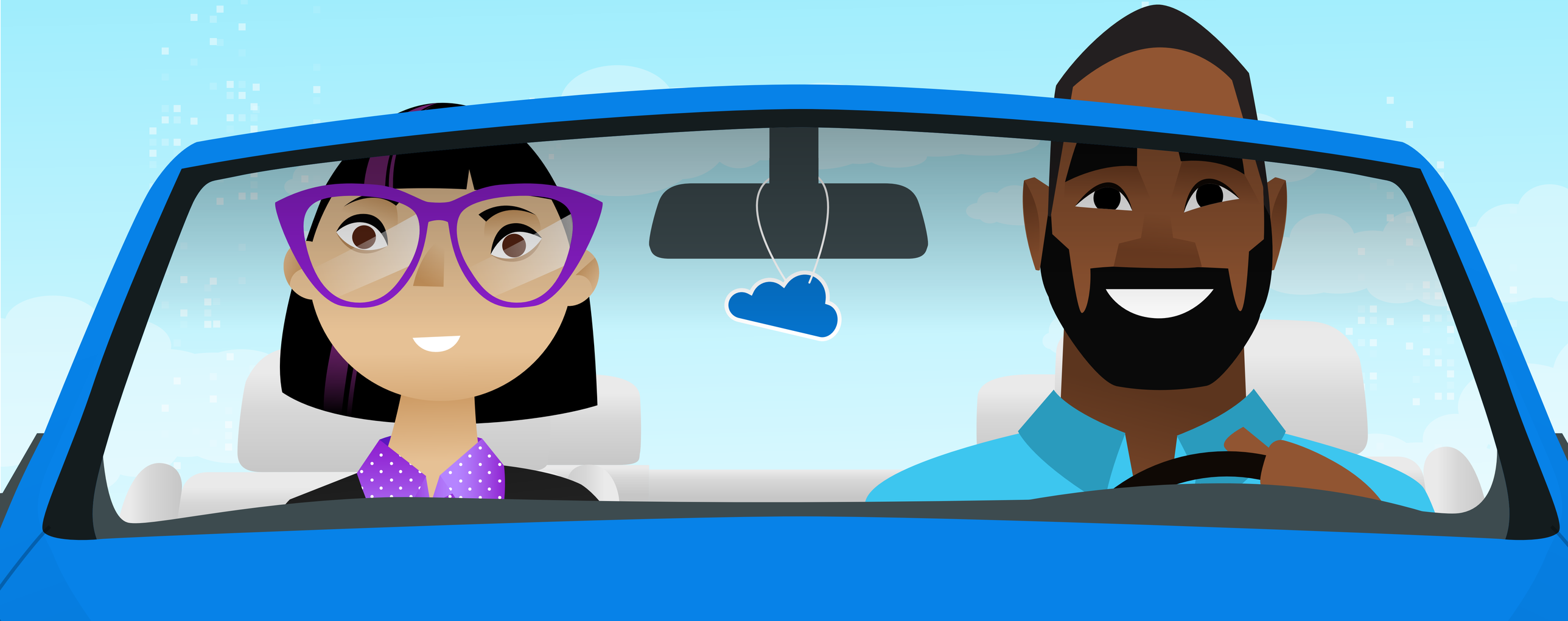
Navigating the Road to Cyber Resiliency

with
Jake and Emmy

DELL Technologies

The Data Protection Landscape: Navigating the Challenges

The intricate landscape of data protection poses a significant challenge for organizations, directly impacting their journey toward digital transformation. The 2024 Dell Global Data Protection Index (GDPI) reveals that a majority of organizations have faced disruptions in the past 12 months[1].



IT and IT security leaders acknowledge these disruptions, expressing concerns about potential future events.

These apprehensions cast doubt on their confidence in achieving backup and recovery service level objectives (SLOs), with many lacking a “very confident” stance in their organization's capabilities. Adding to these concerns, data loss events are inflicting notable financial repercussions on organizations[1]. While various causes of data loss persist, cyberattacks have emerged as a prominent threat.

79% of organizations are concerned they will experience a disruptive event in the next 12 months[1]

60% of organizations are not very confident in their ability to meet their backup and recovery SLOs[1]

Cybersecurity and Cyber Resiliency

The menace of cyberattacks continues to grow, causing substantial organizational disruption. According to the 2024 GDPI, over half of IT decision-makers report experiencing a cyberattack or incident preventing data access in the last 12 months.

Cybersecurity awareness permeates all organizational levels, with many adopting a Zero Trust approach to elevate their cybersecurity maturity. Organizations are crafting actionable roadmaps to reduce their attack surface, detect and respond to cyber threats, and implement recovery measures. Zero Trust is not a product but an architectural approach encompassing the entire IT ecosystem, addressing people, processes, and products.

Cyber resiliency, foundational to a Zero Trust framework, focuses on data recoverability post-attack. With cyberattacks preventing data access at an all-time high, organizations grapple with balancing investments in prevention and recovery. The market's myriad technologies and solutions, coupled with a lack of internal resources for planning, make the journey to cyber resiliency perplexing.

Dell and our trusted partners stand ready to guide you toward a more secure digital future.

52% of IT decision-makers report their organization has suffered a cyberattack or incident that prevented access to data within the last 12 months[1]

75% of organizations are concerned their existing data protection measures may not be sufficient to cope with ransomware threats[1]

Assess your cyber resiliency: Cyber Resiliency Vulnerability Assessment | ESG Research

▶ esg-global.com

Getting Started: Enhancing Cyber Resiliency

Initiating the journey to cyber resiliency requires internal alignment across all organizational levels. Recognizing the business need, allocating resources, establishing timelines, and defining budgets are crucial steps.

This proactive approach prevents unmet expectations, project delays, and suboptimal outcomes.

The essence of cyber resiliency lies in swiftly restoring business operations post-attack. Ensuring access to the right people, resources, and expertise is critical. Organizations lacking essential skills can collaborate with technology service providers to bolster their teams.

While safeguarding all data is vital, organizations should prioritize identifying critical data, applications, and infrastructure for secure recovery and prompt resumption of essential operations.

Strengthen your cyber resilience foundation by leveraging the #1 data protection appliance[3]

Get the performance, efficiency, and scale you need to ensure your data is always protected with PowerProtect appliances.

Keep up with relentless data growth, secure mission-critical apps, and meet the needs of emerging workloads wherever they're located. PowerProtect simplifies data protection operations and reduces risk, enabling you to meet SLAs while lowering costs.

UP TO
38%
Faster Backups[4]

UP TO
45%
Faster Restores[4]

TYPICALLY
65:1
Deduplication[5]

TYPICALLY
30%
More Logical Capacity[5]

Target Appliances

PowerProtect Data Domain appliances enable your organization to protect, manage, and recover data at scale. As the #1 data protection appliance[3], DD series sets the bar for efficient data management from edge to core to cloud, and includes the ecosystem support and comprehensive data protection customers have come to appreciate from Data Domain.

Integrated Appliances

Experience modern data protection with an integrated appliance based on PowerProtect Data Manager.

Easy to configure and manage, the PowerProtect Data Manager Appliance provides a unified user experience and automates discovery and protection of databases, VMs, file systems, and Kubernetes containers.

Manageability Matters

Dell gives you powerful management tools for appliances on-premises and in-cloud. These tools simplify lifecycle operations while enabling new features, like Smart Scale.

PowerProtect DD Management Center simplifies management of multiple PowerProtect Data Domain appliances, physical or virtual. DD series works with CloudIQ for cloud-based proactive monitoring, machine learning, and predictive analysis across multiple Dell products.

Cyber Resilience Data Protection: Dell PowerProtect Cyber Recovery

Traditional backup and disaster recovery solutions may leave organizations exposed to cyber threats. PowerProtect Cyber Recovery, a key element of a cyber resilience strategy, goes beyond traditional methods. It provides additional layers of physical and logical security at the solution, system, and data/file level. This ensures critical data is preserved with integrity, confidentiality, and availability for recovery.

PowerProtect Cyber Recovery focuses on protecting critical data on-premises or in the cloud, recovering businesses post-cyberattack or ransomware incidents.

This solution, leveraging professional services and technology, incorporates three key elements:

Immutability

Data written to the data vault must be "locked" to prohibit deletion or changes.

Isolation

The components of the data vault must be physically and logically isolated.

Intelligence

Data in the vault undergoes analysis to ensure it remains unmanipulated or corrupted

PowerProtect Cyber Recovery protects your data where it lives.

On-Premises

Provides maximum control of data and infrastructure with a secure on-premises vault protected with an operation air gap and multiple layers of physical and logical security.

- On-premises in an air-gapped secure Cyber Recovery vault
- Compliance-level hardware-based immutability and NTP tamper protection
- CyberSense identifies threats and helps enable assured recovery

Colocation

Extends our proven and modern PowerProtect Cyber Recovery solution to a secure cloud environment, providing customers with another layer of isolation for their critical data.

- Logically isolated, secure Cyber Recovery vault
- Multiple options for recovering post-attack to enable resumption of normal business operations with confidence

Public Cloud

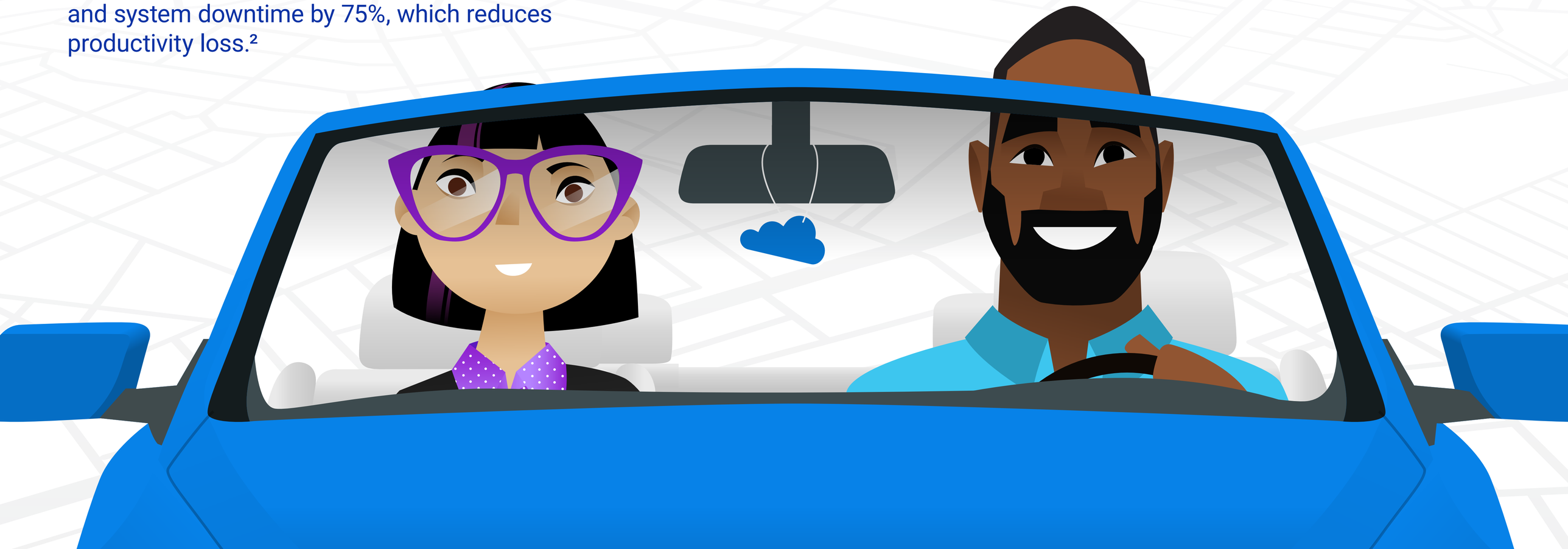
Delivers a fast, easy-to-deploy public cloud vault to secure, isolate, and recover critical data and systems from cyberattacks.

- Logically isolated, secure Cyber Recovery vault
- Multiple options for recovering post-attack to accelerate data recovery with confidence

PowerProtect Cyber Recovery is the first and only solution to receive endorsement for meeting all of the data vaulting requirements of the Sheltered Harbor standard, protecting U.S. financial institutions from cyber threats like ransomware.

A new study by Forrester, The Total Economic Impact™ of Dell PowerProtect Cyber Recovery, highlighted a reduction of time spent on data recovery by 80% and system downtime by 75%, which reduces productivity loss.[2]

40% of organizations are using a cyber vault with physical and logical separation of data from the production environment[1]



Dell Services

Dell can help with Advisory Services for strategic assessments, Managed Services to monitor and manage unified security operations, and Integration Services to design and integrate tools and technologies. Ensure peace of mind against cyberattacks by harnessing Dell Services to elevate your cyber resilience through a comprehensive cyber recovery program. This integrated solution seamlessly combines people, processes, and technology to establish a robust last line of defense for your business. With this safeguard in place, you can confidently direct your focus towards growth and innovation.

- Create a lean, mature, trusted cyber recovery capability customized for your business needs
- Leverage adaptable recovery methods based on the impact of the attack
- Gain flexible solutions that respond to evolving business needs
- Reduce risk through preparedness

"Many organizations don't consider the insider threat. We understand that a large number of attack vectors are internal, and we still have to protect against that. Cyber Recovery Vault is extremely important to us because it also helps safeguard against those internal threats."

Anthony Bryson, Ph.D.,
Chief Information Security Officer,
Town of Gilbert, AZ

"Two Dell products in particular have been key in helping us withstand cyber attacks globally: PowerProtect Cyber Recovery and PowerProtect DD."

Steven Harpe,
Chief Operating Officer,
State of Oklahoma

"With the PowerProtect Cyber Recovery vault, we were able to get back up and running in about four hours, rather than weeks."

Manuel Salinas,
Director of Technology,
San Felipe Del Rio CISD

Modern, Simple, Resilient Data Protection for the Road Ahead

As organizations increasingly turn to public cloud solutions, implement hybrid operational models, and manage the dual nature of generative AI as both a powerful defensive asset and a source of new cybersecurity complexities, the criticality of data protection is more evident than ever. Yet, securing and safeguarding digital assets is becoming a more complex challenge for many. In a landscape continuously threatened by cyberattacks, it is essential for businesses to adopt measures that bolster the resilience of their operations.

Modern
Deploy solutions designed to protect all workloads and use cases across multicloud, on-premises, and edge environments cost-effectively.

Simple
Simplify data protection with consumption flexibility, ease of deployment, and streamlined operations.

Resilient
Create secure infrastructure that optimizes resilience to ensure your organization can recover from destructive cyberattacks.

52% of organizations believe integrating generative AI will provide an advantage to their cybersecurity posture[1]

88% of organizations agree that the adoption of generative AI will generate large volumes of new data, necessitating protection and security measures[1]

NAVIGATING THE ROAD TO CYBER RESILIENCY SUMMIT AHEAD

DELL Technologies

Learn more at dell.com/dataprotection

1. Dell 2024 Global Data Protection Index, conducted by Vanson Bourne

2. The Total Economic Impact™ of Dell PowerProtect Cyber Recovery Cost Savings And Business Benefits Enabled by PowerProtect Cyber Recovery with CyberSense, AUGUST 2023

3. Based on revenue from the IDC 1Q23 Purpose-Built Backup Appliance (PBBA) Tracker

4. Based on Dell internal testing compared to the previous generation, January 2023. Actual results may vary.

5. Based on Dell internal testing and field telemetry data, January 2023. Actual results may vary.