Gartner Research

4 Ways Generative AI Will Impact CISOs and Their Teams

Jeremy D'Hoinne, Avivah Litan, Peter Firstbrook

29 June 2023

Gartner®

4 Ways Generative AI Will Impact CISOs and Their Teams

Published 29 June 2023 - ID G00793265

By Analyst(s): Jeremy D'Hoinne, Avivah Litan, Peter Firstbrook

Initiatives: Cyber Risk; Artificial Intelligence; Build and Optimize Cybersecurity Programs

ChatGPT and large language models are the early signs of how generative AI will shape many business processes. Security and risk management leaders, specifically CISOs, and their teams need to secure how their organization builds and consumes generative AI, and navigate its impacts on cybersecurity.

Additional Perspectives

- Invest Implications: 4 Ways Generative AI Will Impact CISOs and Their Teams (19 July 2023)

Overview

Impacts

- A proliferation of overoptimistic generative AI (GenAI) announcements in the security and risk management markets could still drive promising improvements in productivity and accuracy for security teams, but also lead to waste and disappointments.
- Consumption of GenAI applications, such as large language models (LLMs), from business experiments and unmanaged, ad hoc employee adoption creates new attack surfaces and risks on individual privacy, sensitive data and organizational intellectual property (IP).
- Many businesses are rushing to capitalize on their IP and develop their own GenAI applications, creating new requirements for AI application security.
- Attackers will use GenAI. They've started with the creation of more seemingly authentic content, phishing lures and impersonating humans at scale. The uncertainty about how successfully they can leverage GenAI for more sophisticated attacks will require more flexible cybersecurity roadmaps.

Recommendations

To address the various impacts of generative AI on their organizations' security programs, chief information security officers (CISOs) and their teams must:

- Initiate experiments of "generative cybersecurity AI," starting with chat assistants for security operations center (SOCs) and application security.
- Work with organizational counterparts who have active interests in GenAI, such as those in legal and compliance, and lines of business to formulate user policies, training and guidance. This will help minimize unsanctioned uses of GenAI and reduce privacy and copyright infringement risks.
- Apply the AI trust, risk and security management (AI TRiSM) framework when developing new first-party, or consuming new third-party, applications leveraging LLMs and GenAI.
- Reinforce methods for how they assess exposure to unpredictable threats, and measure changes in the efficacy of their controls, as they cannot guess if and how malicious actors might use GenAI.

Strategic Planning Assumptions

By 2027, generative AI will contribute to a 30% reduction in false positive rates for application security testing and threat detection by refining results from other techniques to categorize benign from malicious events.

Through 2025, attacks leveraging generative AI will force security-conscious organizations to lower thresholds for detecting suspicious activity, generating more false alerts, and thus requiring more — not less — human response.

Introduction

The level of hype, scale and speed of adoption of ChatGPT has raised end-user awareness of LLMs, leading to uncontrolled uses of LLM applications. It has also opened the floodgates to business experiments and a wave of AI-based startups promising unique value propositions from new LLM and GenAI applications. Many business and IT project teams have already launched GenAI initiatives, or will start soon.

CISOs and security teams need to prepare for impacts from generative AI in four different areas (see also Figure 1):

1. **"Defend with"** generative cybersecurity AI: Receive the mandate to exploit GenAI opportunities to improve security and risk management, optimize resources, defend against emerging attack techniques or even reduce costs.

2. **"Attacked by"** GenAI: Adapt to malicious actors evolving their techniques or even exploiting new attack vectors thanks to the development of GenAI tools and techniques.

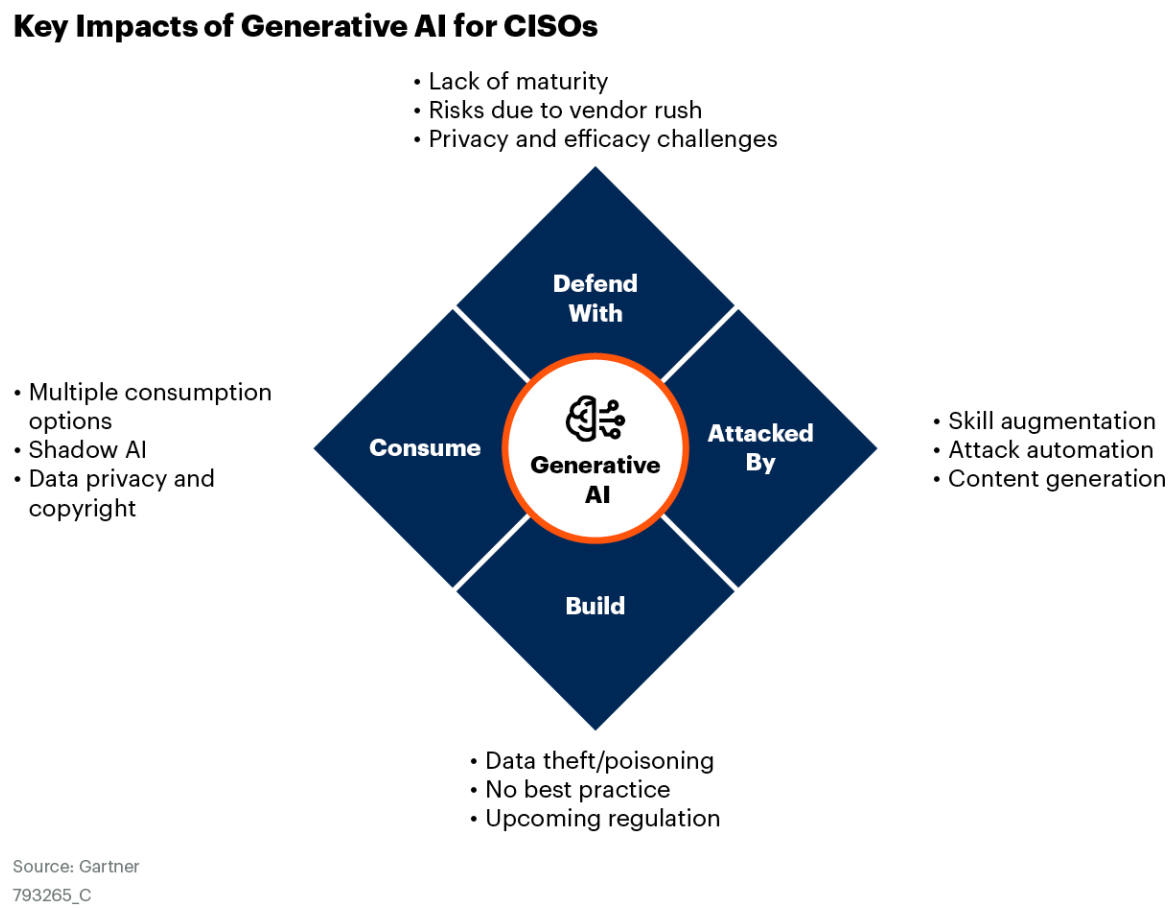
3. Secure enterprise initiatives to **"build"** GenAI applications: AI applications have an expanded attack surface and pose new potential risks that require adjustments to existing application security practices.

4. Manage and monitor how the organization **"consumes"** GenAI: ChatGPT was the first example; embedded GenAI assistants in existing applications will be the next. These applications all have unique security requirements that are not fulfilled by legacy security controls.

> **Businesses will embrace generative AI, regardless of security.**

This research provides clarity through the hype and gives actionable recommendations for each of these four impact areas, enabling CISOs and their teams to quickly adapt to this fast pace of change.

Figure 1: Key Impacts of Generative AI for CISOs



Impacts and Recommendations

Overoptimistic GenAI Announcements in the Security and Risk Management Could Drive Improvements, but Also Lead to Waste and Disappointments

Gartner defines generative cybersecurity AI as GenAI techniques that learn a representation of artifacts from existing (cybersecurity) data or through simulation agents and then use it to generate new artifacts.

As its name suggests, generative cybersecurity AI derives its main use cases from GenAI (see Note 1). Gartner has reviewed more than 30 announcements from security providers. The two most frequent generative cybersecurity AI use cases are **secure application development assistants** and **security operations chatbots**.

Secure Application Development Assistants

Code generation tools (e.g., GitHub Copilot, Amazon CodeWhisperer) are embedding security features, and application security tools are already leveraging LLM applications. Example use cases for these secure code assistants include:

- **Targeting primarily application security teams:**
  - **Vulnerability detection:** Highlights issues in code snippets entered in the prompts or by performing a scan of the source code.
  - **False positive reduction:** Used as a confirmation layer for other code analysis techniques, the feature analyzes the alert and the related code and indicates in conversational language why it might be a false positive.
  - **Remediation assistant:** Suggests updates in the code to fix identified vulnerabilities as part of the finding summary that is generated.
- **Targeting primarily development teams, not security personnel:**
  - **Code generation:** Creates script/code from developers input including natural language comments or instructions, or acts as an advanced code completion tool. Some tools can also indicate whether the generated code resembles an open-source project, or can help validate that code (generated or human written) complies with standard industry security practices.
  - **Unit test creation:** Suggests a series of tests for a submitted function to ensure its behavior is as expected and is resistant to malicious inputs.
  - **Code documentation:** Generates explanations of what a piece of code does, or the impact of a code change.

While the use cases are easy to identify, it is still really early to get relevant qualitative measurement of these assistants. While some ad hoc evaluations of ChatGPT invite caution, [1] specialized providers are investing a lot of resources in these tools and Gartner anticipates broad adoption in the future.

Security Operation Tool Integration

GenAI utilities have made their way into a number of security operations tools from vendors like Microsoft, [2] Google, [3] SentinelOne, [4] CrowdStrike [5] and Cisco. These utilities have the potential to improve the productivity and skill set of the average administrator, and improve security outcomes and communication.

Actionable, objective insight

Position your organization for success. Explore these additional complimentary resources and tools for cybersecurity leaders:

eBook

4 Ways to Achieve Secure Employee Behaviors

Manage human risk and build a security-conscious organization.

Download Now

Research

CISO Foundations: Cybersecurity Talent Strategies for CISOs

Discover tried-and-tested guidance for CISOs responsible for building skilled cybersecurity teams.

Download Now

eBook

3 Must-Haves in Your Cybersecurity Incident Response Plan

Improve your organization's ability to be prepared for a cybersecurity incident.

Download Now

Webinar

The Gartner Top Cybersecurity Predictions 2023-2024

Understand how to create a successful and resilient cybersecurity program built for the digital era.

Watch Now

Already a client?
Get access to even more resources in your client portal. Log In

Connect With Us

Get actionable, objective insight that drives smarter decisions and stronger performance on your mission-critical priorities. Contact us to become a client:

U.S.: 1 855 811 7593

International: +44 (0) 3330 607 044

Become a Client

Learn more about Gartner for Cybersecurity Leaders
gartner.com/en/Cybersecurity

Stay connected to the latest insights

Gartner®