Hexnode Identity and Access Management Solution

Executing access controls over corporate assets

Key benefits

▸ Automate and secure access to mission-critical corporate data.

▸ Ensure regulatory compliance throughout an enterprise.

▸ Reduce the possibilities of internal and external data breaches.

▸ Provide centralized access control and management.

▸ Enhance user experience.

▸ Minimize IT operational expenses.

Identity management (a.k.a. Identity and Access Management) concerns about a comprehensive scheme of policies and methodologies that provides an enterprise workforce with customized access to IT resources. Identity and Access Management secure the IT environment while monitoring the individual network users who utilize technology resources such as organizational data, tools, and devices. The intention of Identity and Access management (IAM) is to establish an improved workflow within the IT teams by managing the roles and access privileges of individual users incorporating both customers and employees in an enterprise.

Why Identity and Access Management?

The prominence of Identity and Access Management solutions has been increasing over the years. An Identity and Access Management system guarantees data protection by helping organizations set up specific guidelines and rules to secure and manage data access while fulfilling compliance requirements in the organization. The rising demands on regulatory compliance and data security standards address the necessity to maintain an IAM suite that monitors and controls user access over an entire enterprise.

Identity and Access Management with Hexnode MDM

With the IAM solution from Hexnode MDM, IT admins can automatically manage access controls and permissions specifically for each network users. This solution enhances business operational efficiency by minimizing the effort, time and expenses that would be needed to regulate the corporate data access. Hexnode's Identity and Access management solution offers seamless access to corporate data, apps, and authentication details while maintaining regulatory compliance requirements. Hexnode implements advanced security management by providing a central identity management platform for enforcing corporate policies and standards across every device and operating systems employed within an enterprise.

hexnode

Features of Hexnode Identity and Access Management

Enforcing authentication

- Controlling identity thefts and malicious attacks by enforcing strong password policies while sustaining all the corporate regulatory requirements.

- Enabling two-factor authentication (2FA) as an additional verification technique for securing all the critical data a user can access.

- Ensuring protected access to user data by the seamless integration of Hexnode with Microsoft Active Directory (AD) and Azure Active Directory (Azure AD).

- Preventing the need for memorizing complex passwords by substituting passwords with suitable certificates that can be applied directly to the MDM portal.

Maintaining security

- Enforcing automated and periodic compliance checks which assure that all the necessary corporate security controls are in place.

- Implementing containerization by creating a virtual container for corporate data.

- Executing system level encryptions for securing the critical company data from being accessed by unauthorized users.

- Remotely setting up VPN on devices for securing the network connectivity.

Managing applications

- Providing instantaneous access to required apps by creating custom app stores.

- Provisioning app catalogs and thus minimizing the time wasted searching for the required apps.

- Whitelisting and blacklisting apps ensure that only certain apps that sustain corporate standards and security are available for users.

- Remotely managing the app permissions to ensure the complete protection of a user.

hexnode