Safe AI for a Resilient Future

Securing GenAI through modern data protection and cyber resilience

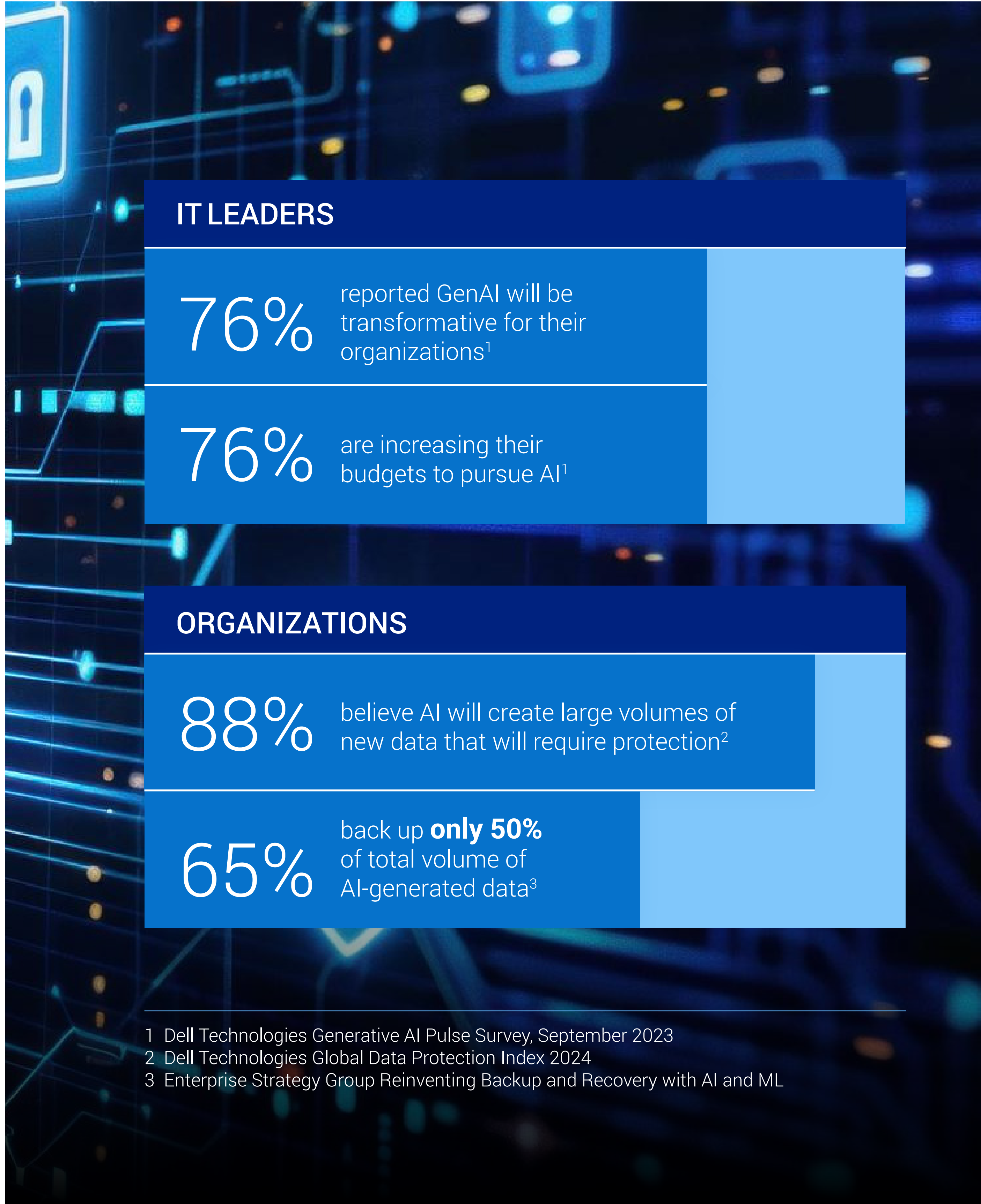
Why safe AI is critical to successful AI

When it comes to AI, one thing is certain: companies of all sizes are feeling its impact. Many IT leaders believe GenAI will be significant, if not transformative, for their organizations. Not surprisingly, there is an indication of increasing budgets to pursue AI initiatives.[1]

However, as expectations for AI skyrocket, protecting AI data and applications is becoming more crucial than ever. While many organizations acknowledge that AI will create large volumes of new data requiring protection, fewer admit to regularly backing up a significant portion of their AI-generated data. This gap between the high expectations for AI and the current data protection measures highlights a critical area that organizations need to address to fully realize the potential of AI technologies.

The significance of safeguarding data and ensuring cybersecurity for mission-critical workloads is well-understood in the IT sector.

> While traditional data protection practices remain relevant, the emergence of AI applications introduces specific security and data protection needs that organizations must address. Recognizing and meeting these evolving requirements is crucial in safeguarding AI technologies.



IT LEADERS

76% reported GenAI will be transformative for their organizations[1]

76% are increasing their budgets to pursue AI[1]

ORGANIZATIONS

88% believe AI will create large volumes of new data that will require protection[2]

65% back up **only 50%** of total volume of AI-generated data[3]

[1] Dell Technologies Generative AI Pulse Survey, September 2023
[2] Dell Technologies Global Data Protection Index 2024
[3] Enterprise Strategy Group Reinventing Backup and Recovery with AI and ML

Understanding the threat of cyber attacks

Analysts are already signaling caution that GenAI applications will create new attack surfaces particularly in the areas of cyber threats and that data protection solutions must be able to avoid the consequences of lost AI data that was not backed up or recoverable.

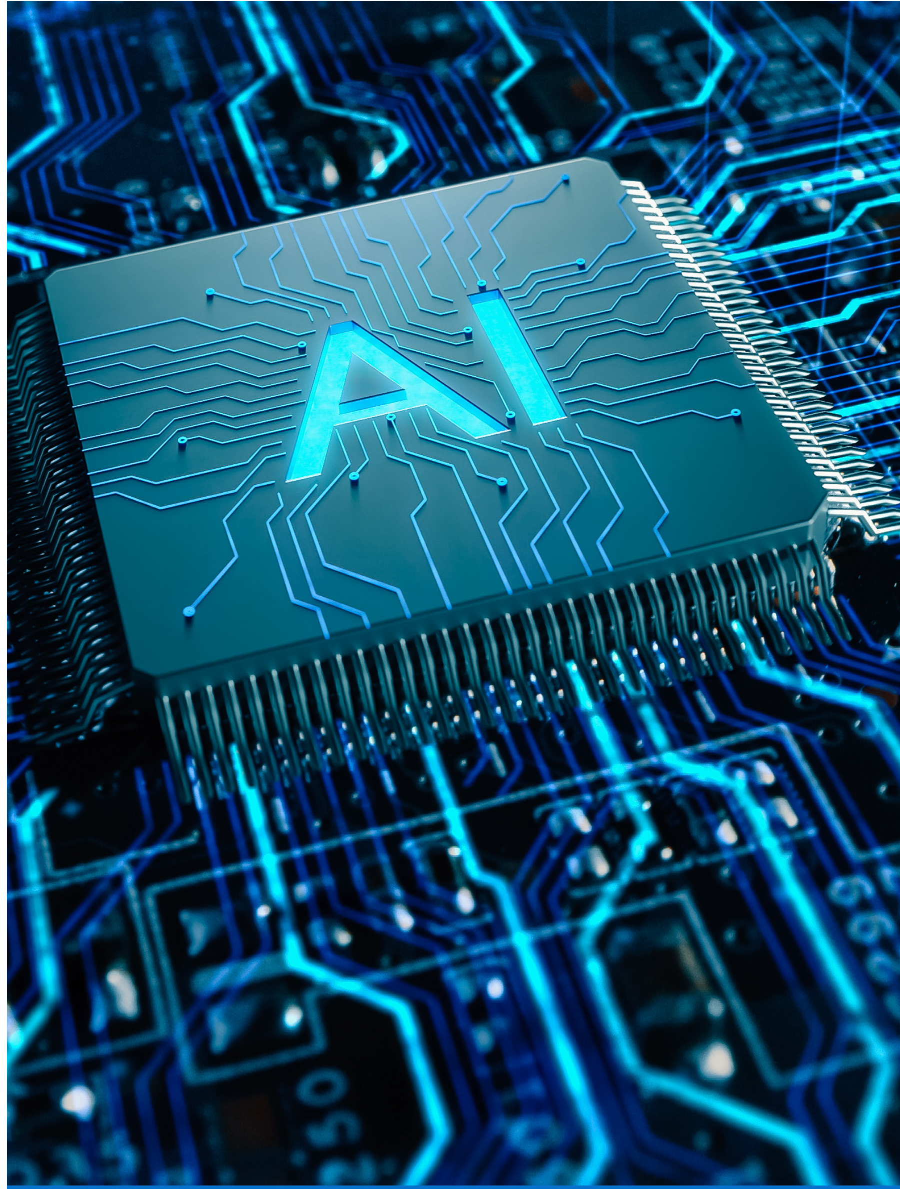
With the increase in AI comes an expected increase in cyberthreats, and with each passing day, cybercriminals adopt ever-more sophisticated techniques that enable them to operate more quickly—and avoid detection.

Some of the most prevalent threats include:

Data poisoning

A cyberattack in which attackers deliberately insert false or misleading information into the training datasets used by machine learning models with an aim to corrupt the model's learning process, resulting in incorrect predictions or flawed decisions. By altering the training data, attackers can degrade the model's performance, introduce biases, or manipulate it to act in ways that favor the attacker.

This type of attack can have significant consequences, particularly in areas like financial fraud detection, autonomous vehicles, healthcare diagnostics, and security systems, where the accuracy and reliability of machine learning models are crucial.



75% of organizations are concerned that their organization's existing data protection measuresare unable to cope with malware and ransomware threats.

2024 Dell Global Data Protection Index

Privacy breaches

A cyberattack in which unauthorized individuals or entities gain access to sensitive, confidential, or personal information, resulting in a compromise of data privacy. This breach can involve the theft, exposure, or misuse of data such as financial records, personal identification details, health information, or intellectual property.

Privacy breaches are often the result of hacking, phishing attacks, insider threats, poor security practices, or vulnerabilities in software.

Such incidents can lead to serious consequences, among them identity theft, financial loss, reputational damage, legal penalties, and erosion of trust.

Ransomware

A type of malware cybercriminals use to encrypt a victim's data or lock them out of their systems then demand a ransom payment—usually in cryptocurrency—to restore access or decrypt the data. If the ransom is not paid within a specified time, the attackers may threaten to delete the data, publish it, or permanently prevent access.

Ransomware attacks can target individuals, businesses, and even critical infrastructure, causing significant financial loss, disruption of services, and potential exposure of sensitive information.

Social engineering

A technique used by cybercriminals to manipulate or deceive individuals into revealing confidential information or performing actions that compromise security, social engineers exploit human behavior — such as trust, curiosity, or fear — to achieve their objectives.

Common tactics include phishing emails, fake phone calls, impersonation, and pretexting, in which attackers pose as trusted individuals or organizations. The goal is often to gain access to sensitive information like passwords, financial details, or personal data, or to gain unauthorized access to secure systems. Social engineering attacks are effective because they target human psychology rather than technological defenses.

> As your organization moves to integrate AI into its systems and decision-making processes, ensuring robust cybersecurity measures remains as critical as ever.

Building a safe foundation for AI

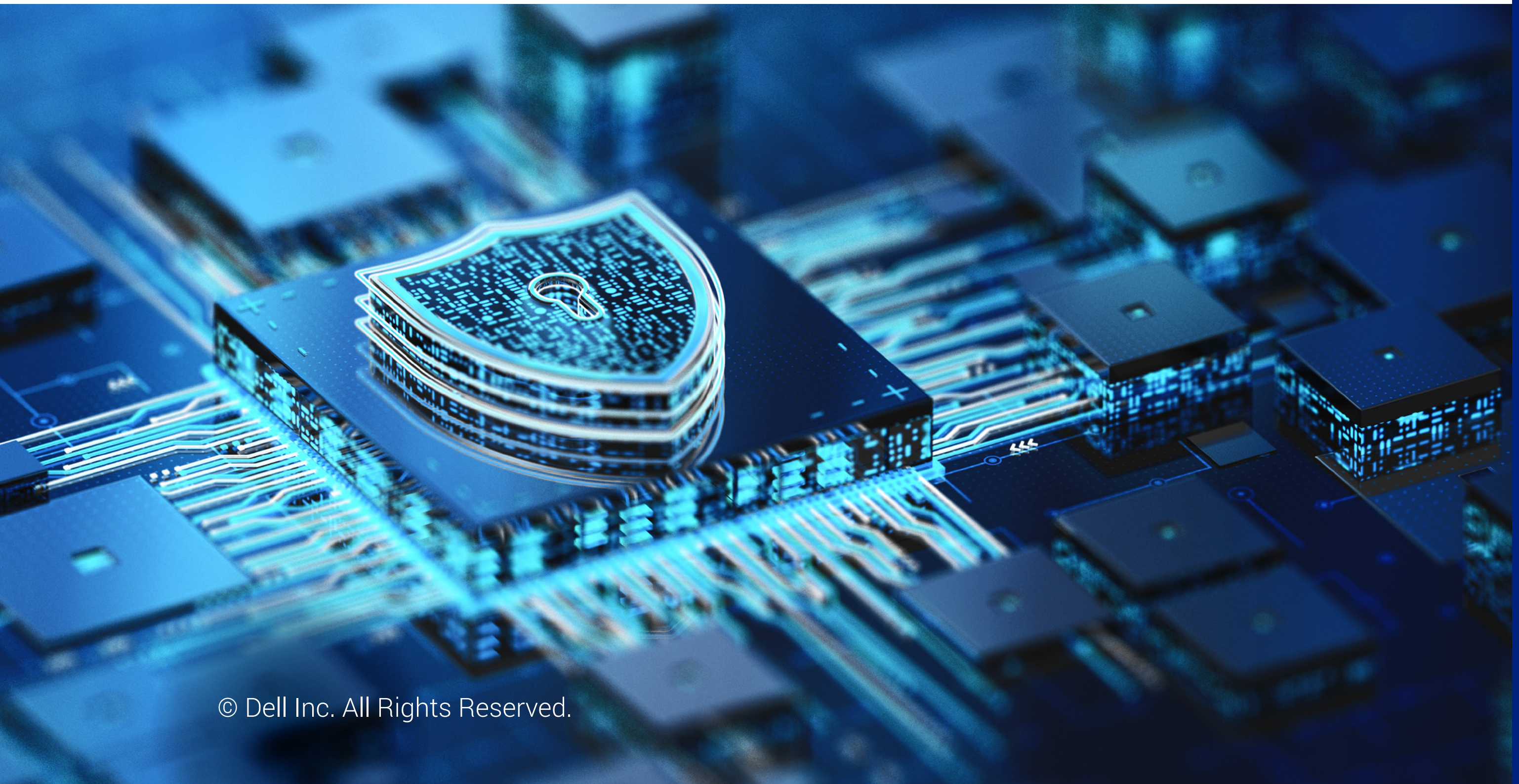
No matter the size of your organization, Dell can secure your AI workloads—and help you achieve your business goals.

AI workloads are as mission-critical as any other business application, and beyond cyber threats they are equally susceptible to any event that can cause data loss and business disruption.

> It's vital for organizations to go beyond the surface and think through the entire AI workflow to ensure comprehensive protection and resiliency.

Secure your AI workloads by protecting everything

Ensure that data protection and cyber resiliency principles are applied to all data, including training inputs, model outputs, and any data involved in Retrieval Augmented Generation (RAG), if used. Additionally, ensure ongoing compliance with all applicable data protection regulations.



What to consider when protecting AI workloads

Data sources

- Location of Data Sources: Training AI models require diverse data sources, including unstructured data, structured data, and data lakes.
- Robustness of Solutions: Ensure that solutions protect data sources for backup, recovery, disaster recovery (DR), and cyber recovery.
- Data Growth and SLAs/SLOs: Consider the rate of data growth and the service level agreements (SLAs) and service level objectives (SLOs) for data protection.

AI models

- Maturity of AI Models: Assess the integration of AI models with data protection and cyber resiliency solutions.
- Protection Solutions: Evaluate the robustness of solutions for backup, recovery, DR, and cyber recovery.
- Environment: Ensure protection for on-premises, public cloud, containers, and virtual machines.
- Training Copies: Maintain copies of models used for training.

Inquiries and responses

- Regulatory and Privacy Requirements: Adhere to compliance requirements for long-term retention of sensitive data.
- Records of Inquiries and Responses: Maintain records for legal protection and data governance.

Why data protection and cyber resilience is important

Delivering better outcomes across the entire AI landscape means ensuring comprehensive data protection and resiliency to address cyber threats, system failures, compliance and legal protection, workload state, and dataset reconstruction.

Cyber resiliency

AI workloads are prime targets for cyber attacks. Threats like data poisoning, ransomware, privacy breaches, and social engineering can disrupt operations and cause significant losses. Cyber resiliency strengthens your AI deployments, ensuring they remain secure against these threats.

Compliance and legal protection

Legal regulation is essential. Long-term retention of sensitive data may be necessary for regulatory requirements and legal protection. Safeguard against IP infringement, misuse of personal identifiable information (PII), and copyright violations.

Workload state and dataset reconstruction

Operational continuity is crucial for business success. Ensure the integrity and performance of your AI workloads by maintaining their state and enabling dataset reconstruction. Whether you need to adjust your models or recover from an incident, our solutions provide the tools to keep your operations running smoothly.

The growing importance of governance, compliance, and auditability for AI

The rapid development of artificial intelligence technologies has spurred a corresponding growth in regulations aimed at ensuring these systems are deployed safely and responsibly. In the context of data protection and cyber resilience, governance, compliance, and auditability play pivotal roles in ensuring that AI systems are designed and operated securely and ethically.

Governance involves establishing and maintaining robust policies and frameworks that ensure AI initiatives are aligned with an organization's strategic goals while adhering to ethical practices. Compliance, on the other hand, ensures that these AI systems meet external regulations and standards, thus protecting organizations from potential legal challenges and financial penalties. Auditability provides a layer of transparency, allowing organizations to trace and verify the processes and decisions made by AI systems, thereby fostering trust among stakeholders.

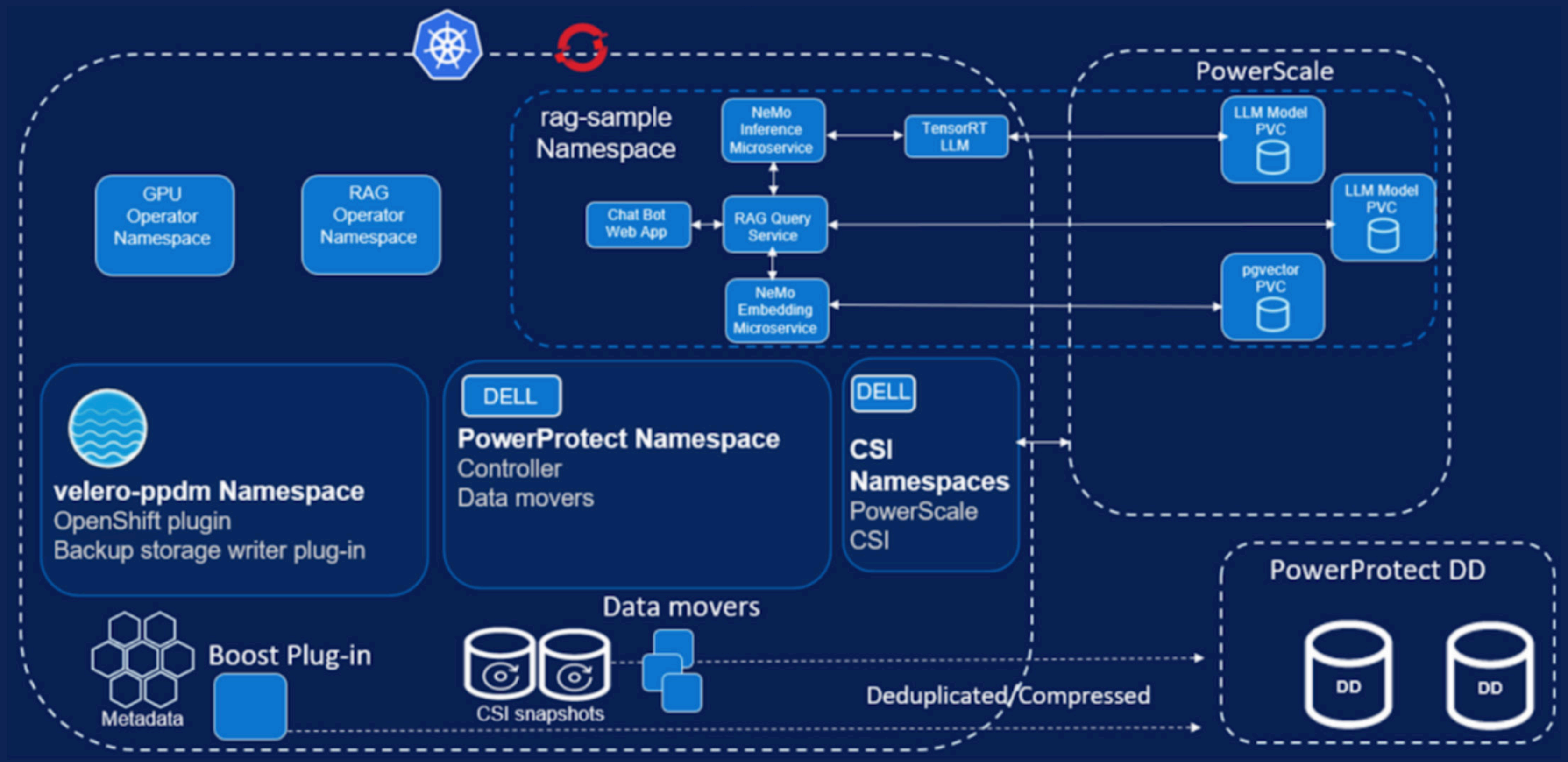
Together, these elements form a comprehensive approach that helps organizations mitigate risks, protect data integrity, and maintain resilience against cyber threats.

Accelerate your AI innovation with the Dell AI Factory

AI factories will power the AI revolution, generating actionable intelligence, fresh content, and new insights in place of physical goods. The Dell AI Factory represents our strategy for embracing and implementing AI, ensuring successful and consistent deployment at any scale and location.

Protecing the Dell Scalable Architecture for Retrieval-Augmented Generation (RAG) with NVIDIA Microservices

Recognizing the pivotal role of data protection in preserving AI infrastructure integrity, Dell has created a Reference Design for AI Data Protection, which is based on the Dell Scalable Architecture for retrieval-augmented generation (RAG) with NVIDIA Microservices. This blueprint can help guide organizations in seamlessly integrating robust data protection measures into their AI frameworks.



Dell cyber resilient data protection for an AI world

Modern

Deploy solutions that are 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 with AI powered resiliency to ensure your organization can recover from destructive cyberattacks.

PowerProtect Data Manager

Protect data and deliver governance across physical, virtual, and multicloud environments with Dell's software-defined platform. PowerProtect Data Manager accelerates IT transformation with simple, agile, and robust protection for diverse workloads, all within a flexible user experience. Maximize operational efficiency and resource utilization by leveraging Dell's trusted protection storage architecture, enabling you to achieve strategic goals without compromising security. Built with resilience at its core, PowerProtect Data Manager equips your organization to tackle multicloud complexities and advanced cyber threats while staying ahead of evolving IT challenges through Dell's continuous innovation.

Disruption-free VM protection

- Ensure availability of all your virtual machines at scale without business disruption.

Native integration

- Dell PowerStore and Dell PowerMax delivers fast, efficient, and secure backup and recovery.

Automated NAS protection

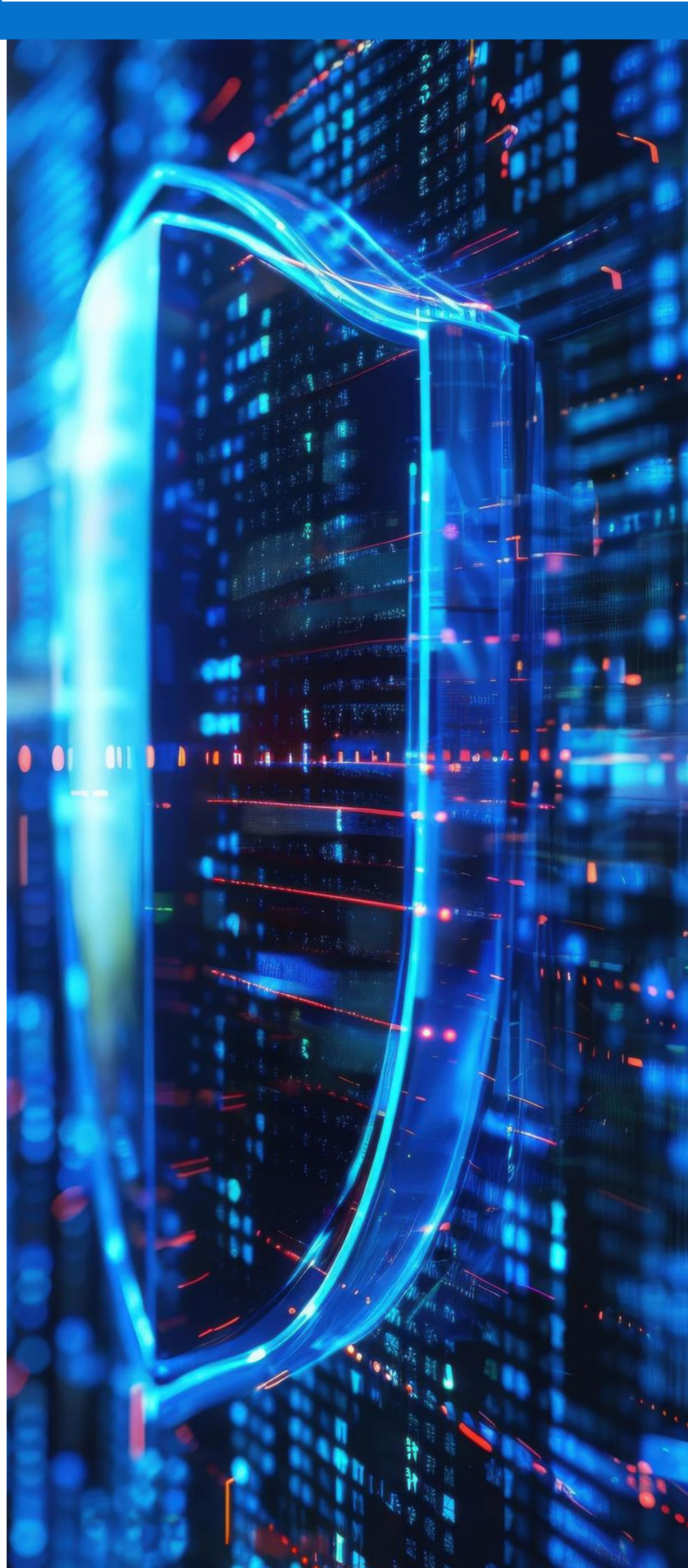
- Achieve improved SLAs through simple, efficient management of NAS backup and recovery.

Native Kubernetes protection

- Discovery, protection and management of production workloads in Kubernetes environments.

Flexible and granular restores

- Simple, flexible and granular restores for your virtual environments.



PowerProtect Appliances

PowerProtect appliances are the industry-leading choice for protecting and managing data, whether on-premises or across multicloud. They are specifically designed and optimized for data protection—resulting in performance, efficiency and security advantages that simplify operations, reduce risk and lower costs.

Build your cyber resilient foundation on trusted PowerProtect appliances. Ensure comprehensive cyber resilience wherever your data lives—whether you are protecting data that is on-premises with PowerProtect Data Domain or PowerProtect Data Manager Appliance, or in multicloud with software-defined Dell APEX Protection Storage.

Efficient

Typically 65:1 deduplication with PowerProtect appliances[4]

The latest generation of PowerProtect appliances delivers:

UP TO 38% faster backups[5]

UP TO 44% faster restores[5]

UP TO 58% faster replication between appliances[5]

UP TO 11% less power consumed[6]

50% less floor space required[7]

[4] When compared to previous generation. Based on Dell internal testing and field telemetry data. April 2021. Actual results may vary.

[5] Based on Dell internal testing comparing a Dell PowerProtect DD9910 appliance vs. a PowerProtect DD9900 appliance, February 2024. Actual results may vary.

[6] Based on Dell analysis compared to the previous generation configured at maximum capacity. Savings in US dollars calculated using power consumption and thermal rating for appliances with expansion shelves and an average electricity price of $.168 per KWH. For estimation purposes only. Actual costs will vary.

[7] Based on Dell internal testing comparing a Dell PowerProtect DD9910 appliance using an optional deep rack vs. a PowerProtect DD9900 appliance. March 2024

Bringing it together

No matter the size of your organization, when it comes to data protection and cyber resilience, one thing is certain: As AI technology continues to evolve at a rapid pace (and with it, increasingly sophisticated threats to critical data), protecting and securing your organization's generative AI workloads is more important than ever.

That's where Dell comes in.

Offering a comprehensive, sophisticated solution that strengthens your AI and ensures data protection and cyber resilience. Dell PowerProtect cost effectively protects all workloads and use cases across multicloud, on-premises, and edge environments; simplifies data protection with flexible consumption models, easy deployment, and streamlined operations; and ensures resilient and secure infrastructure for rapid recovery in the event of a destructive cyberattack.

DELL Technologies

See what Dell cyber resilient data protection can do for you.

LEARN MORE