arcon

Predict | Protect | Prevent

Converged Identity Platform

ARCON Converged Identity Platform: Unravelling the Conundrum of Fragmented Digital Identities

Foreword

Organizations worldwide are embracing digital transformation for higher productivity, agility, and faster innovation. In pursuing digital excellence, cloud-based technologies, hybrid data center setups, and multi-cloud environments have become pivotal to any organization's broader operations strategy as they enable them to scale quickly and efficiently.

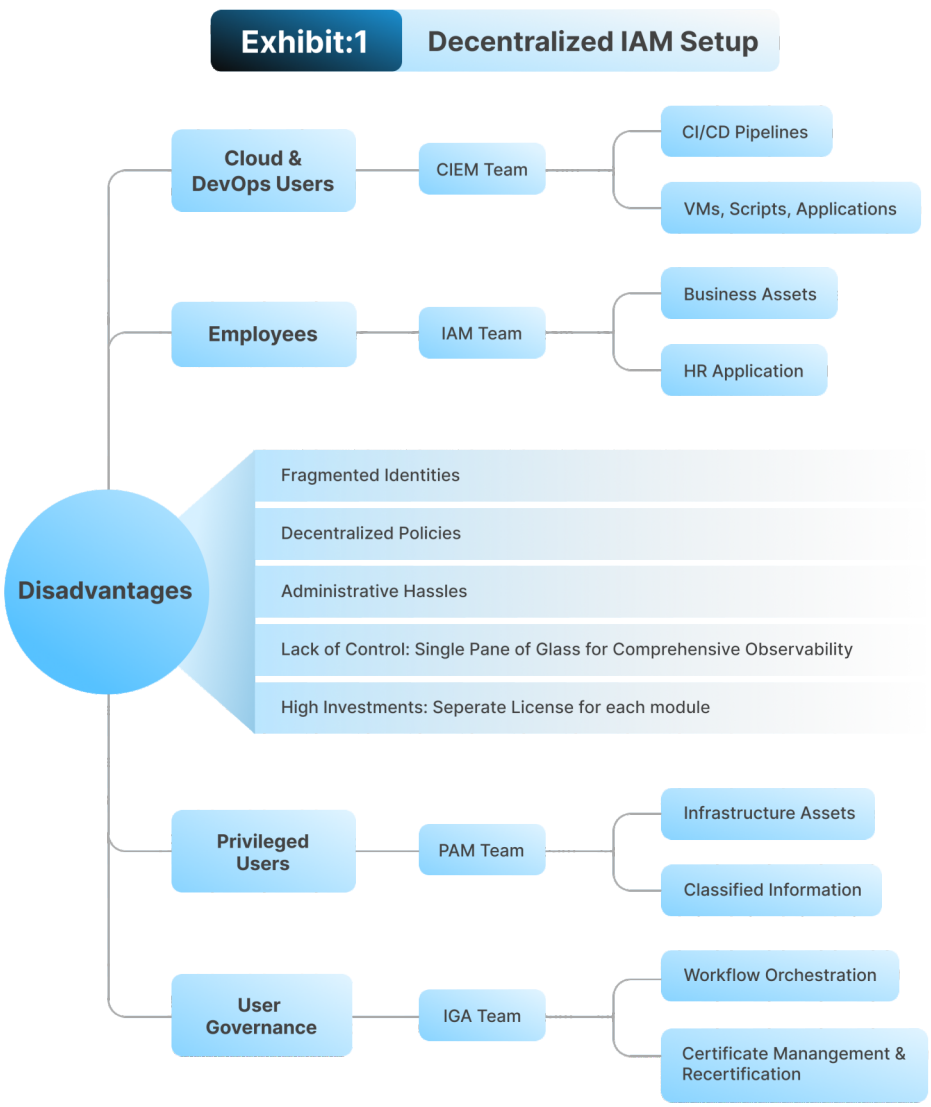
In the given context, importantly, an identity-first security approach has become extremely important. Indeed, when we analyze a typical IT (Information Technology) environment, we will find that an identity is no longer confined to a particular perimeter. Hundreds and thousands of decentralized identities are constantly interacting with distributed computing resources. As a result, many organizations are in a difficult position because decentralized identities result in decentralized polices and controls as well as a lack of context-based identity management.

In other words, what is happening is that organizations, amid digital transformation, have created a large expanse of IT infrastructure realm that operates in silos with multiple access points. Consequently, the traditional IAM architecture has metamorphosed into fragmented structures. Such fragmented architectures are insufficient to manage digital identities, their lifecycles, and their entitlements in a seamless, holistic, and secure manner. It has expanded the identity-based attack vector and led to administrative hassles.

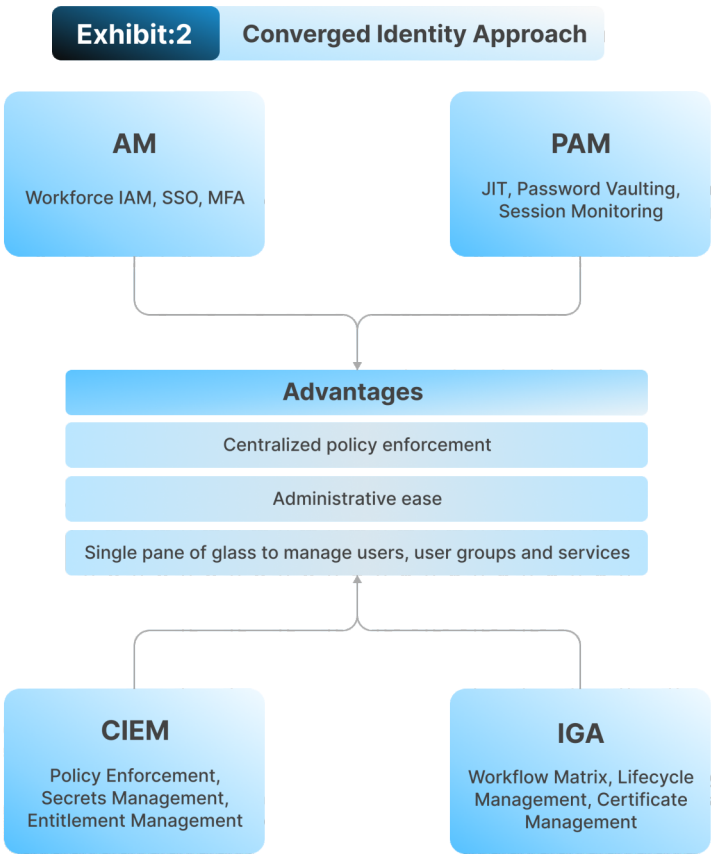
Against this backdrop, it has become imperative for modern organizations to break down barriers created by siloed IAM approach and move towards a converged identity approach that ensures the development of a robust IAM architecture with centralized policy enforcement and controls. It is about time that organizations started treating each identity as a perimeter.

Time to Entwine Access Management Tools in Conjunction: Why Converged Identity is the Future of Identity and Access Management?

The sheer pace at which users and corresponding services are created to administer a wide range of identity-based use cases makes it exceedingly difficult from an administrative point of view. While some use cases are connected to each other, others are unique. For example, organizations deploy Privileged Access Management (PAM) to administer privileged access, IAM for general access management use- cases, and IGA tools to manage the lifecycle and governance of identity alongside ensuring MFA. When done separately in standalone solutions, it is a cumbersome IT administrative process with higher investments and lacks dynamism that is necessary in today's high-velocity access management environment.



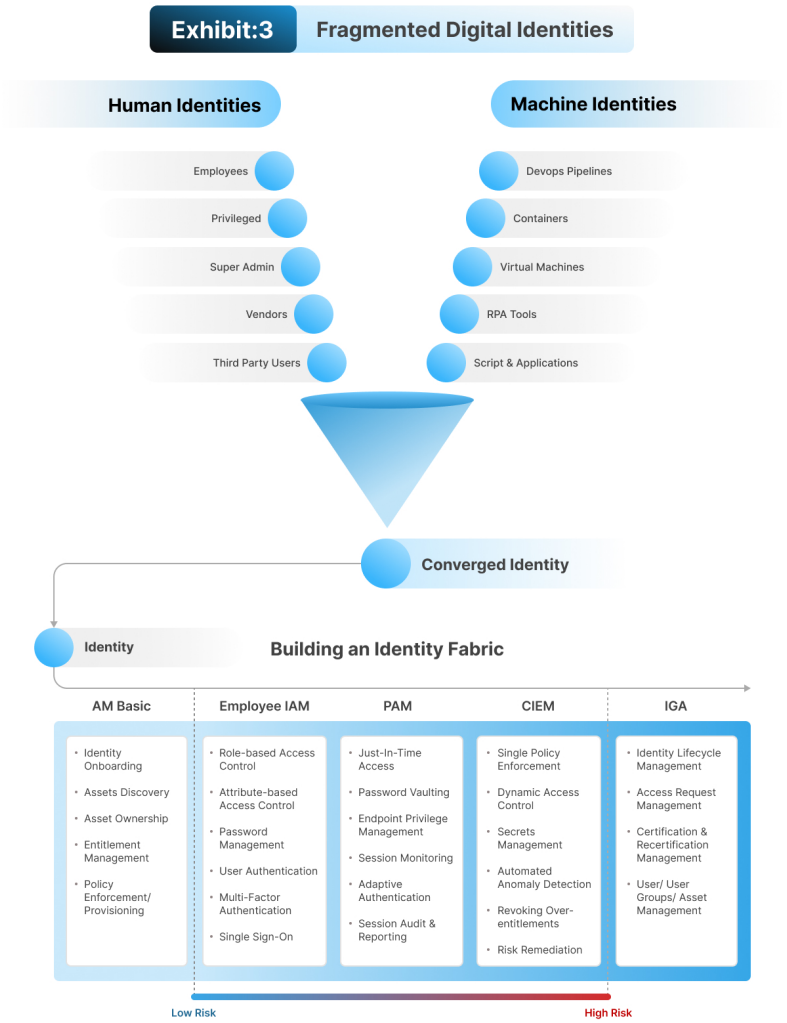
A converged identity approach, on the other hand, provides a single pane of glass to get the complete observability of a digital identity environment, i.e., all human and non-human identities together. It enables entwining all distinct identities under one centralized engine for administering connected or unique use cases at an enterprise level across distributed, hybrid, and heterogeneous IT environments.



The Crux Behind Developing ARCON Converged Identity Platform: Building an Identity Fabric for a Holistic and Robust IAM Structure

The conventional IAM approach depends on legacy methods to manage users, assets, and services. These methods, being static protection methods and lacking dynamic access controls, are insufficient to manage a growing number of applications and services distributed in high-velocity hybrid environments.

Building an identity fabric, on the other hand, ensures a set of processes that allow you to manage users and their entitlements with flexibility across all layers of IT infrastructure. By implementing converged identity, organizations can establish an integrated identity fabric that is secure, interoperable, and provides continuous and context-aware controls as well as centralized management of decentralized identities.



Privileged Access Management (PAM): The PAM module provides capabilities to navigate through all the classic PAM use cases such as credentials vaulting and randomization, auto discovery of assets and onboarding users, fine-grained access control, just-in-time privileges, session management and monitoring as well as customized reporting for audit purposes.

Cloud Infrastructure and Entitlements Management (CIEM): The CIEM module provides capability to address all the advanced functional use cases on the cloud. From vaulting and rotating secrets to secure workloads and DevOps pipelines, the CIEM module offers capabilities for controlling, monitoring, and managing cloud entitlements including risk-based alerts to control overprivileged entitlements and sprawls across multi-cloud environments.

Endpoint Privilege Management (EPM): The EPM module enables organizations to manage the critical business applications in fine-grained control manner ensuring rule-based access to business assets and provides Privilege Elevation and Delegation Management (PEDM) capability for Windows, Linux/Unix and MacOS environments. The EPM module, in addition to RBAC controls offers AI and ML leveraged user behavior analytics to mitigate the risk of anomalous activities; that is, those risky identities that deviate from baseline activities as mandated by the management.

Workforce Identity and Access Management (IAM): The workforce IAM module enables to manage and control users' runtime access to web applications and APIs whilst ensuring authorization and authentication using MFA and SSO controls.

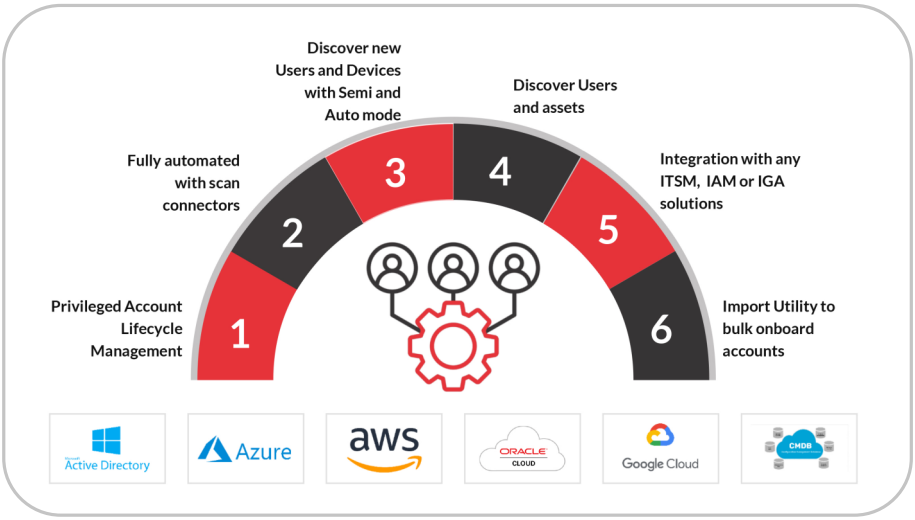
Identity Governance and Administration (IGA): The IGA module enables organizations to manage a complex range of access rights for users, user groups, services, assets, and asset groups. Whether enterprise identity repositories in on-premises data centers or on-cloud, the IGA module supports identity lifecycle management, workflow orchestration and certificate management.

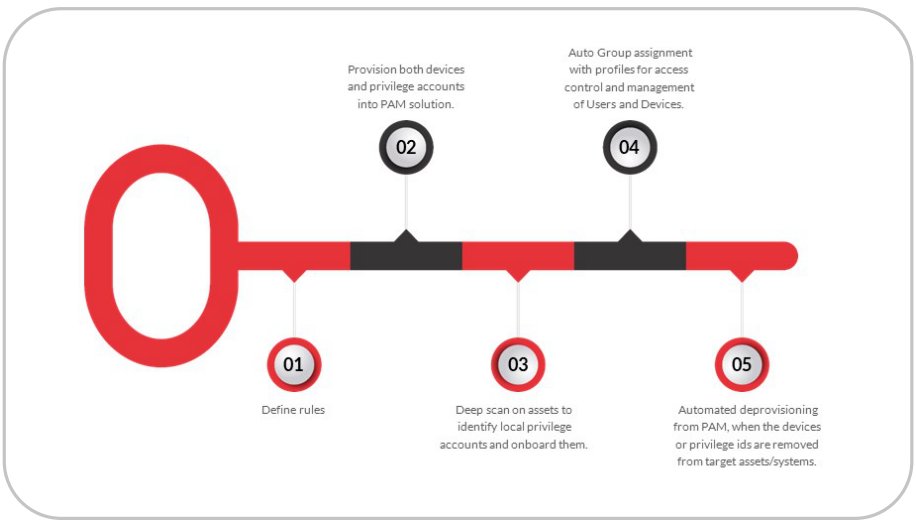
**Additional License Required for EPM and CIEM*

ARCON | Converged Identity Platform

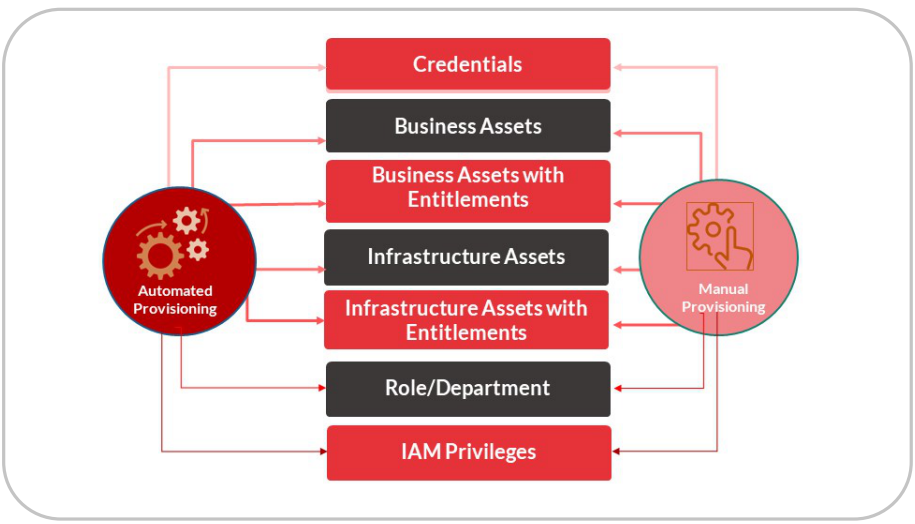
Key Features

Auto-onboarding





Automated & Manual Provisioning



Provisioning / De-provisioning Digital Identities

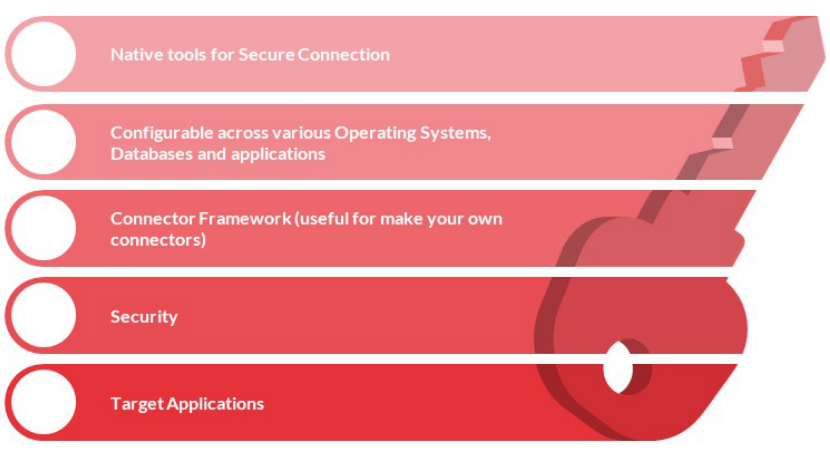
- Run on-demand & Detect all digital identities
- Correlate with existing on-boarded users
- Classify Accounts into:
  - Local/Domain
  - Privileged/Non-Privileged
- Deprovision dormant user accounts
- Handling Transfer Use Cases

Supporting Industry Standards:

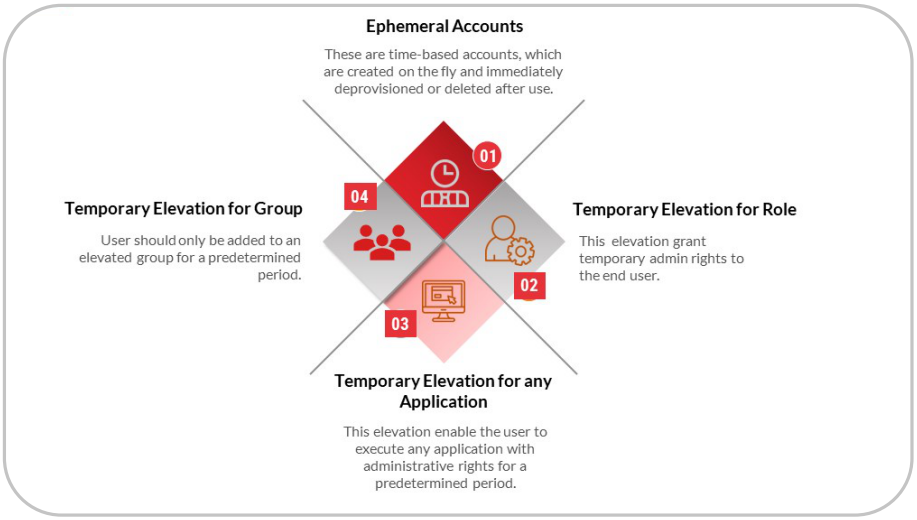
- ✓ SCIM
- ✓ ODBC
- ✓ REST API
- ✓ ARCON Secure Authentication
- ✓ LDAP
- ✓ Scripting
- ✓ SDK

Connector Suite

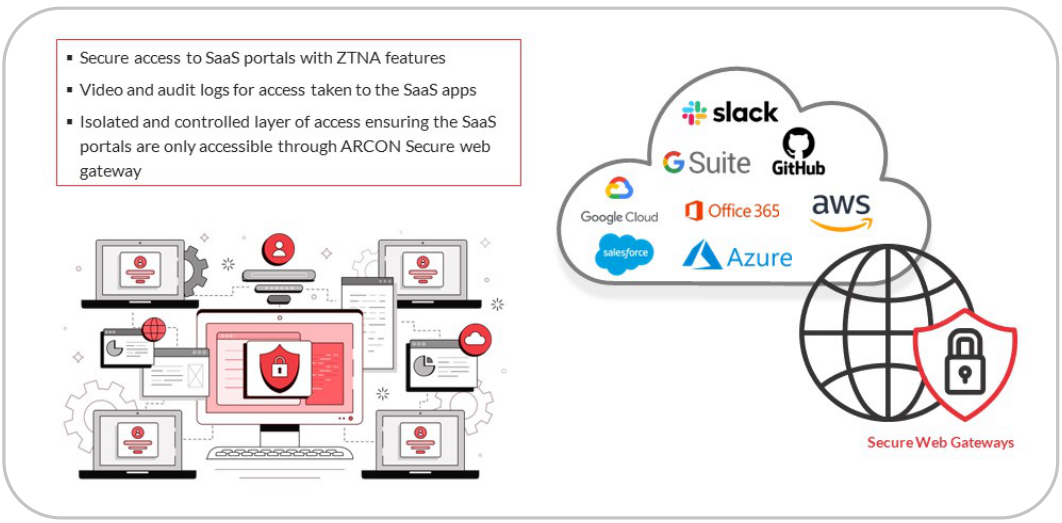
Single Sign-On (Auto Logon)



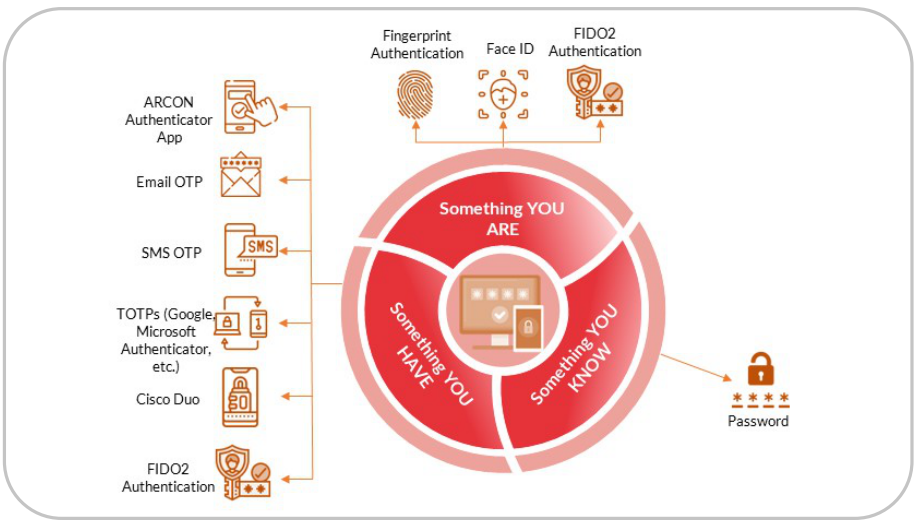
Just-In-Time



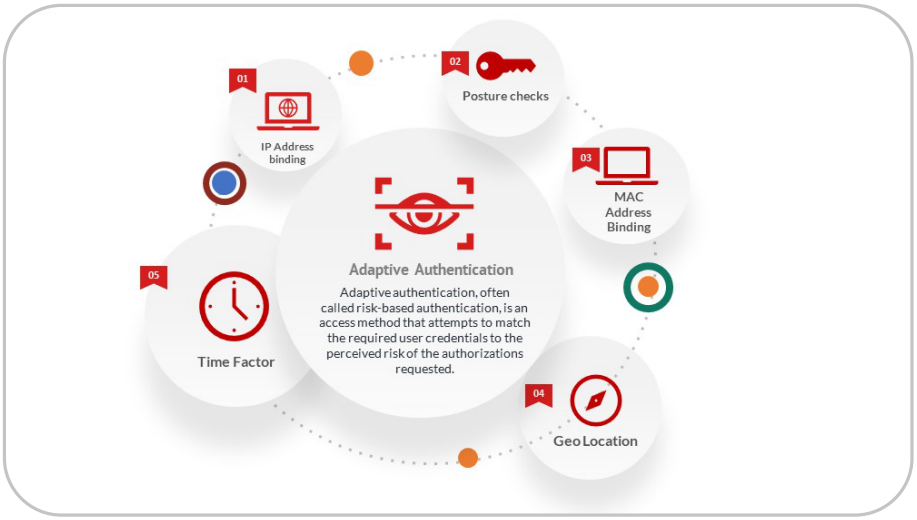
Secure Web Gateways (third party remote access)



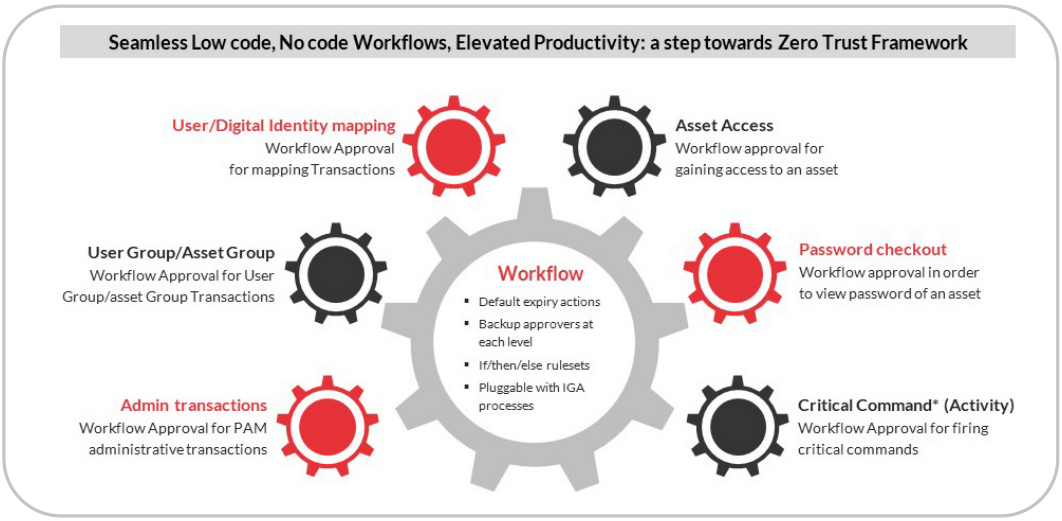
Multi-Factor Authentication



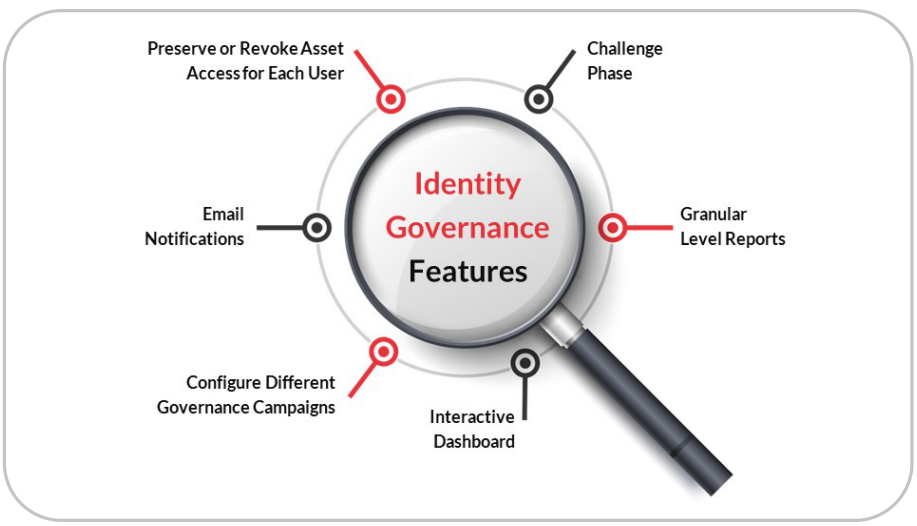
Adaptive Authentication



Workflow

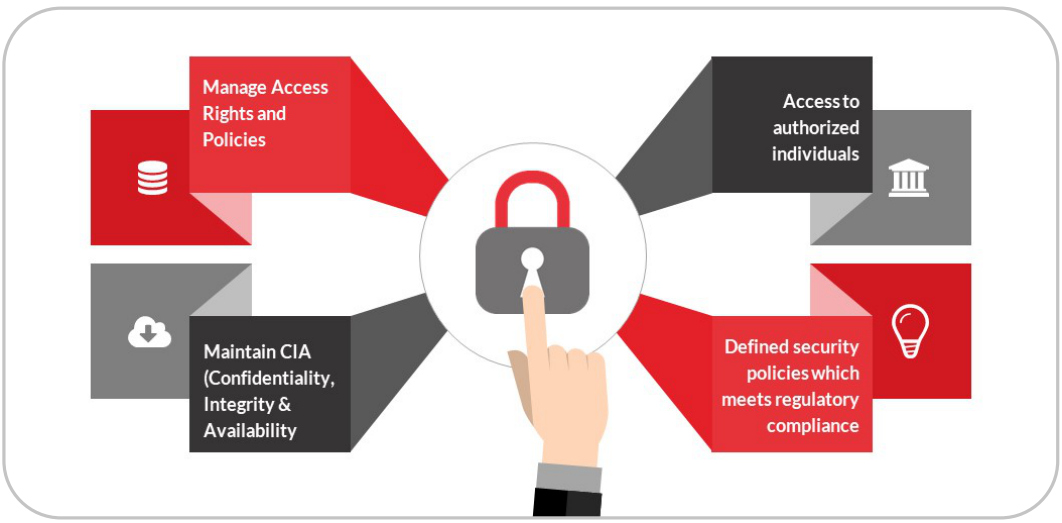


Identity Governance



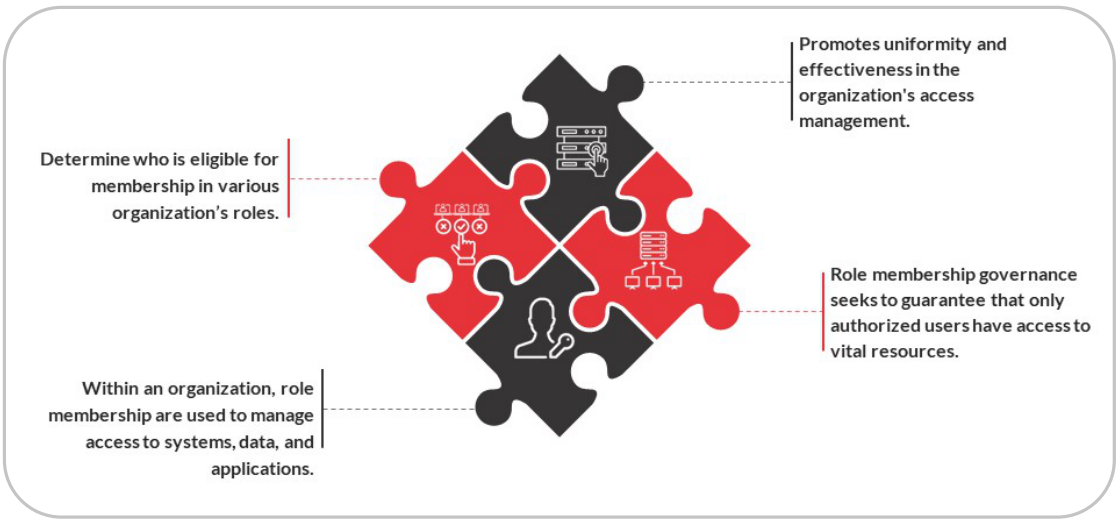
Human Identity Governance

Access Governance

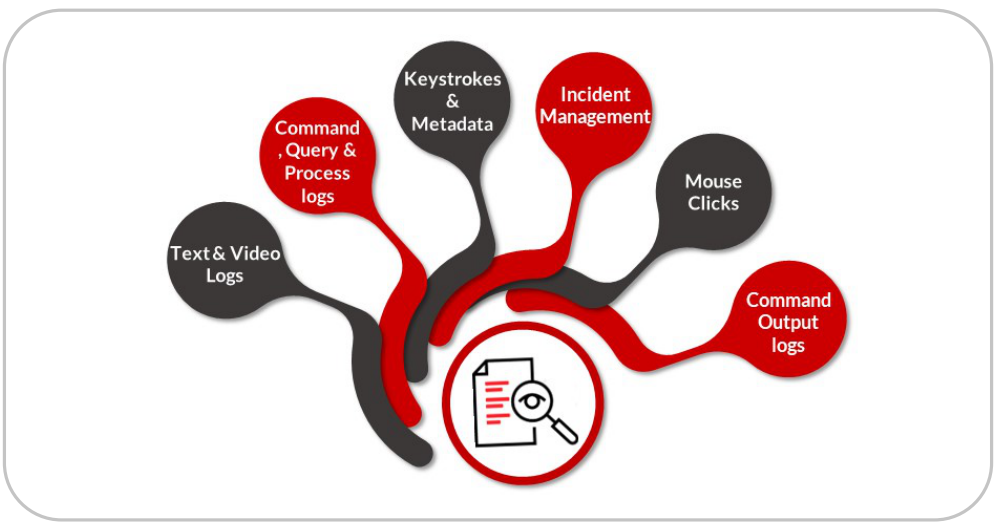


Asset Governance

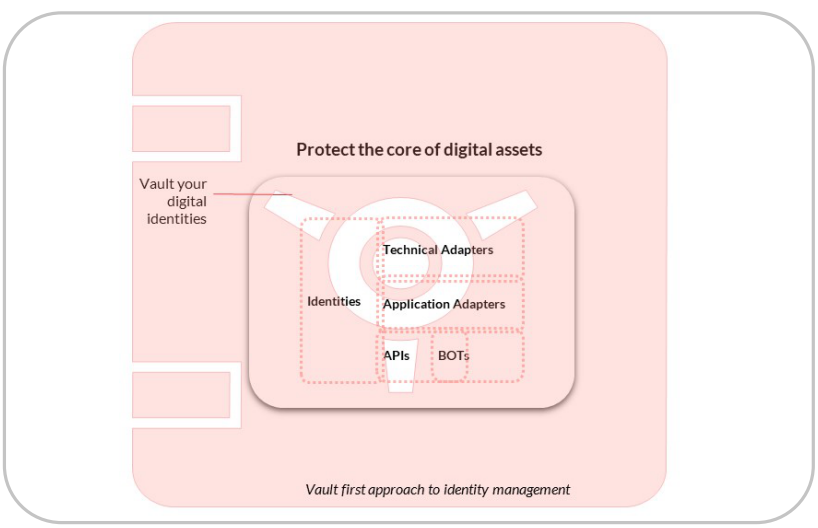
Role/Department Governance



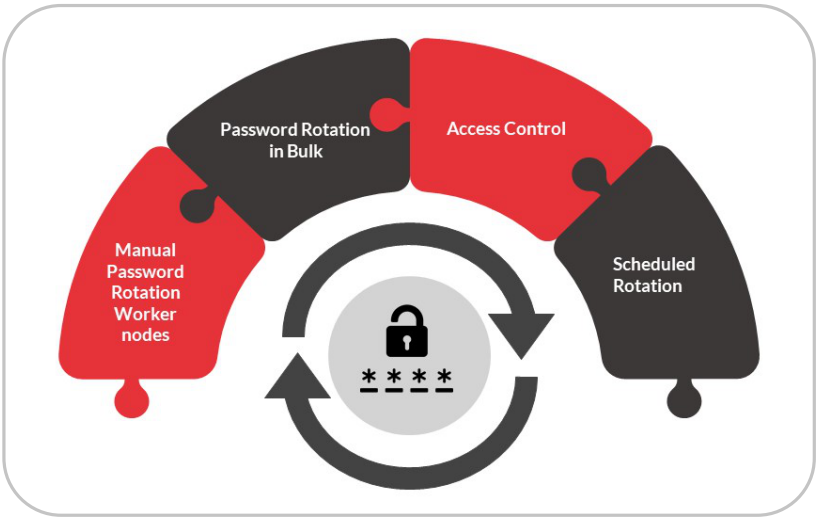
Reporting & Analytics



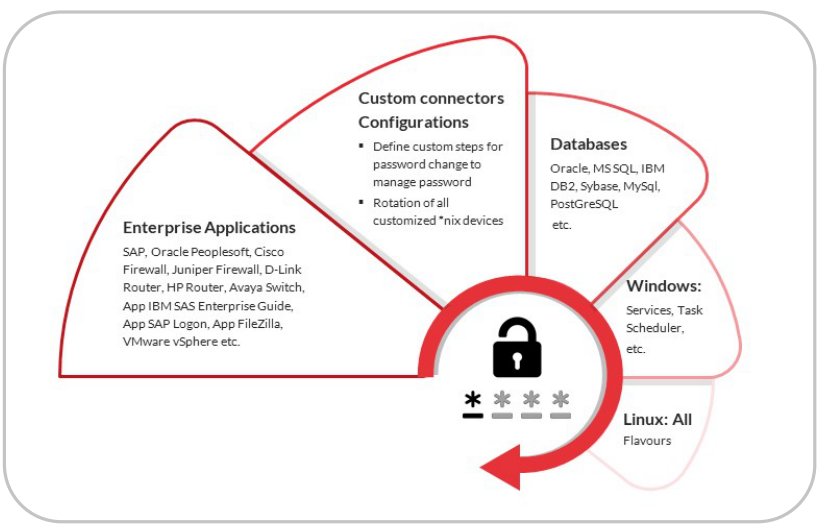
Identity Vault



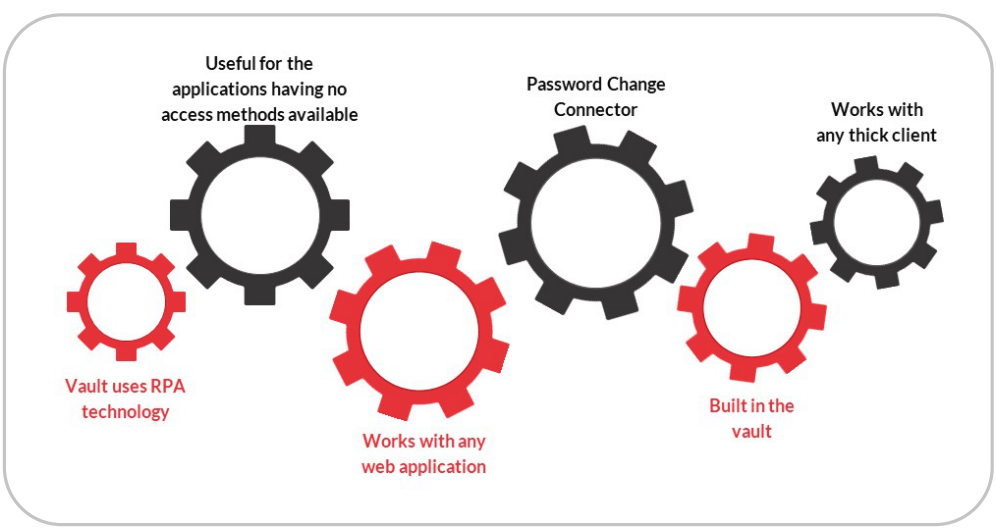
Password Rotation



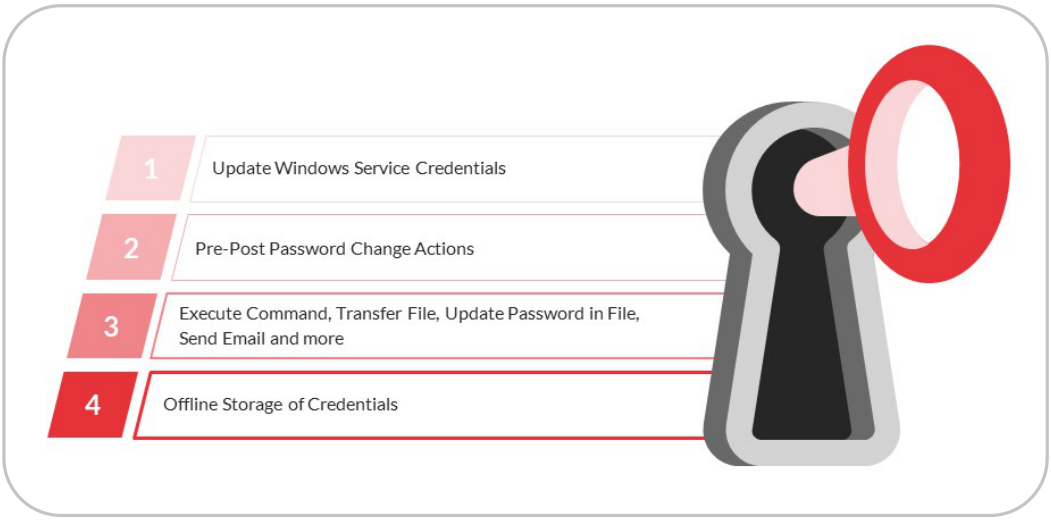
Password Rotation | Supported Connectors



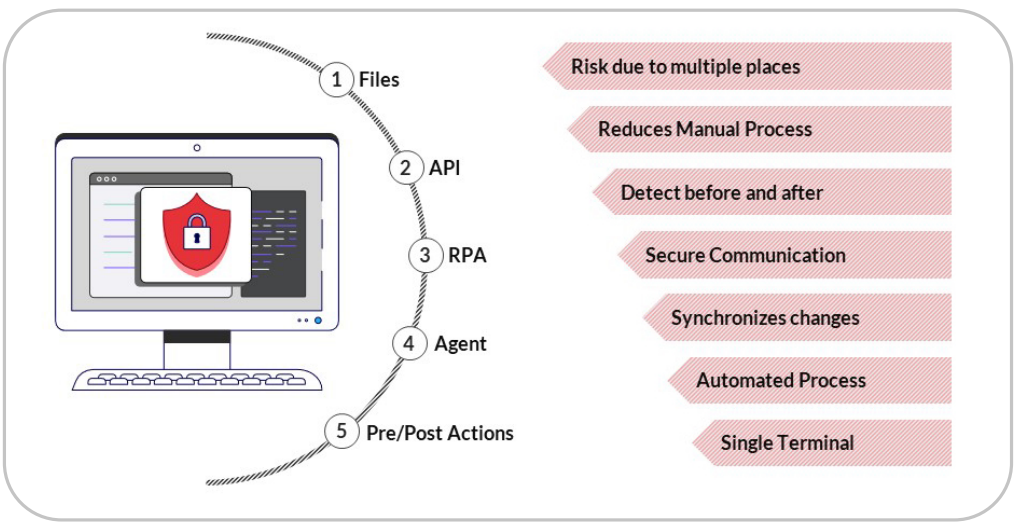
Password Rotation | RPA



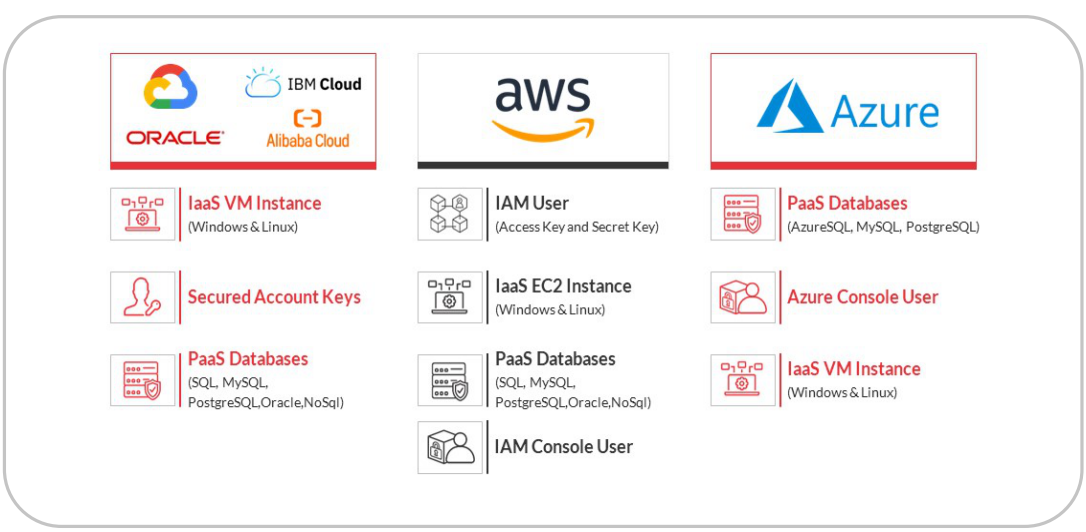
Advanced Credential Management



Application to Application

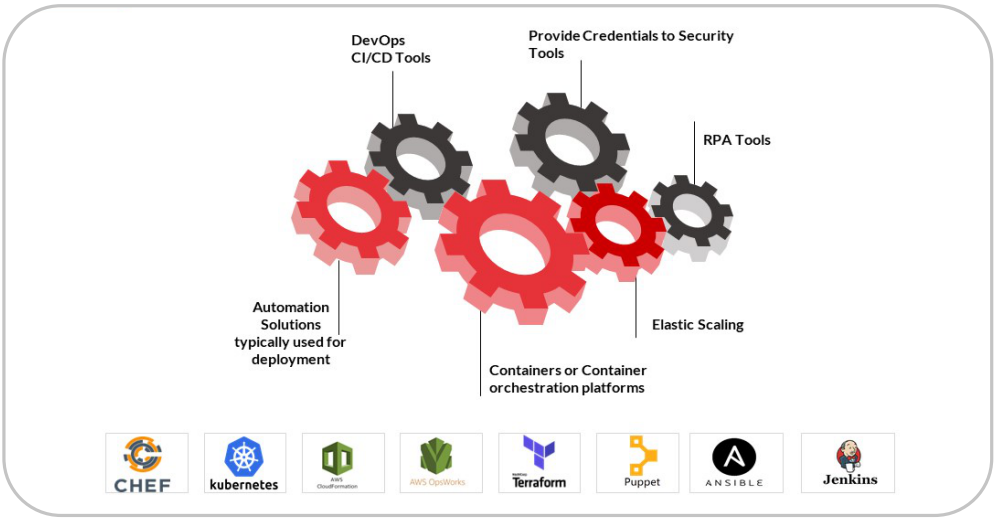


Credential Management

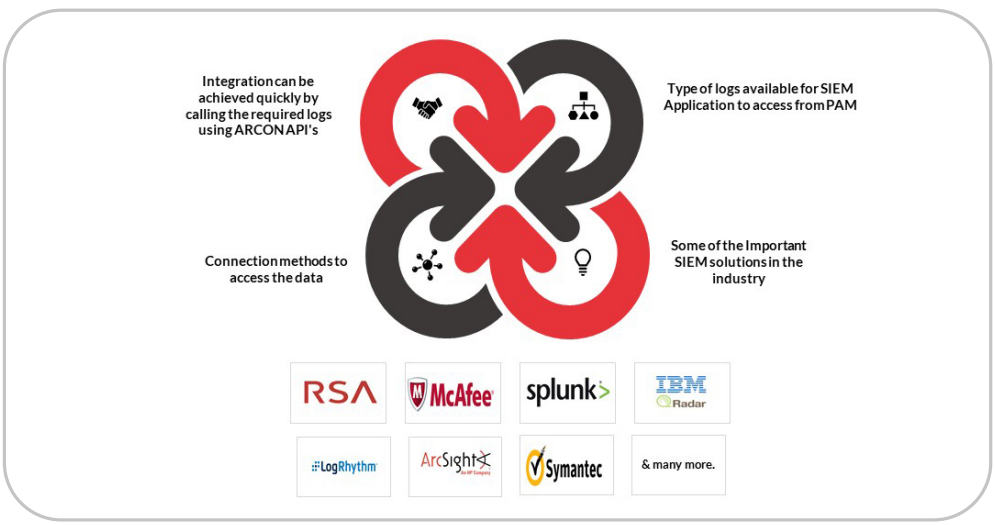


arcon

Integrations- Developer Tools & IaaC

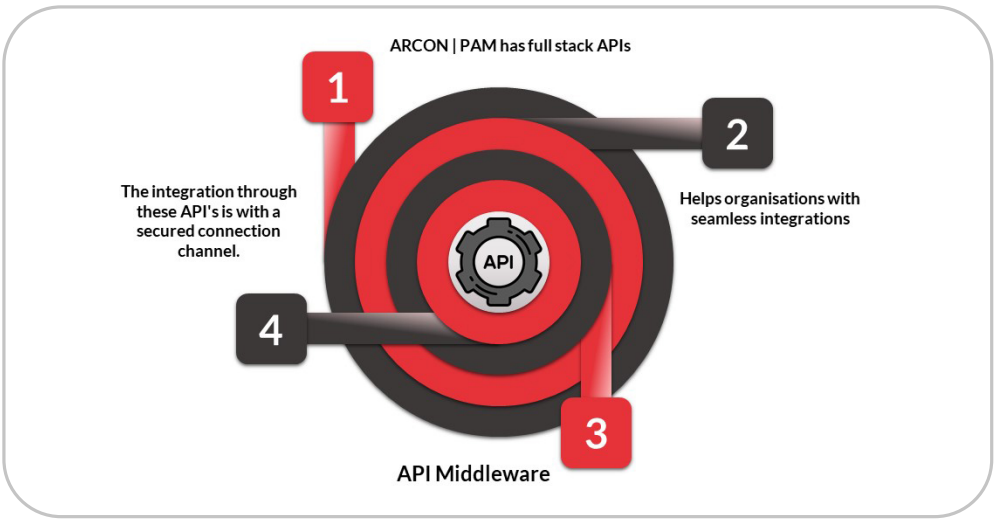


SIEM Tools

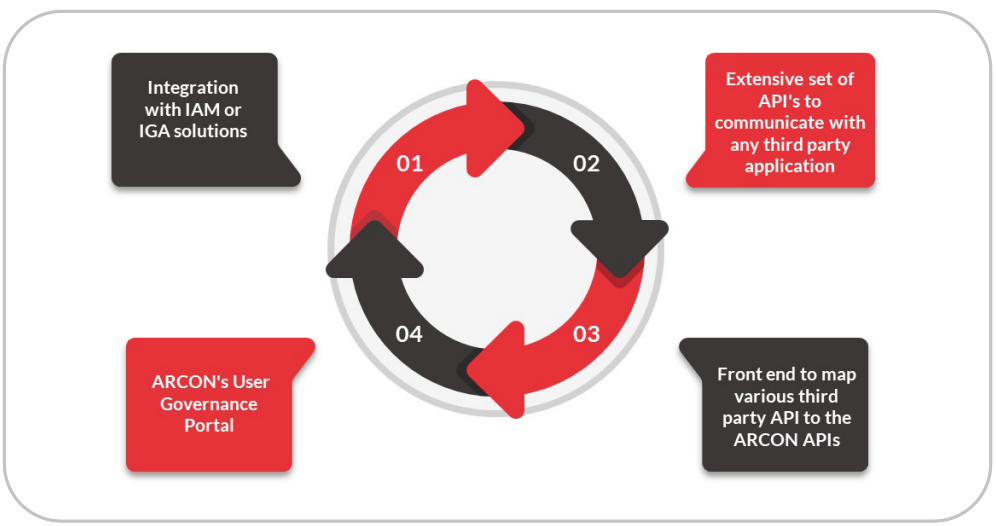


SAML, LDAP, OAuth, OIDC based Integrations

API Integration

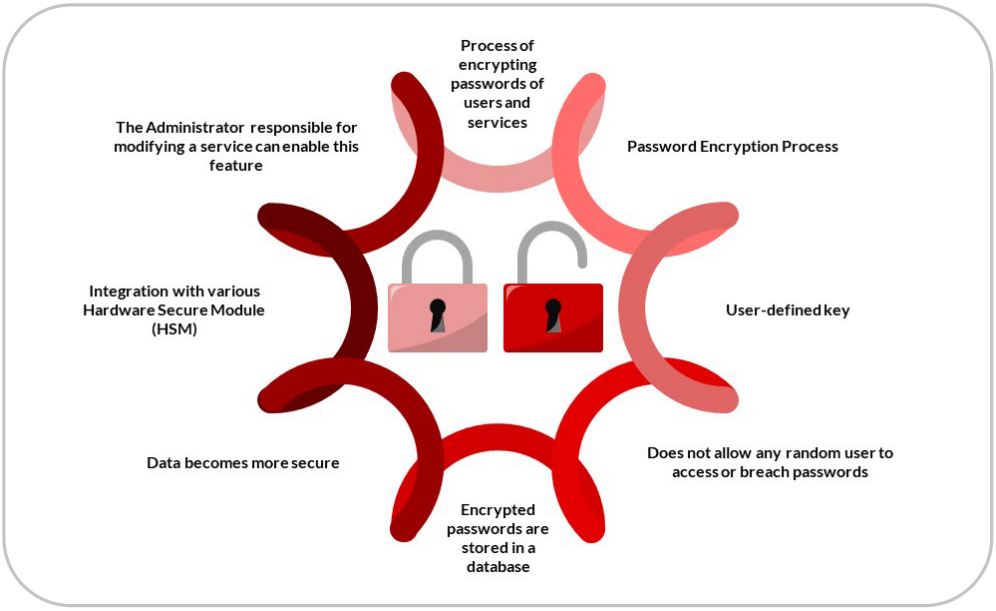


Lifecycle Management Tools

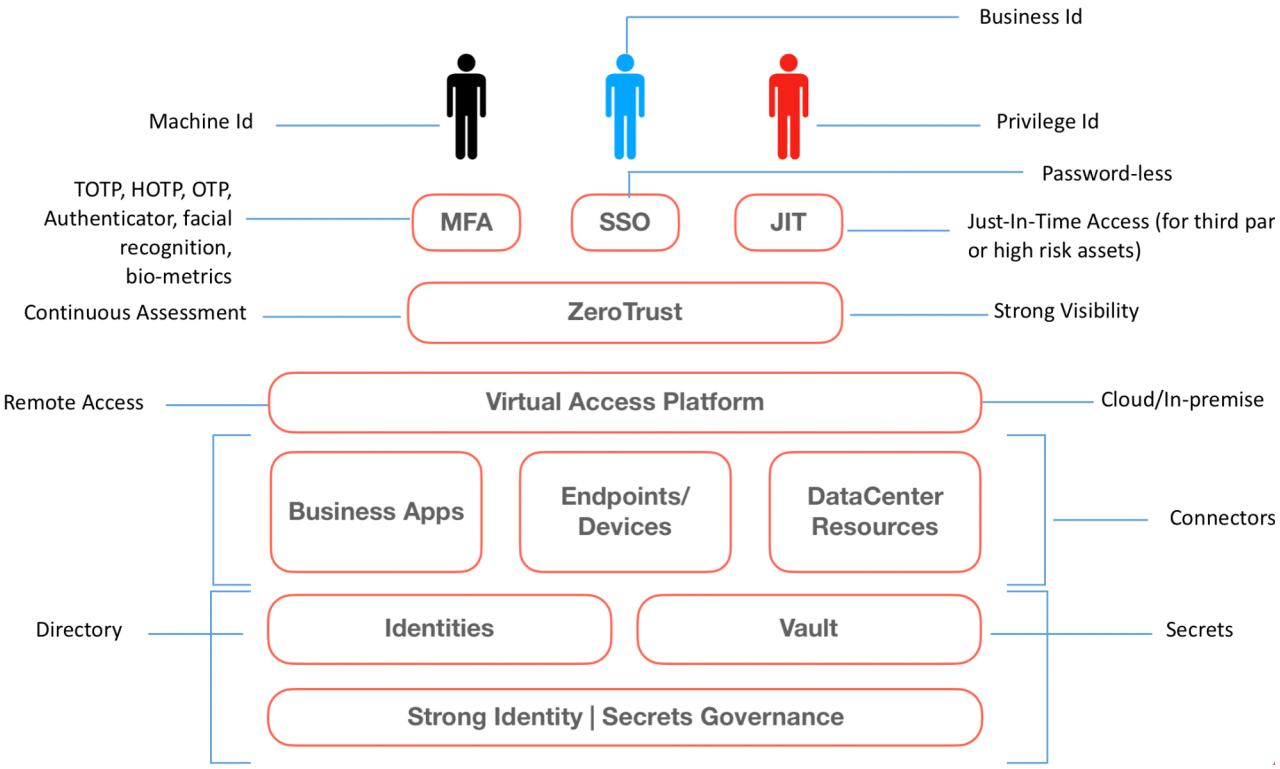


Other Integration Tools Examples

Multi Level Data Encryption with HSM Tools



Converged Identity at a glance



About ARCON

ARCON is a leading enterprise information risk control solution provider, specializing in Privileged Access Management (PAM) and continuous risk assessment solutions. Our mission is to help enterprises identify emerging technology risks and help mitigate them by robust solutions that predict, protect and prevent.