Identity and Access Management

Table of Contents

Contents

Introduction to Identity and Access Management

What it is, and why it's so critical at a high level, indentity and access management refers to the process of creating, managing and using digital identities and for administering access policies. Indentity and access management is comprised of both processes and the infrastructure and services required to support those activities. Through advanced indentity and access management, organizations can establish efficient, federal control and visibility.

In today's promptly changing business and it landscape, primarily new security requirements have developed. Within a few years, organizations have moved from running fundamentally on-premises, tightly controlled environments, to depend on a highly dynamic, distributed network comprised of cloud services, big data environments, mobile applications, the internet of things (iot) and more.

The result is that sensitive resources and systems are increasingly interconnected and wide-open. It teams used to be able to build security systems and processes around the idea of a perimeter. Comprehensive data breaches continue to make headlines, and ransomware, spear phishing and many other threats continue to outbreak businesses. While contending these threats requires a significant and ongoing dedication of budgets and resources, these investments can pastel in comparison to the overwhelming fines associated with data breaches—which can necessitate lost customers and revenues, fines and civil lawsuit. Further, across regions and industries, confidentiality regulations and compliance dictates continue to grow more rigorous, which can further worsen these fines.

Authentication:

Authentication is encompassed of authentication management and session management. Authentication is the module through which a user provides necessary credentials to gain primary access to an application system or a specific resource. Once a user is authenticated, a session is created and referred during the interface between the user and the application until the user logs off or the session is dismissed by other means (e.g. timeout). The authentication element usually comes with a password provision module when the userid / password authentication method is used. By centrally keeping the session of a user, the authentication module provides Single Sign-On service so that the user does not need to logon again when accesses another application or system governed under the same Identity and Access Management Framework.

User Management:

Authentication is encompassed of authentication management and session management. Authentication is the module through which a user provides necessary credentials to gain primary access to an application system or a specific resource. Once a user is authenticated, a session is created and referred during the interface between the user and the application until the user logs off or the session is dismissed by other means (e.g. timeout). The authentication element usually comes with a password provision module when the userid / password authentication method is used. By centrally keeping the session of a user, the authentication module provides Single Sign-On service so that the user does not need to logon again when accesses another application or system governed under the same Identity and Access Management Framework.

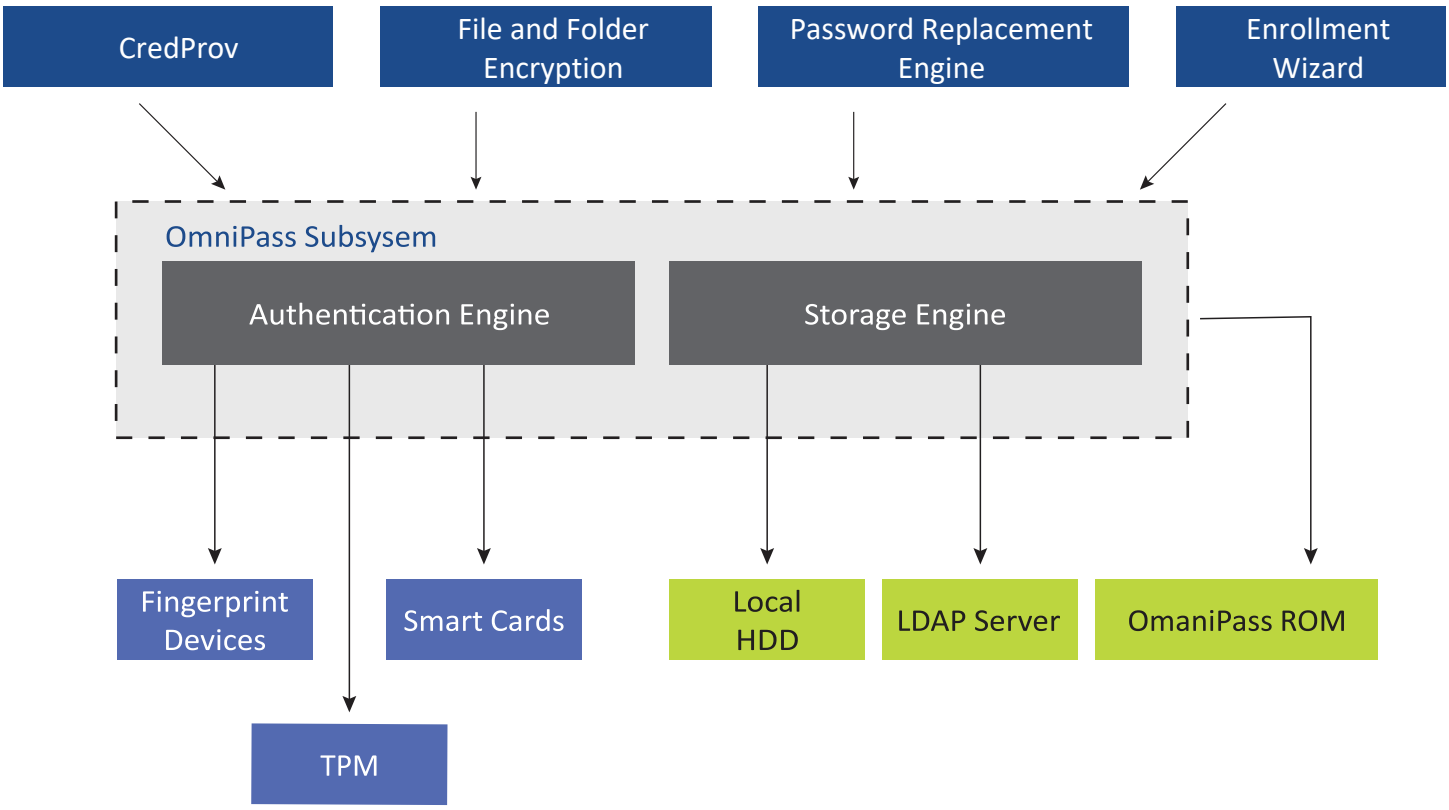
Authorization:

Authorization is the element that defines whether a user is legitimate to access a specific resource. Authorization is performed by scrutiny the resource access request, usually in the form of an URL in web-based application, against authorization rules that are stored in an IAM policy store. Authorization is the core module that outfits role-based access control. Additionally, the authorization model could provide multifarious access controls based on data or information or policies including user attributes,user roles/ groups, actions taken, access channels, time, resources requested, external data and business rules.

Central User Repository:

Central User Repository provisions and delivers identity data to other services, and provides service to verify credentials acquiesced from clients. The Central User Repository grants an aggregate or coherent view of identities of an enterprise. Directory services adopting LDAPv3 standards have become the foremost technology for Central User Repository. Both Meta-directory and Virtual directory can be used to manage incongruent identity data from different user repositories of applications and systems. A meta-directory typically provides a comprehensive set of identity data by amalgamation of data from different identity sources into a meta-set. Generally, it comes with a 2-way data synchronization service to keep the data in sync with other identity sources. A virtual directory delivers a unified LDAP view of associated identity information, behind the scene several databases containing different sets of users are united in real time.

Uniting Identity and Access Management



Enterprise SSO (Single Sign-On)

With Enterprise SSO, passwords are entered and renewed automatically. Users save time and access their applications with no boundaries. Their applications are not reformed, either Windows software or web applications: The Windows domain, CRM portal, or SAP applications, Workforces can get on with their work without distressing about forgotten passwords, and without having to change them regularly according to ever more multifaceted criteria: special characters, length, case, etc.

Ease Access Privileges Administration

By unifying usernames and passwords, Enterprise SSO allows Administrators to expend less time on password management tasks. Handing users for dozens of applications has become time-consuming and also a financial handicap for the company. So certain application, while other have dedicated user bases.

Increase access security

Enterprise SSO eradicates one of the plagues of security: bypassing password procedures. Now, users no longer have to remember a multitude of credentials. They simply have to remember their main password. Enterprise SSO makes it needless to write a password, or share it with a colleague if they overlook theirs. It also avoids numerous use of the same password for some applications. For even greater security, the corresponding Authentication Manager component brings suppleness and effortlessness to managing and using strong authentication methods (smartcards, OTP tokens, biometrics, etc.)

Streamline technology for users

With Enterprise SSO, passwords are entered and renewed automatically. Users save time and access their applications with no boundaries. Their applications are not reformed, either Windows software or web applications: The Windows domain, CRM portal, or SAP applications, Workforces can get on with their work without distressing about forgotten passwords, and without having to change them regularly according to ever more multifaceted criteria: special characters, length, case, etc.

Provide perceptible ROI

Enterprise SSO allows real and quantifiable savings to be certainly made. The ROI generally allows you to recover procurement costs within a year. The reduced time spent on data entry improves the performance of critical employees. And the reduction in the number of calls related to forgot passwords significantly reduces the cost of maintenance.

OmniPass Enterprise Solution

Minimize Employee Password Resets with OmniPass Enterprise Solution.

OmniPass Enterprise will remember your employee's logins and reduce the number of password reset-related help desk calls, resulting in more employee up-time, increased productivity and a reduction expensive support calls.

Multi-Factor Authentication Support

Support true multi-factor authentication using a wide variety of 2-factor devices such as fingerprint readers, smart cards, palm vein readers, tokens, etc., increasing your company's security policies while making the compliance auditors happy.

Gain Control of your Company Logins

Manage all of your employee passwords and logins from a single console to know exactly who is accessing your corporate information.

Simple Integration with your company server

OmniPass Enterprise SSO installs quickly and easily into your Active Directory server.

Works within your processes

Roaming employees can sign in from any PC, using any authentication device.

Meet Compliance

Let OmniPass Enterprise SSO help you get ready for your next HIPPA or Sarbanes Oxley audit by creating comprehensive auditing reports tracking logins, access to workstations, websites, applications anywhere sensitive data may reside.

About Infopercept - Infopercept is one of the fastest-growing comprehensive cybersecurity companies in India, serving global clients. It provides platform led managed security services that covers all areas of cybersecurity, including defensive, offensive, detection and response, and security compliance. Infopercept has its own cybersecurity platform, 'Invinsense,' which integrates tools such as SIEM, SOAR, EDR, deception, offensive security, and compliance tools. Its cybersecurity and MDR services include dedicated teams of experts, ensuring that organizations have 24x7 cybersecurity operations support.

Imprint

Publisher

3rd floor, Optionz Complex, CG Rd, Opp. Regenta Hotel, Navrangpura, Ahmedabad, Gujarat 380009, INDIA

Contact
sos@infopercept.com
www.infopercept.com/knowledge/whitepapers