

WHITE PAPER

# The Increasing Importance of Cyber Resilience in an AI-driven World

## Why AI Is Different

By Jon Brown, Sr. Analyst  
Enterprise Strategy Group

August 2025

# Contents

Executive Summary .....	3
The AI Transformation Imperative .....	4
What's Driving AI Transformation .....	4
An "AI or Die" Moment in Business .....	5
The Dual Challenge: Securing AI While Using AI for Security .....	6
Thoughtful, Strategic Adoption Is Key .....	6
The Unique Features of AI Workloads .....	7
AI Is a High-performance Workload .....	7
Data Centric Vulnerabilities of the AI Workload .....	7
Distributed Computing Vulnerabilities of the AI Workload .....	8
Defining Cyber Resilience for AI Environments .....	8
AI Compliance Requirements: Navigating an Evolving Regulatory Landscape .....	9
New Thinking Required .....	9
The Dell AI Factory with NVIDIA .....	10
Key Components of the Dell AI Factory with NVIDIA .....	10
Continuous Monitoring and Validation Approaches .....	12
Conclusion .....	12

## Executive Summary

Artificial intelligence (AI) is revolutionizing business operations, driving productivity, competitive advantage, and operational efficiency. However, the unique demands of AI workloads introduce significant security challenges that traditional tools are ill-equipped to address. With almost half (47%) of organizations citing AI as a critical skills gap in their teams and another 37% of organizations citing cybersecurity skills as a constraint, organizations are struggling to balance the business desire for immediate AI deployment while enabling constrained security teams time to assess the novel risks associated with the technology (see Figure 1).<sup>1</sup> Once the risks are understood, security teams will move forward addressing gaps in their security strategy, tools, and operations; either themselves or in collaboration with key partners to protect their use of AI. As businesses increasingly rely on AI for mission-critical processes, the risks of compromised or inaccessible AI systems grow exponentially, threatening not only operational continuity but also revenue, reputation, and long-term competitiveness.

AI workloads depend heavily on GPUs for training and inference, yet traditional security tools lack the capability to monitor or secure GPU activity, leaving critical vulnerabilities exposed. The multi-node, multi-cluster nature of AI training expands the attack surface, while massive data volumes strain storage and transmission networks, overwhelming conventional security solutions. AI systems also require real-time processing, dynamic model updates, and advanced protection for sensitive data—areas where traditional tools fall short. Emerging threats, such as adversarial attacks, insider tampering, and model theft, further amplify the risks.

The consequences of compromised AI systems can be severe. A successful attack could disrupt business operations, delay decision-making, and erode customer trust. For organizations that depend on AI to automate workflows, optimize supply chains, or deliver personalized customer experiences, downtime or data breaches could result in significant financial losses, regulatory penalties, and reputational damage. As AI becomes integral to business strategy, ensuring its security and resilience is no longer optional—it is a business imperative.

Dell Technologies, in partnership with NVIDIA, offers a robust, full-stack computing solution designed to enhance overall cybersecurity posture while also meeting global regulations and compliance requirements. By integrating zero-trust architecture and verifiable confidential computing capabilities, this solution safeguards critical AI assets while maintaining performance and resilience. Leveraging AI to enhance cybersecurity, the Dell-NVIDIA partnership empowers businesses to mitigate risks, ensure uptime, and confidently harness the transformative power of AI.

**Figure 1.** Top 5 Areas With Problematic Shortages of Skills

**In which of the following areas do you believe your IT organization currently has a problematic shortage of existing skills? (Percent of respondents, N=846, multiple responses accepted)**



Source: Enterprise Strategy Group, now part of Omdia

<sup>1</sup> Source: Enterprise Strategy Group Research Report, [2025 Technology Spending Intentions Survey](#), December 2024.

# The AI Transformation Imperative

According to research from Enterprise Strategy Group, 77% of respondents reported that AI at their organization is in production, in pilot/POC, or part of a near-term or long-term plan.<sup>2</sup> A new [UN Trade and Development \(UNCTAD\) report](#) projects the global AI market will soar from \$189 billion in 2023 to \$4.8 trillion by 2033—a 25-fold increase in just a decade.

## What's Driving AI Transformation

AI represents the most significant technological lever for competitive differentiation in decades, with potential impacts across virtually every business function. Enterprise Strategy Group research indicates that forward-thinking organizations are prioritizing AI implementation in key areas, including software development, research, IT operations, and customer service.

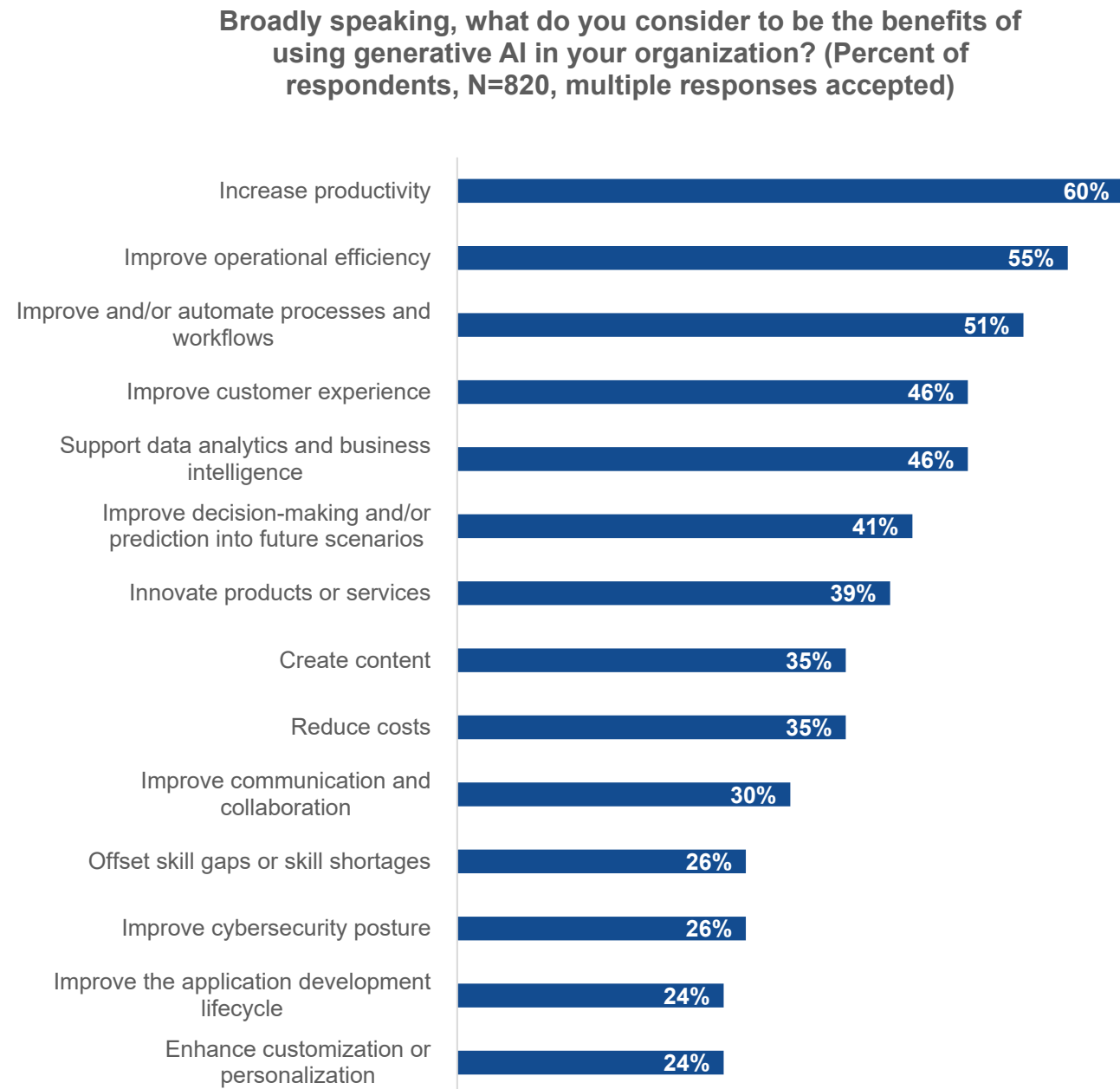
These strategic focus areas aren't arbitrary; they highlight critical areas where AI-driven transformation can fundamentally alter competitive positioning. The difference between excellence and mediocrity in these functions often determines market leadership status or, in increasingly competitive sectors, organizational survival.

Ultimately, leaders see AI adoption as a means to enhance productivity, improve operational efficiency, and aid in automation (see Figure 2). AI's transformative potential includes:

- **Enhanced decision intelligence.** AI systems can identify subtle behavioral patterns and market signals invisible to human analysts, dramatically improving data-driven decision-making and capital allocation strategies.
- **Operational excellence.** The technology drives unprecedented efficiency through intelligent process automation, supply chain optimization, and innovation acceleration.
- **Business velocity.** AI significantly compresses time to market and response cycles across all business functions.

---

<sup>2</sup> Source: Enterprise Strategy Group Research Report, [The State of the Generative AI Market: Widespread Transformation Continues](#), September 2024.

**Figure 2.** Benefits Leaders Expect to See From AI Adoption

Source: Enterprise Strategy Group, now part of Omdia

As organizations move from AI pilot projects to full-scale implementation, those that develop comprehensive, resilient AI strategies aligned with their core business goals will likely build lasting competitive advantages. These advantages will go beyond just reducing costs, enabling real market differentiation and disruption of competitors through better customer experiences, innovative products, and superior operational models.

### An “AI or Die” Moment in Business

AI has the potential to accelerate disruption. Traditional digital transformation takes years to achieve, but AI-driven disruption can happen in months, and there is a compounding effect where businesses can build on their early AI successes and accelerate the pace of change. In financial services organizations, this could be AI-powered risk

assessment and personalized offerings; in healthcare, this could be AI-assisted diagnostics and treatment optimization; manufacturing organizations could see predictive maintenance and more autonomous operations; retail organizations could see inventory optimization and marketing personalization; and in professional services

### **Oregon State University Secures Ocean Research With Dell AI Factory with NVIDIA**

Oregon State University deployed Dell AI Factory to manage and protect critical data for the NSF Ocean Observatories Initiative, which collects oceanographic data from over 900 instruments for global scientific research. The university's system:

- Secures petabytes of irreplaceable scientific data for 30+ years.
- Defends against 130,000+ cyberthreats with zero downtime.
- Achieves 160:1 data reduction ratio, protecting 16.6 PB of data.
- Enables seamless migration with no service disruption.
- Supports AI-driven research with PowerEdge servers and NVIDIA GPUs.

such as accounting and legal, knowledge workers can save hours with AI augmentation.

AI will likely also affect talent acquisition and retention, as AI adoption by an organization sends a potent symbol to the existing and potential workforce. Top talent will likely gravitate toward organizations that are AI-forward.

However, implementing AI is not without significant risks. While we might be in an “AI or die” moment, it is of paramount importance to get AI implementation right.

### **The Dual Challenge: Securing AI While Using AI for Security**

With AI systems having access to organizations' most important intellectual property, cybersecurity threats are a primary concern. Thus, a dual challenge emerges: Organizations must secure AI implementations while also leveraging AI to enhance their security posture. Enterprise Strategy Group research showed that generative AI is making a difference in security operations, with 43% of organizations saying that the addition of generative AI capabilities is helping them operate more efficiently.<sup>3</sup>

## **Thoughtful, Strategic Adoption Is Key**

The adoption of AI is a mission-critical endeavor that will take significant planning. Partner selection, the process of an organization deciding which products and services it will use to gain competitive advantage, is a key determinant of its success.

And, while the imperative is stark, the path forward is clear. Organizations that approach AI with the proper strategy, including infrastructure and security, will thrive and succeed. Part of that strategy is building in cyber resilience to ensure that, even under attack, the system can still execute and deliver. Leading technology firms NVIDIA and Dell are leading the way for safe and effective AI adoption and taking cyber resilience seriously.

<sup>3</sup> Source: Enterprise Strategy Group Research Report, [The Future of SecOps in an AI-driven World](#), April 2025.

# The Unique Features of AI Workloads

AI can present new challenges, and once fully adopted, will become a mission-critical workload with unique challenges in performance, data security, and architecture.

## AI Is a High-performance Workload

While AI is a unique and rapidly evolving workload, it shares many fundamental requirements with other mission-critical systems that organizations have managed for decades. Like traditional enterprise applications, AI systems demand robust infrastructure designed for reliability and high availability to ensure continuous operation. However, AI workloads present distinctive challenges in usage forecasting. Organizations must build infrastructure capable of handling unexpected computational spikes and variable resource demands that are characteristic of AI training and inference operations.

Secure performance optimization is also particularly crucial in the AI context, where computational efficiency directly impacts both operational costs and time to insight. Organizations must implement the proper monitoring, tuning, and scaling capabilities to maintain optimal performance. Additionally, AI systems require disaster recovery planning, including regular testing, clearly defined recovery time and point objectives (RTO/RPO), and well-documented execution procedures. This comprehensive approach ensures that, even in crisis scenarios, AI capabilities remain resilient and recoverable, protecting the substantial investments organizations make in AI development and deployment while maintaining business continuity.

## Data Centric Vulnerabilities of the AI Workload

AI workloads present distinct security challenges centered around their data-centric nature. Unlike traditional applications, AI systems process massive volumes of data that often contain sensitive and proprietary information, making them exceptionally attractive targets for threat actors. These vast data repositories represent not just operational assets but potential goldmines of intellectual property and confidential information.

As LLMs become mission-critical workloads with high visibility across organizations, the broad attack surface makes them prime targets. Malicious actors can strategically manipulate training data to introduce backdoors, biases, or vulnerabilities that compromise model integrity. Over time, models might also experience “creep”—the gradual expansion of a machine learning model’s functionality or purpose beyond its original intended use. This can lead to unintended consequences, including biases, inaccuracies, and even harmful outcomes. The insidious nature of these threats lies in their detection difficulty; compromised models might continue to function normally in most scenarios while harboring hidden vulnerabilities that activate only under specific conditions. When such issues

### Confidential Computing: Anjuna Seaglass and NVIDIA Deliver for Public Sector

A member of NVIDIA Inception, a program for cutting-edge startups, **Anjuna** is collaborating with NVIDIA to advance GPU-accelerated confidential AI for enterprises.

By integrating Anjuna Seaglass with the latest NVIDIA Hopper architecture GPUs, organizations are able to accelerate deployment of high-performing large language models (LLMs) without compromising trust, security, and privacy.

Leveraging NVIDIA LaunchPad, the **U.S. Navy** successfully tested Llama3 LLMs on confidential NVIDIA H100 GPUs. The seamless integration with Anjuna Seaglass enabled the U.S. Navy to create and **deploy confidential environments in less than one hour**, a remarkable feat, while obtaining high-speed processing with maximum performance. This integration yielded several key benefits for the U.S. Navy:

- **Security without compromise:** High processing speed enabled maximum performance of NVIDIA confidential GPUs with full privacy.
- **Trust fully verified:** The integrity and trustworthiness of LLMs were validated through attestation reports.
- **Complete data privacy:** Malicious entities were protected against in all three states: in use, in motion, and at rest.

are finally detected, organizations require sophisticated remediation capabilities to identify affected data, isolate compromised model components, and restore systems to a known-good state without disrupting critical business operations. This complex security landscape demands specialized protection strategies beyond traditional cybersecurity approaches.

## Distributed Computing Vulnerabilities of the AI Workload

The distributed architecture inherent to AI training introduces a complex security landscape that traditional cybersecurity approaches struggle to address effectively. Modern AI training operations typically span multiple compute nodes and clusters—sometimes across different physical or cloud environments creating an exponentially larger attack surface compared to conventional workloads. This distributed nature means threat actors have numerous potential entry points, with each node representing a possible vulnerability.

Securing communication channels between these distributed components presents particularly difficult challenges, as data must flow continuously between nodes while maintaining integrity and confidentiality. A compromise of even a single node can potentially undermine the integrity of the entire training process, corrupting models or introducing vulnerabilities that might remain undetected until deployment. This risk is magnified by the fact that AI infrastructure often represents an organization's most significant high-performance computing investment—the crown jewel of its technology stack.

While complete prevention of all security incidents may be unrealistic, organizations can maintain operational resilience through properly designed systems that emphasize reducing the attack surface, timely threat detection, rapid recovery, and continuity. This reality is driving investment priorities across industries. According to Enterprise Strategy Group research, improving cybersecurity and resiliency against cyberattacks is the top justification for increasing IT spending,<sup>4</sup> reflecting the growing recognition that robust cyber resilience is essential for AI-driven enterprises.

## Defining Cyber Resilience for AI Environments

NIST defines [cyber resilience](#) as, “The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.” For AI systems this means:

- Reducing attack surfaces.
- Implementing detection mechanisms for AI-specific vulnerabilities.
- Anticipate, withstand, recover, and restore AI models and training data to known-good states within defined RTO and RPO.
- Establishing architectural safeguards such as architecting AI systems using internal and proprietary data to not connect to external networks (aka “air gapping”)
- Utilizing immutable storage to prevent unauthorized modification of training data.
- Maintaining strict segmentation between development, testing, and production AI environments.

Scalability is essential, ensuring that security controls grow with AI workloads without compromising protection or performance.

---

<sup>4</sup> Source: Enterprise Strategy Group Research Report, [2025 Technology Spending Intentions Survey](#), December 2024.

## AI Compliance Requirements: Navigating an Evolving Regulatory Landscape

Organizations must navigate an evolving regulatory landscape for AI, building flexibility into compliance strategies. Key frameworks include:

- **EU Artificial Intelligence Act:** Categorizes AI systems by risk levels with corresponding requirements.
- **NIST AI Risk Management Framework:** Provides voluntary guidance for managing AI risks.

There are also a host of industry specific regulations. These include:

- **Financial services:**
  - FINRA guidelines on AI supervision in trading and risk assessment.
  - DORA (Digital Operational Resilience Act): EU Mandated strengthening of financial services digital ability to prevent, withstand, respond to, and recover from IT-related disruptions and cyberthreats.
- **Healthcare:** HIPAA implications for AI systems processing protected health information.

Successful AI deployment requires adaptable governance frameworks addressing both broad regulations and industry-specific requirements. Organizations deploying AI must establish governance frameworks that can adapt to this changing regulatory landscape while addressing both horizontal regulations and industry-specific requirements. This demands continuous monitoring of regulatory developments and the ability to quickly implement new compliance measures as regulations mature and expand.

### New Thinking Required

Artificial intelligence and the infrastructure that supports it require a lot of new thinking. What is needed is a high-performance system that offers scalability, reliability, and cyber resilience so that, even in the face of adversity or attack, organizations that rely on AI to get work done will always have access to a clean, trustworthy, and accurate AI platform.

As AI workloads become mission-critical, organizations face a paradox: The same technology creating new vulnerabilities and threat vectors can be leveraged to provide new, unprecedented security capabilities. AI becomes a tool for cybersecurity, enabling advanced threat detection, anomaly identification, and automated response mechanisms that can operate at machine speed to counter sophisticated attacks.

Selecting the right technology partners is crucial for AI success. Organizations should ideally choose to work with leaders that have a proven track record, demonstrated expertise, roadmaps, flexibility to meet them where they are, and access to resources to help them deliver AI. Two undisputed leaders are Dell and NVIDIA. Their combined expertise creates an unparalleled foundation for secure AI

### DORA: Digital Operational Resilience Act

DORA is an EU regulation that went into effect on January 17, 2025 and establishes a framework for Information and Communications Technology (ICT) security and operational resilience in the financial sector, ensuring that financial entities within the EU can withstand, respond to, and recover from severe operational disruptions.

Key components of DORA include:

- **ICT risk management.** Financial entities must implement robust risk assessment and mitigation strategies with senior management approval and oversight.
- **Incident management.** Organizations must establish structured processes for handling and reporting ICT-related incidents within strict timeframes.
- **Digital resilience testing.** Regular testing of systems and processes is mandatory, with advanced testing required for significant entities.
- **Third-party risk management.** Enhanced oversight of ICT service providers is required, with specific contractual provisions.
- **Data protection.** Organizations must implement data protection strategies such as encryption of data at rest and in transit, protection of data in use through encryption or equivalent measures in protected environments, network connection encryption, and strong cryptographic key management.

This emphasis on protecting data in use is a significant advancement in regulatory requirements, driving organizations to implement more sophisticated data protection strategies.

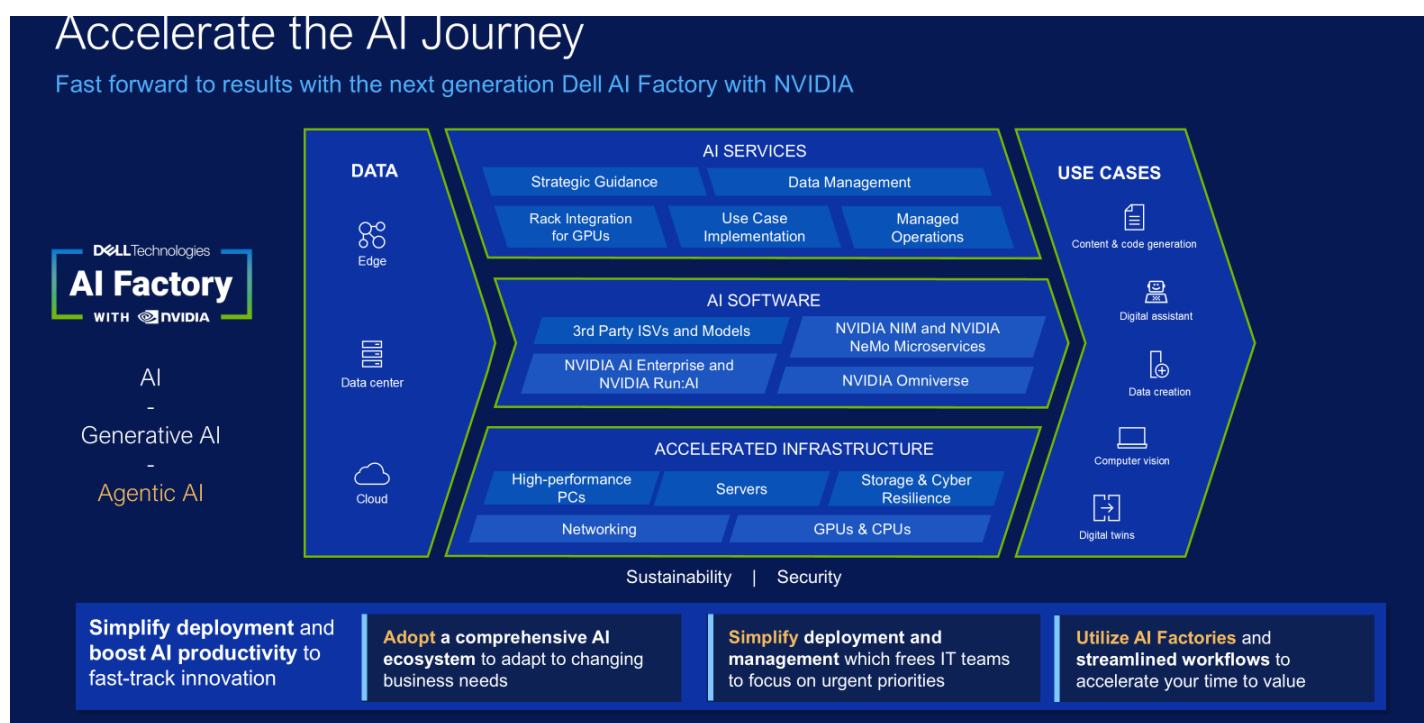
implementation, offering end-to-end solutions that address the full spectrum of challenges from infrastructure deployment to ongoing operational security.

Let's take a closer look at how these two leaders address cyber resilience for AI.

## The Dell AI Factory with NVIDIA

The Dell AI Factory with NVIDIA is the industry's first and only end-to-end enterprise AI solution,<sup>5</sup> designed to speed AI adoption by delivering integrated Dell and NVIDIA capabilities to accelerate organizations' AI-powered use cases, integrate their data and workflows, and enable them to design their own AI journey for repeatable, scalable outcomes.

**Figure 3.** Dell AI Factory with NVIDIA



Source: Dell Technologies

### Key Components of the Dell AI Factory with NVIDIA

- **Infrastructure:** The Dell AI Factory with NVIDIA utilizes NVIDIA-certified systems, storage solutions, cyber resilience, and networking specifically designed to handle demanding AI workloads. Dell offers a wide range of infrastructure solutions, from client devices and workstations to multi-rack data center deployments. This infrastructure is designed to be flexible to adapt to the evolving AI landscape. The solution leverages NVIDIA accelerated computing, including advanced cooling solutions to handle the high-power requirements of AI systems.
- **AI software and models:** The Dell AI Factory with NVIDIA integrates powerful AI software, including NVIDIA AI Enterprise and NVIDIA NIM microservices for agentic AI, and NVIDIA Omniverse for physical AI. These tools

<sup>5</sup> Based on Dell analysis, July 2024. Dell offers solutions with NVIDIA hardware and software engineered to support AI workloads from PCs with AI-powered features and workstations to Servers for High-performance Computing, Data Storage, Cloud Native Software-Defined Infrastructure, Networking Switches, Data Protection, HCI and Services.

accelerate AI workflow development and deployment, streamline operations, and help organizations develop and scale AI applications.

- **Data:** Data is crucial for training and powering AI models. Dell provides solutions to manage, prepare, and ensure the security and governance of critical enterprise data, including cyber-resilience solutions like Dell PowerProtect. The Dell AI Factory with NVIDIA includes solutions for accessing, processing, and leveraging data efficiently, such as the Dell Data Lakehouse, the Dell AI Data Platform, and the NVIDIA AI Data Platform.
- **Ecosystem:** The Dell AI Factory with NVIDIA relies on a dynamic ecosystem of AI and security and solutions vendors, including partnerships with companies like NVIDIA, Hugging Face, and Microsoft. Dell helps organizations navigate this ecosystem to identify suitable partners and implement integrated solutions for simplified AI deployment and operation.

The Dell AI Factory with NVIDIA is a fully integrated ecosystem of hardware, software, and services, designed to deliver measurable value, efficiency, and innovation. It features NVIDIA Blackwell architecture, confidential computing for shared infrastructure, and NVIDIA AI Enterprise to provide a secure software supply chain, vulnerability management, and secure container build processes. By eliminating costly integrations and streamlining adoption, it empowers businesses to focus on achieving impactful outcomes. Backed by industry-leading expertise and partnerships, this solution scales with your goals, enabling smarter, more adaptive operations. Together, Dell and NVIDIA are driving transformative AI innovation, revolutionizing industries, and shaping the future.

Dell's AI Factory with NVIDIA, supported by the PowerProtect portfolio, provides comprehensive cyber-resilience solutions specifically designed for AI workloads. Dell follows a "security-by-design" principle in the architecture of the PowerProtect Portfolio.

Additionally, this integrated approach addresses several unique challenges across the AI lifecycle:

Dell PowerProtect protects AI workloads at each lifecycle stage with verified data integrity, continuous threat monitoring, and rapid recovery tools. Immutable backups, isolated storage for critical assets, and multi-cloud coverage help organizations prevent disruptions and recover AI operations throughout its lifecycle, including:

- **Ingestion.** During data ingestion, PowerProtect secures backed-up raw data as it enters the pipeline, using advanced encryption and access controls to keep data sets untampered.
- **Preparation.** As raw data is transformed for use, PowerProtect secures data sets through robust backups and monitors for cyber anomalies, such as unauthorized changes or malicious tampering, to help maintain clean and reliable data for AI training.
- **Model training.** Model training often involves complex, distributed environments. PowerProtect provides robust backup and recovery frameworks combined with integrated threat detection to protect training data, model artifacts, and checkpoints from cyberthreats and data loss. Native immutability capabilities help ensure that backed-up models and data remain unaltered, supporting reliable recovery and reducing the risk of tampering with stored assets.
- **Deployment.** As models move into production, PowerProtect secures backed-up assets, configurations, and APIs, while continuous threat monitoring helps ensure rapid, reliable recovery, supporting uninterrupted business operations.
- **Inference.** In the inference phase, where real-time insights drive outcomes, PowerProtect enables organizations to quickly restore corrupted data or models, minimizing downtime and maintaining seamless operations.

With isolation and multi-cloud protection, PowerProtect enables organizations to stay resilient amid evolving threats—offering confidence, security, and business continuity across the entire AI lifecycle. Its advanced recovery orchestration simplifies and accelerates the process of restoring data and workloads, supporting seamless recovery and ensuring operational continuity when it matters most.

The orchestrated recovery functionality enables rapid restoration of AI services following disruptions, delivering directly on the promise of cyber resilience.

Dell provides specialized security for RAG implementations through NVIDIA NIM and NeMo Microservices, which provide guardrails for AI compliance and safety, as well as high accuracy data extraction.

This integrated approach ensures organizations can maintain operational continuity, data privacy, and accuracy of their AI systems while protecting against the evolving threat landscape.

## Continuous Monitoring and Validation Approaches

Dell and NVIDIA's approach to ongoing AI security includes:

- **An Open REST API architecture** that provides the flexibility and control organizations need over data protection workflows, enabling seamless integration of continuous monitoring systems to detect potential threats in real time. The Workload State Maintenance functionality preserves and restores AI workload states as needed, addressing the challenge that “when it is detected, we need a way to fix it” when confronting data contamination or model bias.
- **Data set reconstruction capabilities** that enable thorough validation through seamless integration of recovered data sets, ensuring AI systems can be restored to known-good states within defined objectives. The solution's compliance capabilities meet stringent regulatory requirements with built-in monitoring and validation tools, addressing the reality that changing and advancing regulations require flexibility in AI security approaches.
- **Security and resilience services** provide comprehensive end-to-end security architecture for AI implementations, with strategic advisory services and 24/7 managed detection and response for infrastructure, data, applications, and AI models. The approach aligns with the Open Web Application Security Project's (OWASP) Top-10 risks and embeds security throughout the AI lifecycle—from build time to runtime—by implementing control points that enforce guardrails, prevent data leaks, ensure compliance, and detect malicious activities. This security posture is enhanced by NVIDIA's GPU-accelerated continuous monitoring system, which addresses traditional security tools' limitations by detecting anomalies in real time across massive AI data sets, enabling organizations to fill critical skills gaps and confidently adopt AI with built-in resilience and business continuity.

## Conclusion

AI represents a transformative force in business, offering unparalleled opportunities for productivity, innovation, and competitive advantage. However, the unique demands and vulnerabilities of AI workloads require a proactive approach to cyber resilience, ensuring that AI systems remain secure, reliable, and operational. The Dell AI Factory with NVIDIA supported by PowerProtect addresses these challenges head-on, providing organizations with a comprehensive solution that combines high performance, resilience, scalability, and robust security.

By integrating validated architectures, NVIDIA accelerated computing, and by securing data in use through confidential computing, the solution simplifies the implementation of AI protection strategies, bridging the skills gap in both AI and cybersecurity. Its scalability ensures that organizations can seamlessly grow their AI infrastructure across diverse environments, from cloud to edge, as AI transitions from experimental to mission-critical. Furthermore, its legal protection capabilities ensure compliance with evolving regulations, safeguarding sensitive AI data and maintaining governance over AI systems.

As AI becomes a cornerstone of business operations, downtime or compromised systems could result in significant financial, operational, and reputational risks. Dell and NVIDIA's partnership delivers a state-of-the-art solution designed to mitigate these risks, offering organizations the confidence to recover from incidents while maintaining the integrity of their AI operations. By combining Dell's infrastructure expertise with NVIDIA's advancements in GPU

acceleration, confidential computing, and AI-driven security, businesses can build resilient AI systems that are prepared to meet the challenges of today's sophisticated cyberthreat landscape. With the Dell AI Factory with NVIDIA, organizations can confidently harness the power of AI while safeguarding their most critical assets.

To learn more visit [www.dell.com/nvidia-ai](https://www.dell.com/nvidia-ai).

©2025 TechTarget, Inc. All rights reserved. The Informa TechTarget name and logo are subject to license. All other logos are trademarks of their respective owners. Informa TechTarget reserves the right to make changes in specifications and other information contained in this document without prior notice.

Information contained in this publication has been obtained by sources Informa TechTarget considers to be reliable but is not warranted by Informa TechTarget. This publication may contain opinions of Informa TechTarget, which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent Informa TechTarget's assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, Informa TechTarget makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.


Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of Informa TechTarget, is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact Client Relations at [cr@esg-global.com](mailto:cr@esg-global.com).

---

**About Enterprise Strategy Group**

Enterprise Strategy Group, now part of Omdia, provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

 [contact@esg-global.com](mailto:contact@esg-global.com)

 [www.esg-global.com](http://www.esg-global.com)