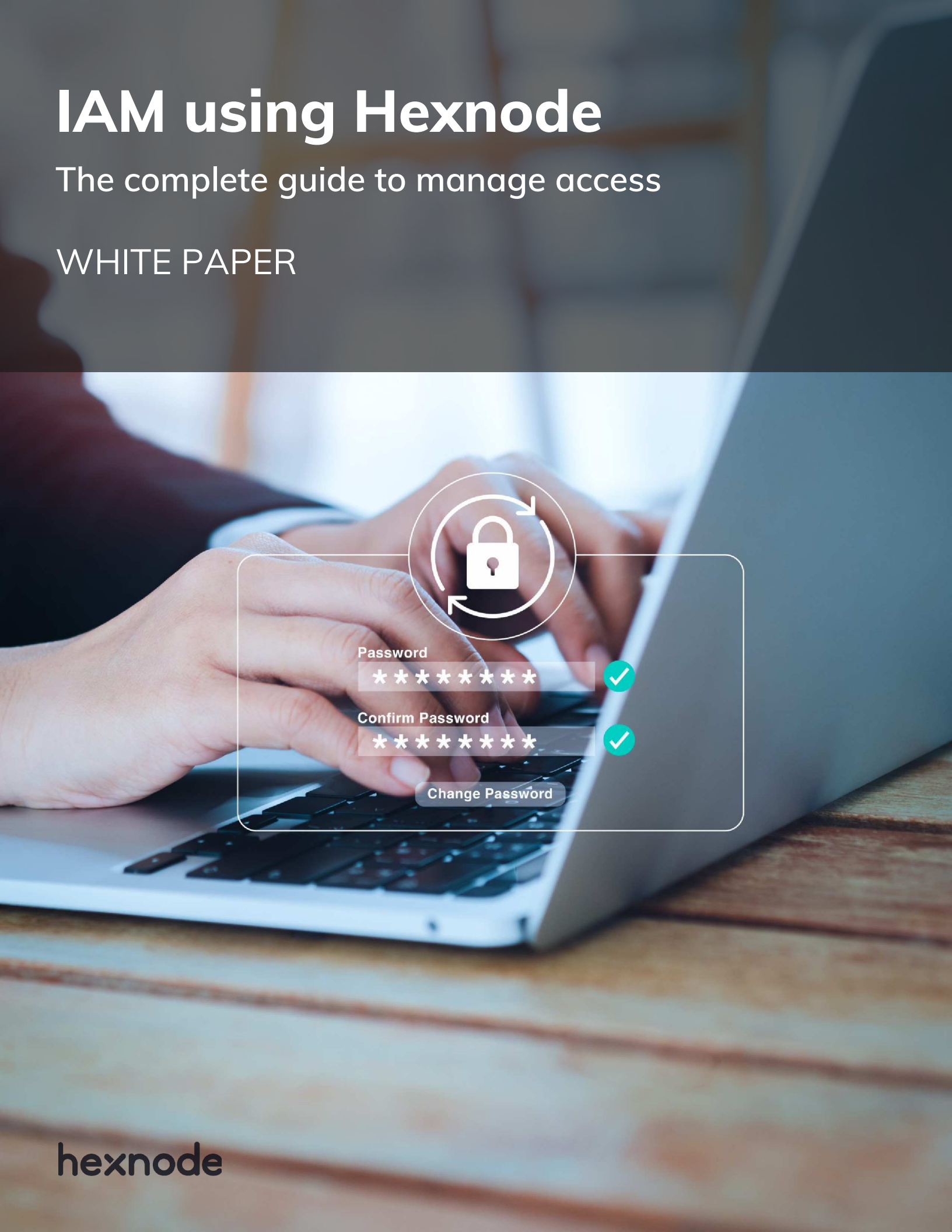
IAM using Hexnode

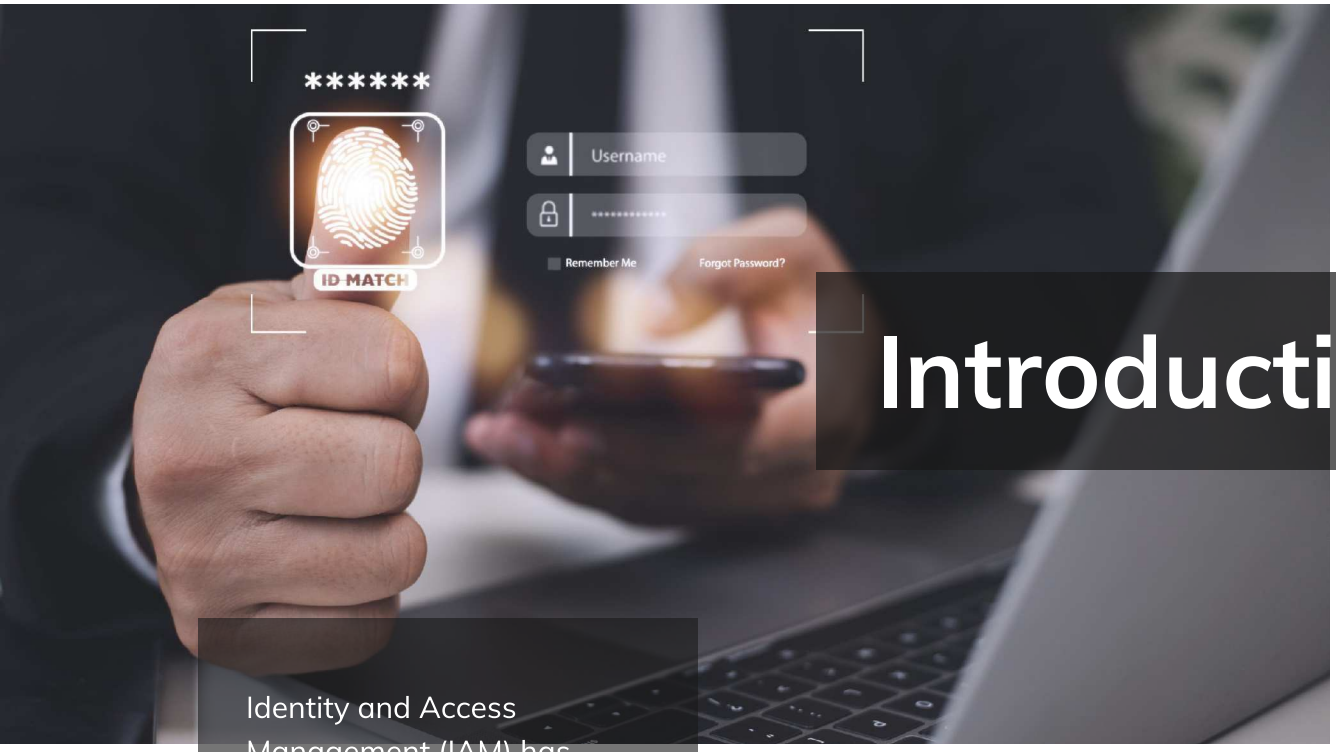
The complete guide to manage access

WHITE PAPER



hexnode

TABLE OF CONTENTS



Introduction

Identity and Access Management (IAM) has become a critical aspect of modern business environments as organizations become more digitized and reliant on technologies. Businesses can implement effective IAM solutions and ensure the security of their digital assets.

IAM is a security framework that manages and governs digital identities and access privileges across an organization's IT infrastructure. It also provides a centralized and systematic approach to manage user identities, user authentication, and authorization of access to different IT resources. Furthermore, it involves processes, policies, and technologies that ensure only authorized users have access to sensitive data and resources while preventing unauthorized access, data breaches, and cyber-attacks.

ACCESS MANAGEMENT OVER THE YEARS

The concept of IAM emerged in the 1990s when organizations started deploying multiple applications and systems that required user authentication and access control. Initially, IAM was a simple process of managing user accounts and passwords for individual systems.

However, as the number of systems and applications increased, organizations realized the need for a centralized approach to manage user identities and access control.

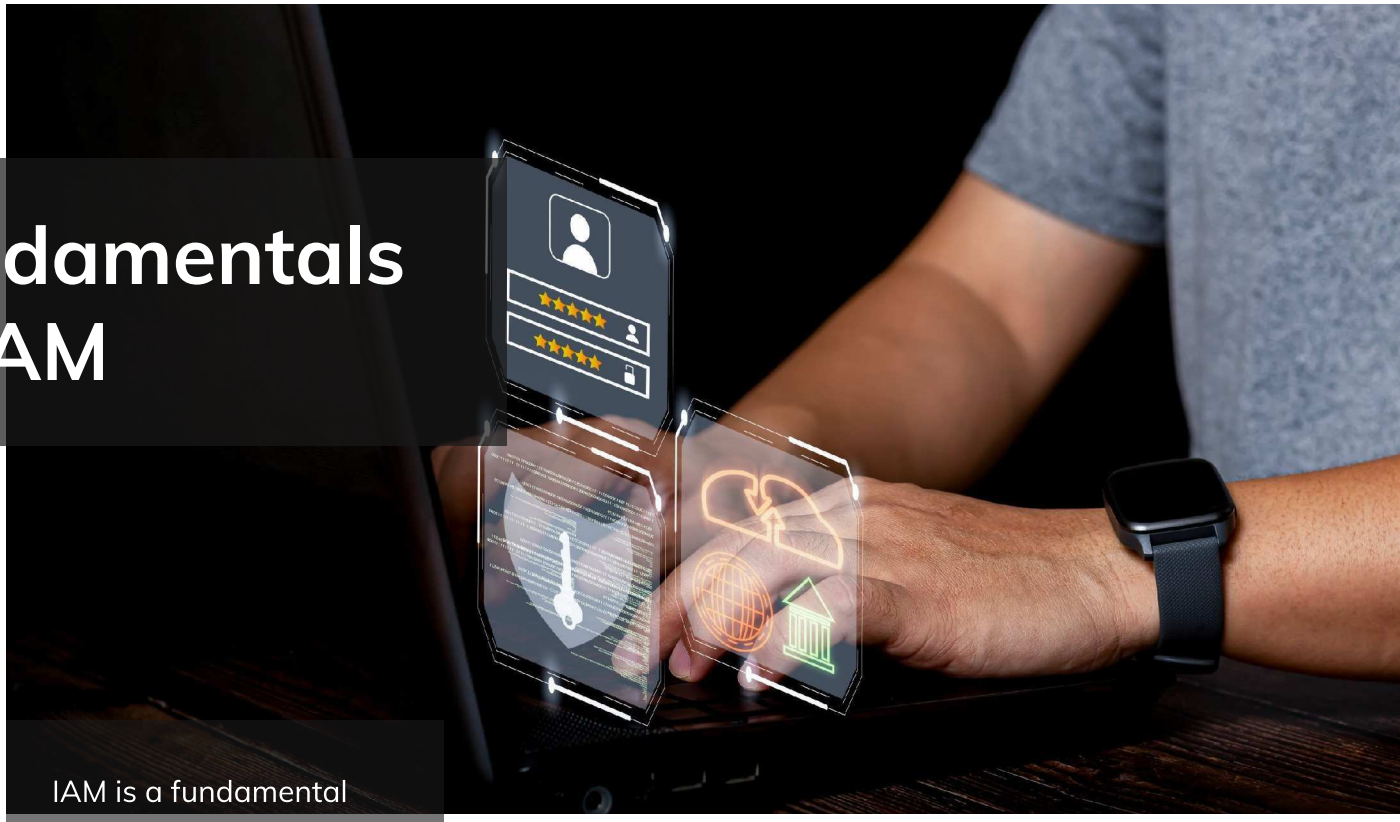
The first-generation IAM solutions focused on managing user accounts and passwords across different systems. Later, the second-generation IAM solutions introduced the concept of Single Sign-On (SSO), which allowed users to access multiple systems and applications with a single set of credentials.

The third-generation IAM solutions introduced the concept of Identity Governance and Administration (IGA), which included identity lifecycle management, access request management, and access certification processes.

In the late 2010s, as digital environments and endpoints diversified, the adoption of a Zero Trust approach to IAM gained prominence. This strategy provided an additional layer of protection and confidence to organizations concerned about the security of their network and data, and it still continues to this day. However, sometimes systems require users to prove who they are before allowing them to do things. This can slow things down and make it harder for people to get their work done.

Today, IAM solutions have evolved to provide comprehensive identity and access management capabilities, including identity governance, identity analytics, access management, and privileged access management.

1 Fundamentals of IAM



IAM is a fundamental aspect of modern security architecture that ensures only the right people have access to the right resources at the right time. It involves processes, policies, and technologies to manage digital identities and control access to applications, data, and other resources.

WHAT IS IDENTITY

The concept of IAM emerged in the 1990s when organizations started deploying multiple applications and systems that required user authentication and access control. Initially, IAM was a simple process of managing user accounts and passwords for individual systems.

TYPES OF IDENTITIES

There are various types of identities in an organization's IAM system. The three primary types of identities are:

- **User Identity:** A user identity represents a person within an organization. It includes attributes such as username, password, email address, and other PII.

- **Device Identity:** A device identity represents a physical device within an organization. It includes attributes such as MAC address, IP address, and other device-specific identifiers.
- **Service Identity:** A service identity represents an application or service within an organization. It includes attributes such as API key, client ID, and other service-specific identifiers.

AUTHENTICATION vs. AUTHORIZATION

Authentication and authorization are two essential concepts in IAM.

Authentication

Authentication is the process of verifying a user's identity. It is typically achieved by using a username and password combination. Other authentication methods include biometric authentication, token-based authentication, and certificate-based authentication.

Multi-factor Authentication (MFA)

Multi-factor authentication (MFA) is a security mechanism that requires users to provide two or more authentication factors to verify their identity. MFA provides an extra layer of security and makes it more challenging for attackers to compromise user accounts.

Passwords and other authentication methods

Passwords are the most commonly used authentication method. However, they are vulnerable to various attacks, such as brute force attacks, phishing attacks, and social engineering attacks. To overcome these vulnerabilities, organizations can use other authentication methods such as biometric authentication, token-based authentication, and certificate-based authentication.

Authorization

Authorization is the process of granting or denying access to resources based on the user's identity. It is typically achieved by assigning roles or permissions to users based on their job function or responsibility.

Types of access control

There are various types of access control mechanisms in an organization's IAM system. The four primary types of access control are:

- **Discretionary Access Control (DAC):** Discretionary Access Control (DAC) is an access control system that enables data providers and storage network managers to create policies using access control lists (ACLs) and capability tables. The owner of the resource has control over who can access it and what kind of access they have, making it the least restrictive access control system. DAC is commonly used in computer security to distribute verified information to other users and restrict access to specific tools, applications, and data. It is available in Microsoft operating systems and enables the resource's owner to regulate security permissions for specific items directly.

- **Mandatory Access Control (MAC):** Mandatory Access Control (MAC) is a hierarchical access control system that governs access privileges based on the data's sensitivity and the information's clearance. MAC enforces access restrictions, preventing users from modifying access controls while utilizing it. A centralized authority governs access privileges in MAC, and it delegates access administration to a third party. MAC simplifies access security by minimizing the necessity for extensive software, computers, and devices. In order to access the data, users must provide personal information.

- **Role-based Access Control (RBAC):** Role-Based Access Control (RBAC) is an access control approach that provides, or limits access based on organizational responsibilities rather than individual identities. RBAC combines role assignment, authorization, and permissions into a complex system. This solution is also known as Rule-Based Access Control since it determines who has access privileges to the data required for their function in the company. RBAC saves time and effort by granting access according to employees' responsibilities, rather than individual identities. Different positions within an organization may be granted modifying access while others may simply be granted viewing access.

- **Attribute-based Access Control (ABAC):** Attribute-Based Access Control (ABAC) is a type of access control that evaluates various attributes or properties of a component involved in an

access event, such as the user, the object, the action, and environmental factors. ABAC maintains access privileges by analyzing a collection of rules, policies, and relationships based on these factors. For example, access to business-critical data can be determined using ABAC by attributes such as team, unit, citizenship, IP address, or other factors that may affect the authorization outcome. ABAC provides more fine-grained control and flexibility than other access control methods.

USER MANAGEMENT

User management is the process of creating, maintaining, and deleting user identities in an organization's IAM system. It includes tasks such as onboarding new users, updating user profiles, and offboarding users who are no longer with the organization.

2 IAM Processes

IAM Processes involve a range of activities that are critical to enhancing security, improving user productivity, and reducing the risk of data breaches. With IAM processes, organizations can streamline user access management, improve security, and reduce costs associated with managing user accounts.

IDENTITY PROVISIONING

Identity provisioning is the process of creating, modifying, and deleting user accounts and permissions within an organization. It involves defining roles and permissions for users and ensuring that they have access to the resources they need to perform their job functions.

Identity provisioning can be done manually or automated through an IAM system. Additionally, automated identity provisioning helps to reduce errors and ensure that users have access to the right resources at the right time.

ACCESS REQUESTS AND APPROVALS

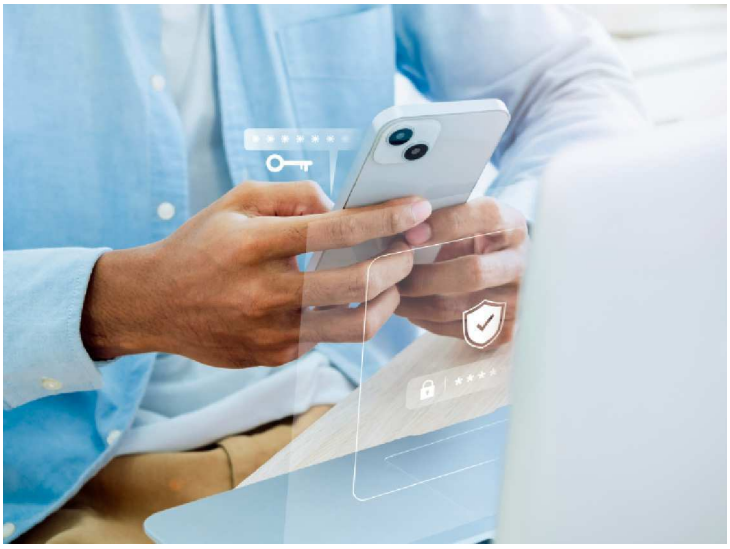
Access requests and approvals is the process of requesting and granting access to resources within an organization. Users can request access to resources, and their request is typically reviewed and approved by an authorized individual, such as a manager or administrator. Access requests and approvals help ensure that only authorized users have access to sensitive information and systems. The process can be automated through an IAM system, which allows for easier tracking and management of access requests and approvals.

PASSWORD MANAGEMENT

Password management ensures that users create strong passwords and that those passwords are stored securely. It involves enforcing password policies, such as minimum length and complexity requirements, and providing tools for users to reset their passwords if necessary. Furthermore, password management is critical to protecting against unauthorized access and data breaches.

SINGLE SIGN ON (SSO)

Single Sign-On is a user authentication service of allowing users to log in once and access multiple applications without having to enter their credentials each time. SSO also eliminates the need for users to remember multiple usernames and passwords, making it easier and more convenient to access resources. SSO can be implemented using various IAM Standards and Protocols, such as SAML and OAuth. An IAM system can provide a central place to manage SSO for different applications and services.



3

The significance & benefits of IAM

Implementing an IAM solution provides numerous benefits to organizations, including increased security, improved compliance, streamlined user access, reduced IT costs and workload, and better user experience.

IAM IN MODERN BUSINESS ENVIRONMENTS

In today's digital world, where data breaches and cyber-attacks are becoming more common, IAM has become a critical component of any organization's security infrastructure. IAM helps organizations to secure their digital assets by providing a centralized approach to manage user identities and access control across different applications, systems, and networks. Furthermore, the solutions help IT teams to implement access control policies that restrict access to sensitive resources based on job roles, project needs, and other criteria. This helps to reduce the risk of data breaches caused by unauthorized access attempts by both external and internal threats.

Listed below are the advantages of adopting IAM solutions:

Increased security

IAM solutions help organizations to secure their sensitive information and IT resources by ensuring that only authorized personnel have access to them. Furthermore, it provides a centralized platform for managing user identities, access rights, and permissions, enabling organizations to detect and prevent unauthorized access attempts.

Improved compliance

The solutions help organizations to meet regulatory requirements such as HIPAA (Health Insurance Portability and Accountability Act), GDPR (General Data Protection Regulation), and PCI DSS (Payment Card Industry Data Security Standard). Also, it provides audit trails that demonstrate compliance with regulatory requirements by logging user access and actions.

Streamlined user access

The IAM solutions streamline user access to multiple systems and applications, simplifying the process of user account creation, management, and removal. This helps IT teams to manage access to multiple systems more efficiently, and it improves user productivity by reducing the need to manage multiple login credentials.

Reduced IT costs and workload

IAM solutions help to reduce the costs associated with managing user access and account lifecycle by automating many of the tasks involved. By streamlining user access management and automating tasks such as password resets, it frees up IT teams to focus on other critical tasks.

Better user experience

By giving users a single sign-on (SSO) capability, they can access multiple resources with a single set of credentials. This not only makes it easier for users to access the resources they need but also reduces the likelihood of password-related security incidents.

4

Challenges in IAM and best practices

IAM challenges are a reality in today's digital landscape, but with a well-structured strategy and adherence to best practices, organizations can ensure the security, compliance, and efficiency of their systems while minimizing potential risks.

WHAT ARE THE CHALLENGES IN IAM?

With the rise of cloud-based services, having a proper IAM strategy has become very important. This means that it gets more difficult for companies to manage user identities and make sure that the right people have access to the right applications and resources. More users mean more usernames, passwords, tools, and URLs to monitor and manage. Let's see the most common challenges associated with IAM:

Password repetition and fatigue

Having a SaaS-based approach in a company initially makes it easier for users to access apps and resources, but as the number of services increases the user will have more usernames and passwords to manage as all these service providers will have

their criteria for user identity, password, and custom URL. As a result of this, users tend to use reuse passwords and even usernames of one app for another. This is a major security risk taking into account the amount of data that can be accessed if one service is breached. Also, when there is more data to remember manually, the chances of the user forgetting some passwords is high.

Errors associated with manual user provisioning and de-provisioning

Ideally speaking, when an employee joins a company, the person will be handed a set of credentials and that person should be able to use anything and everything they need to do their work properly. When an employee leaves the company, the access and credentials should be revoked, making sure that the person can't access anything thereafter.

The problem with the above-mentioned process is that even now some of these processes are manually done. So, it is highly likely that some users might not get the required access on time. Without the use of a proper IAM solution, central management of access to all these apps and tools won't be possible. In a scenario where IAM is not proper, offboarding an employee is going to be an even bigger issue since the accesses have to be revoked manually.

Compliance visibility

Knowing who has access to what tools is a major requirement when it comes to IAM. And this is an even bigger issue when it comes to meeting compliance standards. Apart from who has access to what, you also need to know where it is getting accessed from and also what the users are doing with it. This is one of the biggest challenges faced by companies while implementing an IAM strategy.

Access management for remote work

The fact that cloud applications are accessible from any internet-connected device is one of its many advantages. With the addition of more mobile devices to workplaces, organizations now have more endpoints to manage and control. These devices are access points to apps and tools, which means companies and businesses have more URLs and passwords to take care of.

Users and administrators should be able to overcome the difficulty of accessing resources from any location or device with the use of a cloud-based IAM solution. Not only should it offer web-based SSO for every user application, but it also needs to be aware of the user's context, including their location, device, and behavior. This provides a high level of assurance that the user is who they claim to be. Currently, rather than being at the network level, the perimeter is at the identity level.

BEST PRACTICES TO FOLLOW DURING IAM IMPLEMENTATION

By now it should be clear how important IAM is in the present corporate landscape. But, how to implement a proper IAM strategy in an organization, what is the best way to approach an IAM implementation, is still in doubt. The difference between a good security strategy and a bad one might come down to how your IAM was set up. The setup of your Identity and Access Management (IAM) system could potentially determine how effective or ineffective a security strategy is. So, here are some of the best practices to follow while building a robust IAM strategy:

Zero-trust approach

Many businesses and organizations still rely on traditional trust structures for their tools and resources. While this approach is straightforward and efficient, it may not provide the best security. In the traditional setup, once a user logs into a tool or network, the device retains the credentials, eliminating the need to log in again. However, this convenience poses a significant security risk if the device falls into the wrong hands, as unauthorized individuals gain immediate access to all logged-in services.

To address this security concern, the zero-trust approach offers a solution. The fundamental idea behind zero-trust is simple: never trust anyone until their identity is verified, and always grant the least amount of access required. This means that users must undergo constant verification, and they will only be granted access to the specific resources they need, reducing potential security vulnerabilities. By adopting the zero-trust model, organizations can bolster their security measures and minimize the risk of unauthorized access to sensitive data and systems. With this constant authentication requirement, IAM policies can be fortified by making sure that users must verify themselves to access company resources.

Strong password policy

Passwords might not be the first thing that comes to mind when you think about strengthening your IAM strategy. And with the introduction of Single Sign-On, people are more prone to believe that having strong passwords is not that important anymore. But this is so far away from the truth. The importance of having a strong password can't be stressed enough, especially if you are using SSO.

If you are using SSO in your organization, make sure that the users are protecting the primary account with a complex, unique, and hard-to-guess password. It is common practice to forget the importance of having a strong password policy when using Multi-Factor Authentication along with SSO. But having MFA with SSO is not going to be a replacement for having a strong password. It's just an added layer of security. So be sure to implement a strong password policy and have a proper audit schedule to check the strength of passwords used in the organization.

Multi-Factor Authentication

We saw the importance of passwords when it comes to validating user identity. You might have gotten off on the wrong foot about MFA and SSO from that section. But MFA is like an additional layer of security for identity validation. In this day and age, just login credentials aren't enough. MFA adds an additional step in the user validation/authentication process.

MFA makes it necessary to provide two or more modes of authentication so that the user can log in to their account. These modes may include biometrics, codes or authentication links sent to trusted devices or email IDs and so on. In this way, organizations can make sure that only the right people can access the right resources.

Take extra care in securing sensitive data

Securing your most valuable assets is security 101 regardless of the industry you are in. But to do this you have to first identify which assets are most important for you. The same thing can be applied to organizational data also. Once you have identified which data is the most sensitive, you can take measures to protect it at all costs.

The most basic thing you can do is limit access to such data. By limiting access, you can ensure that only those in need have access to high-value data. The second thing you can do is find the systems in which the data is stored and secure those systems with multiple layers. And if it is stored in the cloud, it is necessary to keep track of what all services have access to this data and limit that access too. We will see about role-based access in a bit.

Principle of least privilege and role-based access control

This is an extension of the last point. In the principle of least privilege, organizations are advised to restrict access and permissions as much as possible, but it should not affect users' day-to-day work. This can be done using role-based restrictions, meaning if your role requires you to access a set of resources, you will be allowed to access it. But if the role doesn't require a set of resources, then under no circumstances will the user be allowed to access that resource.

Another common method to ensure the least privilege is to use attribute-based control, where access is restricted based on different attributes like the user's team, location, and so on. Putting the restrictions in place doesn't finish the job. To limit capabilities whenever possible, you must constantly audit usage, minimize pointless existing permissions, and provide system function permissions. In order to prevent single administrators from having a lot of permissions they don't need, it's especially crucial to restrict and modify administrative capabilities. Adopt privileged access management (PAM) best practices and divide responsibilities to prevent over-provisioning access to specific individuals.

Use IAM solutions that go well with existing tools

When integrating new IAM technologies into your organization, just like with any other tool, ensure they integrate seamlessly with your current tools. Skipping this step could cause trouble because you might need to change the configuration of your old tools if the new tool doesn't work with them. No organization is looking forward to reconfiguring already installed tools. Therefore, when selecting the IAM tools you need, make sure they integrate seamlessly with all your other products.

Regular audit

All the above-mentioned practices are good only if they are applied and constantly audited. With more tools and users being added to organizations each day, auditing should be one of the primary practices you should follow. Only with auditing can you ensure that only the right people are getting access to the right data. With the help of auditing, organizations can find unused and abandoned accounts and de-provision them to reduce the risk of data leakage.

COMPLIANCE, AUDITS AND IAM

With more compliance standards and regulations coming up, compliance audits are common for IT organizations in the current scenario. Any IT organization that completes a compliance audit should be in the clear for IAM compliance since most of these audits consider IAM compliance as priority number one.

To stay IAM compliant, organizations must be aware of all the elements of IAM that affect the overall compliance of the organization. And to protect the security, reliability, accessibility, and privacy of information, these IAM components must be put in place into the entire compliance strategy. Some of the major elements of IAM that can affect compliance are listed below:

- Unique access ID and access permissions: Organizations must ensure that every user has a unique ID and also make sure that access to systems, tools, and data is properly managed and recorded.
- Approval of access: Organizations must have a proper hierarchy for access requests and approval processes.
- Updating and renewing accounts and access
- Inactive accounts management: Organizations must have a proper system in place to deal with unused and inactive accounts, like having a time period after which the account will be retired.
- Revoking or disabling accounts: Organizations should set up a proper list of conditions under which user accounts will be disabled or revoked.
- Admin's remote access: Organizations must define the admin's control over user accounts and access.
- Segregation of duty for admins
- Authentication of access and user validation
- Password management
- Management of user sessions: Organizations must set rules to terminate user sessions like a certain inactivity period or location-based restriction.
- Protection of critical data
- Identification, authentication, and validation of devices

An organization's compliance with regulations like GDPR, HIPAA, NIST, and others can be verified through continuous proactive management of IAM policies and related operations, supported by periodic audits and reviews.

5 IAM Solutions

The diverse landscape of IAM solutions offer a variety of options, from the scalable and flexible cloud-based solutions to the more secure and controlled on-premises solutions. This empowers organizations with a comprehensive array of tools to fortify and manage their digital ecosystems.

ON-PREMISES VS. CLOUD-BASED IAM SOLUTIONS

Securing your organization starts with protecting and managing identity and access. IAM systems are now available mainly in two forms for organizations to choose from, on-premises and cloud-based. Let's see what each of these forms of IAM solutions are:

On-premises IAM solutions

On-premises IAM solutions are also similar in terms of their functionalities, but the difference is that it makes use of a combination of hardware and software to control everything. This type of IAM solution generally makes use of dedicated servers, software, and databases to store, manage and control identity, policies, and authentication.

IT admins have complete access to the user identities and can easily configure the IAM solution to meet the organization's specific needs.

Cloud-based IAM solutions

Cloud-based IAM solutions allow organizations and IT admins to manage and configure user identities over the air. It also allows organizations to control and monitor user access to cloud-based tools and services remotely and securely. This means that admins can create users, set up access policies, assign roles to users, define role-based access, and monitor user activity across different online services used by the company. Cloud-based IAM solutions are usually a combination of identity providers (IDPs) along with other cloud services. The IDPs act as the centre for user identity management and authentication.

Why is cloud-based IAM solutions better than on-premise IAM solutions?

Both have their pros and cons, but cloud-based IAM is gaining more popularity these days due to its flexibility and adaptability. Here are some reasons why you should consider cloud-based IAM solutions over on-premises ones:

- Cloud-based IAM solutions offer a single, centralized portal where everything regarding identity and access management can be configured and monitored. For on-premises ones, you might have to rely a lot on hardware.
- Scalability is one region where on-premises loses a lot of interest. For cloud-based IAM solutions, scaling up or down is very easy.
- Cloud-based IAM solutions offer ease of accessibility since there is no hardware involved. In terms of security updates and configurations are also easy due to the lack of hardware involved.
- Another highlight in the case of cloud-based IAM solutions is that it is easier to integrate it with other services and tools.
- Last but certainly not least, cloud-based IAM solutions are cheaper compared to on-premises, since on-premises IAM solutions involve the installation of a lot of hardware components.

FEATURES AND CAPABILITIES TO LOOK FOR IN AN IAM SOLUTION

When picking the right IAM solution for your organization, you will be bombarded with a lot of options. So, you must be informed about what to look out for in an IAM solution. Here are some of the most important things to look out for in an IAM solution:

Multi-factor authentication

We have seen how MFA helps in securing identities by adding an additional layer of security during user authentication. IAM solutions should be capable of enforcing MFA for all users across the organization.

Single Sign-On

Single Sign-On is the process where you login into your account once and that account will be used to log in and verify your identity across various other services automatically. Almost all modern IAM solutions offer this feature and if the IAM you are looking for doesn't offer this feature, you might have to reconsider your choice.

Options to manage 3rd Party vendors

IAM solutions with third-party vendor management capabilities offer third-party subcontractors a higher degree of information while limiting privilege misuse.

Incident response

IAM solutions should be able to identify and respond immediately in the case of a security breach. Modern IAM solutions not only just notify admins of cyber incidents but also takes action to mitigate the effects of the attack.

Cloud-based

We saw earlier how cloud-based IAM solutions are slowly replacing on-premises ones. If you are planning for the future, it is better to go with a cloud based IAM solution.

Ease of use

The IAM solution should be easy to understand and use. Even though IAM solutions provide complex functionalities, it should be easy for users to understand how to operate the tool.

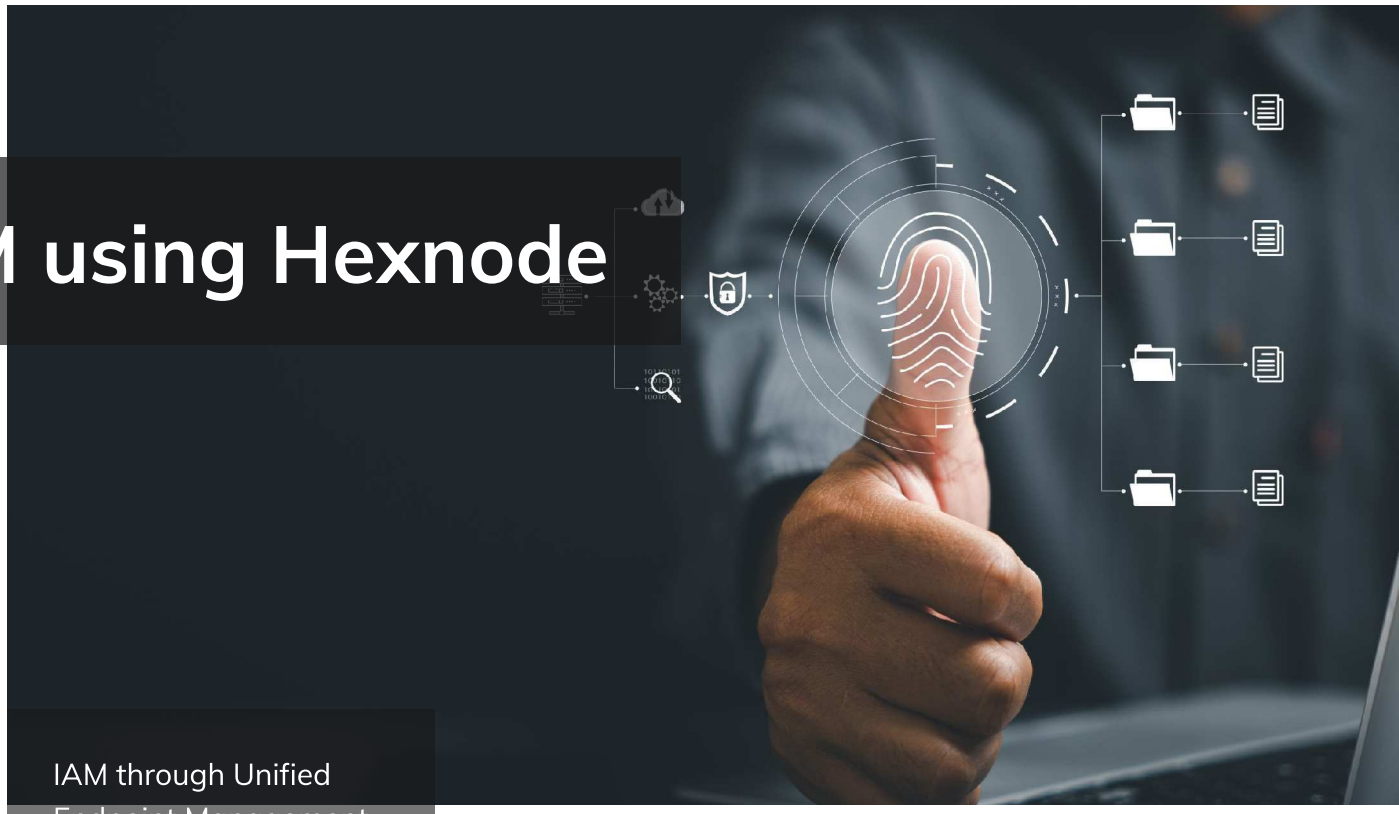
Compatibility

The IAM solution must possess compatibility to adapt and work with different network architectures, tools, and operating systems. While there are affordable products available, many of them lack support for different platforms. Therefore, ensuring compatibility is important.

Reporting

IAM solutions should have the capability to generate comprehensive reports showcasing all activities performed on the platform. These reports should include details about systems accessed, login times, and the type of authentication used. This feature is essential for effectively monitoring security risks and ensuring compliance with regulations and policies.

6 IAM using Hexnode



IAM through Unified Endpoint Management (UEM) is a powerful approach that streamlines security and access control. With Hexnode UEM, organizations can establish a cohesive security framework that adapts to the modern complexities of managing identities across a wide range of devices and platforms.

WHAT IS HEXNODE UEM?

Hexnode UEM (Unified Endpoint Management) is a comprehensive mobile device management solution designed to manage and secure a wide range of endpoints in an organization. UEM allows administrators to efficiently manage mobile devices, such as smartphones and tablets, as well as other endpoints like laptops, desktops, wearables, and IoT devices, from a single unified platform.
Some of the main features offered by Hexnode include:

- **Automated device provisioning:** Make provisioning and deployment of a bulk number of corporate devices easier with Hexnode's array of Zero-Touch enrollment and configuration options.
- **Policy Management:** Define and enforce policies to configure device settings, security controls, and application usage across all managed endpoints.

- **Application Management:** Facilitate the installation, update, and removal of applications on managed devices.
- **Security Management:** Implement security measures like device encryption, remote wipe, and passcode enforcement to protect sensitive data.
- **Remote Management:** Perform various remote actions such as locking, locating, and troubleshooting devices from the UEM console.
- **Content Management:** Control access to corporate content and ensure secure file sharing and collaboration.
- **Reporting and Analytics:** Obtain insights into device usage, compliance status, and security risks through comprehensive reports and analytics.
- **Integration and Compatibility:** Hexnode UEM is designed to integrate with other IT systems and is compatible with various platforms, including iOS, Android, Windows, macOS, and more.

Apart from all these endpoint management features offered by Hexnode, it also offers a wide range of identity and access management functionalities. This can empower organizations to make access to company resources smooth and reduce any downtime that might be caused in the process of granting access.

HOW CAN A UEM HELP IN IAM?

In the present day, all the major UEM providers have started to add IAM capabilities to their arsenal. And through integrations with identity providers and IAM vendors like Okta and Active Directory, UEMs help get the most out of these tools.

Currently, UEMs might not encompass the complete array of IAM solution features. However, they do include functionalities such as enforcing MFA, managing multiple work identities, and implementing group policies. These capabilities contribute significantly to the UEM arsenal and serve as a valuable augmentation to any IAM strategy. Moreover, UEMs also offer the ability to define access based on specific conditions for tools and software.

Lately, the rising demand for remote device management has put UEMs at the forefront. This trend has led even organizations without other management solutions, such as an IAM system, to adopt UEMs. Fortunately, these organizations can still ensure data security, as UEMs provide fundamental IAM functionalities. Even organizations having existing IAM software in their grasps have the option to use both IAM and UEM together since most leading UEMs offer integrations with leading IAM providers.

HEXNODE'S IAM CAPABILITIES

Now that we have seen what Hexnode is and how a UEM can help in boosting the efficiency of IAM tools, we can move on to the IAM capabilities offered by Hexnode:

User authentication

IT admins can use Hexnode UEM to push organization-wide password policies to make sure that every user is using a strong and complex password. Additionally, Hexnode supports MFA to secure access to the management portal using authenticator apps from third parties, such as Google Authenticator and Microsoft Authenticator.

Network configuration

With the help of Hexnode, organizations can configure and set up network settings for endpoints so that the devices can access company resources only from secure networks. Network configurations offered by Hexnode include Wi-Fi, VPN, APN, and certificates.

Containerization

Hexnode offers containerization features to separate work data from personal data in the case of personal devices. This ensures that the data doesn't get mixed up and also ensures the safety of corporate data.

Encryption

As if containerization weren't enough, enterprises can enforce system-level encryption on endpoints by pushing device encryption policies with Hexnode. This prevents unauthorized people from accessing critical company resources.

Controlling access to apps and content

With Hexnode, IT admins can restrict users from accessing unwanted apps and websites using its allowlisting or denylisting features. You can also configure app permissions for managed apps from the Hexnode console so that apps have access only to the necessary permissions.

Compliance checks

To make sure that your endpoints comply with corporate laws. You can create compliance settings using Hexnode and identify non-compliant endpoints. Companies can make sure that the relevant corporate security controls are in place by enforcing automated and regular compliance checks.

HEXNODE'S INTEGRATION WITH DIRECTORY SERVICES AND IDPs

Hexnode offers native integrations with leading IDPs and IAM providers like Azure AD, Active Directory, Google Workspace, and Okta. With these integrations in place, Hexnode can import, store and secure user data from the IAM tools. It doesn't stop there; you can onboard devices and users using the directory credentials and enforce validation of technician to the Hexnode portal using MFA and SSO. As a bonus, you can create, maintain and manage groups using the directory credentials and use the groups for deploying policies and other management configurations in bulk.

Conclusion

IAM emerges as a keystone for digital security, encompassing user identity, access control, and data protection. The absence of a robust IAM strategy escalates the risk of unauthorized data breaches. As remote work surges, an elevated IAM approach becomes essential, effectively addressed through a blend of best practices and streamlined tools like UEMs or MDMs.

With all the points mentioned in this whitepaper, it should be evident how important IAM is to digital security. In the absence of a proper IAM strategy, the risk of unauthorized access to sensitive data is extremely high. So, following the best practices and implementing the IAM features mentioned in this article you can secure your corporate data to a great extent.

With more remote work becoming more common, the need for IAM also will keep on increasing. More devices and more users accessing corporate resources remotely require a more robust IAM strategy. To make things easier, you can make use of a solid UEM like Hexnode along with your IAM tools to simplify and streamline the whole process of identity and access management.

Mitsogo Inc., United States (HQ), 111 Pine St #1225,
San Francisco, CA 94111
Tel: Intl +1-415-636-7555, Fax: Intl +1-415-646-4151