kyndryl

Kyndryl Cyber Incident Recovery with Dell Technologies

Customer challenges

CTOs, CIOs, CSOs, and IT professionals are under increasing pressure from escalating expense and data loss risks due to cyber threats. Cybersecurity issues represent as high as 32% of recent unplanned outages[1]. Even with shrinking capital expense budgets, the costs and time spent on data and application protection, business continuity, and regulatory compliance are growing. The average cost of a ransomware attack is $4.54M, and average time to identify and contain a data breach is as high as 277 days[2].

With exponential growth in sophisticated cyber threats and related expenses, organizations need innovative and powerful solutions to protect their critical data. That is why Kyndryl and Dell Technologies have created a fully managed solution that helps customers simplify and manage complex data recovery and restoration issues.

Solution benefits

The Kyndryl Cyber Incident Recovery with Dell Technologies solution includes complete data protection services, with advanced technology, expertise, and standards. Customers get 24/7 access to technical experts and resiliency innovation. This solution isolates and protects your mission-critical business applications and data, on- and off-premises and in the cloud.

Kyndryl Cyber Incident Recovery with Dell Technologies helps you pre-empt cyberattacks and mitigate risks with machine learning and intelligent analytics.

1. Early identification and detection and rapid recovery from a cyberattack, ensuring business continuity and fast service restoration
2. Insight and high information availability
3. Scalability and adaptability to meet changing business demands
4. Reduced TCO and improved ROI

Network-based, air-gapped, remote vault

With Kyndryl Cyber Incident Recovery with Dell Technologies, your data is secured in a highly limited network-based air-gapped vault. The vault is a remote security-rich cyber recovery environment for your data. Immutable storage preserves the integrity, confidentiality, and availability of the vault data. Data in the vault is analysed to identify potential cyber infections. If—and when—a cyberattack occurs, the most current clean data copy in the vault is identified and recovered. The clean data is tested in a secure clean room in the vault before restoring it to the production environment.

Learn more about the Kyndryl and Dell partnership and joint solutions.

Not if but when a cyberattack happens

Watch a video about the challenges enterprises face when it comes to protecting and restoring business-critical data. Kris Lovejoy, Global Security & Resiliency Practice, Kyndryl, shares her perspective.

Why Kyndryl?

Kyndryl has deep expertise in designing, running, building, 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 customers to unlock potential.

For more information

To learn more about how Kyndryl Cyber Incident Recovery with Dell Technologies can help your organization, visit Kyndryl Security and Resiliency or contact your Kyndryl representative. Or visit kyndryl.com

kyndryl

1. The State of Hybrid Resilience, 2020, 451 Research, commissioned by Kyndryl https://www.kyndryl.com/content/dam/kyndrylprogram/cs_ar_as/The_State_of_Hybrid_Multicloud_Resilience.pdf
2. Cost of a Data Breach Report 2022 by Ponemon Institute and IBM Security. https://www.ibm.com/downloads/cas/3R8N1DZJ