Empower your business with cyber resilience

kyndryl

The Heart of Progress™

Content Guide

Empowering enterprise resilience with minimized downtime

With cyber threats on the rise, resilience is more important than ever.

As digital transformation and hyperconvergence create unintended gateways to risks, vulnerabilities, attacks, and failures, a cyber resilience strategy is vital for your business. It can help your business to reduce risks, financial impact and reputational damages.

92%

of respondents said their organization has experienced an adverse event in the past two years that compromised or disrupted IT systems*

$4.45M

was the average cost of a security breach in 2023**

kyndryl

*_State of IT Risk Survey_, Kyndryl, 2023

**_Cost of a Data Breach Report 2023_, Ponemon Institute and IBM Security, 2023

Five tips to empower your organization with a cyber resilience strategy

kyndryl

1 Proactive threat intelligence

Establish robust threat intelligence capabilities to identify and anticipate cyber threats.

2 Risk-based approach

Focus on protecting critical assets and data while conducting risk assessments, implementing appropriate controls, and continuously evaluating the effectiveness of security measures.

3 Zero-trust architecture

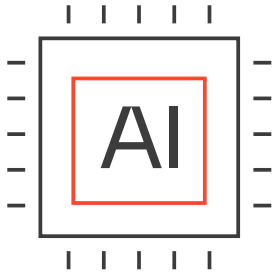
Implement zero-trust principles that assume no user or device should be inherently trusted.

4 Privacy and data protection

Protect sensitive information and support compliance with relevant laws to safeguard personal data and uphold customer trust.

5 Response and recovery

Minimize the business impact of cyber disruption and automatically recover critical business processes and data across the entire IT infrastructure.



Harnessing AI for elevated security

In the evolving global landscape, the rise of generative AI presents both opportunities and challenges.

When it comes to this new era in enterprising computing, taking a more proactive approach to cybersecurity is essential.

$143B

Enterprise spending on generative AI solutions is forecasted to reach $143 billion by 2027*

But Kyndryl survey data found that only...

17%

of the executives surveyed said their companies have documented a position on responsible AI**

kyndryl

GenAI Implementation Market Outlook: Worldwide Core IT Spending for GenAI Forecast, 2023-2027, IDC, October 2023

**What C-suite leaders say about generative AI at scale*, Kyndryl, 2024

Five strategies to empower secure and responsible AI at your organization

1 **Shore up your defense**

Prioritize robust data governance and responsible AI practices/guidelines specific to your industry.

2 **Accelerate threat intelligence**

Automate SOC tasks with AI to enhance efficiency and use AI to fast-track the development of advanced predictive models.

3 **Shift from reactive to proactive**

Move from a reactive security posture to a cyber resilience approach. Leverage AI insights to improve decision-making.

4 **Manage the cyber skills gap**

Bridge the cyber skills gap by leveraging AI-driven tools for threat detection and response.

5 **Enhance security trainings**

Implement AI-driven simulations and exercises to train analysts while preparing your team to respond to real-time threats.

Embracing zero trust principles for enhanced protection

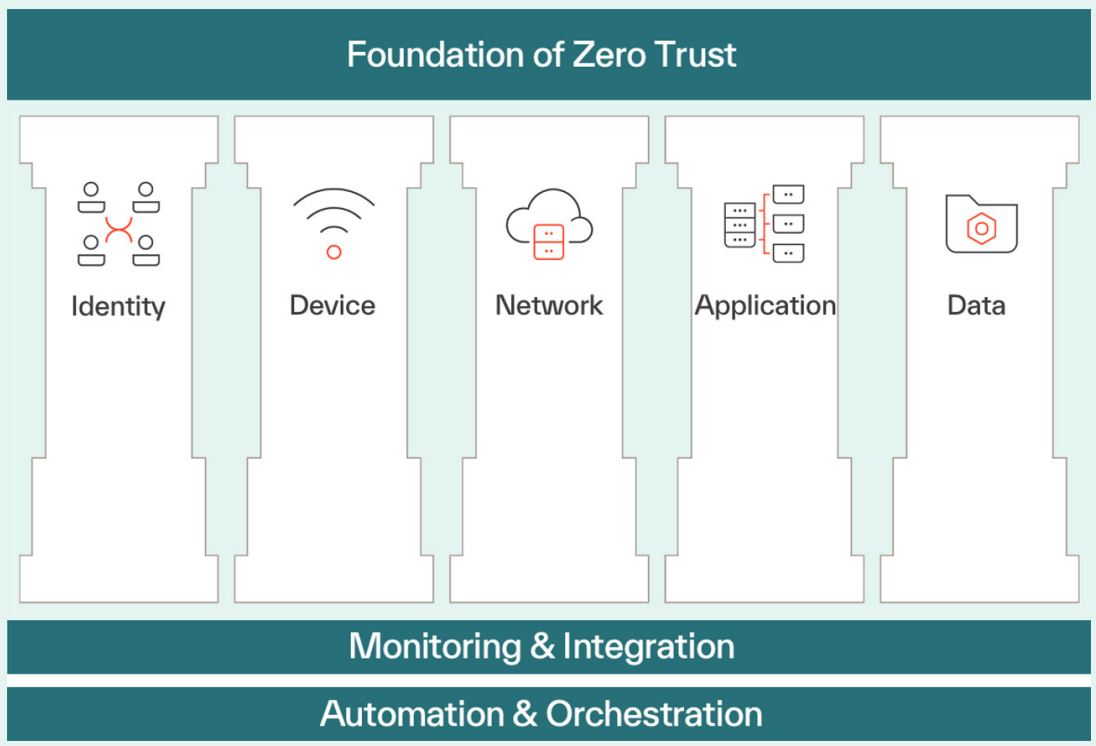
We believe that if done right, zero trust can help enterprises improve cybersecurity, user experience and productivity — while also reducing risk of damage and loss.

63%

of organizations world-wide have either fully or partially implemented a zero-trust strategy*

79%

of organizations that have fully or partially implemented zero trust have strategic metrics to measure progress, and of that 79%, 89% have metrics to measure risk*



kyndryl

*2024 State of Zero-Trust Adoption Survey, Gartner, April 2024

Three tips to empower a successful zero-trust strategy

1

Change your perspective

Zero trust requires a mindset shift. Historically, security operations have been heavily siloed, with one department in charge. Zero trust is an enterprise model that involves five cross-departmental pillars: identity, device, network, application and data.

For a zero trust policy to work, the departments that handle these pillars must come together and take a close look at:

- How to approach security
- How to invest in security
- How to execute a collaborative approach across the five pillars of zero trust

2

Approach zero trust in phases

Zero trust model implementation should be an ongoing process, approached in phases. That makes the optimal place to start with zero trust implementation different for every enterprise.

Process-wise, however, the first step remains the same: determine your priorities. Establish what matters most to your company from a risk-perspective. This is a key and fundamental starting point to any successful “zero-trust” strategy.

Zero trust is a process with no real end point, so it is important to remain focused on the real, tangible benefits of this strategy.

3

Embrace new business opportunities

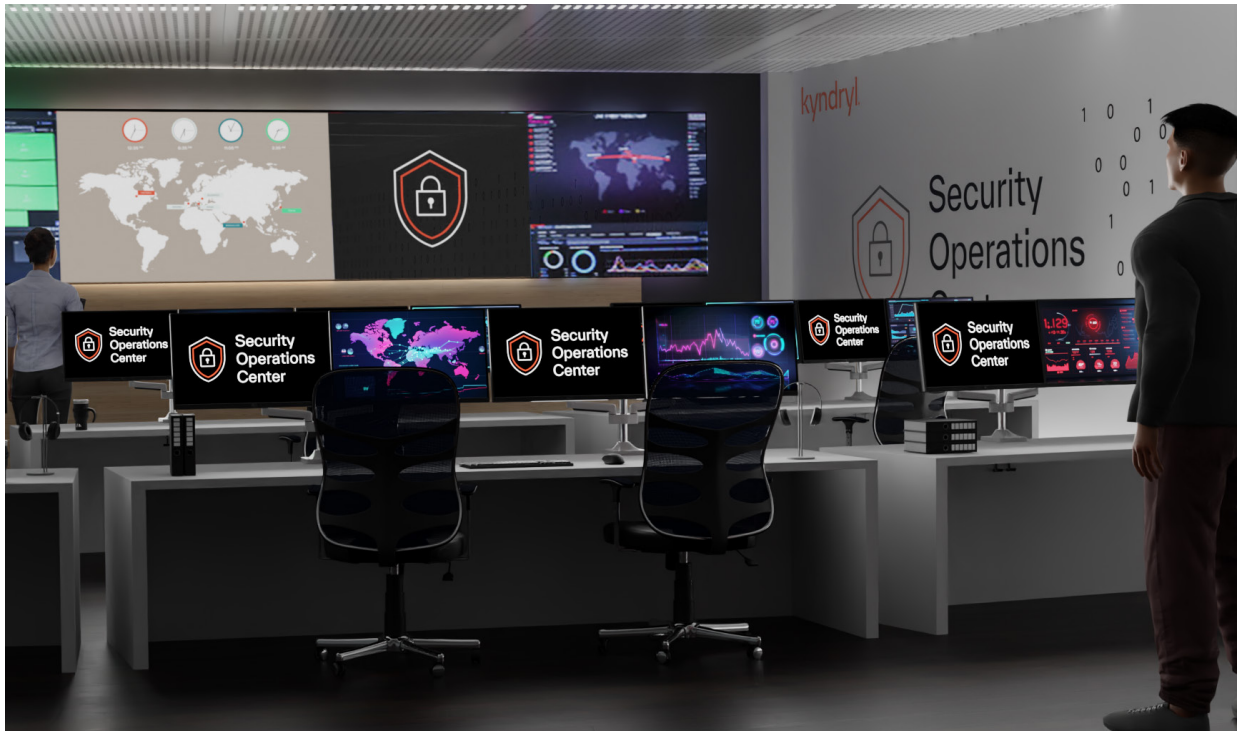
Once you’ve helped your enterprise understand zero trust, it’s time to see what the strategy has to offer.

First and foremost, zero trust opens new opportunities. It enables your team to conduct business in new, more secure ways and futureproof operations to better protect against increasingly sophisticated hacking methods.

By applying broader controls and verification processes, zero trust enables distributed workforces and their distributed computing systems to do work with sensitive data from wherever they are, more efficiently and more securely.

Strengthening cyber resilience

in an evolving threat landscape



With a cyber resilience strategy, companies can better anticipate, protect against, withstand and recover from cyber incidents of all kinds. Enterprises that focus on cyber resilience and take a few proactive steps will have an advantage.

$60B is how much software supply chain attacks are estimated to cost businesses worldwide by 2025, up from $46B in 2023*

69% of respondents indicated that their organizations were targeted by successful ransomware attacks in the past year**

kyndryl

*2023 Software Supply Chain Attack Report, Snyk, October 2023

**Ransomware Study: Organizations Are Less Prepared than They Believe to Recover from Ransomware Attacks, IDC White Paper, sponsored by Kyndryl, December 2023

Five actions organization can take to reduce cyber risks, minimize impact and speed recovery

1 Evolve the role: from CISO to Chief Resilience Officer (CRO)

The CISO must become the CRO, focusing on embedding resilience into every aspect of the organization.

2 Defense, resilience, and recovery assessment

Move beyond traditional cybersecurity by ensuring your defenses, resilience, and recovery capabilities are robust and up to date.

3 Enhance real-time visibility

Implement observability platforms for real-time visibility into your entire IT estate to manage threats effectively.

4 Partner for transparency in testing

Collaborate with developers to ensure transparency in software testing, especially for rapid updates.

5 Control software protections

Take a phased approach to software updates and configurations to control risks and maintain stability.

kyndryl

Navigating regulatory compliance for business success

As critical infrastructure industries digitize, maintaining the resilience of digital systems is essential to protect against cyber threats and ensure operational continuity.

With new regulations emerging from the EU, U.S., and other global entities, businesses must adapt their strategies to comply and thrive in this evolving landscape.

71% of respondents report that they've experienced a cybersecurity-related incident*

84% agreed or strongly agreed that their organization relies heavily on IT assets to operate critical business processes*

50% of respondents who experienced an attack reported that their business operations were disrupted*

*State of IT Risk Survey, Kyndryl, 2023

kyndryl

Five tips to prepare your organization for global cyber resilience regulations

1 **Engage the board and entire business**

Cybersecurity requires board-level involvement and enterprise-wide engagement. It's not just a niche issue; it affects everyone.

2 **Identify your "minimum viable company"**

Focus on protecting the core parts of your business that are critical to operations and success.

3 **Conduct a comprehensive inventory and risk assessment**

Know your assets and vulnerabilities to protect the most crucial elements of your IT estate.

4 **Prepare and practice crisis management**

Develop and regularly test a crisis management plan to be ready for inevitable cyber disruptions.

5 **Adopt and update a zero trust framework**

Implement a zero trust approach and continuously evolve your cyber resilience strategy to stay ahead of threats.

kyndryl

Preparing for the future with quantum readiness

As a new era approaches, enterprises must prepare for the transformative impact of quantum computing.

With all that's at stake—including sensitive data, financial assets, intellectual property, and your organization's reputation—it's crucial to ensure your systems are quantum safe to protect against emerging cyber threats.

Failing to prepare for the quantum era could expose your business to data breaches, regulatory penalties, and a significant loss of trust from customers and stakeholders.

93% of respondents agree that quantum technologies will have significant implications for their regulatory frameworks*

98% of electronic data is safe today, but as quantum computing power advances, it will quickly decode the current encryption methods protecting that data**

kyndryl

*_Quantum Security for the Financial Sector: Informing Global Regulatory Approaches_, World Economic Forum, January 2024

**_Quantum Hacking Demands New Tools Now_, Boston Consulting Group, September 2024

Three steps to jumpstart a journey to quantum readiness

1

Assess your security posture

Evaluate current risks

Identify strengths and weaknesses through internal and external assessments.

Embed quantum risk

Integrate quantum risk considerations into governance and cybersecurity models.

Impact analysis

Understand the potential regulatory, financial, and reputational consequences of quantum breaches.

2

Raise organizational awareness

Educate and engage

Inform your workforce about quantum computing's benefits and risks.

Identify stakeholders

Find champions within your organization to sponsor quantum-safe initiatives.

Update regularly

Share emerging quantum-safe practices and encourage active participation.

3

Define and execute a quantum-safe strategy

Prioritize investments

Focus on securing technology, cryptographic systems, and third-party suppliers.

Plan the transition

Decommission outdated technology and validate new standards.

Ongoing approach

Continuously reassess and reprioritize as quantum threats evolve.

kyndryl

Schedule a 30-minute, no-cost strategy session with a cyber resilience expert.

Let's talk.

For more ways to be cyber smart, visit:

kyndryl.com/perspectives

kyndryl.com/news