DELL Technologies

NVIDIA

Top 5 security considerations for Generative AI (GenAI)

Accelerate your adoption of a secure and scalable infrastructure foundation with Dell AI Factory with NVIDIA

The Transformative Potential of GenAI

GenAI has potential to change the game in ways that visionaries are only beginning to imagine.

76%

of IT and business leaders believe that GenAI will deliver transformative value for their organization.[1]

AI

Advanced analysis and logic-based techniques that interpret events and support and automate decisions and actions.

GenAI

Technologies and techniques that leverage large amounts of data to generate new content from natural language prompts or other non-code and non-traditional inputs.

Simulation

- Digital twin
- Synthetic data
- Design frameworks
- Prediction

Content creation

- Coding
- Mathematics
- Writing/speech
- Image/video
- Audio

Content discovery

- Natural language search
- Large dataset analysis
- Knowledge management
- Personalized education and training

User experience

- Real-time translations for 70+ languages
- Personalized interactions using natural facial expressions and body language

1 Dell Technologies Innovation Catalyst Study, February 2024

Increased Potential, Increased Risk

It's tempting for business leaders to want to move quickly, bypassing implications involving data, compliance, governance, and other risks. But GenAI is a double-edged sword when it comes to security.

Benefits

- Improved threat detection
- Enhanced operational efficiency
- Personalized security awareness training

Drawbacks

- Increased attack sophistication
- Advanced social engineering
- Shadow AI

33%

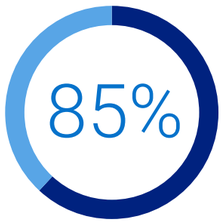
of respondents listed cybersecurity as the top GenAI risk their organizations is working to mitigate.[2]

2 McKinsey Global Survey on AI: The state of AI in early, May 2024

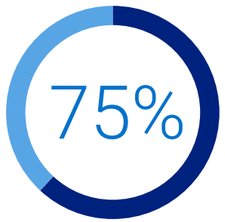
CONSIDERATION 1

The New Threat Landscape

Along with GenAI's promise comes a sobering reality: attackers are creating new and more intricate attacks that can bypass conventional defenses, making it difficult for cybersecurity teams to keep up.



of respondents believe AI has made cybersecurity attacks more sophisticated.[3]



of security professionals saw an increase in attacks over the past 12 months.[4]

To protect against these emerging threats, companies must focus on minimizing the attack surface through penetration testing, monitoring, and auditing for example.

3 2024 Human Risk in Cybersecurity Survey, EY, May 2024
4 Voice of SecOps Report "Generative AI and Cybersecurity: Bright Future or Business Battleground?" 2023

Emerging Attack Vectors

Advanced malware
Increasingly sophisticated malware that uses GenAI to "self-evolve," continually changing its code to go undetected by existing security, such as signature-based detection.

Highly personalized phishing emails and campaigns
Increasing frequency of authentic-looking malicious emails that lack usual scam signs.

Convincing deep fake data
Identity theft, financial fraud, and misinformation made easier by the ability to mimic human actions, such as writing, speech, images, or video.

Automated reconnaissance
Information gathering that identifies vulnerabilities and weaknesses in a potential target's network or system to facilitate more targeted attacks.

CONSIDERATION 2

Deployment and Implementation Risks

Organizations that want to capitalize on the potential benefits of GenAI need large amounts of high-quality data – inputs that models can use to produce the best outcomes. But data and risk go hand-in-hand. Before leveraging any information, companies must carefully evaluate and account for their unique requirements, inputs, and risks.

Large language model (LLM) vulnerabilities

GenAI services are vulnerable to prompt injection attacks, whereby attackers manipulate outputs to bypass security guardrails or gain unauthorized access to files that may have been used in refining the model.

Data poisoning

Attackers can deliberately feed altered data to an LLM during the training phase. This can lead to the model being vulnerable to attacks through backdoors embedded in the data. A real-world example is attacking and exploiting spam filters by training them on spam emails.

Regulatory complexity

Regulators worldwide are racing to understand, control, and guarantee the safety of GenAI. While GenAI models are subject to current data sovereignty rules that dictate how data is stored, processed, and used, governing bodies are still defining oversight of IP and copyrighted information. Adherence to regulations can be costly, but failure to comply with established and emerging regulations could result in fines and other penalties.

CONSIDERATION 3

Shadow AI

Many employees today already use public text, image, and video generators like ChatGPT to augment their daily workstreams. However, when these tools are used without proper governance they pose a critical threat for organizations trying to secure corporate intellectual property and data. This unauthorized use of GenAI is known as Shadow AI.

Loss of intellectual property

Already, companies are dealing with the loss of intellectual property from employees sharing sensitive information in public GenAI tools.

Source code data leakage

Developers attempting to optimize source code by using ChatGPT have caused data leakage.

To address the challenges of Shadow AI, companies should implement a company-wide council or board with the authority to make decisions involving secure AI governance.

Where does your data reside? Where should workloads be placed?

AI works best when it's paired with your data, wherever it lives. With complete control over infrastructure and LLMs, there's no risk of IP loss or source code data leakage.

Costs

Leveraging on-prem implementations can lower TCO by up to 75% over 3 years.[5]

Security & privacy

Create secure AI / GenAI environments across the organization with on-premises workflows and operations. Exercise strict control over data security and adherence to compliance regulations, particularly for industries that handle sensitive data.

5 Based on Enterprise Strategy Group research commissioned by Dell, comparing on-premises Dell infrastructure versus native public cloud infrastructure as a service, April, 2024. Analyzed models show a 7B parameter LLM leveraging RAG for an organization of 5k users being up to 38% more cost effective while a 70B parameter LLM leveraging RAG for an organization of 50k users being up to 75% more cost effective. Actual results may vary. Economic Summary

CONSIDERATION 4

Evaluation Criteria

Over the last year, the AI community has increasingly focused on three key issues: responsible development and deployment, assessing impact, and mitigating risks. As companies evaluate GenAI models, they must take into account some important caveats:

No Consistent Reporting Requirements

Leading developers primarily test their models against different responsible AI benchmarks. Because of this significant lack of standardization in reporting, it is difficult to methodically compare the risks and limitations of top AI models.

Copyrighted Material in Outputs

The outputs of popular LLMs may contain copyrighted material, potentially violating the law and putting companies who use the material at risk of penalties.

Vulnerabilities are Increasingly Complex

Researchers are finding less obvious strategies that cause LLMs to exhibit harmful behavior, such as asking models to infinitely repeat random words.

Developers Lack Transparency

In many cases, AI developers are not forthcoming regarding their training data and methodologies. This hinders efforts to further understand the robustness and safety of AI systems.

CONSIDERATION 5

Security Benefits

Alongside GenAI's security risks are its potential security benefits. GenAI is becoming a crucial ally in cybersecurity, opening novel avenues of protection.

You can now start building scalable security operations with faster access to richer insights and automatic threat detection—delivering efficiency and supplementing understaffed security teams.

Threat Detection and Response

By analyzing historical data and identifying patterns and anomalies, GenAI can recognize new and evolving threats in real time. It can continuously monitor network traffic, system logs, and user behavior and promptly identify irregular activities that may signify security threats.

The result is powerfully adaptive threat detection, enabling quick response to changing attack vectors and providing a proactive defense mechanism against emerging cyber threats.

Threat Simulation and Training

With GenAI, companies can simulate a wide range of cybersecurity threats and attack scenarios in a controlled environment. As a result, teams are better prepared to identify, respond to, and mitigate cyber threats when time is of the essence.

In-depth Analysis and Summarization

GenAI empowers teams to investigate data from different sources or modules, enabling them to conduct traditionally time-intensive, tedious data analysis faster and with more accuracy. Teams can also create natural-language summaries of incidents and threat assessments, improving efficiency and increasing team output.

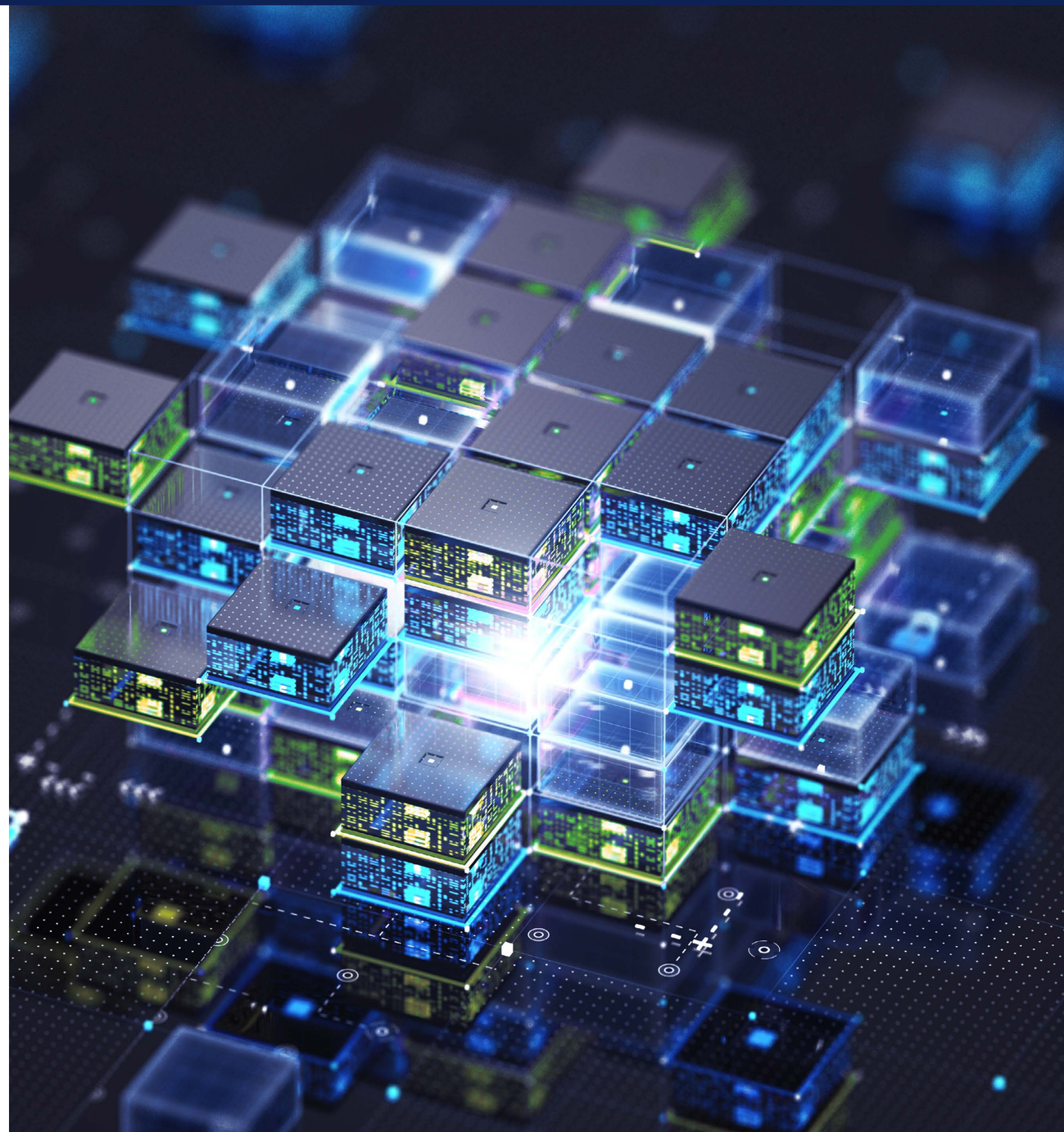
Personalized Security Awareness Training

By wrapping conversational AI on top of GenAI and incorporating an AI Avatar into the user interface, organizations can deliver personalized interactions (available at scale 24/7) using natural facial expressions and body language. This can be used for security training and education, providing a more natural, customized, and interactive learning experience, automated assessments, and more.

The Dell AI Factory with NVIDIA

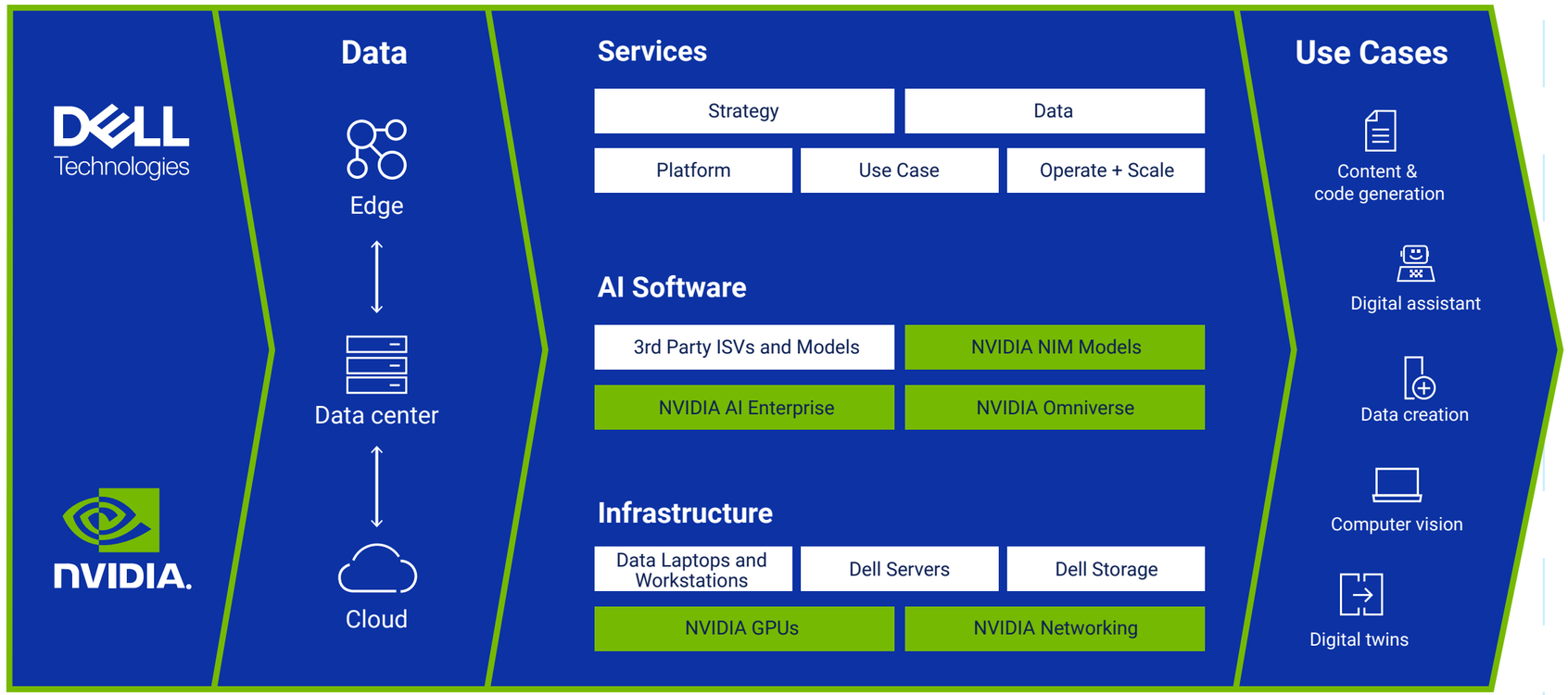
Accelerate your AI journey and securely transform your data into insights with the industry's first comprehensive, turnkey AI solution. The Dell AI Factory with NVIDIA addresses the complex needs of enterprises seeking to leverage AI and GenAI. With leading infrastructure and services together with NVIDIA AI software, you can increase time to value for your projects by simplifying development and deployment.

- Reduce risk of compromise with infrastructure that features intrinsic security, including root of trust and other key features.
- Protect your data from leakage that could result in loss of intellectual property with an on-premises AI solution that you control.
- Meet strict compliance and data sovereignty requirements by bringing AI to your data with secure access.
- Protect your stakeholder's privacy by controlling where and who has access to your data.



The Dell AI Factory with NVIDIA

INDUSTRY'S FIRST END-TO-END ENTERPRISE AI SOLUTION



Data fuels the AI factory and your use cases

Your most valuable data is on-premises and at the edge. Dell Technologies helps you bring AI to that valuable data and is a leader in storing, protecting and managing it.

Use case to outcomes

The AI factory produces business outcomes powered by your highest priority use cases. Dell Technologies simplifies the deployment of your most important AI use cases with validated solutions and tailored services.

Don’t let security risks stifle innovation

Let us help you navigate the world of AI and GenAI, so you can reap the rewards.

STRATEGY PLANNING

Free Accelerator Workshop for GenAI

- Start your journey to developing a winning strategy
- Address challenges and gaps, prioritize objectives, and identify opportunities
- Get a readiness assessment for a deeper dive into infrastructure requirements, AI models, operational integrations, and more

TECHNICAL PREPARATION

Ready-to-use mobile lab

Jumpstart your journey to success. Includes a Dell Mobile Precision Workstation 5690 / 7780 with NVIDIA GPUs and two days of consulting services to help you get started.

- Portable sandbox environment for GenAI testing and demonstration
- Pre-validated with NVIDIA AI Workbench platform ready for developers
- Initial chatbot use case implemented with your data
- Cost-effective, low-risk approach to experiment and build GenAI skills

DELL MOBILE PRECISION WORKSTATION 5690 / 7780 WITH NVIDIA GPUS

GET STARTED TODAY

DELL Technologies AI Factory WITH NVIDIA