

Generative AI In Cyber Security Market In 2029

*The Business Research Company's
Generative AI In Cyber Security Market In
2029*

LONDON, GREATER LONDON, UNITED KINGDOM, December 19, 2025 /EINPresswire.com/ -- "Generative AI In Cyber Security Market to Surpass \$8 billion in 2029. Within the broader Information Technology industry, which is expected to be \$12,712 billion by 2029, the Generative AI In Cyber Security market is estimated to account for nearly 0.1% of the total market value.

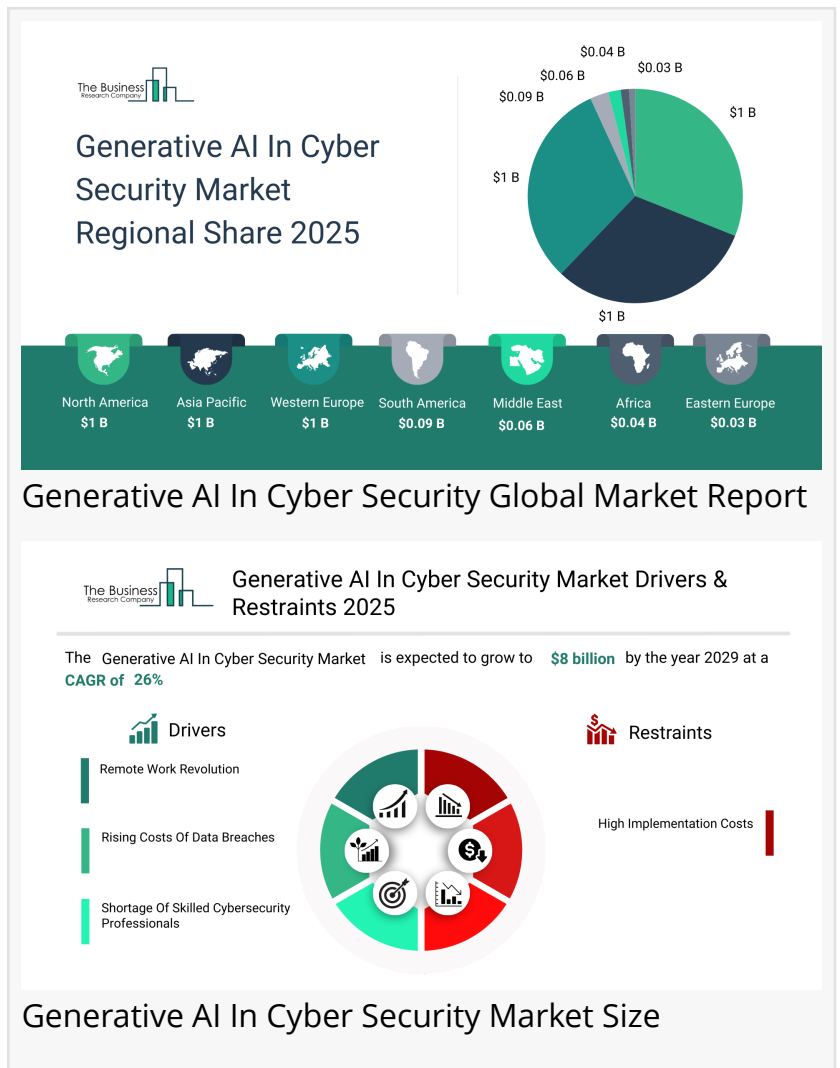
Which Will Be the Biggest Region in the Generative AI In Cyber Security Market in 2029

North America will be the largest region in the generative AI in cyber security market in 2029, valued at \$3,290 million. The market is expected to grow from \$1,025 million in 2024 at a compound annual growth rate (CAGR) of 26%. The exponential growth is supported by the remote work revolution and rising costs of data breaches.

“

It will grow to \$6.86 billion in 2029 at a compound annual growth rate (CAGR) of 22.7%”

*The Business Research
Company*



Which Will Be The Largest Country In The Global Generative AI In Cyber Security Market In 2029?

The USA will be the largest country in the generative AI in cyber security market in 2029, valued at \$3,000 million. The market is expected to grow from \$918 million in 2024 at a compound annual growth rate (CAGR) of 27%. The exponential growth can be attributed to increasing technological advancements.

Request a free sample of the
Generative AI In Cyber Security Market
report:

https://www.thebusinessresearchcompany.com/sample_request?id=19459&type=smp

What will be Largest Segment in the
Generative AI In Cyber Security Market
in 2029?

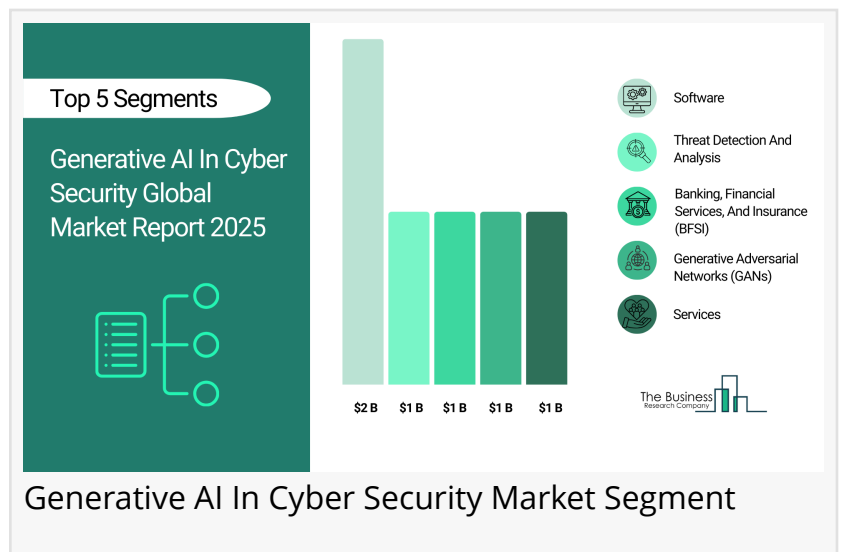
The generative AI in cyber security
market is segmented by type into
threat detection and analysis,

adversarial defense, insider threat detection, network security and other types. The threat detection and analysis market will be the largest segment of the generative AI in cyber security market segmented by type, accounting for 37% or \$2,980 million of the total in 2029. The threat detection and analysis market will be supported by advanced machine, learning capabilities, detection of unknown threats (zero-day attacks), volume of security data, enhanced threat intelligence, customization and adaptability, and regulatory and compliance pressure.

The generative AI in cyber security market is segmented by component into hardware, software and services. The software market will be the largest segment of the generative AI in cyber security market segmented by component, accounting for 62% or \$4,953 million of the total in 2029. The software market will be supported by scalability of security solutions, behavioral analytics for insider threat detection, integration with existing security infrastructure, adaptive and evolving threat intelligence, data protection and privacy compliance, efficient cloud security, and real-time incident response.

The generative AI in cyber security market is segmented by technology into generative adversarial networks (GANs), variational autoencoders (VAEs), reinforcement learning (RL), deep neural networks (DNNs), natural language processing (NLP) and other technologies. The generative adversarial networks (GANs) market will be the largest segment of the generative AI in cyber security market segmented by technology, accounting for 29% or \$2,357 million of the total in 2029. The generative adversarial networks (GANs) market will be supported by increase in synthetic data generation, adversarial training for robust models, automated security testing, fraud detection, privacy preservation, and evasion of traditional security mechanisms.

The generative AI in cyber security market is segmented by end-use into banking, financial services and insurance (BFSI), healthcare and life sciences, government and defense, retail and e-commerce, manufacturing and industrial, information technology (IT) and telecommunications, energy and utilities and other end-uses. The banking, financial services and insurance (BFSI) market will be the largest segment of the generative AI in cyber security market segmented by end-use, accounting for 28% or \$2,213 million of the total in 2029. The banking, financial services



and insurance (BFSI) market will be supported by enhanced fraud prevention, improved incident response times, predictive threat intelligence, AI-powered risk management, cost-effective security operations, and adaptive security measures.

What is the expected CAGR for the Generative AI In Cyber Security Market leading up to 2029?
The expected CAGR for the generative AI in cyber security market leading up to 2029 is 26%.

What Will Be The Growth Driving Factors In The Global Generative AI In Cyber Security Market In The Forecast Period?

The rapid growth of the global generative AI in cyber security market leading up to 2029 will be driven by the following key factors that are expected to reshape industrial quality assurance, manufacturing processes, and enterprise cyber defense worldwide.

Remote Work Revolution - The remote work revolution will become a key driver of growth in the generative AI in cyber security market by 2029. Remote working refers to a professional setting where employees are permitted to work from home or any other place other than the actual office of their employer. The surge in remote work has broadened organizations' attack surfaces, making cybersecurity mesh essential as a flexible and adaptive security framework that safeguards users and devices irrespective of their location. Generative AI models will be crucial in enhancing cloud security and ensuring robust protection for remote networks. As a result, the remote work revolution is anticipated to contributing to annual growth in the market.

Rising Costs Of Data Breaches - The rising costs of data breaches will emerge as a major factor driving the expansion of the generative AI in cyber security market by 2029. As organizations face escalating financial and reputational risks from breaches, the need for advanced AI-driven solutions to prevent, detect, and respond to threats is growing. Generative AI's ability to predict and simulate cyberattacks, along with its role in automating security measures, is becoming a critical factor in reducing breach costs and enhancing organizational resilience, fueling its market growth. Consequently, the rising costs of data breaches is projected to contributing to annual growth in the market.

Shortage Of Skilled Cybersecurity Professionals - The shortage of skilled cybersecurity professionals within digital manufacturing processes will serve as a key growth catalyst for the generative AI in cyber security market by 2029. As digital transformation accelerates, the demand for cybersecurity expertise will continue to outpace supply, leaving organizations vulnerable. These AI-driven solutions will help to bridge the talent gap, enabling organizations to strengthen their cybersecurity defenses despite a limited workforce. Ultimately, the shortage of skilled professionals will drive further adoption of AI, reshaping the cybersecurity landscape and providing more effective protection against evolving threats. Therefore, this shortage of skilled cybersecurity professionals projected to supporting to annual growth in the market.

Access the detailed Generative AI In Cyber Security report here:

<https://www.thebusinessresearchcompany.com/report/generative-ai-in-cyber-security-global->

What Are The Key Growth Opportunities In The Generative AI In Cyber Security Market in 2029? The most significant growth opportunities are anticipated in the generative AI in cyber security software market, the generative AI in cyber security for threat detection and analysis market, the generative adversarial networks (GANS) based generative AI in cyber security market, and the generative AI in cyber security for banking, financial services, and insurance (BFSI) market. Collectively, these segments are projected to contribute over \$9 billion in market value by 2029, driven by the rising sophistication of cyber threats, increasing adoption of AI-powered proactive security solutions, growing demand for automation in threat monitoring and response, and the need to protect sensitive financial and enterprise data across digital ecosystems. This surge reflects the accelerating adoption of generative AI technologies that enable predictive threat detection, adaptive response, real-time anomaly analysis, and enhanced enterprise cyber resilience, fueling transformative growth within the broader generative AI in cybersecurity industry.

The generative AI in cyber security software market is projected to grow by \$3,480 million, the generative AI in cyber security for threat detection and analysis market by \$2,058 million, the generative adversarial networks (GANS) based generative AI in cyber security market by \$1,646 million, and the generative AI in cyber security for banking, financial services, and insurance (BFSI) market by \$1,473 million over the next five years from 2024 to 2029.

Learn More About The Business Research Company

The Business Research Company (www.thebusinessresearchcompany.com) is a leading market intelligence firm renowned for its expertise in company, market, and consumer research. We have published over 17,500 reports across 27 industries and 60+ geographies. Our research is powered by 1,500,000 datasets, extensive secondary research, and exclusive insights from interviews with industry leaders.

We provide continuous and custom research services, offering a range of specialized packages tailored to your needs, including Market Entry Research Package, Competitor Tracking Package, Supplier & Distributor Package and much more.

Disclaimer: Please note that the findings, conclusions and recommendations that TBRC Business Research Pvt Ltd delivers are based on information gathered in good faith from both primary and secondary sources, whose accuracy we are not always in a position to guarantee. As such TBRC Business Research Pvt Ltd can accept no liability whatever for actions taken based on any information that may subsequently prove to be incorrect. Analysis and findings included in TBRC reports and presentations are our estimates, opinions and are not intended as statements of fact or investment guidance.

Contact Us:

The Business Research Company
Americas +1 310-496-7795
Europe +44 7882 955267
Asia & Others +44 7882 955267 & +91 8897263534
Email: info@tbrc.info

Follow Us On:

LinkedIn: <https://in.linkedin.com/company/the-business-research-company>"

Oliver Guirdham
The Business Research Company
+44 7882 955267
info@tbrc.info

Visit us on social media:

[LinkedIn](#)

[Facebook](#)

[X](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/876469519>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2025 Newsmatics Inc. All Right Reserved.