LOGICALIS
Architects of Change

Platinum
Business
Partner

IBM

Solution Brief

Generative AI and Cybersecurity: The Double-Edged Sword

How to tackle AI-related cyber risk with the right security strategy

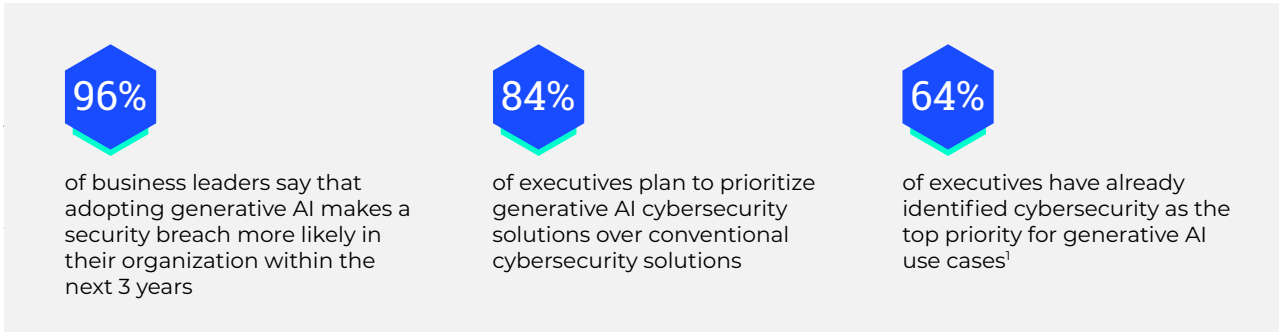
Generative AI: A Paradox in Cybersecurity

In cybersecurity, generative artificial intelligence (AI) is a double-edged sword.

On the one hand, it offers new tools, tactics, and strategies that can enhance security and streamline workflows. With the right approach, generative AI can act as a force multiplier that improves the security posture, while driving more productivity and efficiency.

At the same time, however, cyber attackers also have access to the same capabilities. Generative AI empowers them with new levels of speed, scale, and sophistication, while also enabling less technically savvy actors to engage in cyber crime.

To adapt to this new frontier in the cybersecurity landscape, it is important to understand both sides of the battle: how cyber attackers will use generative AI and how you can use generative AI to secure your organization.



The Two Battle Fronts: AI & the Organization

There are two main ways cybercriminals can use generative AI to attack.

Attacking Your Organization

Generative AI can dramatically enhance attackers' productivity, allowing them to execute more attacks faster, with more precision, and at a larger scale.

Tools, such as ChatGPT, can and have been used to craft highly personalized phishing attacks, and a security engineer at HYAS InfoSec[2] also showed how to build a mutating, polymorphic malware program with ChatGPT's API.

Deepfake phishing, which uses deepfaked audio or video to deceive their targets, grew by 3,000%[3] in 2023, and this number will only grow as generative AI technology becomes more sophisticated and prevalent. In early 2024, IBM researchers demonstrated an even more alarming technique, "audio-jacking,"[4] which involves the use of generative AI tools to hijack live audio calls and manipulate what is being said without the speakers knowing.

1. https://www.ibm.com/downloads/cas/A2Y9AYED
2. https://www.hyas.com/blog/blackmamba-using-ai-to-generate-polymorphic-malware
3. https://onfido.com/landing/identity-fraud-report/?ref=hackernoon.com
4. https://securityboulevard.com/2024/02/ibm-shows-how-generative-ai-tools-can-hijack-live-calls/

"We were able to modify the details of a live financial conversation occurring between the two speakers, diverting money to a fake adversarial account (an inexistent one in this case), instead of the intended recipient, without the speakers realizing their call was compromised...Alarmingly, it was fairly easy to construct this highly intrusive capability."

- Chenta Lee
Chief Architect, Threat Intelligence, IBM Security

Attacking Your AI Models

Another vulnerability is the AI models themselves.

Malicious attackers can undermine the integrity of those models by poisoning that training data and forcing those models to behave in certain ways or to generate incorrect output. Cybercriminals can also "jailbreak" large language models (LLMs) using natural language prompts, which effectively removes ethical and policy guardrails.

IBM® X-Force®[5] researchers have shown that jailbroken LLMs can be compelled to leak confidential financial information, create vulnerable and malicious code, and offer poor security recommendations.

The Counterbalance: AI as a Force Multiplier in Cybersecurity

IT and cybersecurity leaders face ongoing challenges, from an ongoing talent shortage to growing infrastructure complexity to expanding attack surfaces. In spite of these challenges, some of which are exacerbated by generative AI, this new technology also opens the door to new tools and possibilities. With the right approach, generative AI can help maximize cybersecurity time and talent, enabling teams to take on more challenges at a lower cost.

Here are a few ways that generative AI can help:

- Generative AI tools can automatically create incident reports for various stakeholders, which can then be personally tailored based on their level of technical expertise and their areas of interest.
- Using natural language as input, generative AI-based cybersecurity tools can accelerate threat hunting and detect new threats based on attack patterns.
- To help analysts interpret data more quickly and expedite investigations, these solutions can provide simple explanations of log data.
- With curated threat intelligence, security teams can hone in on campaigns and threats that are most relevant to their organization.

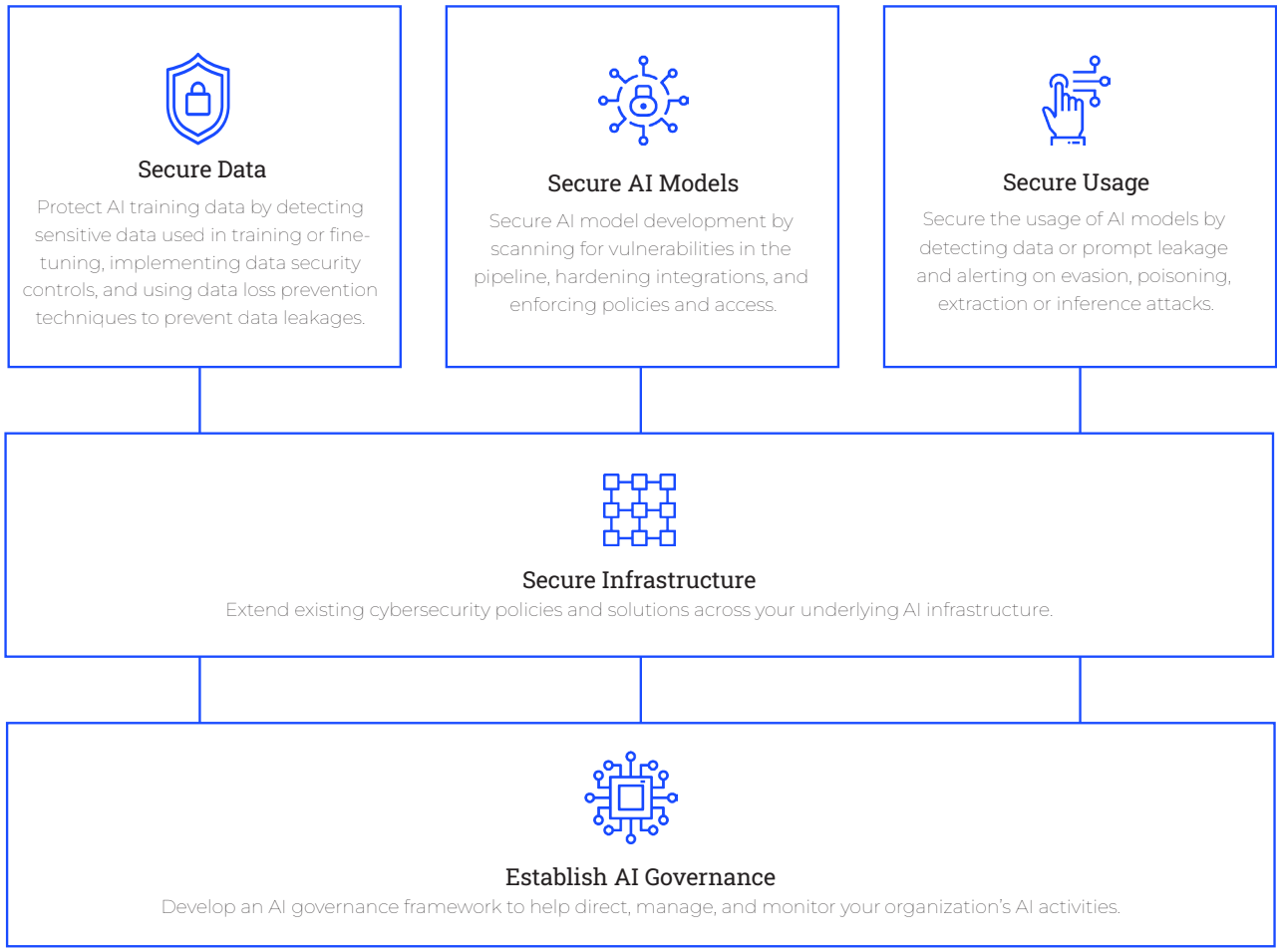
5. https://securityintelligence.com/posts/unmasking-hypnotized-ai-hidden-risks-large-language-models/

These use cases are certainly compelling and they can significantly improve efficiency, productivity, and security postures. Yet with the introduction of generative AI across the organization and the supply chain, it is critical to develop and implement security frameworks to help secure AI against risk.

The IBM Framework for Securing Generative AI

In their rush to adopt generative AI, many organizations are sidestepping best practices when it comes to security, coding, and data. Exploitable software flaws, exposed data, and other vulnerabilities can all create new security risks. Adopting the right framework can help prevent such mistakes and ensure that your organizations build more secure, trustworthy AI.

IBM's framework for securing generative AI[6] provides a foundation for protecting trusted foundation models, generative AI, and data. This approach will help secure AI at each stage of the pipeline, from data collection and handling through model inference and use.



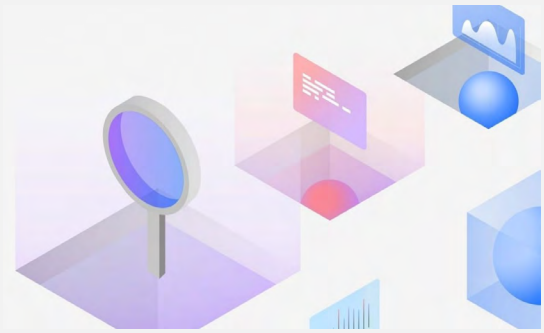
6. https://www.ibm.com/downloads/cas/A2Y9AYED

From Strategy to Application: Bolstering AI with the Right Tools

Generative AI poses risks and it comes with challenges, but it also presents an opportunity to enhance cybersecurity, maximize talent, and streamline security workflows. An industry leader in cybersecurity and AI, IBM's portfolio of security solutions provide transformative, AI-powered solutions that optimize time while keeping cybersecurity teams in charge and ahead of threats.

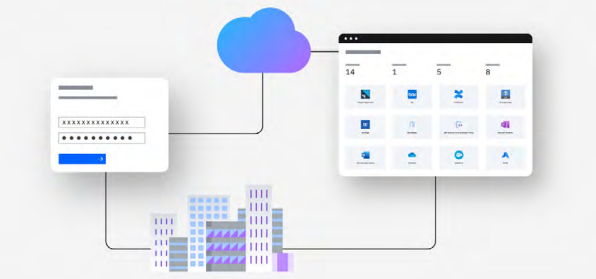
IBM Security® QRadar® Suite

Advanced AI threat intelligence and automation designed to empower security analysts to work with greater speed, efficiency, and precision across their core toolsets.



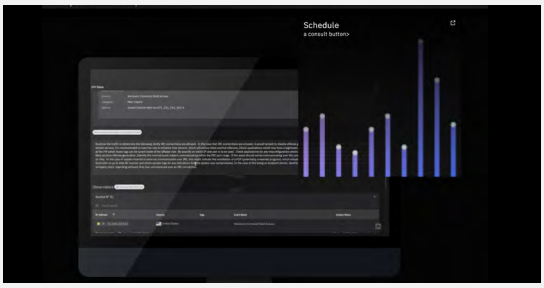
IBM Security® Guardium®

An AI-powered data security platform that provides superior data monitoring, quicker identification of data threats, and complete visibility throughout the data lifecycle, while helping address data compliance needs.



IBM Security® Verify

Deep, AI-powered context for both consumer and workforce identity access management, protecting users and apps, inside and outside the enterprise.



IBM Security® Managed Detection and Response Services

With a unified, AI-powered approach and visibility across networks and endpoints, threat hunters can take decisive actions and respond to threats faster.

Preparing for the Security Risks and Opportunities of Generative AI

Generative AI is a double-edged sword that provides powerful new capabilities for both attackers and defenders. While cybercriminals can leverage generative AI for more sophisticated and large-scale attacks like deepfakes, malware creation, and model poisoning, organizations can use it as a force multiplier to enhance threat detection, incident response, and overall security postures.

To stay ahead of evolving, generative AI-powered threats, organizations need a comprehensive strategy utilizing the right security tools and frameworks. IBM's modern security portfolio takes full advantage of generative AI's capabilities to secure data, models, usage, infrastructure and governance.

Take the Next Step in Generative AI-Powered Security

with Logicalis and IBM

An IBM Platinum Partner, Logicalis is prepared to help you tackle generative AI head on and make full use of IBM's AI-powered cybersecurity portfolio. From Professional and Managed Services to consulting and infrastructure, we have extensive experience helping enterprise customers modernize and transform with IBM. By partnering with IBM and Logicalis, you can implement transformative AI-driven cybersecurity solutions that amplify their defenses for the new era of AI threats and opportunities.

Schedule a free executive briefing to find out how we can help.

Schedule a free executive briefing.
logicalis-hub.com/ibm

LOGICALIS
Architects of Change

Platinum
Business
Partner
IBM