Enterprise Strategy Group™ by TechTarget

Generative AI for Cybersecurity: An Optimistic but Uncertain Future

Generative AI (GenAI) introduces new risks as employees connect to GenAI applications, share data, and build homegrown large language models. Security professionals are also anxious about how cybercriminals may use GenAI as part of attack campaigns. Despite these risks, generative AI holds great cybersecurity-boosting potential as well. TechTarget's Enterprise Strategy Group recently surveyed IT and cybersecurity professionals with visibility into current GenAI usage and strategic plans to gain insights into these trends.

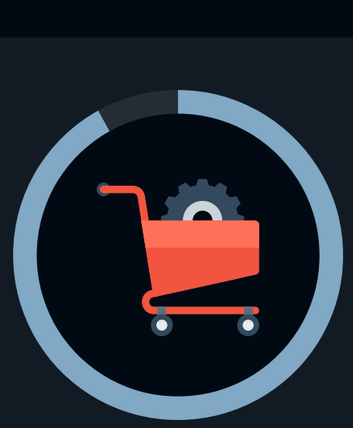
Notable findings from this study include:

86%
of organizations have **blocked or plan to block access to GenAI sites.**

76%
of cybersecurity professionals believe GenAI provides an advantage to cyber-adversaries.

51%
of cybersecurity professionals believe GenAI makes it easier for unskilled hackers to develop more advanced attacks.

42%
of cybersecurity professionals are optimistic about the potential impact of GenAI for cybersecurity defenders.



92%
of organizations would be willing to replace existing security technologies based on another vendor's GenAI capabilities.

71%
of organizations **still want a staff member to review low-risk recommendations** provided by a GenAI application before taking manual remediation actions.

For more from this Enterprise Strategy Group study, read the full research report, ***Generative AI for Cybersecurity: An Optimistic but Uncertain Future.***

LEARN MORE

Source: Enterprise Strategy Group Research Report, *Generative AI for Cybersecurity: An Optimistic but Uncertain Future,* April 2024.