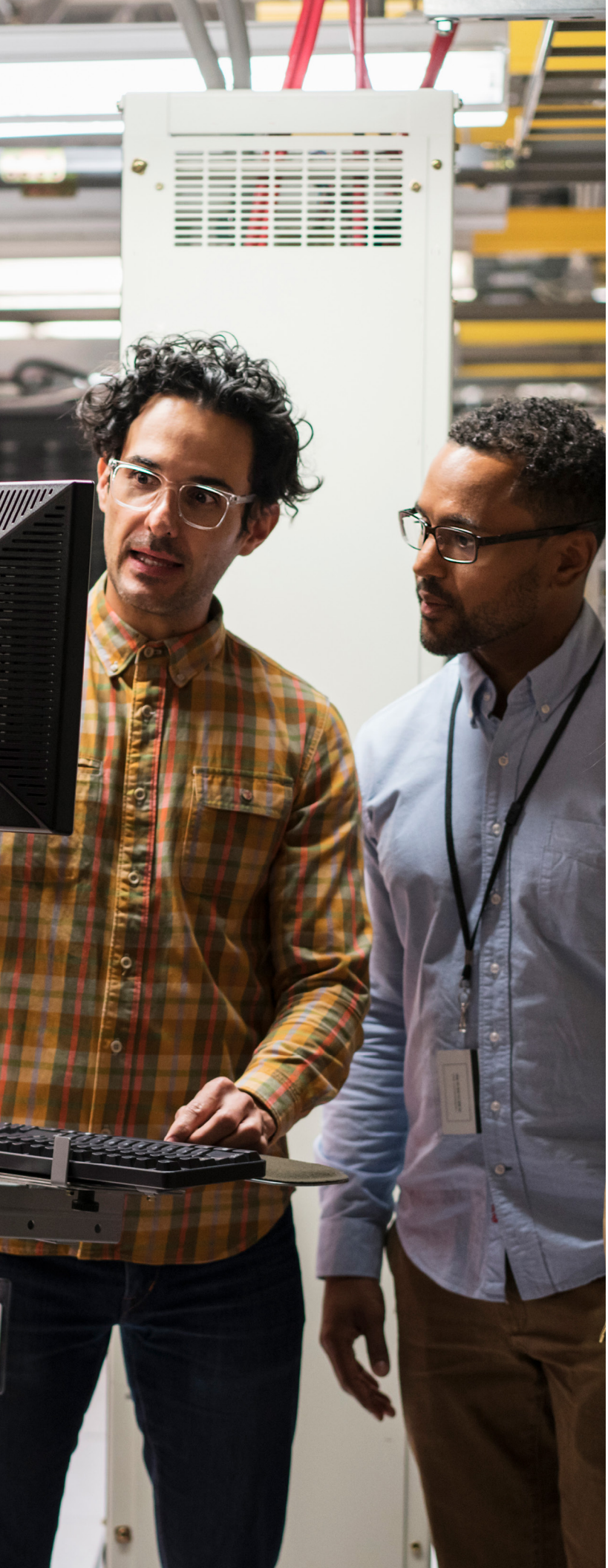

kyndryl

Kyndryl Zero Trust Services

Customer challenges

Organizations have invested in layered, in-depth security point solutions. However this is a siloed approach which makes it difficult for customers to prevent security breaches and cyber incidents in a rapidly evolving IT environment.

CISOs, CIOs and business leaders need a new mindset, strategy and architecture to break the siloed approach towards security and enable an integrated framework underpinned by governance across all five elements– identity, device, network, apps, and data.

The Zero Trust stance is “never trust, always verify.” According to the U.S. National Security Agency, “Zero Trust should be able to prevent, detect, and contain intrusions significantly faster and more effectively than traditional, less integrated cybersecurity architectures and approaches”.[1]

Zero Trust cybersecurity model

Zero Trust is a cybersecurity framework that helps you manage threats beyond traditional network boundaries. Zero Trust assumes there is no inherent trust granted to users based on specific attributes such as physical location or ownership. Due to the evolution of the traditional IT boundaries, workload and workforce distribution, and cloud and digital adoption, traditional security practices are insufficient to ensure enterprise security and resiliency. The growing sophistication and frequency of attacks and consequentregulatory requirements is fueling a need for new trust architecture. Before and during access to applications, data, and systems, Zero Trust requires all users to be authenticated, authorized, and continuously validated for security.

Kyndryl Zero Trust framework includes a prioritized approach. We start by securing what is most important and risky, selecting the right use cases based on the business objectives, and leveraging Zero Trust public frameworks.

With Zero Trust, users and applications are granted access only when and where they need it, enforcing a dynamic and continuous system of verification for users and their devices. It enables enterprises to better protect data and minimize the potential impact of an attack, while also facilitating a more localized, rapid response.

Solution highlights

Zero Trust Services from Kyndryl is a modern cybersecurity strategy that integrates multiple visibility points, automates detection and response, and performs risk-aware access decisions. It strengthens and streamlines protection of critical applications, data and systems; and leverages intelligent automation to drive reduced cost and complexity.

Many organizations use cyber security protocols that extend trust to employees working from an office location, typically only requiring validation in the morning. With Zero Trust Services, all endpoints and accounts are suspect. This is a new security mindset. The expectation is that systems will be breached, so security is positioned as if there is no perimeter. Continued and ongoing validation of communication is enforced. The key benefits of Zero Trust Services include:

1. Leveraging your existing security investments for quicker results and better returns on investment (ROI)
2. Driving prevention by identifying risks and recommending solutions across complex hybrid environments
3. Providing multi-disciplinary security expertise
4. Applying Zero Trust principles to secure business outcomes

Proven reference architecture for faster-time-to-value

Zero Trust Services is designed for organizations to reduce cyber threat risks, meet compliance goals, and maximize transformation outcomes. Kyndryl offers unique technical expertise across technologies and platforms, a portfolio of IP enablers, and a broad ecosystem of partners. With continuous security, availability, and compliance, Kyndryl Zero Trust Services reduces disruptions to deliver improved user experiences. Our proven reference architecture helps you achieve faster time-to-value. These services help you mitigate risks and protect your enterprise data by:

→ Providing gap analysis for transitioning to the cloud

→ Helping discover, classify, protect and monitor critical data access and usage

→ Delivering 24/7 protection to monitor, automate, and enforce security policies and compliance requirements

→ Enabling development of scalable, quickly-deployed solutions

→ Implementing controls across identities, devices, data, applications, infrastructure, and networks

Depending on organizational readiness, Zero Trust implementation can be complex. We feel that a phased approach, where you align Zero Trust priorities with your risk tolerance—or with other IT transformation initiatives—is best. Kyndryl consults with you to convert recommended strategies into transformational programs tailored to the needs of the business.

Kyndryl Zero Trust offerings include:

→ Identity and access management

→ Endpoint security

→ Network security

→ Application and workload security

→ Data protection

→ Analytics, automation and orchestration

At Kyndryl, we see Zero Trust as five integrated security pillars: identity, device, network, application, and data. With Zero Trust, security becomes a 360-degree integrated system where communication and collaboration across these pillars or departments is key. Identities, passwords, and network assets are centralized in trusted repositories.

Zero trust requires a fundamental shift in the security mindset on an organizational level. This approach isn't a one-stop-shop policy or product. Instead, it's a dynamic and evolving security process with no fixed end point.

By adopting this risk-based and adaptive policy, enterprises are empowered to build a set of security practices uniquely suited to their changing needs and goals. That's why at Kyndryl, we take an individualized, phased approach. We align Zero Trust with each enterprise's individual risk profiles as well as with their other major IT transformation initiatives, focusing on what matters most to the security and future of the business.

Use cases

Due to the COVID-19 pandemic-era boom in workforce distribution and a move towards hybrid cloud infrastructures, the Zero Trust security strategy and mindset are quickly becoming more important.

A Zero Trust approach can be formulated based on an assessment of your most mission-critical IT assets. Examples of common use cases follow.

Multi-location access to enterprise hybrid-cloud

Improvement of the access experience for employees

→ Mobile users “out in the wild”
→ Remote corporate location (satellite physical location)
→ Internal to HQ

Common use cases for zero trust principles

Contracted services/ non-employee access

→ Visitor
→ OT maintenance contractor
→ IT vendor/consultant

Move to cloud

→ CI/CD pipeline, application and infrastructure

Cloud to cloud integration

→ System to system communication and controls for distributed workloads

Collaboration across enterprise boundaries

→ Federation across B2B organizations

IoT

→ Manufacturing
→ IoT sensors (dumb devices)
→ Electric vehicles
→ Smart metering/ smart grid
→ Smart building

BYOD

→ Business users leveraging personally-owned devices

Privileged access to critical infrastructure

→ Local or domain administration accounts, service accounts

Enterprise with public or customer facing services

→ B2C use case

Figure 1: Examples of common use cases

Why Kyndryl?

Kyndryl has deep expertise in designing, running, and managing the most modern, efficient, and reliable technology infrastructure that the world depends on every day. We are deeply committed to advancing the critical infrastructure that powers human progress. We're building on our foundation of excellence by creating systems in new ways: bringing in the right partners, investing in our business, and working side-by-side with our customers to unlock potential.

For more information

Talk to a Kyndryl expert—schedule a 30-minute strategy session at no cost. Explore the Kyndryl Cyber Resilience website. Contact Kyndryl for Kyndryl services sales or any other enquiries. Or visit us at kyndryl.com

kyndryl

1. "Embracing a Zero Trust Security Model," National Security Agency of the United States, Feb. 2021. https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF