

Advancing the future of AI

[Learn more >](#)

UNDERSTANDING THE HOWS OF AI DEPLOYMENT

In this series, Dell Technologies explores and deep dives into AI and genAI-related solutions for both enterprises and SMBs in APAC.

Sponsored by Dell Technologies



# Dulling the impact of AI-fueled cyber threats with AI

BrandPost • By Dell Technologies

Oct 24, 2024 • 5 mins

Artificial Intelligence • Generative AI



CREDIT: SHUTTERSTOCK

IT leaders are placing faith in AI. Consider **76 percent of IT leaders** believe that generative AI (GenAI) will significantly impact their organizations, with 76 percent increasing their budgets to pursue AI.

But when it comes to cybersecurity, AI has become a double-edged sword. While poised to fortify the security posture of organizations, it has also changed the nature of cyberattacks.

Take for instance large language models (LLMs) for GenAI. While LLMs are trained on large amounts of information, they have expanded the attack surface for businesses. From prompt injections to poisoning training data, these critical vulnerabilities are ripe for exploitation, potentially leading to increased security risks for businesses deploying GenAI.

What's worrying is that this list is only going to be more extensive as the capabilities of AI expand and fuel more sophisticated cyberattacks. After all, the growth of AI is expanding alongside the growing complexity of cybercrime, with the **global cost of cybercrime** swelling by a staggering 1,237 percent.

## Artificial Intelligence: A turning point in cybersecurity

The cyber risks introduced by AI, however, are more than just GenAI-based. These days, digital spoofing, phishing attacks, and social engineering attempts are more convincing than ever due to bad actors refining their techniques and developing more sophisticated threats with AI. It can also create cyber threats that are harder to detect than before, such as AI-powered malware, which can learn from and circumvent an organization's defenses at breakneck speed.

Data privacy in the age of AI is yet another cybersecurity concern. Threat actors have their eyes set on AI-powered cybersecurity tools that gather information across data sets, which can include confidential information. This puts businesses at greater risk for data breaches. Moreover, this can cause companies to fall short of regulatory compliance, with these data potentially being misused.

Businesses' increased use of AI, too, is transforming cybersecurity roles. As responsibilities evolve, this can lead to a wider cybersecurity skill gap. And while the cyber risks introduced by AI can be countered by incorporating AI within security tools, doing so can be resource-intensive. Businesses will need to invest in hardware and infrastructure that are optimized for AI and this may incur significant costs.

With businesses still navigating their use of AI, it's no surprise many organizations are not prepared for AI-powered attacks yet. Almost 90 percent surveyed in the **Dell Global Data Protection Index** acknowledge that AI will create large volumes of data that need protection but only 65 percent are backing up as little as 50 percent of their AI data.

## Fighting fire with fire

For these reasons, organizations that wish to curb the burgeoning impact of AI on their cyber risks need to be particularly vigilant while taking advantage of the abilities of AI to stem this tide of attacks.

With AI capable of analyzing vast amounts of data, it can detect anomalies across their operations, such as spikes in network traffic, unusual user activities, and even suspicious mail. This approach also reduces the time taken for companies to respond to attacks. Automation, too, can be applied to processes such as cyber threat hunting and vulnerability assessments while rapidly mitigating potential damage in the event of a cyberattack.

Moreover, AI can reduce false positives more effectively than rule-based security systems. Contextualizing patterns and identifying potential threats can minimize alert fatigue and optimize the use of resources. Organizations can even take pre-emptive steps to stop future attacks before they happen with AI's predictive capabilities.

AI can also personalize training for employees more vulnerable to social engineering attacks. Then there's reinforcement learning, a type of machine learning model that trains algorithms to make effective cybersecurity decisions. This allows businesses to anticipate tactics used by cybercriminals to bolster their defenses.



## Boost your cybersecurity with AI

Don't let potential security risks slow down your pace of innovation. Consider some of these practices to maximize AI use for cybersecurity—and against AI-powered cyberattacks.

- **Set up trusted devices and infrastructure** to minimize unauthorized access
- **Deploy data security measures** such as data classification, encryption, and data protection to protect sensitive data sources
- **Proactively address threats** through security measures, continuous monitoring, and regular updates
- **Respond to cyber threats swiftly** by automating several security processes, such as blocking the IP address of identified threats
- **Invest in cybersecurity solutions** that deliver market-leading, specialized protection for AI workloads, such as **Dell PowerProtect Cyber Recovery**, which protects and isolates critical data from ransomware and other sophisticated threats; **Dell APEX Backup Services**, which delivers unified data protection for GenAI use cases; and **Dell PowerProtect Data Domain** and **Dell PowerProtect Data Manager**, which serves as a resilient foundation for defending AI infrastructures.

**Find out more about leveraging the AI edge to defend against today's escalating cyber threats.**

ADVERTISEMENT



Advancing the future of AI

Building one of the world's fastest supercomputers

[Learn more >](#)

Related content

**BRANDPOST**  
Sponsored by Dell Technologies  
Choosing the best AI models for your business

By Dell Technologies  
Oct 17, 2024 • 4 mins

Generative AI • Artificial Intelligence

**BRANDPOST**  
Sponsored by Dell Technologies  
The success of GenAI models lies in your data management strategy

By Dell Technologies  
Oct 09, 2024 • 5 mins

Generative AI • Artificial Intelligence

**BRANDPOST**  
Sponsored by Dell Technologies  
Does your SMB have the foundation in place for GenAI?

By Dell Technologies  
Oct 04, 2024 • 5 mins

Generative AI • Artificial Intelligence

**BRANDPOST**  
Sponsored by Dell Technologies  
Give your enterprise a head start in the GenAI race

By Dell Technologies  
Sep 26, 2024 • 5 mins

Generative AI • Artificial Intelligence


PODCASTS

VIDEOS

RESOURCES

EVENTS

ADVERTISEMENT



Better data ↓  
↑ Smarter AI

That's data intelligence

[Explore](#)

SUBSCRIBE TO OUR NEWSLETTER

From our editors straight to your inbox

Get started by entering your email address below.

Enter your email here

[SUBSCRIBE](#)

ADVERTISEMENT

Don't miss your chance to join the CIO Experts Network.

Join the Experts Network and get involved with CIO as a potential content creator, speaker or influencer.

[SIGN UP TODAY](#)



Show me more

- POPULAR
- ARTICLES
- PODCASTS
- VIDEOS

01

**NEWS**  
Freshworks lays off 660 — about 13 percent of its global workforce — despite strong earnings, profits

By Evan Schuman  
Nov 07, 2024 • 6 mins

CRM Systems • Staff Management

Artificial Intelligence



02

**PODCAST**  
Extreme Networks' Nabil Bukhari on why your AI strategy is failing

Nov 06, 2024 • 64 mins

IT Leadership



03

**VIDEO**  
Nobli9 tracks service-level objects for faster reliability response

Nov 06, 2024 • 16 mins

Application Performance Management

Network Monitoring

