



FEBRUARY 19, 2024

The Protective Paradox: How Artificial Intelligence Helps Solve AI Cybersecurity Risks

[Read More →](#)

AI: The bad,
the ugly,
the good in
cybersecurity

[Get the facts](#)[Blog Post](#) > [The Protective Paradox: How Artificial Intelligence Helps ...](#)

AI: The bad,
the ugly,
the good in
cybersecurity

[Get the facts](#)

For cybersecurity, artificial intelligence (AI) is both shield and sword. By implementing AI-driven tools, businesses are better protected against potential cyberthreats. By arming themselves with these same solutions, however, attackers are finding new ways to cut through defenses and compromise key systems.

The result is a protective paradox: Even as AI cybersecurity risks grow, they represent the best defense against itself. Here's what companies need to know about navigating the new reality of AI.

Slash and Learn: The Emerging Risks of AI

The past year has put AI in the spotlight as large language models (LLMs) and tools like ChatGPT and DALL-E have captured consumer attention. As noted by Thomas Schmitt, Global Director of security for Anheuser-Busch InBev and moderator of the recent CES tech conference panel, *Our Newest Cyber Threat is AI and AI is Our Biggest Defense*, "AI itself is not new, but LLMs and generative AI have sparked creativity." This creativity, however, isn't reserved for those with good intentions.

Just as AI makes it possible to write new stories or create new art, it also opens the door to new cyberattack vectors capable of circumventing current IT defenses.

According to Dr. Amit Elazari, Co-founder and CEO of OpenPolicy, "The biggest threat is not prompt injection or data poisoning. Instead, it's going back to the foundation of defense and attack — the attackers are always ahead." Attackers have the luxury of experimenting with new AI technologies to see what works and what doesn't, while defenders are compelled to respond.

The evolving nature of new tools also creates AI cybersecurity risks. Put simply, these solutions can learn from their mistakes, meaning that when one attack fails, the next will incorporate data from that failure to improve the outcome. In practice, this can take the form of advanced social engineering. By utilizing available public data, knowledge of human behavior, and past defender actions, attackers can leverage AI to create advanced phishing and ransomware campaigns that are more likely to fool even experienced users.

Keep Humans in the Loop

According to Nicholas Parrotta, Chief Digital and Information Officer and President of [Digital Transformation Solutions](#) at HARMAN, "AI models are wrong a lot of the time. We need humans in the loop. For example, we just launched a large language model for health, and physicians are at

the center of this model."

In fact, without humans, risk increases. What we're seeing now is the explosion of what AI means. It's beyond an abstract computer solving problems, it's a car driving itself or process automating itself. Ultimately, AI is a tool for humans. If we take humans out of the loop, we're increasing the threat level.

Use the Right Tools

"From a HARMAN perspective, we're seeing the rise of simple, smart, and secure experiences," said Parrotta. This isn't an either/or situation; users want all three components simultaneously. As a result, companies must deploy tools that meet these expectations. For example, [HARMAN's Digital Transformation Solutions](#), can help businesses blend physical and digital resources to deliver dynamic results. HARMAN has also partnered with NVIDIA to develop AI-powered solutions for detecting and preventing cyberattacks.

Double Down on Defense

Companies need to double down on security by design and [red-team exercises](#), which the National Institute of Standards and Technology defines as an exercise that can demonstrate real-world situations to better identify security capabilities. The technology is going to continue to evolve and businesses need to take part in the conversation.

Opposites Attract

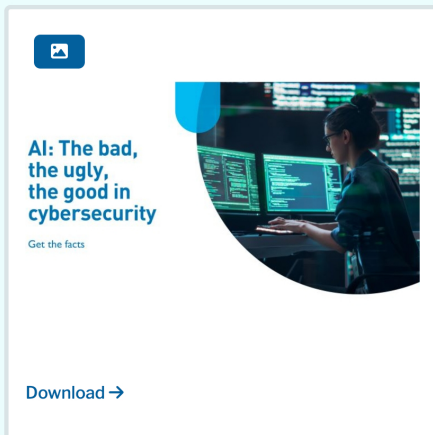
AI has arrived. [Generative tools](#) have gone mainstream, and LLMs are making inroads into enterprise-scale business strategy.

But with benefits come drawbacks. Malicious actors are now using AI to compromise key operations and leveraging the learning capabilities of these solutions to stay ahead of security teams. The paradox? By reducing AI cybersecurity risks, enterprises can embrace intelligent technologies to spot potential problems, take immediate action, and give security professionals time to react.

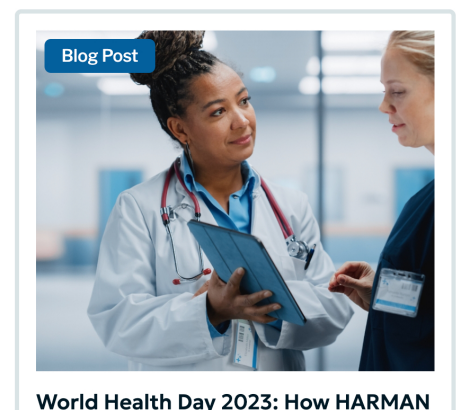
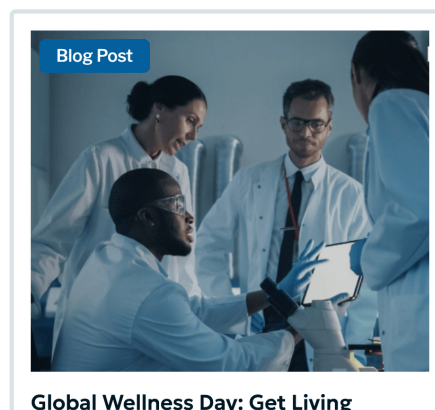
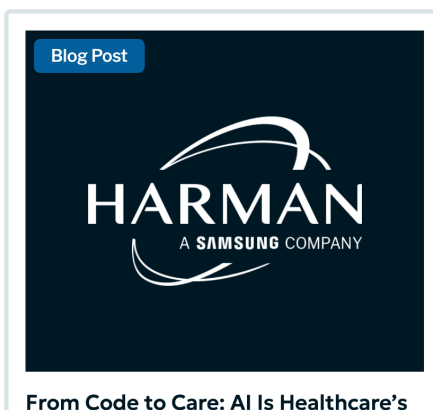
Curious about the emerging role of AI security? [Check out the full CES session here.](#)

By Doug Bonderud

Downloads



Related Articles



Most Significant Disruptor

[Read More →](#)

Healthy with HARMAN

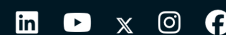
[Read More →](#)

Innovations Aim to Deliver “Health for All”

[Read More →](#)

Sign up to receive news and blog updates

[Subscribe](#)



Quick Links

[Harman Automotive](#)
[Harman Newsroom](#)
[Lifestyle](#)
[Contact Us](#)

Company Info

[About Us](#)
[Our Mission](#)
[Leadership](#)
[Our Brands](#)

Resources

[Privacy Policy Statements](#)
[Terms of Use](#)
[Cookies Statement](#)
[Careers](#)
[Sitemap](#)

© 2026 HARMAN International. All Rights Reserved.

If you are using a screen reader and are having problems using this website, please call (800) 645-7484 for assistance.

