

The Evolution of Identity Access Management: From Traditional to Converged



Table of Contents

03	 	Introduction	
04	 	Security and risk professionals are overwhelmed	
05	 	Security risks are on the rise	
06	 	Compliance risks are escalating	
		Why best-of-breed solutions are falling short in identity access management	07
09	 	CYMMETRI Converged Approach to Workforce IAM	
		Business benefits of Workforce IAM	09
		What business outcomes look like with Workforce IAM	10
		Why Cymmetri Workforce IAM?	11
		Comprehensive IAM platform	12
		How Cymmetri Workforce IAM works	14
		How it works	15
20	 	Rethinking Your IAM Strategy and Approach	





In today's fast-paced digital world, organizations are racing to keep up with the demands of the rapidly evolving business landscape. To ensure that your workforce can efficiently perform their tasks and achieve business goals, quick and easy access to applications, tools, and platforms is essential. However, the current business environment presents unprecedented complexity, posing challenges in meeting the on-demand identity and access requirements of your employees while adhering to strict compliance regulations and minimizing risks.

Several technology and business trends contribute to the increasing number of identities that security and risk professionals must handle. Remote work has become the new normal, with a majority of the workforce conducting business outside traditional office settings. This distributed work setup demands urgent measures to ensure business continuity and resilience, especially with the rise in internal and external cyber threats.



Embracing cloud-based applications and services has become a widespread practice across industries, with a staggering **94%** of businesses already using such services.

The cloud offers significant advantages, making the implementation of new apps faster, easier, and more cost-effective. However, the growing number of applications also means an increased burden on security and risk professionals who must manage diverse applications with varying security access controls.

Moreover, organizations are facing frequent changes in employee and contractor roles, resulting in constant flux. As a result, security and risk teams are continuously managing access changes for employees moving into new roles, business units, or requiring different levels of access. Traditional identity and access management (IAM) solutions often struggle to keep up with these frequent changes, creating operational challenges for organizations.

To address these complex challenges, businesses need modern and flexible identity access management solutions that can adapt to the dynamic nature of the modern enterprise. Such solutions should provide secure and efficient access to applications and resources while ensuring compliance with regulations and safeguarding against potential risks and threats.

Security and Risk Professionals are Overwhelmed

These ongoing trends have led to a significant surge in identity data, resulting in the creation and constant changes of numerous new identities, roles, and permissions on a daily basis. As a consequence, security and risk professionals today find themselves fatigued, attempting to manage an overwhelming volume of identities, roles, and entitlements, all while striving to mitigate risks and maintain compliance.

This identity explosion places an immense burden on security and risk teams, as they must ensure that each identity possesses only the necessary access rights and privileges. Unfortunately, the lack of enterprise-wide visibility into the identity landscape and the context surrounding access requests and certifications often leaves teams feeling overwhelmed. Consequently, they may resort to rubber-stamping access requests and certifications without being able to thoroughly validate each one's necessity. This approach is far from ideal, as the repercussions of such oversight can be severe both from a security and compliance perspective.



According to estimates, organizations globally have to manage and protect a staggering **3.2 billion** identities and activities, further emphasizing the scale of the challenge at hand.

To effectively address this issue, security and risk professionals require comprehensive solutions that provide holistic visibility, context, and efficient management of identities, roles, and access permissions to ensure robust security and compliance practices.

Security Risks are on the Rise

In recent years, there has been a remarkable surge in the scale, severity, and frequency of security breaches. For four consecutive years, unauthorized access has remained the leading cause of such breaches, accounting for a staggering 50% of all compromised records.

The financial ramifications of security breaches have also experienced significant growth. These costs go beyond substantial fines, encompassing expenses associated with remediation efforts, user notification, loss of business, and other associated costs.

As the threat landscape continues to evolve and cyber-attacks become increasingly sophisticated, organizations must adopt robust security measures, including comprehensive identity and access management solutions, to safeguard their sensitive data and protect against devastating financial consequences.



The extent of these breaches is alarming, with over **2 billion** usernames and passwords breached, representing a **35%** increase compared to the previous year.



The average cost of a data breach in India has risen steadily each year, more than doubling between 2019 and 2022, reaching a staggering **INR 800 million+.**



Compliance Risks are Escalating

In the current business landscape, organizations worldwide are grappling with increased regulatory scrutiny and compliance demands to safeguard identity and data. Noncompliance with these regulations can result in severe financial penalties, with fines for large enterprises potentially reaching millions of dollars.



For instance, companies have already faced penalties totalling **€1.64 billion** as of January 28, 2022.



Collectively, GDPR fines have now reached over **€4 billion**.

Additionally, regulatory noncompliance fines can have significant impacts, as demonstrated by a global insurance provider recently being fined \$10 million for failure to comply with SOX regulations, and a Tennessee-based management company being fined \$2.3 million for a HIPAA breach caused by compromised administrator credentials.

The challenge faced by today's security and risk professionals lies in the limitations of existing identity and access management (IAM) and governance solutions, which are slow, complex, and built on outdated concepts. These solutions were not designed to handle the complexity that modern enterprises encounter.

To address these challenges, many enterprises have adopted a best-of-breed IAM strategy to simplify the governance and management of users' access, roles, and permissions. However, these solutions often suffer from being siloed, difficult to administer, and costly due to interoperability issues.

Furthermore, while they may excel in specific areas such as identity management, access management, or identity governance, they only offer partial solutions. As a result, organizations must integrate multiple disparate solutions, creating a patchwork that is time-consuming, expensive, and fails to deliver a strong return on investment.

Over time, the effectiveness of these best-of-breed solutions diminishes, mainly due to their reliance on manual processes that cannot keep up with the rapid increase in new identities, applications, and permissions in today's dynamic business environment. Consequently, security and risk teams struggle to process the mounting identity data manually, leading to delays in making appropriate access decisions. To effectively address these challenges and enhance security, organizations require modern IAM solutions that can seamlessly manage the growing complexity of identity and access management in a dynamic and automated manner.



Why best-of-breed solutions are falling short in identity access management

Best-of-breed solutions, which offer specialized capabilities in specific areas of identity access management (IAM), are falling short in addressing the complexities and challenges of modern IAM for several reasons:



Integration Complexity:

Best-of-breed solutions are often built on different architectures and may lack standardized interfaces, making their integration with existing systems and applications complex and time-consuming. This integration challenge leads to data silos, hindering the flow of critical identity information across the organization.



Lack of Interoperability:

These solutions are designed to excel in their specialized areas, but they may not work seamlessly together. As a result, organizations often find it challenging to maintain a cohesive and unified IAM strategy across their IT ecosystem, leading to fragmented identity management practices.



High Total Cost of Ownership (TCO):

While best-of-breed solutions may appear cost-effective initially, their maintenance, integration, and licensing costs can quickly add up. Managing multiple systems requires additional resources and increases the overall TCO compared to a unified IAM platform.



Complex Administration and Governance:

Implementing multiple IAM solutions can lead to administrative overhead, as each solution may have its own set of policies, procedures, and user interfaces. This complexity makes it challenging for administrators to manage identities, roles, and access rights efficiently.



Limited Scalability:

Best-of-breed solutions may not scale well to accommodate the growing number of identities and access requirements in today's dynamic business environment. As organizations expand, they may face challenges in managing a large and diverse user base effectively.



Inadequate Identity Visibility:

Using multiple solutions may result in fragmented views of identity data, making it challenging for security teams to gain a comprehensive understanding of user behavior, potential risks, and access patterns across the organization.



Inconsistent User Experience:

Different IAM solutions can lead to inconsistencies in the user experience, with varying authentication methods and access procedures for different applications. This can result in confusion for users and potentially compromise security.



Limited Automation and Adaptability:

Best-of-breed solutions may lack the automation capabilities needed to respond to rapidly evolving security threats and changing business requirements. Manual processes can lead to delays and errors in identity management.



Complicated Compliance Management:

Maintaining compliance with regulatory requirements and internal policies becomes more complex when dealing with multiple IAM solutions. Compliance audits may become more cumbersome and time-consuming.



Fail to deliver promised ROI



CYMMETRI Converged Approach to Workforce IAM

In response to the increasing complexity that organizations encounter today, a comprehensive and innovative approach to IAM is essential. CYMMETRI Workforce IAM, built on four foundational pillars - identity management, access management, Privilege access management and identity governance, offers a unified solution designed to secure user access, enhance productivity, and strengthen overall security. Specifically tailored to meet the IAM needs of enterprises and large organizations, this unified solution is user-friendly, AI-driven, and built on the CYMMETRI Identity Cloud, a scalable and high-performance platform that provides a single platform to manage all identities.

Business benefits of Workforce IAM

Implementing a Workforce IAM (Identity Access Management) solution can bring several significant business benefits to an organization. Some of the key advantages include:



Enhanced security with increased scalability:

Workforce IAM helps strengthen the organization's security posture by providing centralized control over user identities, access rights, and permissions. It ensures that employees have appropriate access to the resources they need and prevents unauthorized access, reducing the risk of data breaches and insider threats.



Increased Productivity:

With streamlined authentication and single sign-on capabilities, Workforce IAM simplifies the login process for employees. This convenience boosts productivity by reducing the time spent on managing multiple login credentials for various applications and systems.



Improved Compliance:

Workforce IAM solutions often come with built-in compliance features that help organizations adhere to industry regulations and data protection laws. It enables better audit trails, reporting, and enforcement of access policies, which can be critical in meeting regulatory requirements.



Cost Savings:

A unified Workforce IAM platform can help reduce operational costs by eliminating the need for multiple disparate IAM solutions. It simplifies administration, lowers maintenance expenses, and minimizes the risk of security incidents, which can lead to costly data breaches and legal repercussions.



Faster Onboarding and Offboarding:

Workforce IAM facilitates the automated provisioning and deprovisioning of user accounts, making the onboarding and offboarding process for employees more efficient. This reduces administrative overhead and ensures that access rights are granted or revoked promptly, reducing the risk of security gaps during transitions.



Future-Proofing:

Investing in a robust Workforce IAM solution helps future-proof the organization against evolving security threats and technological advancements. It ensures that the organization can adapt to new business requirements and technologies without sacrificing security or user experience.

By 2025, **70%** of new access management, governance, administrative, and privileged access deployments will be converged identity and access management platforms

- Gartner



What business outcomes look like with Workforce IAM

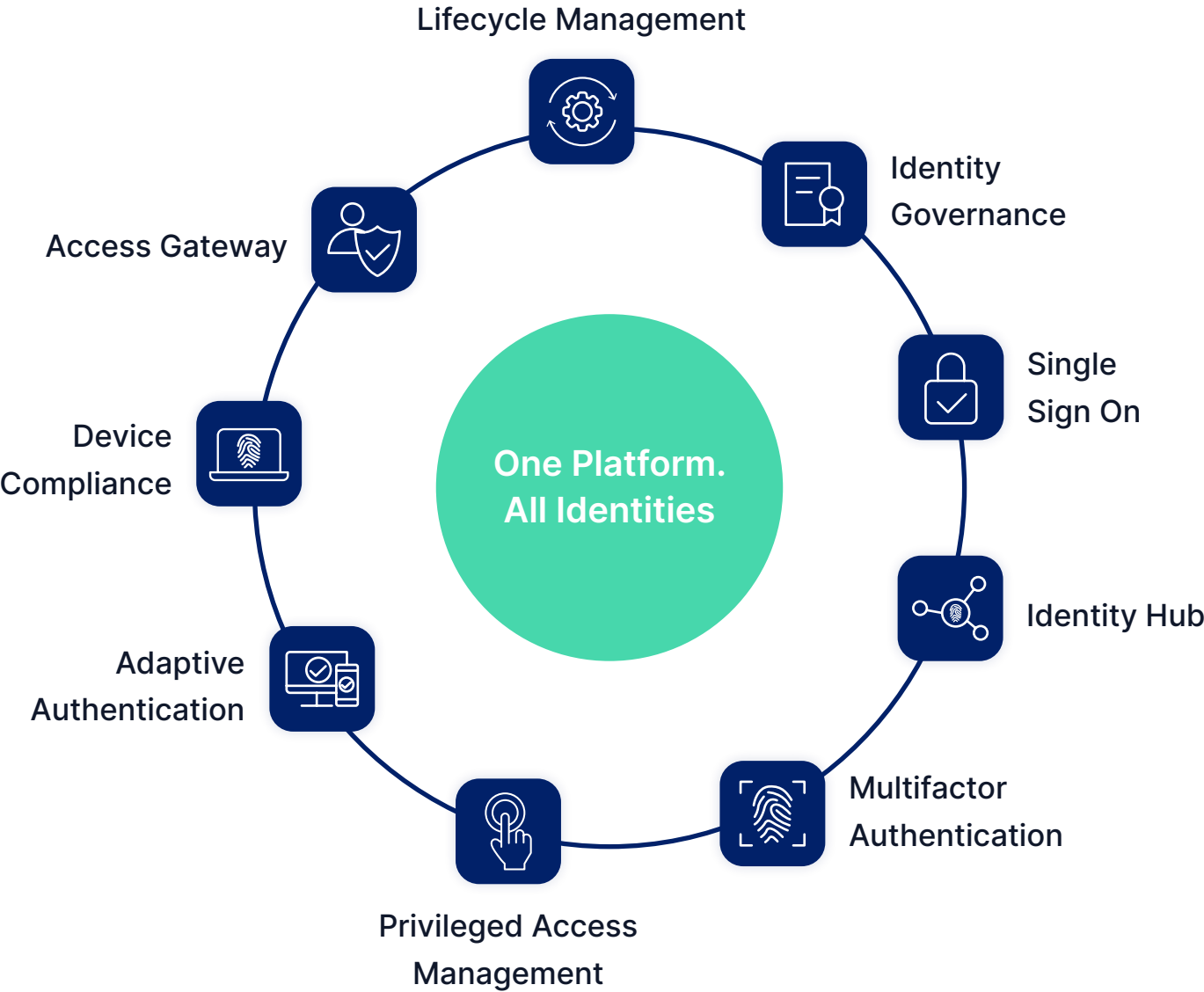
Real-world customer experiences frequently showcase the benefits of adopting a converged IAM platform. While initial business outcomes often emphasize the automation savings within the first year, it is crucial to recognize that the ongoing savings are equally remarkable. By consolidating legacy IAM solutions, implementing advanced process automation, and reducing workloads, enterprises can achieve substantial cost savings and enhance workforce productivity. As an illustration of business value, consider the example of CYMMETRI Governance solution.





Why Cymmetri Workforce IAM?

Cymmetri Workforce IAM is specifically designed to cater to the needs of large and intricate enterprise use cases and demands. The converged solution incorporates distinct elements that set it apart, which include:





Comprehensive IAM platform



This unified workforce IAM solution enables organizations to efficiently manage, secure, and govern all identities across their entire lifecycle from a centralized platform. It offers effective adherence to governance policies, enforcement of least-privileged access, and the establishment of a robust Zero Trust security environment.

The converged workforce identity access management (IAM) solution comprises several key elements that work together to provide comprehensive and efficient identity management, access control, and governance. These elements include:



Identity Management:

This component focuses on the creation, maintenance, and management of user identities. It includes features like user provisioning, self-service registration, and identity synchronization to ensure accurate and up-to-date identity information.



User Lifecycle Management:

The solution covers the entire user lifecycle, from onboarding to offboarding. It simplifies the management of access rights and permissions, ensuring that employees have appropriate access throughout their tenure with the organization.



Access Management:

This element is responsible for controlling user access to resources and applications. It enables single sign-on (SSO), multi-factor authentication (MFA), and adaptive access controls to ensure secure and frictionless user experiences.



Compliance and Audit Capabilities:

The converged IAM solution provides robust compliance and audit features, allowing organizations to track and report access activities to meet regulatory requirements and internal policies.



Identity Governance:

Identity governance involves defining and enforcing policies for access control, entitlements, and roles. It includes features such as access certification, segregation of duties (SoD) analysis, and automated policy enforcement to maintain compliance and reduce security risks.



Scalable Cloud Architecture:

The solution is built on a cloud-native architecture designed to handle the scalability and resiliency needs of large enterprises. It efficiently processes and analyzes access data to support growing user bases and fluctuating workloads.



Tenant Isolation:

The unique security and privacy model of the solution ensures full tenant isolation, protecting data from potential disruptions caused by other tenants in a shared cloud environment. This isolation enhances data security and privacy, even at an enterprise scale.



Automation and AI:

The solution leverages automation and artificial intelligence (AI) to streamline identity and access management processes. Automated provisioning, access requests, automated low-risk approvals, and AI-driven risk assessments improve operational efficiency and enhance security.



Zero Trust Security Model:

The converged IAM solution adopts a Zero Trust security approach, where every access request is continuously verified and authenticated, regardless of the user's location or device. This model minimizes the risk of unauthorized access and insider threats.



How Cymmetri Workforce IAM works

Our Identity Platform Solution

A comprehensive and modern approach to identity management and access control.



Partner Managed Portal





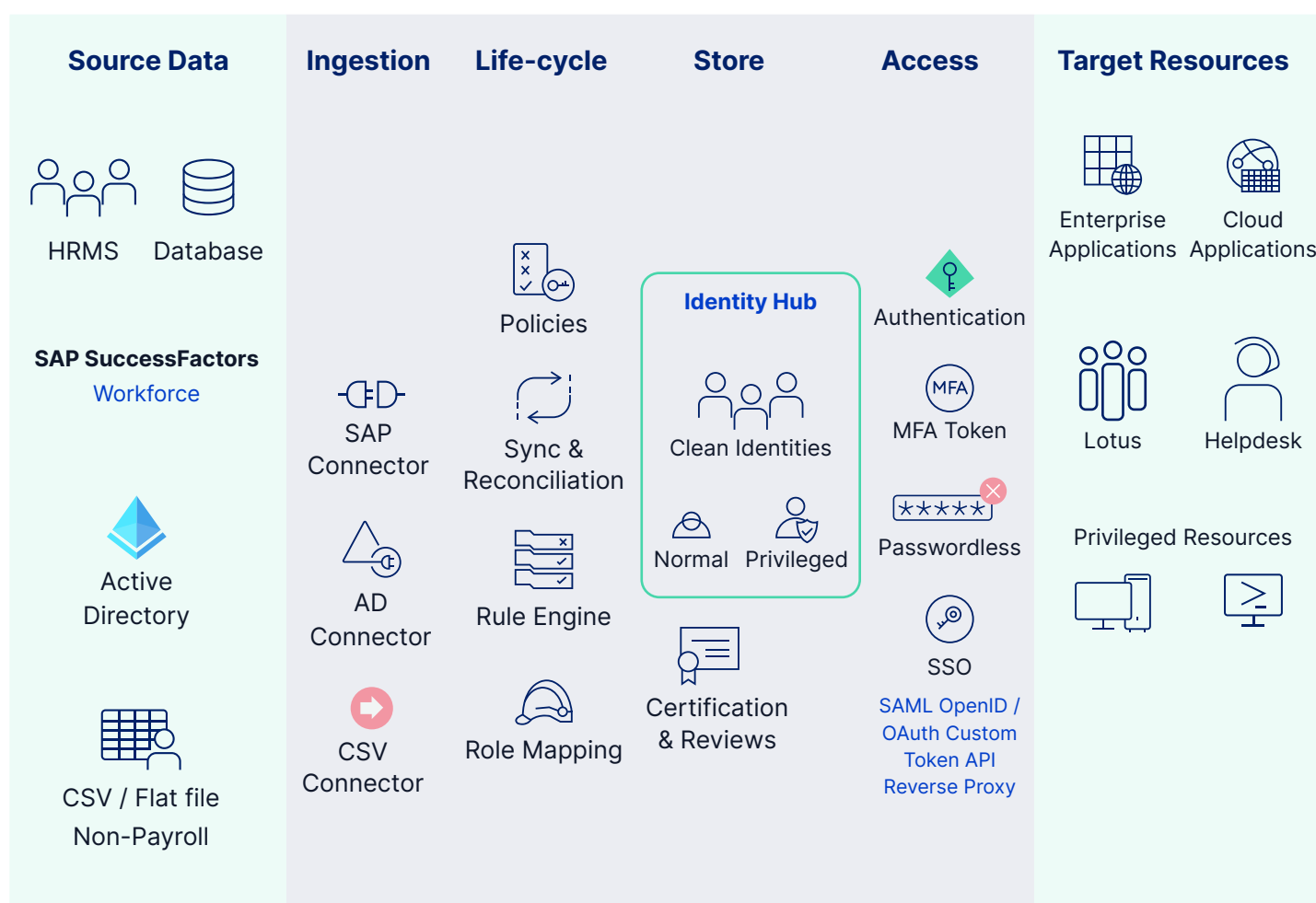
Identity & Access Platform

Cymmetri Converged IAM solution comprises four foundational pillars: Identity Management, Access Management, Privilege Access Management, and Identity Governance. The Converged IAM platform helps organizations manage, secure, and govern all identities and resources.

360-degree view of Identities in identity Hub

Cymmetri Identity Management enables enterprises to efficiently handle user identities and control their access to business applications and resources through automated identity lifecycle management. Organizations can effortlessly create user accounts, manage access permissions, and offer self-service options, including password resets, throughout the entire identity lifecycle. This results in increased workforce productivity by providing quick and seamless access to essential business resources, enabling employees to perform their jobs more effectively.

How it works





✓ **User onboarding**

Enterprise users are onboarded to Cymmetri platform with multiple approaches. Cymmetri connects to the source of truth systems such as HRMS, AD or both. Cymmetri synchronizes from the source systems to the target applications in the enterprise. Once the user identity is created in Cymmetri, the default application or birth-right application will be automatically entitled to users as per the entitlement process.

✓ **Application onboarding**

Easily and swiftly integrate new business applications using a selection of preconfigured application templates from Cymmetri application catalog. Automate user and application assignments based on roles, streamlining the process of provisioning access efficiently. Seamlessly integrate with both custom-built applications and native applications, ensuring smooth and efficient connectivity across your entire application ecosystem.

✓ **Identity lifecycle management**

Streamline and automate the entire joiner, mover, and leaver lifecycle stages for all users, including employees, contractors, and partners. Accelerate the onboarding process, ensuring swift access to essential business applications and resources, enabling them to start their roles promptly and efficiently.

✓ **Identity workflows**

Cymmetri has an internal workflow engine designed for managing access approval and deprovision approvals in the system. The workflow engine can be enabled specific to each application and manage the entitlements process through the workflow.

The workflow has an approval user association process more commonly called approval matrix. For application access, the approval can be one level and go up to multiple levels of approval.

✓ **Secure access**

Cymmetri Access Management ensures the security of access to both modern and legacy business applications and resources, providing a seamless experience for end users. With features like self-service registration, single sign-on (SSO), federation, and multi-factor authentication (MFA), the platform offers a perfect balance of security and user convenience, enhancing the overall access experience.

✓ **Access Management**

Cymmetri Access Management enables the authentication of users and their roles-based access rights in provisioned applications. Here the Attribute Based Access Control & Roles based Access Control configurations in the Provision Rules engine allows the seamless access entitlements for all types of users.



✓ **Adaptive Authentication**

Cymmetri provides ability to use attributes of user's authentication attempt to provide an adaptive authentication experience that allows for achieving high security without significantly compromising on user authentication experience. The available options of the adaptive checks are:

- IP Address Checks
- Device Trust
- Location Based Checks
- Impossible Travel Scenario
- Short-lived Domain Checks
- User Behaviour Checks
- Device Health Checks
- Breached Passwords Checks



✓ **Multi-factor authentication (MFA)**

To provide a strong user authentication process, Cymmetri provides additional factor validation during authentication, aka Multi-Factor Authentication. Using the MFA, the user is required to provide access confirmation before being signed in or SSO.

Cymmetri supports multiple configurable factors such as:

- Cymmetri Authenticator Mobile Application with Push Notifications
- SMS authentication
- Secret Question & Answers
- Google Authenticator
- FIDO based Biometric authentication

✓ **Single sign-on (SSO)**

Cymmetri Self Service console is a portal which allows users to authenticate and get access to entitled applications with SSO, thus eliminating the need to provide username and password for each application access.

✓ **Authorisation**

Cymmetri allows the secure authorization of user's and their ability to work on the enterprise applications. This is achieved by provisioning the user to the required applications based on the organization policies for enabling access. Cymmetri through its provisioning rules allows seamless authorization for enterprise applications with no human involvement.





✓ **Federation**

Cymmetri provides Identity Federation capabilities which allow you to setup the user's authentication journey with different authentication sources. Cymmetri provides option to add multiple identity providers such as:

- Active Directory
- LDAP
- Google (SAML)
- Azure (SAML)
- Salesforce (SAML)



Cymmetri supports adding multiple Identity providers and defining the authentication policies to ensure the users authenticate using the appropriate authentication source.

✓ **Govern identities**

Cymmetri Identity Governance presents a cloud-native governance solution specifically designed to address security and compliance challenges for large, intricate enterprises at scale. Leveraging our unique cloud architecture and proprietary AI and ML technologies, the solution evaluates and determines employees' access rights to applications and data. By generating AI-driven recommendations and confidence scores, the platform empowers organizations to make faster and more informed decisions, and even automates low-risk choices, reducing IT teams' workload.

With Cymmetri Identity Governance, organizations can integrate AI into their governance processes and programs to achieve the following:

- Reduce the burden of excessive access certification tasks
- Enable managers to focus on critical, high-risk access decisions
- Facilitate quicker access decision-making

Cymmetri approach to identity governance encompasses three core components: access certification, access requests, and segregation of duties, making it the most comprehensive offering in the industry.

✓ **Access certifications**

Cymmetri Identity Governance provides for managing user certification through its Campaign Management feature. As part of user access review, a campaign can be set up to automatically process the user entitlements and send the review request to the appropriate approvers in the system. The approver can certify in bulk by either approving or revoking the access of the required users. The revocation of access is in real-time.

✓ **Access requests**

The user can request for access to applications (with role) which are not part of the birth-right access. Access to requested applications can be auto provisioned or enabled only after an approval has been granted by all approvers. The approver associations are configured as part of the application-level workflow.



✓ Segregation of duties

As a part of strong governance controls, Cymmetri provides configuration for Segregation Of Duties or SoD. Every large organization faces the complexity of providing adequate access to its users to allow business as usual practices. However, over time, as more applications and their entitlements come into play, the ability to restrict the access controls involves greater risk.

Cymmetri's SoD attempts to mitigate the access gaps and more than required access to users by defining appropriate business roles and responsibilities and managing them over a long period of time.

Secure privileged access for administration

✓ PAM (Privilege Access Management)

● Session Recording

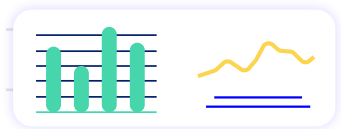
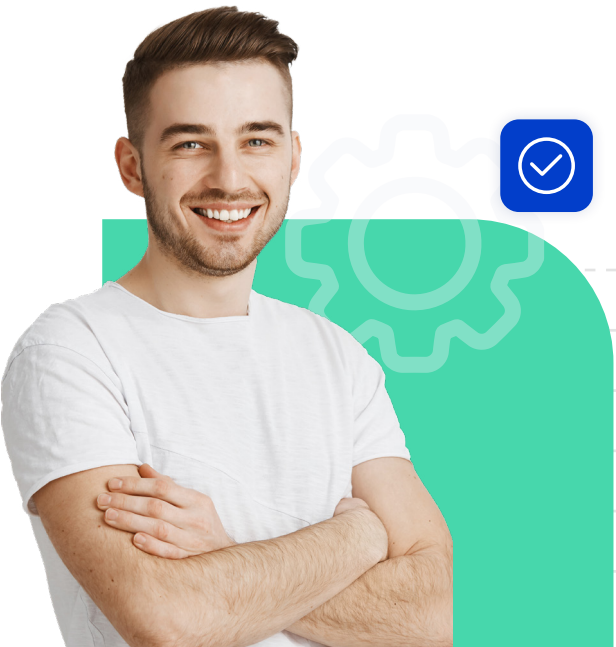
Cymmetri PAM allows monitoring of user sessions for compliance and forensic requirements. Ability to record the commands on specified systems as well as complete session recording of user activity can be configured. Session recording can be setup for specific user accounts such as administrators, partners.

● Vault

Cymmetri PAM securely stores the access credentials of resources in its Vault. The privileged user accessing the resource does not know the password and instead authenticate their access using Cymmetri or Active Directory credentials. The Vault can manage secrets, tokens, passwords, certificates, and encryption keys.

● Device Compliance

Cymmetri Workforce IAM empowers enterprises to attain a comprehensive grasp of their identity provisioning, administration, compliance, and employee access management requirements. Combining AI capabilities with human oversight, organizations can achieve greater adherence to governance policies, enforce least-privileged access, and establish a robust Zero Trust security environment.



Rethinking Your IAM Strategy and Approach

As organizations face the ever-evolving challenges of a digital-first world, rethinking their Identity and Access Management (IAM) strategy and approach becomes imperative for ensuring robust security, optimizing productivity, and maintaining compliance. The traditional siloed and manual IAM solutions are no longer sufficient to cope with the complexities of modern enterprises. To thrive in today's dynamic landscape, businesses must adopt a converged IAM approach that unifies identity management, access management, and identity governance under one comprehensive platform

The Cymmetri Workforce IAM solution is purpose-built to tackle the intricacies of modern digital business. It empowers your organization to efficiently manage, secure, and govern all identities across their entire lifecycle through a unified platform. With this converged IAM solution, you can rapidly secure user access, enhance productivity, and reinforce security measures on an enterprise-scale.

The time has come to shift your perspective, strategy, and approach to IAM. Embrace Cymmetri Workforce IAM as the solution that meets the demands of the present and unlocks the potential of your organization.





About Kathreftis AI,

Kathreftis (Mirror for Security Posture) is not a conventional cybersecurity company. We are striving to build something bigger for the digital world, a change that will help protect organizations and individuals alike. We are taking small steps to achieve this goal. Though we are small in numbers, our efforts are focused on creating a significant impact that will help create a more agile and secure digital environment.enhance productivity, and reinforce security measures on an enterprise-scale.

Visit: www.Cymmetri.com

Connect with us —————>



sales@cymmetri.com



www.linkedin.com/company/cymmetri/