



# **MANAGE & SECURE ACCESS TO YOUR APPLICATIONS WITH RAINBOW SECURE**

[WWW.RAINBOWSECURE.COM](http://WWW.RAINBOWSECURE.COM)

# WHAT IS IDENTITY AND ACCESS MANAGEMENT?

---

Identity is the foundation of digital transformation



Cloud computing and mobile devices have transformed the modern workplace. An increasingly global workforce has the flexibility to work from anywhere using free and low-cost software as a service (SaaS) applications to solve productivity and collaboration challenges. Large enterprises are migrating applications and computing to the cloud to modernize their architecture, and lines of businesses are taking advantage of new cloud services to build custom apps for their specific needs. The enterprise has benefited from the surge of new technology with greater productivity, but digital transformation has also introduced three new challenges.

# NEW CHALLENGES

## CHALLENGES DUE TO DIGITAL TRANSFORMATION



**Security risk**

**Security risk:** Before the cloud revolution, IT served as a technology gatekeeper. The apps and platforms you managed and secured were contained within the network perimeter, and everyone that signed into your corporate resources was first validated by the firewall. Those days are over. Your workforce has more control over the technology they use, much of which is accessed via the internet. Cyber attackers have learned to exploit these vulnerabilities. Even when a legacy password or 2FA is presented, that does not mean it is presented by a legitimate user.



**Administrative burden**

**Administrative burden:** The explosion of endpoints provides users more ways to connect but this also creates an administrative nightmare. Many enterprises aren't aware of all the tools employees use and even when they do have a good inventory, the sheer number of cloud apps means you need to manage multiple identity systems, increasing costs and compounding existing security risks.



**Poor user experience**

**Poor user experience:** Users also feel the pain. They love the flexibility but are frustrated by the number of credentials they need to remember. They also don't like the stress of creating long complex credentials, changing it frequently and need to carry devices everywhere.

*User Identity security & management is at the center of any digital project, that's why you need to excel at it.*

# IDENTITY AS THE CONTROL PLANE

## IAM SOLUTIONS SOLVE THESE CHALLENGES



Secure identities

The common denominator across these pain points is inefficient systems for verifying identity. Identity has replaced the network perimeter as the new control plane. You need solutions that connect the disparate tools, architecture, devices, services, and clouds across the enterprise to better protect the organization and manage access for both employees and external partners



Best user experience

Identity and access management (IAM) solutions unite access under one system, giving you more control. They provide seamless collaboration across the boundaries of your organization while improving the security of your corporate resources. A good IAM solution lets you connect your users to all their work applications—whether they are in the cloud or on-premises—through one set of credentials. IAM solutions are designed to give users access to only the resources they need and block unauthorized users from accessing data they shouldn't. You manage user access rights and permissions from a centralized portal, reducing much of the manual processes involved in provisioning and deprovisioning user accounts. IAM solutions also provide tools to manage security policies across your identities and apps. The best IAM solutions safeguard identities, improve the user experience, and increase administrative efficiency.



Increase administrative efficiency

*User Identity security & management is at the center of any digital project, that's why you need to excel at it.*

# A UNIVERSAL IDENTITY PLATFORM

---

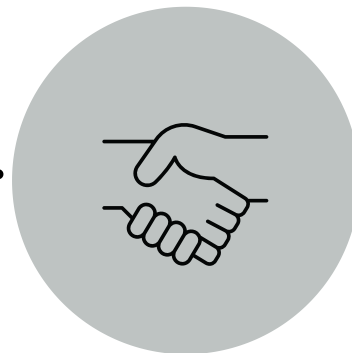
Rainbow Secure is a comprehensive IAM solution in the cloud. It gives directory management, application access, and advanced identity protection. Rainbow Secure empowers organizations to manage and secure identities for employees, partners, and customers to access the apps and services they need.



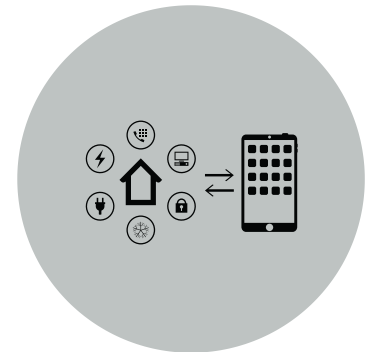
**Connect your  
workforce to any app**



**Protect and  
govern access**



**Engage with customers  
and partners**



**Accelerate adoption  
of your apps**

# RAINBOW SECURE FOR ALL YOUR APPLICATIONS

---

## **One identity for all of your apps**

Rainbow Secure lets you manage a common identity for each user across your cloud and hybrid infrastructure to access all the applications they need, including cloud and on-premises line of business applications. Manage all your identities from a universal platform, increasing administrative efficiency and giving you more control. Apply granular security policies to each of the applications used in your organization.



# RAINBOW SECURE FOR ALL YOUR APPLICATIONS

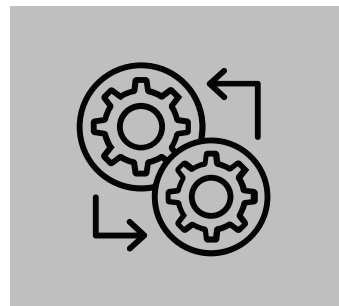
## Save time and money

Rainbow Secure SSO is pre-integrated with hundreds of applications, including popular options like Office 365, Sharepoint, MS PowerApps, MS Dynamics, Salesforce, Slack, Google Workspace, NetSuite, IBM Aspera, Workday, ServiceNow, SuccessFactors, Adobe, Concur, Workplace by Facebook, and all apps hosted on cloud platforms including Microsoft Azure, Google Cloud, AWS, IBM Cloud and Oracle Cloud making it simpler for you to make those apps available to your users. With one console, deploy consistent policies and monitor access rights. You can automate workflows for user provisioning and lifecycle management and save time and resources with self-service account management. You can seek our technical services for identity integration to inbound user information from HR tools as a source-of-truth, eliminating the need for custom scripts or manual processes to manage user attributes.

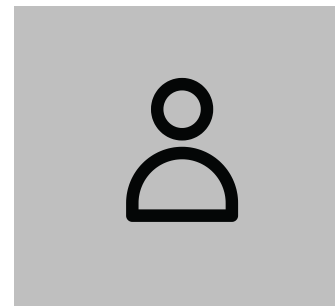
Apps configured through Rainbow Secure SSO enable single sign-on (SSO) for seamless access, meaning users don't have to remember credentials for each app account or reuse weak passwords and risk a data breach. Accounts that have been configured for automatic provisioning give users immediate access to new resources. For inbound provisioning from HR tools, our custom integration services for Rainbow Identity ensures new hires have access to all of their relevant resources on day one. You also save money by monitoring app and license usage by given user group or project team.



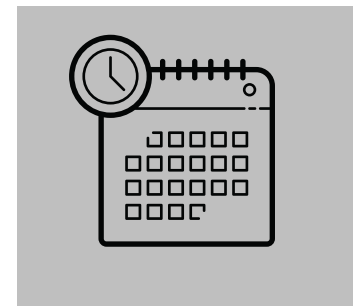
**Time and  
money savings**



**Built-in  
SaaS integrations**



**Single sign-on**



**Day one  
user access**

# RAINBOW SECURE FOR ALL YOUR APPLICATIONS

---

## Provide more secure access to all your apps

Rainbow Secure gives you comprehensive identity protection across all your apps – both SaaS apps and your on premises line of business applications. Whether the user is requesting access into Office 365, Salesforce or Slack, Rainbow Secure ensures their identity is confirmed before granting access. Multi-layer Multi-factor Graphical options lets users in and keep hackers out. You can also setup security access governance policies to ensure users only have access to what they need, when they need it and where they need it from. You can require users to request permission for access, and you can set a time limit for how long they can access the application and conduct regular compliance reviews of the access.

Rainbow Secure leverages the power of the AI Monitoring, Risk Analytics, Machine learning and threat alerting to analyze access and usage data across all our products and services to uncover access pattern and map it with expectations for given user or role. Rainbow Secure Advanced threat protection looks at device, location, access request and other contextual information to evaluate the risk of the sign-in. We help you setup security access governance policies that automatically apply security measures, such as blocking an access request, requiring a password reset or step up to MFA when a sign-in is deemed risky or particular policy conditions are met.



**Application  
security measures**



**Identity protection**



**Access governance**



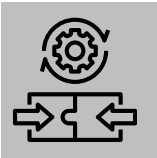
**Conditional  
Access Gateway**



# HOW TO MANAGE & SECURE APPS WITH RAINBOW SECURE

---

Rainbow Secure makes it simple to stay in control and reduce security and IT support costs using automation, self-service, and policy enforcement.



## Rainbow Secure integrations

Rainbow Secure is a Single Pane of Glass for securing and managing access to all cloud and on premise custom apps. Rainbow Secure provides technical services and integrations to help you automate the creation, maintenance, and removal of user identities in popular SaaS applications based on source of identity truth you adopt. You can automatically create new accounts in the right systems for new people when they join your team or organization. When people leave a team or organization, you can set policies that will automatically deactivate their accounts from the right systems. By automating these tasks, you can ensure that the identities in your apps and systems are kept up-to-date based on changes in the directory, your team, or your HR system, reducing errors and time.



## Secure hybrid access

Rainbow Secure helps you give access to your organization's resources by providing access rights to a single user or to an entire user group in identity store (Rainbow Secure Identity, Azure AD, Okta or other 3rd party Identity Store). Using groups lets the resource owner set access permissions for all the members of the group, instead of having to provide the rights one-by-one. This is a more secure method as you are less likely to accidentally give an individual inappropriate access, and it can save you time. You can also dynamically scale your group management by having enrollment be automated through identity attribute based policies.”

# HOW TO MANAGE & SECURE APPS WITH RAINBOW SECURE

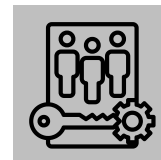
---

Rainbow Secure makes it simple to stay in control and reduce costs using automation, self-service, and policy enforcement.



## Automated provisioning

Industry standard architecture and white glove premium tech support makes it easy to configure and connect any one of the hundreds of pre-integrated apps to your tenant. These apps all support a SSO experience, and it is simple to configure the apps for Rainbow Secure Conditional Access on a per-app basis or for enterprise-wide policies. Once you've added the app and configured it for your needs, users with authorized access can easily find it in the Rainbow Secure SSO Apps portal, a centralized portal for end-user app discovery and launch.



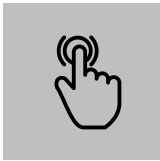
## Group management

Use Rainbow Secure Identity & Access Management Module to sync with user groups defined in Azure AD or your choice of 3rd party identity store and gain the centralization and security benefits of security access governance.

# HOW TO MANAGE & SECURE APPS WITH RAINBOW SECURE

---

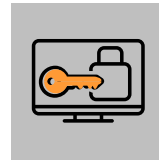
Rainbow Secure makes it simple to stay in control and reduce costs using automation, self-service, and policy enforcement.



## Simplified user access

Some tasks don't require an IT professional to complete, and Rainbow Secure Identity Management Module lets you delegate those to others in the organization. You can empower team, department or project leads to create and manage their own security groups in Rainbow Secure Identity Management Module. Group owners can approve or deny membership requests, or they can delegate control of group membership.

Users can also discover and explore the breadth of their access from the Rainbow Secure SSO (Single Sign on) Apps portal, and easily SSO to any app they have been granted access to. My Apps will show any SaaS app, on-premises app, and custom app as well as key corporate portals where access has been granted on a per-user basis or per-user group basis and apps can be grouped into collections to streamline visibility.



## Modernize authentication with stress free security

Use next gen multi-layer multifactor graphical security to provide secure stress free end-user security experience to SaaS and your custom apps connected through the Rainbow Secure SSO application gallery. Users can login and verify using Colors and Styles powered Rainbow Secure Password or passwordless zero-trust OTP login methods. Businesses are protected against 10+ types of cyber threats including brute-force, phishing, keylogger, password reuse, credential stuffing attacks, DDOS Ransomware and cyber frauds.

Rainbow Secure Advanced Threat Protection module protects systems from advanced cyber threats and BOT attacks using AI Monitoring, Risk Analytics and Threat alerting.

Further leverage the security collaboration benefits by optionally integrating with 3rd party threat intelligence sharing platforms.

# SECURE ANY APP, ON ANY CLOUD USING RAINBOW SECURE, GAIN COST SAVINGS AND PRODUCTIVITY

Over 100+ active, unique apps connected.

Get started today

[www.rainbowsecure.com](http://www.rainbowsecure.com)

