BENORI

Dual Impact of Generative AI on Cybersecurity: Breakthroughs and Breaches

JANUARY 2025

If cybercrime were a country, it would be the third-largest economy in the world after the United States and China, underlying the massive cost of global cybercrime damages. In this growing threat landscape, generative AI (GenAI) is strengthening cybersecurity defenses while being exploited by malicious actors to fuel cyberattacks.

The launch of OpenAI's ChatGPT in November 2022 sparked a GenAI revolution, with SaaS vendors quickly enhancing tools with GenAI-powered features. However, this growth has led to rising cybersecurity concerns. According to the Identity Theft Resource Center, the widespread use of GenAI apps in the workplace has coincided with a 78% increase in data breaches. “GenAI has broadened the attack surface for applications, creating new types of attacks that didn’t exist before,” says the co-founder of AI-led security startup, SydeLabs.

Role of GenAI in Facilitating Cyberthreats

GenAI, through a growing ecosystem of GPT-based tools, is lowering the technical barrier for threat actors, enabling more frequent and sophisticated cyberattacks. By automating and enhancing the precision of attacks, it allows malicious actors to develop sophisticated malware and execute complex threats with greater efficiency. The IBM X-Force Threat Intelligence Index 2024 found that GenAI capabilities lead to a 99.5% reduction in the time needed to craft an effective phishing email. Furthermore, a substantial 85% of security professionals witnessed an increase in cyber-attacks over the past 12 months, attributing the rise of bad actors using GenAI.

GenAI is a double-edged sword in cybersecurity, enabling advanced cyberattacks and robust defenses. While threat actors leverage it for sophisticated phishing, automated malware, and precise exploits, cybersecurity teams use it to enhance threat detection, automate responses, and strengthen digital defenses. This ongoing race demands continuous innovation from cybersecurity SaaS providers to stay ahead and protect against increasingly complex threats.

Select ways in which GenAI is exploited by cybercriminals are:

Exploitation Types	Description
Automated Code Generation	GenAI automates the rapid creation of malware variants with unique characteristics but similar functionality that can bypass signature-based detection. For instance, in June 2024, a campaign was discovered by researchers from HP Wolf Security where cybercriminals were using GenAI to create code for spreading AsyncRAT, a remote access Trojan that can steal data and harvest credentials.
Deepfake	GenAI's voice cloning ability replicates tone, speech patterns, and accents of individuals with remarkable accuracy. Combined with deepfake videos, these tools impersonate authority figures or familiar contacts, adding credibility to scams. For instance, in January 2024, fraudsters used deepfake videos to impersonate a company's CFO in Hong Kong and tricked a finance employee into transferring an amount of USD 25 million.
Threat Engineering	Threat actors automatically generate targeted written content for scams or misinformation. It includes phishing emails, fake websites, and social engineering scripts difficult to distinguish from legitimate communication. For instance, a study found that 60% of participants were convinced by AI-created phishing attacks, a success rate comparable to that devised by human experts.
Password Cracking	GenAI automates and accelerates targeted password guessing by analyzing publicly available data, such as social media, making brute force attacks faster and efficient. For instance, PassGAN, an ML-based AI password cracker, can crack any seven-character password with numbers, lower and uppercase letters, and symbols in less than six minutes.
Prompt Injection	Prompt injection is an attack against applications that have been built on top of AI models. The prompt sensitivity of AI applications can be exploited for injection attacks, enabling malicious manipulation of outputs. For instance, Remoteli.io, a remote work company, created a Twitter bot, powered by an LLM to respond positively to tweets about remote work. A user crafted a malicious tweet that included a hidden instruction for the bot to make a threat against the president. When the bot processed the tweet, it incorporated her instructions into its response, resulting in the bot unintentionally issuing the threat.

Exploitation Types	Description
Fraud Platforms	Many illicit platforms leverage GenAI to provide services for cybercriminals, such as generating fake identities or automating the execution of scams. These platforms lower the barrier for entry into cybercrime by providing tools that require minimal technical expertise. For instance, GenAI-powered fraud platforms, such as FraudGPT and WormGPT, assist cybercriminals in phishing, malware creation, and generating malicious code. Found on the deep web, these tools are marketed in underground forums.

Role of GenAI in Mitigating Cyberthreats

GenAI is transforming cybersecurity by enhancing threat detection, automating operations, and enabling advanced threat analysis. Its predictive models identify unusual patterns and adapt to emerging risks, reducing breaches and mitigating their impact in the following major ways:

Extract insights from unstructured data by using Natural Language Processing (NLP), to identify hidden attack vectors and empower proactive defense strategies

Simulate realistic cyberattacks by leveraging Generative Adversarial Networks (GANs), a machine learning framework that uses two neural networks to generate training datasets

Automate tasks including firewall configuration and vulnerability scanning, to minimize human errors and improve efficiency

Streamline incident response and reporting by generating clear, actionable insights from logs and alerts

SOCs (Security Operations Centers) and SIEM (Security Information and Event Management)

are the core infrastructure of cybersecurity operations. SOCs use GenAI to detect patterns of potential threats, such as malware or ransomware, that may bypass traditional systems. In SIEM, GenAI improves data analysis and anomaly detection by learning from historical security data, establishing a baseline for normal network behavior, and flagging deviations that could indicate security breaches.

Current Approach of Companies to Integrate GenAI into Cybersecurity

With evolving cyber threats, companies are increasingly adopting GenAI to strengthen defenses against advanced attacks. Software providers, who embed security measures in their platforms, and leading cybersecurity providers have integrated GenAI with advanced analytics and adaptive defenses, leveraging organic and inorganic approaches to stay ahead.

Launching New Products and Enhancing Offerings

FORTINET

The GenAI-powered security assistant streamlines and automates security analyst tasks, while FortiManager leverages GenAI to generate network configuration scripts, troubleshoot issues, and automate vulnerability remediation. (Nov 2024)

Google

Launched Google Threat Intelligence, featuring GenAI-powered Gemini, to enable conversational search across extensive threat intelligence repository, delivering faster insights and enhanced threat protection. (May 2024)

Establishing Innovation and Capability Centers

accenture

Announced the establishment of four Cyber Future Centers. Equipped with GenAI and quantum security solutions. These centers will enhance Accenture's managed security service capabilities. (Nov 2024)

eSENTIRE

Inaugurated an innovation center in India to accelerate the development of Atlas XDR Cloud Platform, focusing on key areas such as low-code, automation, and GenAI.
(Apr 2024)

Acquiring Startups Specializing in GenAI

CISCO

Acquired Robust Intelligence, a security startup providing firewall to protect AI-based applications, to support customers in the responsible and secure adoption of GenAI applications. (Nov 2024)

PROTECT AI

A Seattle-based cybersecurity firm, acquired SydeLabs, an Indian startup specializing in securing GenAI applications. (Jul 2024)

Collaborations to Leverage Combined Expertise and Deliver Innovative GenAI Solutions

paloalto® NETWORKS

Partnered with Accenture to launch a new offering that integrates its Precision AI technology with Accenture's secure GenAI services. (May 2024)

CROWDSTRIKE

Collaborated with AWS to develop Charlotte AI, a GenAI security analyst, to help customers to use natural language queries for advanced threat detection, investigation, and hunting. (May 2023)

The diverse approaches adopted by cybersecurity players to integrate GenAI into their solutions are being positively received by customers. Organizations, such as Pfizer and Fiserv, are leveraging Google's Gemini in their Security Operations to streamline onboarding, improve query response times for cybersecurity analysts, and enhance the efficiency of their security operations. Technical advancements empower end-users to address threats proactively, reduce response times, and maintain robust security postures in an increasingly complex cyber landscape. For instance, Adobe Security's GenAI-based platform is streamlining threat modeling, helping teams easily create robust models while ensuring access to best practices and expert guidance to protect the digital ecosystem. Similarly, Microsoft's new GenAI solution, Microsoft Security Copilot, built on Zero Trust principles, is helping its clients establish end-to-end security to transform digital threat defense and empower security teams in the present era.

OUTLOOK

A Splunk survey published in April 2024 found that 91% of security executives use GenAI, with 46% viewing it as a game-changer for their teams. The future of GenAI in cybersecurity depends on its ability to evolve alongside emerging threats, offering enhanced automation, predictive capabilities, and adaptive defenses. According to VentureBeat, 93% of IT executives are using or considering AI and ML for security, benefiting from improvements such as more efficient threat triage, better detection of zero-day attacks, and reduced false positives. However, to be ahead of cybercriminals, integrating GenAI into existing security frameworks and continuously improving its ability to counter sophisticated threats is crucial.

In this context, cybersecurity players—including consulting firms, core security players, and system integrators—must adopt a structured approach that focuses on technology, process, and people.

People:

Organizations must equip teams with expertise in offensive and defensive GenAI applications while fostering cross-functional collaboration and continuous learning. It will ensure seamless integration of GenAI and responsible deployment.

Process:

GenAI should be integrated into security frameworks to enhance threat detection, response, and mitigation. Organizations should ensure continuous updates to AI models embedded into their workflows to address evolving attack techniques. Collaboration with SaaS companies, governments, and industry bodies is vital for sharing threat intelligence and establishing standardized best practices and governance mechanisms to maintain effectiveness and transparency.

Technology:

Cybersecurity providers must focus on advancements in AI-powered tools that automate threat detection and response workflows, improving efficiency and accuracy. Continuous refinement of AI models is essential to stay ahead of new attack techniques and ensure resilience in a dynamic threat landscape.

Software providers and specialized cybersecurity firms are increasingly adopting GenAI for its ability to enhance efficiency, accuracy, and speed in detecting, predicting, and responding to threats. As AI-powered attacks rise, stricter regulations and standards are expected to ensure the responsible use of AI in cybersecurity. Human oversight will remain essential for managing complex security challenges and making nuanced decisions beyond AI’s capabilities. The future of GenAI lies in cybersecurity leaders’ ability to harness its potential while ensuring its safe and secure application across industries.

REFERENCES:

https://cybersecurityventures.com/the-worlds-third-largest-economy-has-bad-intentions-and-its-only-getting-bigger/

https://saasboomi.org/saas/product/cyber-security-ai-sydelabs/

https://blog.barracuda.com/2024/04/16/5-ways-cybercriminals-are-using-ai--malware-generation

https://www.okta.com/blog/2024/01/how-cybercriminals-are-using-gen-ai-to-scale-their-scams/

https://secureframe.com/blog/generative-ai-cybersecurity

https://www.globenewswire.com/news-release/2024/11/07/2976749/0/en/Fortinet-Continues-to-Expand-Generative-AI-Across-Its-Portfolio-with-Two-New-Additions-to-Simplify-Security-Operations.html

https://cloud.google.com/blog/products/identity-security/introducing-google-threat-intelligence-actionable-threat-intelligence-at-google-scale-at-rsa

https://newsroom.accenture.com/news/2024/accenture-expands-generative-ai-powered-cybersecurity-services-and-capabilities-to-accelerate-clients-resilience-and-reinvention

https://etedge-insights.com/in-focus/trending/esentire-launches-new-technology-innovation-center-in-india/

https://www.cxtoday.com/data-analytics/cisco-to-acquire-robust-intelligence-the-ai-focused-security-startup/

https://blogs.cisco.com/security/robust-intelligence-now-part-of-cisco-recognized-as-a-2024-gartner-cool-vendor-for-ai-security

https://protectai.com/newsroom/protect-ai-acquires-sydelabs

https://newsroom.accenture.com/news/2024/palo-alto-networks-and-accenture-team-to-secure-the-gen-ai-transformation-journey

https://www.crowdstrike.com/en-us/press-releases/crowdstrike-and-aws-to-accelerate-ai-development-in-cybersecurity/

https://medium.com/@costigermano/genai-writes-malicious-code-how-cybercriminals-are-using-ai-to-spread-asyncrat-and-evade-detection-373c2447a107

https://blog.developer.adobe.com/scaling-your-threat-modeling-program-using-genai-934160279889

https://www.microsoft.com/en-us/security/blog/2023/11/15/microsoft-unveils-expansion-of-ai-for-security-and-security-for-ai-at-microsoft-ignite/

Benori is a trusted partner for knowledge solutions across the globe, serving clients from a wide range of industries including Professional Services, Financial Services, Consumer & Retail, Technology & Internet, Industrials & Manufacturing, and more. Our customized solutions strengthen the insights value chain of our clients, empowering them with key insights needed to drive intelligent decision-making and accelerate growth.

Headquartered in India, Benori is uniquely positioned to deliver multilingual research needs of global clients, powered by its digital agility, deep research capabilities and a highly experienced leadership team. Adopting a 360-degree approach, our team employs a combination of diverse methodologies including primary research, secondary research and data modeling, and offers detailed foresight on market trends, competitive shifts, regulatory changes and technological advancements.

Powering Growth Through Knowledge

✉ info@benoriknowledge.com

www.benori.com

BENORI