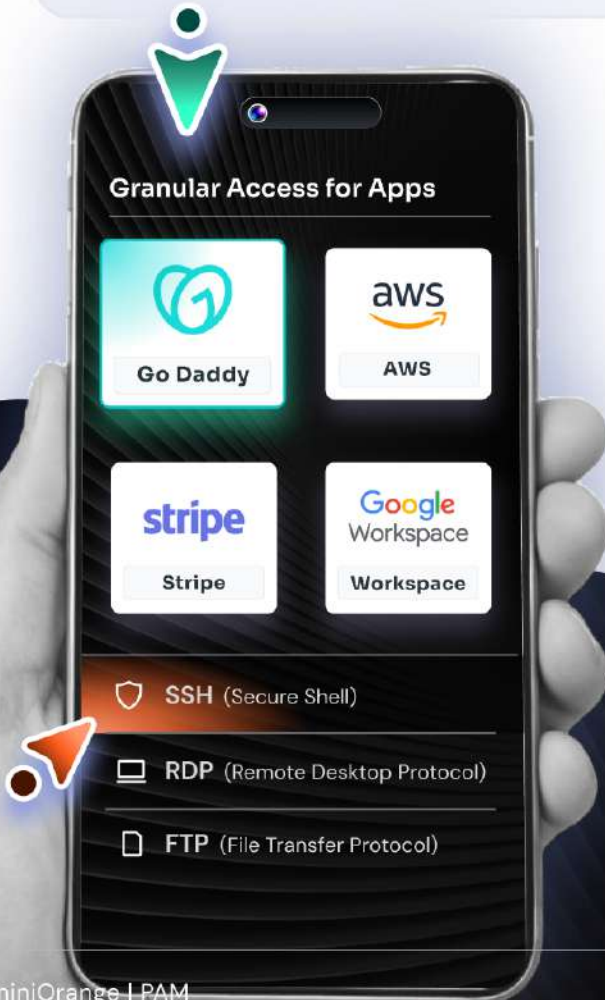
1

### Granular Access Control

Define precise access permissions for users and groups. Minimizes risk by enforcing the privilege of least privileges across your environment.

### Session Monitoring & Control

Track privileged sessions in real-time, intervene during suspicious activities, and maintain full visibility to protect critical systems through recorded sessions.





## Auditing & Reporting

Generate detailed audit logs and reports to fulfill compliance and forensic-related requirements. Gain insights into user actions and improve security posture.

**Centralised Password Vault**

	danielshaw	••••••	View
	liambrown	••••••	View
	emilyhall	••••••	Hide
	amelawhite	••••••	View
	amelawhite	••••••	Hide
	amelawhite	••••••	View

## Password Vault & Rotation

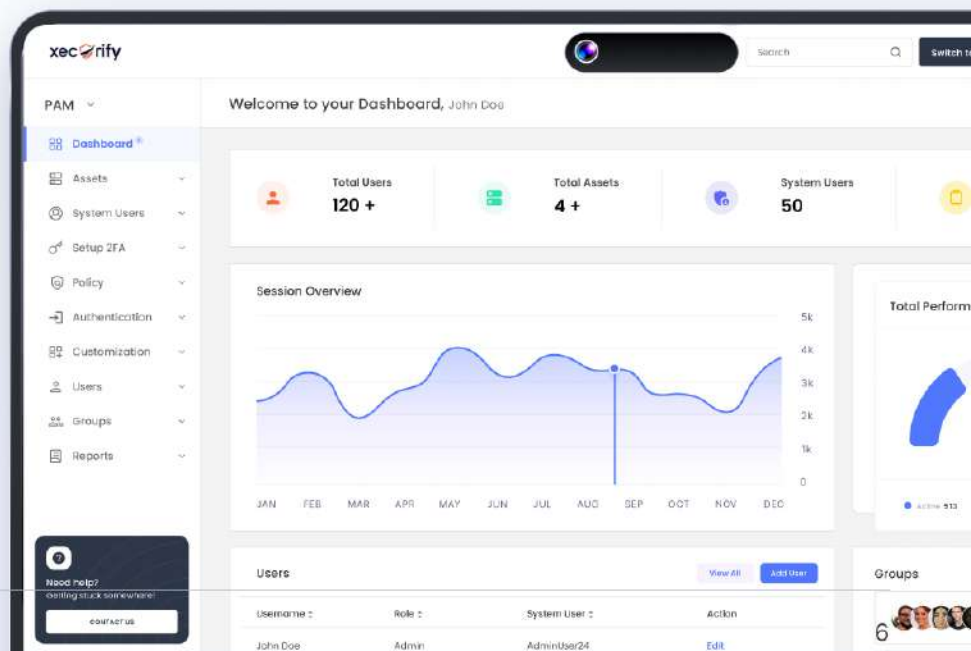
Securely store and rotate credentials with an encrypted vault. Automate password updates to eliminate manual errors and improve security.

## Resource Access

Enable secure access to critical resources via web or thick clients. Ensure seamless connectivity while maintaining robust security measures.

## Endpoint Privilege Management

Protect privileged identities and access on endpoints for all windows mac and linux devices



# Identity Governance & Administration (IGA)

Strengthen Your Security Posture By Centrally Governing User Access Across All Applications And Systems. Implement Robust Access Controls With Entitlement Management, Access Reviews, Access Request Management, Segregation Of Duties (SoD), And Automated Provisioning.

Access Certification

Segregation of Duties (SoD)

Access Request

Orphan Account Detection

Multi-level Reviewers

Compliance Reporting

Role-based Access Control (RBAC)

## Access Governance

Eliminate access risks and security gaps. Deliver a centralized governance experience that gives the right access to the right people at the right time.

Organization Wide Governance

Policy Enforcement

## Role Based Access Control (RBAC)

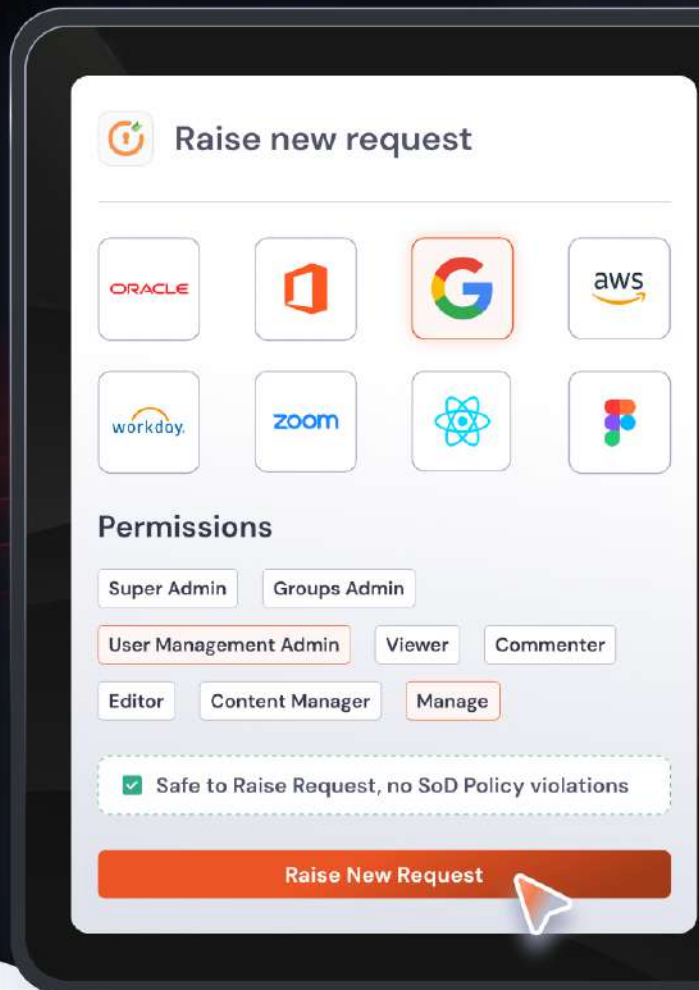
RBAC assigns and governs application access using business roles, enabling automated provisioning, accurate permission mapping, and consistent policy enforcement across cloud and on-premise environments.

Centralized role management

Granular access control

Automated user provisioning

Dynamic role assignment



## Access Request

Enable users to request access to applications, roles and entitlements and control access rights and permissions for their entire identity lifecycle while using predefined approval processes and workflows.

Applications

Permissions

Roles

### New Access Request

Access to:  Google Workspace

Request: Super Admin access for Google Workspace

 Severe SoD Policy violations Detected

Requested By: John Doe

Reassign

Reject

 Recommended

Approve

### Quarterly Finance Review

Your Quarterly finance review is here, Review permissions for accounts and take your decision.

Review: Ethan Shaw

Permissions: Read access for Workday Application

 Safe to Approve, no SoD Policy violations

Reassign

Reject

Approve

 Recommended

## Segregation of Duties (SoD)

Segregation of Duties (SoD) in IGA prevents fraud and error by ensuring no single user has overlapping permissions to initiate and approve the same critical business process or sensitive transaction.

## Access Certification

Access Certification is a periodic IGA process where managers or owners evaluate and verify user permissions. It ensures employees hold only necessary access, preventing "privilege creep" while maintaining security standards and achieving regulatory compliance through automated remediation, detailed audit logs, and continuous enforcement of the Principle of Least Privilege.

## Compliance Reporting

Deliver audit-ready reports to meet ongoing compliance requirements. Provide auditors with detailed, real-time reports that includes identity governance and administration data about what resources are in your environment, who has access to them, when, and why that access was granted and terminated.

# Customer Identity & Access Management (CIAM)

B2B CIAM

B2C CIAM

## Passwordless Login

No more password management hassles and vulnerabilities, deliver a seamless user login experience.

Biometric

FIDO

Passkeys

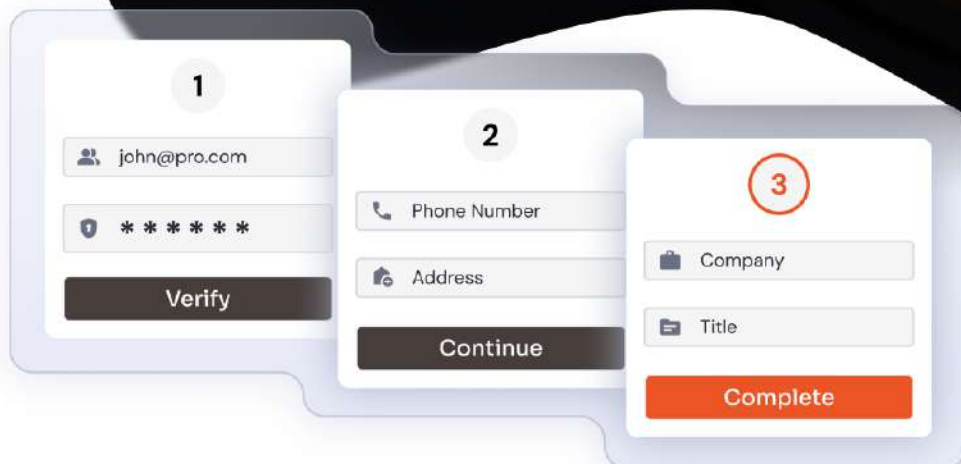
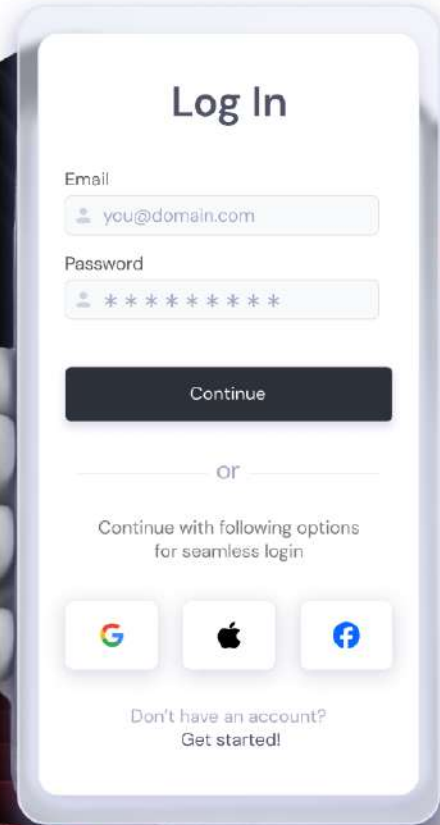
Magic Link

## Progressive Profiling

Request essential details initially and minimize friction, boost user registration, and accelerate conversions. Collect user data incrementally and personalize customer experiences by tailoring recommendations and curating targeted marketing campaigns.

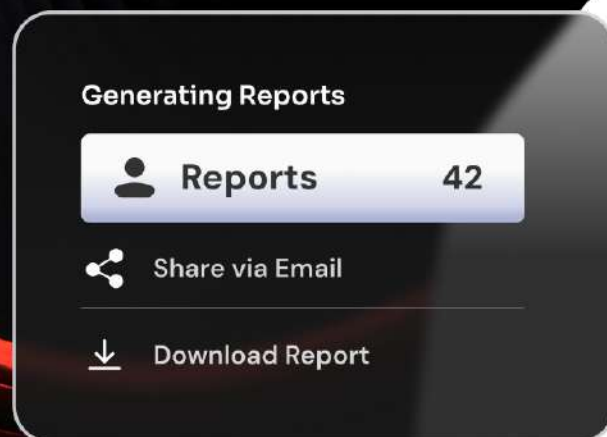
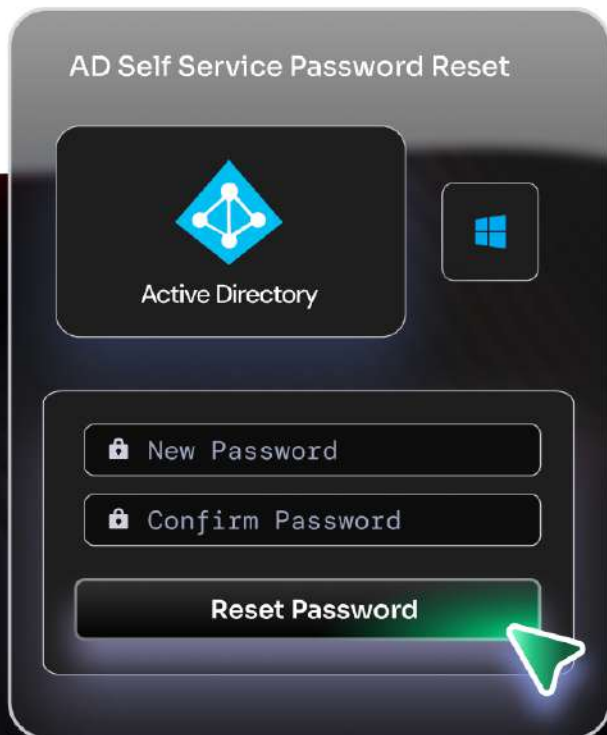
## User Profile Management

User Profile Management centralizes user identities, synchronizes attributes across systems, and enables accurate lifecycle updates with a unified identity view.



# ★ AD Management & Auditing

Seamlessly manage Active Directory operations, improve security and compliance with advanced auditing features, and empower users with self-service capabilities to reduce administrative overhead with miniOrange Active Directory utility tools.



## AD Management

Allow your IT teams to manage users, automate provisioning, and enforce policies from one unified AD management platform. Built for hybrid environments, this Active Directory management software makes directory operations faster, safer, and future-ready.

AD Object Management

GPO Management

AD Workflow & Automation

AD Bulk Management

## Self Service Password Reset

AD self service password reset tool specifically integrates with Active Directory, allowing organizations to streamline password recovery, reduce helpdesk load, and maintain seamless access for users across hybrid environments

## AD Auditing & Report

Track every change in Active Directory with precision. Our Active Directory auditing software monitors user activity, detects suspicious behavior, and ensures complete visibility into your AD environment.

Windows Logon Auditing

Password Policy Auditing

Privileged User Monitoring

# ✦ Unified Endpoint Management

## (MDM, DLP, CASB)

Shielding business data and managing access control with ease. Prevent data leaks from your Cloud SaaS apps, Endpoints, and Mobile Devices in real-time. Keeping enterprise data safe – anytime, anywhere.

### Mobile Device Management (MDM)

Remotely manage your workforce devices, whether company owned or BYOD. Configure device security policies, enforce app restrictions, and remotely wipe devices to protect sensitive data, all in one click.

Device Enrollment

Message broadcasting

Network Management

Location Tracking And Geofencing

Kiosk Mode

Remote Troubleshooting



## MDM Features

Zero Touch Enrollment

Remote Lock and Wipe Devices

Secure Corporate Data Containers

Application and Profile Management

Prevent Data Sharing/Screen Recordings

Prevent Hard Reset

### Cloud Access Security Broker (CASB)

Secure business data on SaaS apps with real-time restrictions, managing device approvals, and data access permissions on the cloud. Set custom policies that meet your security requirements and make you compliance ready!

Shadow IT Discovery

Device & Session Control

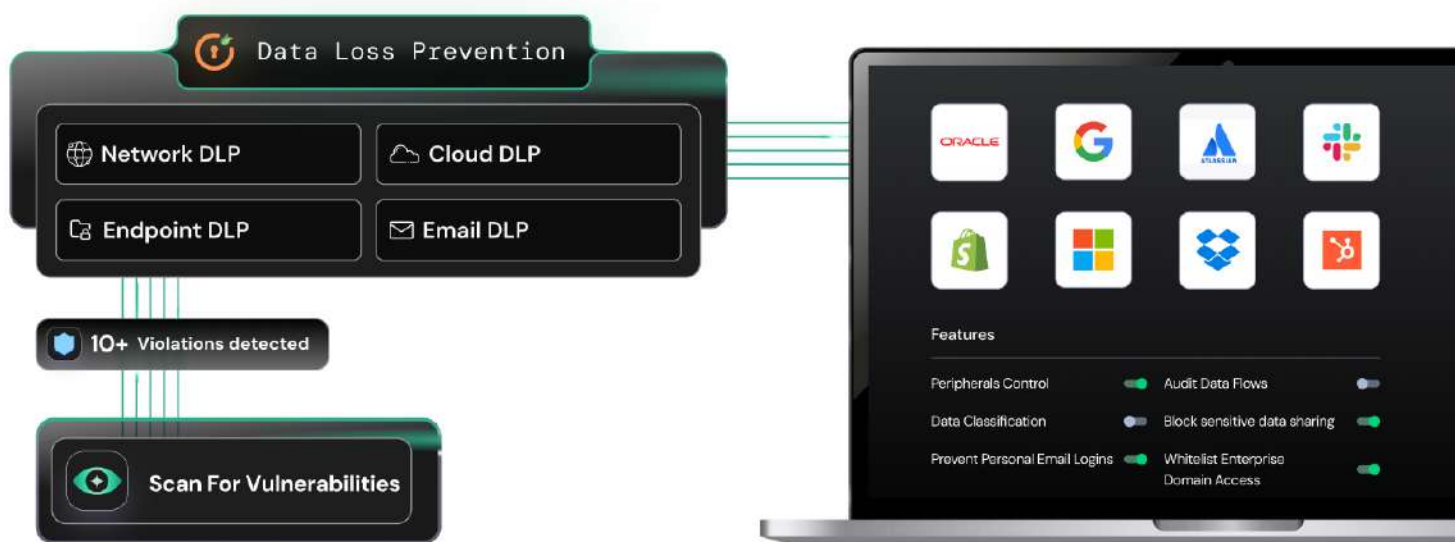
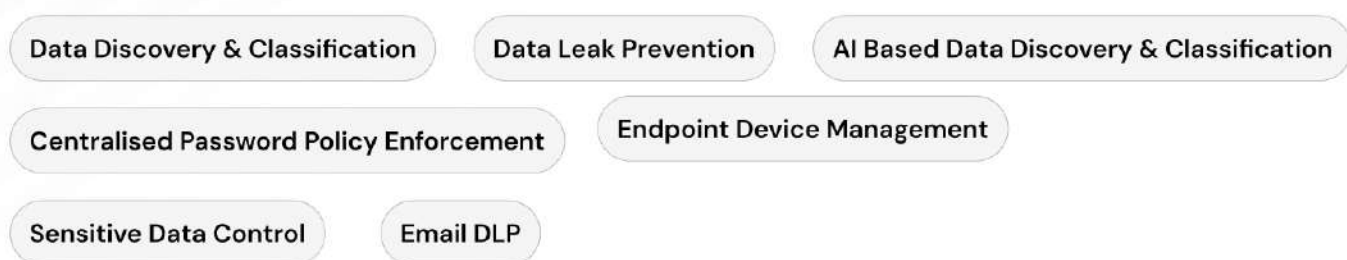
Real Time Threat Monitoring

SaaS Usage Visibility

## Data Loss Prevention (DLP)

Data Loss Prevention delivers comprehensive data discovery, real-time monitoring, and policy-based protection across endpoints, cloud applications, databases, and enterprise communication channels. It helps organizations prevent data leakage, control unauthorized data movement, and maintain full visibility into sensitive information.

With **email DLP, employee monitoring, device tracking, and password policy enforcement**, the solution reduces insider risk, secures data in motion and at rest, and strengthens compliance readiness without impacting user productivity.



## Data Classification

Gain complete control over personal data to prevent exposure and meet regulatory requirements with confidence.



# Data Privacy & Protection

Move privacy beyond obligation to business advantage. Protect critical data, demonstrate measurable accountability, and create experiences customers trust.

## Data Privacy and Automation

Protect sensitive data across its lifecycle with continuous visibility, automation, and built-in security controls.

AI-Powered Data Discovery & Classification

Encryption, Masking, And Policy Enforcement

Data Retention, Minimization & Verified Deletion

Real-Time Monitoring With Compliance Reporting

## Consent Management

Build transparent, auditable permissions across every user interaction and application.

Capture Consent At Sign-Up And Login

Manage Permissions From A Central Interface

Maintain Audit-Ready Consent Records

Automate Consent Renewal And Updates

The image displays a central dashboard titled "Data Privacy & Protection Dashboard" with the subtitle "Comprehensive overview of identity management, data protection, and DPDP compliance".

**Dashboard Widgets:**

- Applications:** 24 (22 SSO enabled)
- Active Consents:** 1,456 (100% DPDP compliant)
- Protected Devices:** 487 (All devices secured)
- Data Sources Overview:**
  - Patient Database (PostgreSQL) - 1,234 PII records - HIGH
  - Billing System (MySQL) - 432 PII records - MEDIUM
  - Email Server (Exchange) - 876 PII records - MEDIUM
  - File Storage (S3 Bucket) - 854 PII records - LOW
- Recent Activity:**
  - Security Team Incident:** Reported critical incident: INC-005 - Unauthorized Access to Patient Database (1,250 records affected) (1 hour ago)
  - System security:** Blocked external file sharing attempt by Dr. Priya Deshmukh (Patient SSN detected) (2 hours ago)

**Side Panels:**

- Consent Management:**
  - Capture Consent:
  - Central Permission Control:
  - Audit Logs Enabled:
- AI Automation Core:**
  - AI Data Discovery:
  - Encryption & Masking:
  - Retention Policies:
- PII Protection Control:**
  - 80% Scan Complete
  - Scanning: PDF Types, Files, CSV, Employee only...
  - Files: Patient\_data\_2024.pdf, invoices\_2023.csv, insurance\_claims.xls, patient\_contacts.pdf

## PII Protection or PII Discovery & Classification

Gain complete control over personal data to prevent exposure and meet regulatory requirements with confidence.

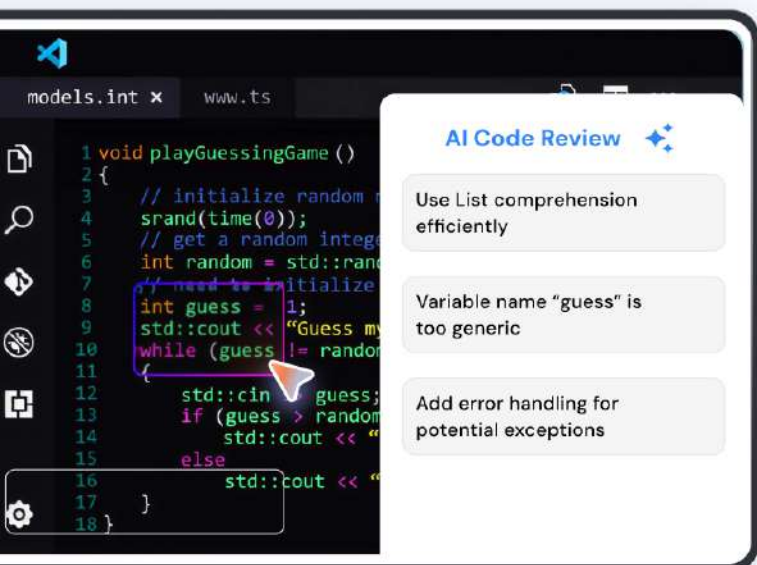
Discover And Classify PII Across All Environments

Control Access To Personal Data Based On Policies

Stop Unauthorized PII Transfer In Real Time

Track Every PII Interaction With Tamper-Proof Logs

# AI Integrated Solutions

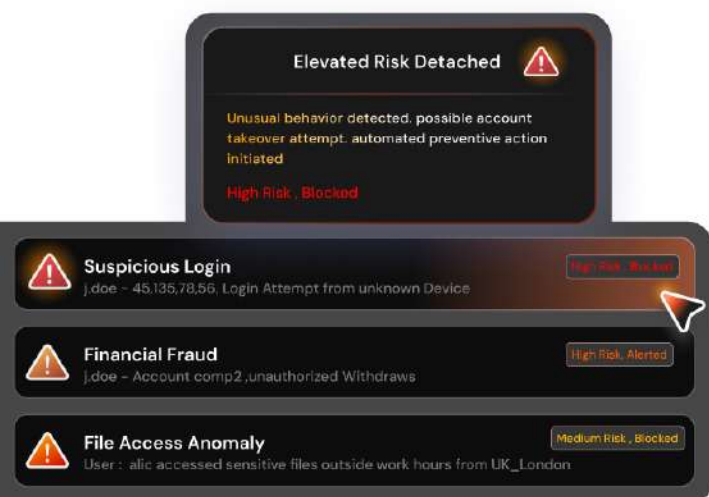


## AI Code Reviews & Vulnerability Detection

Automate code reviews using the AI model of your choice. This plugin comes with a preset of industry standard coding guidelines, with additional support for custom rules that might be specific to your organization. Comments, suggestions and status changes will automatically be added to the PRs, with an added layer of role based access for security.

## Anomaly and Behavior Detection

Risk engine leveraging machine learning model to compute risk score, that acts as a behavioural intelligence layer over the application layer. Instead of relying only on predefined rules or known attack signatures, it continuously learns how users, devices, and systems normally behave – and identifies deviations that may indicate fraud, compromise, or insider threats and automatically takes preventive action or flags it based on severity & impact.



## Securing AI Agents

Secure autonomous systems that make decisions, chain actions, and move faster than manual controls. Manage what AI agents can access, how they authenticate, and when permissions should change.

AI Agent Authentication

Access Management

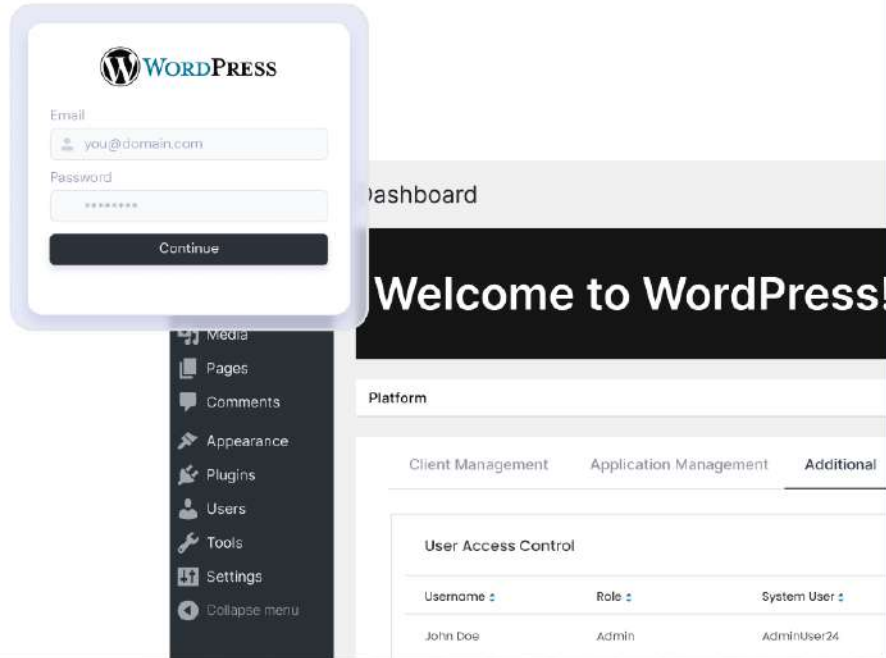
Non-Human Identity Management

Audit and Compliance Visibility

# Securing Your WordPress Sites

Secure your WordPress site with our comprehensive suite of advanced security solutions. Additionally, improve user management, simplify operations, and protect your digital ecosystem with efficient integrations and powerful tools.

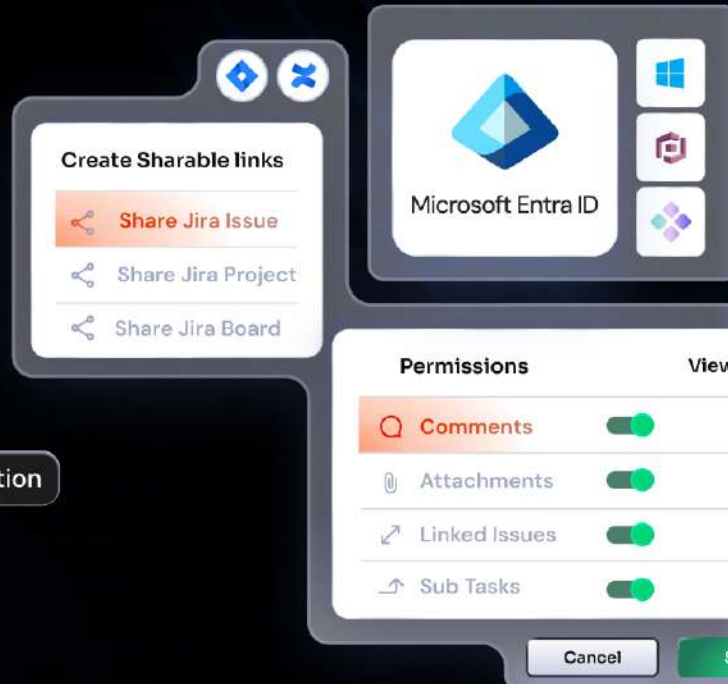
- SSO    MFA
- Microsoft 365 Integrations
- User Provisioning    Salesforce ISV
- Web Agency    API Solutions
- Directory Services (LDAP/AD Integrations Cloud and Intranet)



# Securing Atlassian

We deliver a complete suite of solutions to secure your Atlassian ecosystem. From authentication to user provisioning, our apps protect data, streamline workflows, and integrate seamlessly to deliver enterprise-grade performance.

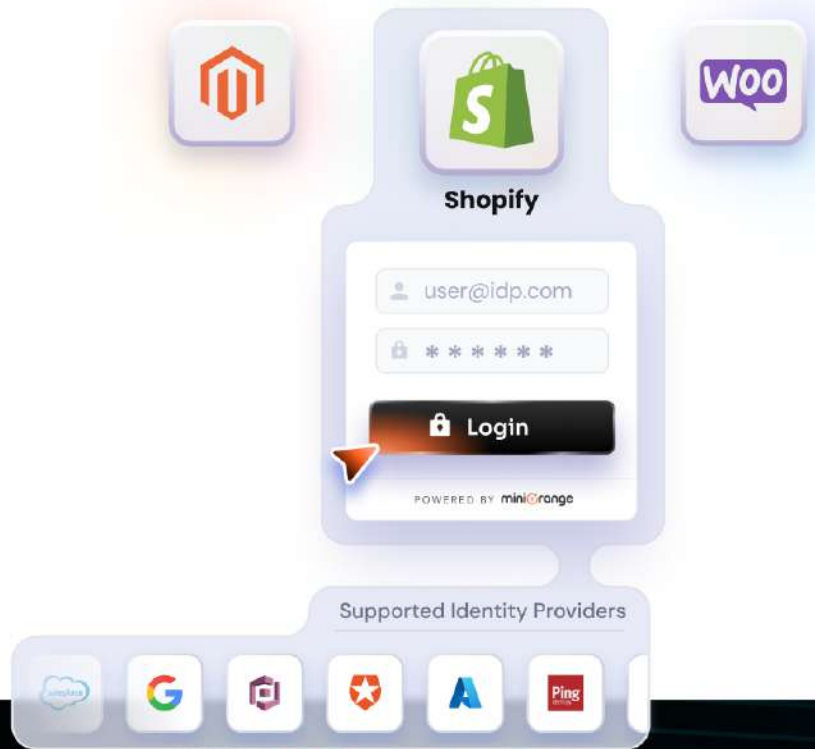
- SSO    MFA    SCIM
- Secure Share    AD Integration
- Application Access and Governance Workflow (DC)
- Automated User Management    Enhanced API Authentication
- AI based Code Reviews & Vulnerability Detection



# Securing E-commerce

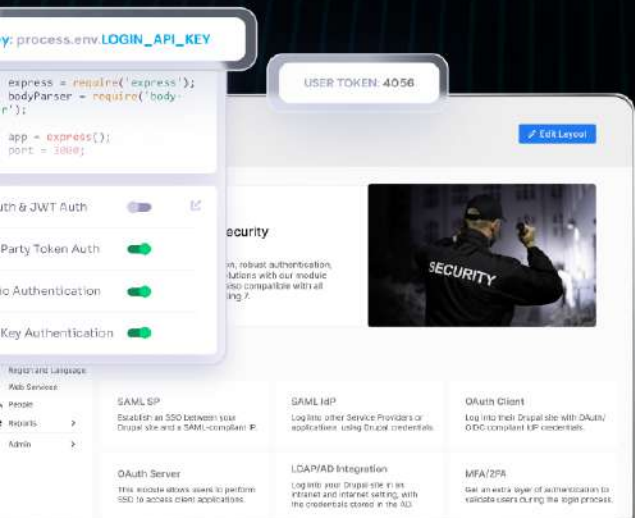
Protect and optimize your E-Commerce store with miniOrange – offering advanced security, automation, provisioning, and loyalty solutions for B2B, B2C, and DTC merchants, ensuring seamless store management.

- SSO
- MFA
- User Provisioning and Inventory Sync
- SMS & WhatsApp Notifications
- Lock store & Secure access
- Headless Store Authentication



# Securing Drupal

miniOrange empowers Drupal sites with seamless IAM (Identity and Access Management Solutions), offering robust security, Single Sign-On (SSO), Multi-Factor Authentication (MFA), and user provisioning for enhanced efficiency and protection.



- SSO
- MFA
- Headless Integration
- Session Management
- API Authentication
- User Provisioning and Sync
- Web3 Integration
- Office 365 Integration

# Why us?

## 24x7 Global Support

Our global teams provide round-the-clock assistance to address any challenges you may encounter from any corner of the world.

## Security Experts

Get assistance directly from our team of experts & engineers instead of chatbots. No AI-generated bluff.

## Cost-Effective

We offer the most cost-effective Identity Solutions available at competitive, customized & flexible pricing packages.

## Ease of Adoption

Our enterprise solutions are user-friendly & simple, leading to fast user adoption. Removing unnecessary workforce training.

## Tailor-Made Solutions

Our solutions are customizable as per your unique organizational needs. One-stop solution for your security requirements.

## Unified Portal

Access all configured apps via desktops or mobile devices through a single, customizable, self-service portal.

## Flexible Deployment Options



100%  
On-Premise



Multi-Tenant  
Cloud



Private  
Cloud


## Contact Us

Scan to know more 



info@xecurify.com



 +1-9786589387



www.miniorange.com

 +91-9717845846

# They Know Why.





Secure **Identity, Access**  
& **Data** Everywhere