kyndryl.

Kyndryl IAM Design and Implementation Services

Customer Presentation
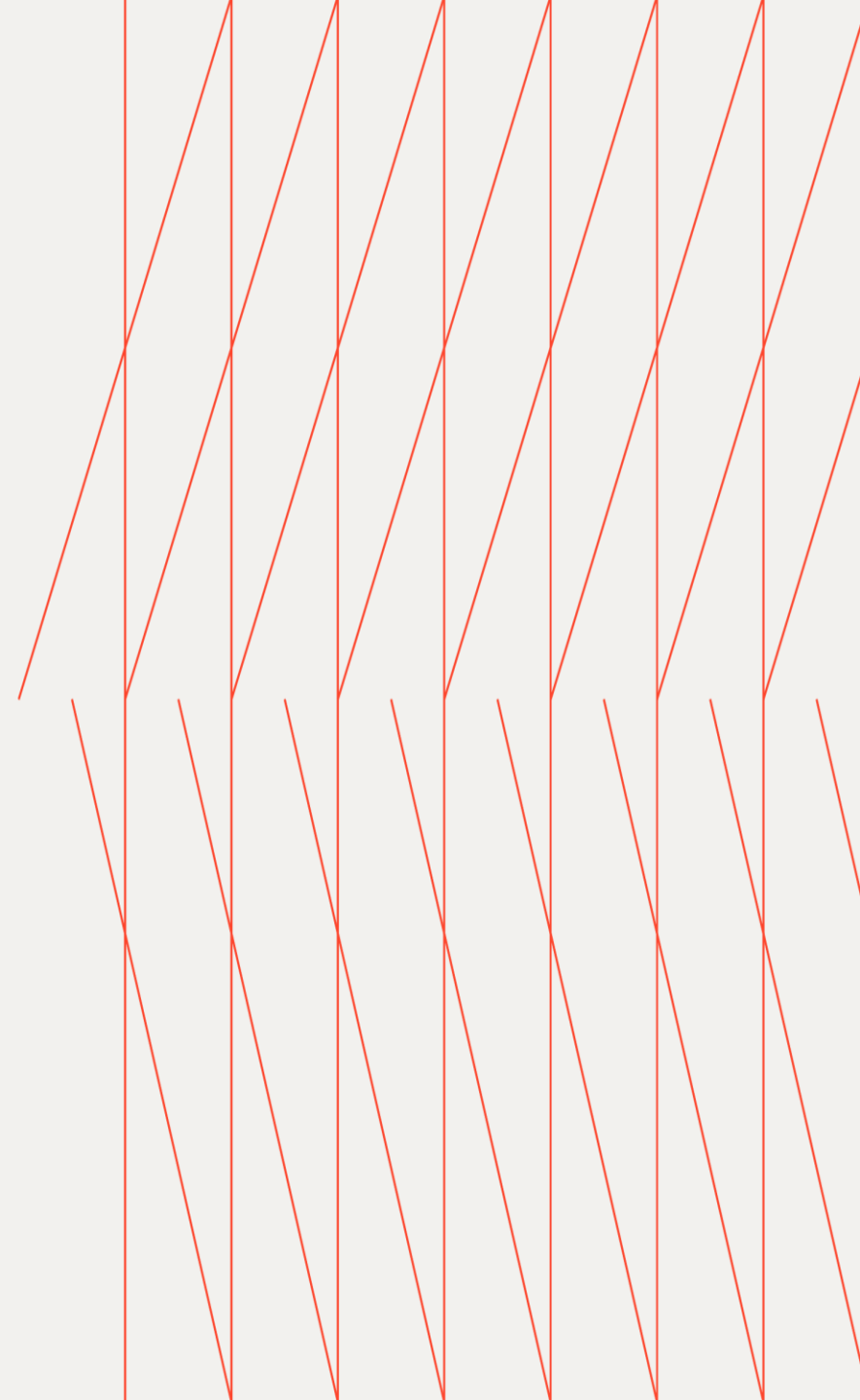
Contents

kyndryl.

What sets Kyndryl Security & Resiliency apart:

- Extensive partner ecosystem to support best-in-class technology solutions
- Improved ability to identify and respond to security threats
- More efficient security teams with flexible, modular delivery models

Leader

NelsonHall's 2024 Cyber Resiliency Services NEAT Assessment | Cybersecurity Services 2022 RadarView Report by Avasant

7500+

Skilled Security and Resiliency practitioners globally

500+

Security and Resilience patents

30+ years

Experience in IT services

50+

countries with Kyndryl Security and Resiliency presence

6

Global Security Operations Centers

40+

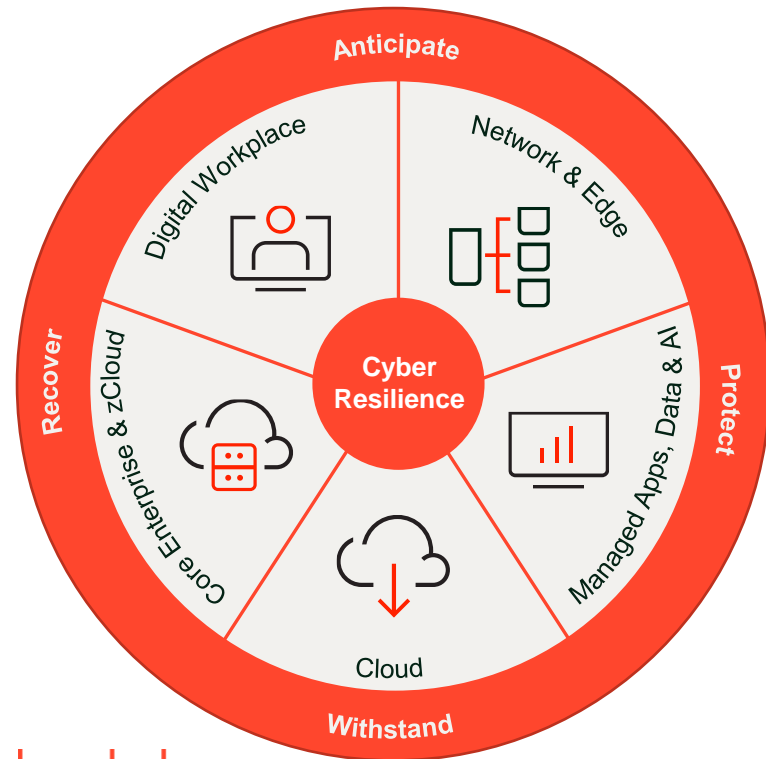Security and Resiliency alliances and strategic partners

kyndryl

Kyndryl's Cyber Resilience Framework

cyber resilience

[**sahy**-ber ri-**zil**-y*uh*ns, -**zil**-ee-*uh*ns]

noun

The ability to anticipate, protect against, withstand and recover from adverse conditions, stresses, attacks and compromises of cyber-enabled business.

Security Assurance Services

Assess and benchmark resilience maturity, gain visibility into significant threats and vulnerabilities, manage compliance

– Risk Management
– Offensive Security Testing
– Compliance Management

Zero Trust Services

Protect critical business data and applications in a security-rich infrastructure

– Identity & Access Management
– Endpoint Security
– Network Security
– Data Protection & Privacy
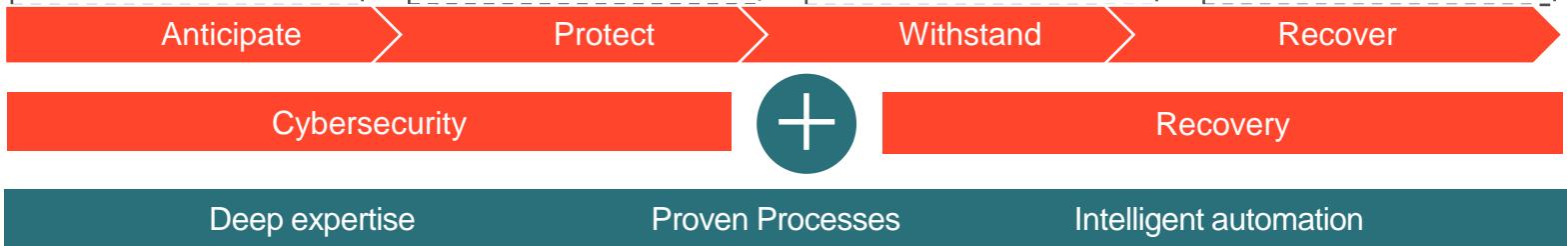
Security Operations & Response Services

Discover and respond to a detected security incident

– Incident Response and Forensics
– Threat Detection & Response
– Vulnerability Management
– Security Operations Center (SOC) Services
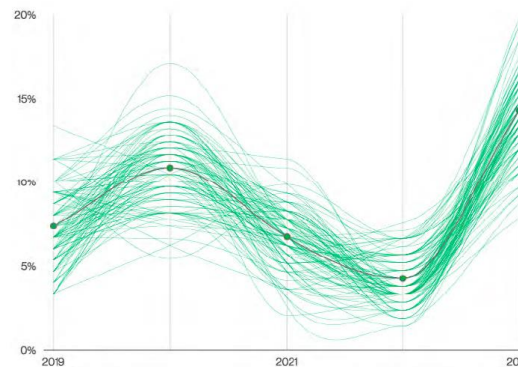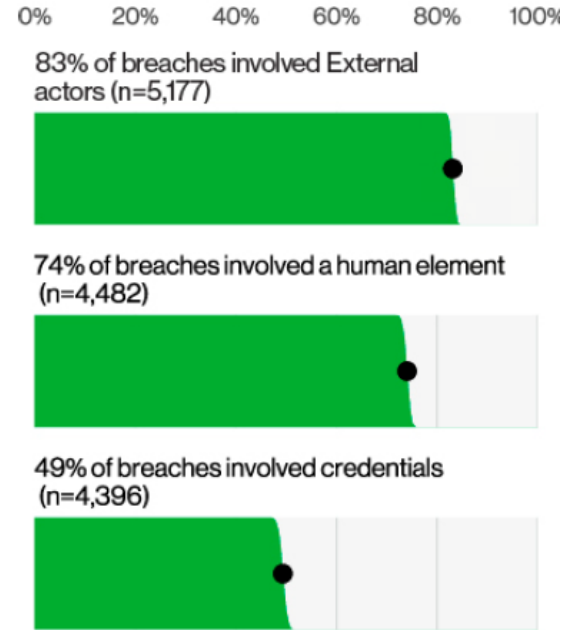– Security Operations as a platform

Incident Recovery Services

Mitigate impact of disruption with capabilities to automatically recover critical business processes and data

– Cyber Incident Recovery
– Managed Backup Services
– Hybrid Platform Recovery
– Data Center Design & Facilities

Anticipate	Protect	Withstand	Recover

Cybersecurity	+	Recovery

Deep expertise	Proven Processes	Intelligent automation

kyndryl.

Defending against identity-based threats has the greatest impact of any cyber security strategy

0% 20% 40% 60% 80% 100%

83% of breaches involved External actors (n=5,177)

74% of breaches involved a human element (n=4,482)

49% of breaches involved credentials (n=4,396)

83% of breaches involved external actors. The primary motivation for attacks continues to overwhelmingly be financially driven − at 95% of breaches.

74% of all breaches include human element with people being involved either via error, privilege misuse, use of stolen credentials or social engineering.

The three primary ways in which attackers access an organization are stolen credentials, phishing and exploitation of vulnerabilities.

Privilege misuse breaches paired with fraudulent transactions are significantly on the rise.

kyndryl.

Source: Verizon, 2023 Data Breach Investigations Report

5

Today's digital landscape and its challenges

Rapid increase of **identities** that need to be protected

Accelerated growth of apps, on and off the corporate network, requiring **secure access**

Hybrid work requires seamless, flexible experience while keeping **access secure**

Identity attacks are on the rise – over **1,000 password attacks** per second

---

Evolving regulations with **data privacy** and **security implications**
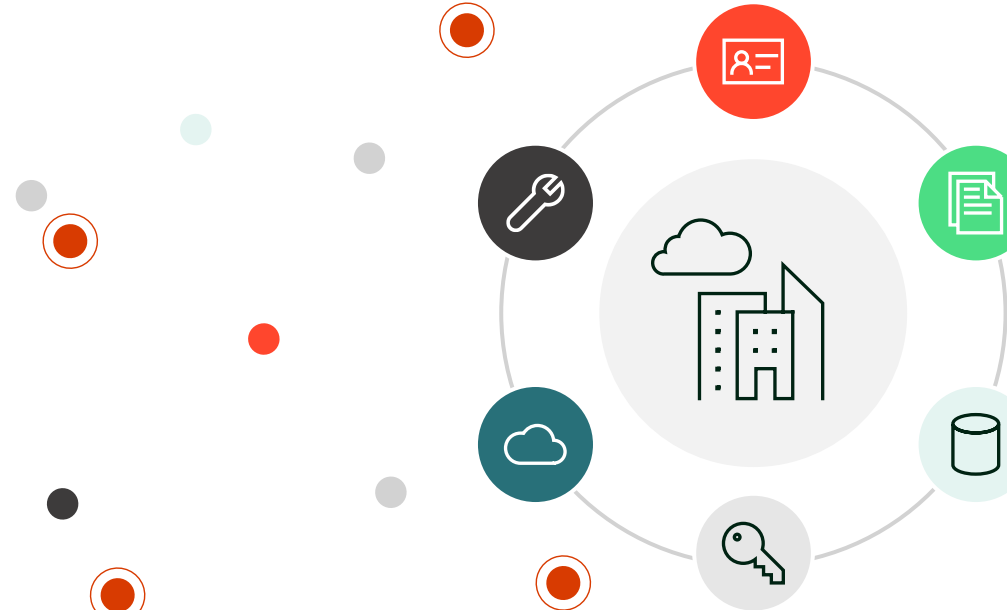
kyndryl

How Kyndryl IAM Design and Implementation Services can help customers

Powered by Microsoft Entra capabilities, Kyndryl IAM Design and Implementation Services provides comprehensive IAM solution design, architecture, and implementation support for a customer's IAM requirements across hybrid and cloud environments. It provides security, simplifies user authentication, governance, integrations and enables secure access to resources. This offering is aligned and underpinned with Zero Trust principles and best practices.

Kyndryl's offering assists enterprises to implement their Zero Trust strategy by:

− Selecting and implementing a Zero Trust framework.

− Aligning business objectives with security goals.

− Identifying and addressing security process friction points.

− Designing intricate solutions to address challenges.

− Executing best practices for effective implementation.

− Managing and overseeing the security program.

− Continuously updating and modernizing security measures.

kyndryl

Foundation of **Zero Trust**

| Identity | Device | Network | Application | Data |

Governance
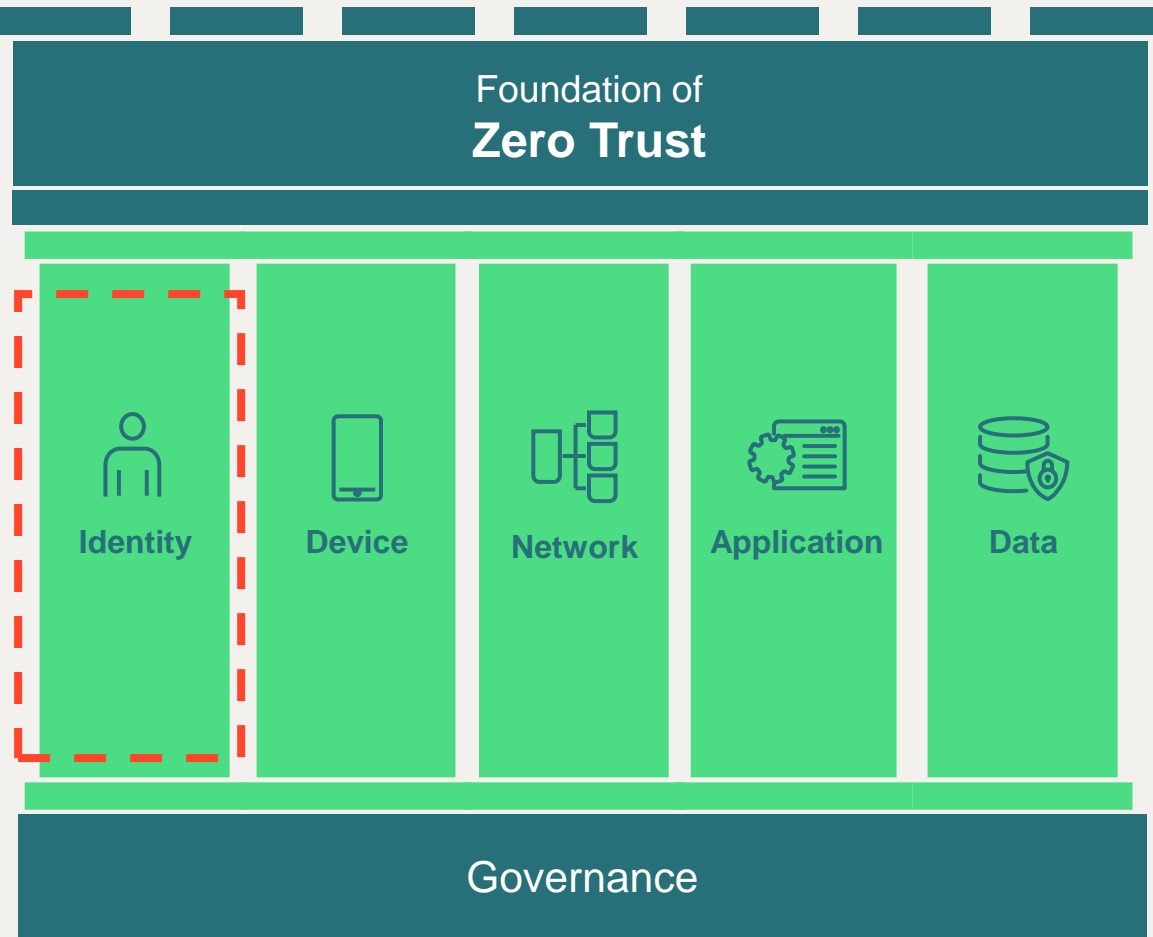
What Kyndryl's solution offers

Design and implementation services for IAM by leveraging Microsoft Entra for both human and non-human actors

B2E
- Hybrid Identities
- Password-less & Seamless Access
- AI / ML Access Control
- Adaptive Auth. & Priveleged Access
- Identity Analytics
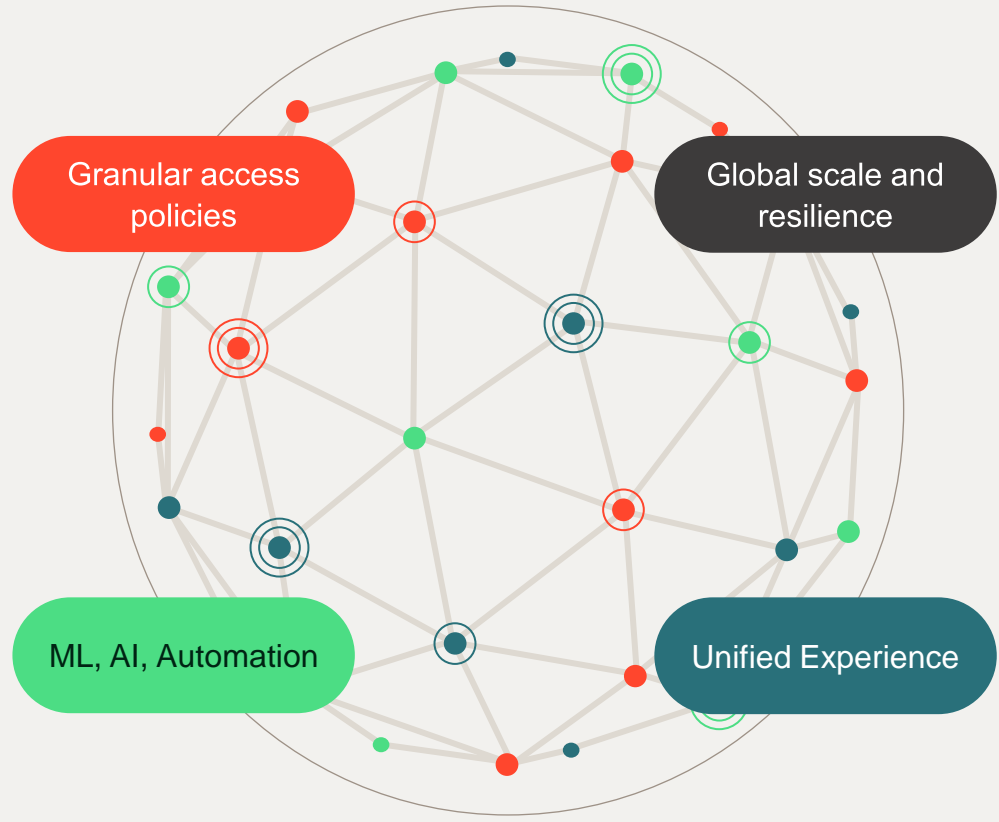- Regulatory Compliance & Governance

B2B
- Quick Partner user onboarding
- Simplified & Secure login process
- Seamless App Access
- Efficient Information Controls
- Controlled Information sharing
- Effective Access Governance

B2C
- User Experience
- Manage Customer identities in scale
- Friction-free login Process
- Meets privacy and data compliance standards
- Gain 360* Customer insights

Human identities

Workload identities

Customers

Partners

Devices

Granular access policies

Global scale and resilience

ML, AI, Automation

Unified Experience

Powered by trillions of security signals

Data

SaaS apps

Cloud-hosted apps and resources

On-premises applications

Websites

kyndryl

# Kyndryl IAM Design and Implementation Services

Overview

In today's digital landscape, where cyber threats and data breaches are a constant concern, Identity and Access Management (IAM) stands as a critical pillar of robust cybersecurity strategies of enterprises. IAM encompasses the policies, technologies, and processes that enable appropriate access to resources by the right individuals at the right time, while also preventing unauthorized access and potential breaches.

Kyndryl's IAM Design and Implementation Services powered with Microsoft Entra capabilities offers design and implementation services for an IAM setup which addresses the enterprise need for a centralized IAM, enhancing security by utilizing cloud native, zero trust principles and focus on a seamless user experience.

Capabilities

- **Unified Identity Platform:** Microsoft's IAM unified platform for managing identities streamlines identity management processes and enables consistent access controls across the entire Microsoft ecosystem.

- **Scalability and Flexibility:** With Kyndryl's IAM offering with Microsoft Entra, organizations can scale their identity infrastructure to meet growing business needs.

- **Enhanced Security:** Advanced security features including multi-factor authentication (MFA), conditional access policies, privileged identity management (PIM), and identity protection capabilities, etc.

- **Simplified User Experience:** Our solution prioritizes user experience in its IAM offerings, ensuring that accessing resources and applications is intuitive and frictionless for end-users while maintaining security.

- **Integration with Microsoft and other Ecosystem:** We offer interoperability by leveraging Microsoft Entra product for cloud-based identity management or integrating with on-premises Active Directory environments.

- **Compliance and Governance:** Microsoft's IAM platform includes built-in compliance features & reporting capabilities to help organizations meet regulatory requirements such as GDPR, HIPAA, and SOC 2.

Kyndryl Identity and Access Management Reference Architecture - Microsoft Entra
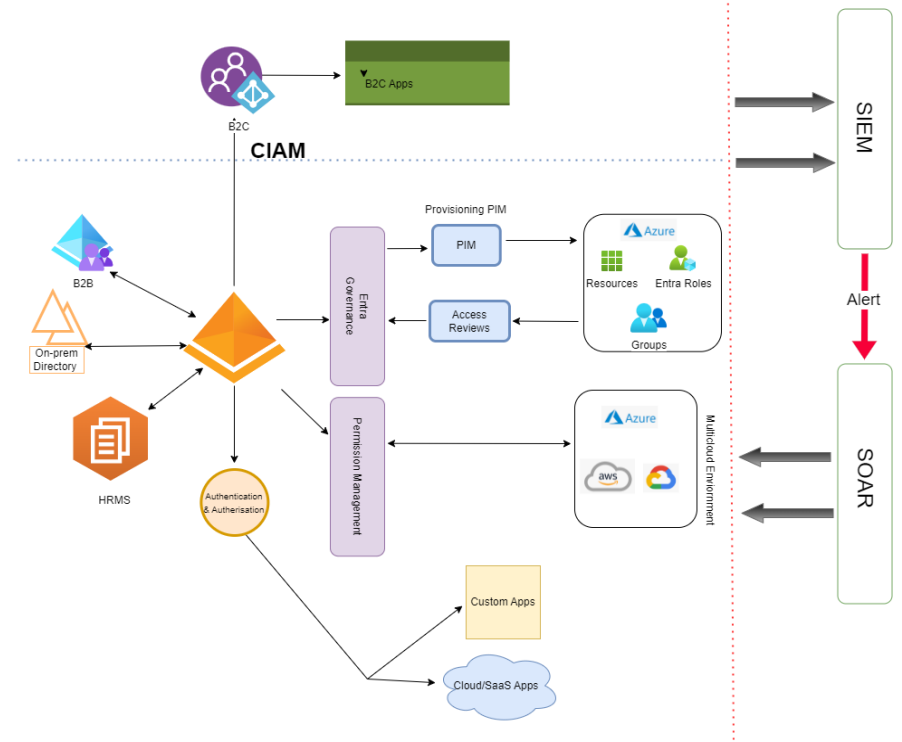
Supported Vendor Products

- Microsoft Entra ID, Microsoft Entra ID Governance, Microsoft Entra External ID, Microsoft Entra Permission Management

kyndryl

Customer Value

Our services safeguard organizations' resources and data through robust authentication and real-time, risk-based access policies, prioritizing user experience. We enable appropriate access to resources for authorized individuals when needed. With a comprehensive customer identity and access management solution, we personalize and secure access to applications for customers and partners alike. By implementing a Zero Trust strategy, we prioritize least privilege for privileged accounts, offering enhanced protection against cyber threats and delivering value to our customers.

Secure adaptive access

Seamless user experiences

Unified identity management

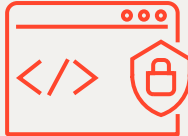Improve Productivity

Strengthen Security
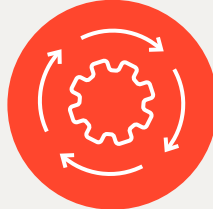
Automate routine tasks

Secure partner and customer access
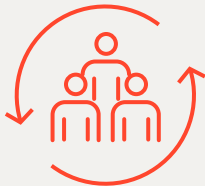
Create people-centric experiences

Accelerate development of secure applications

kyndryl

Thank You

kyndryl