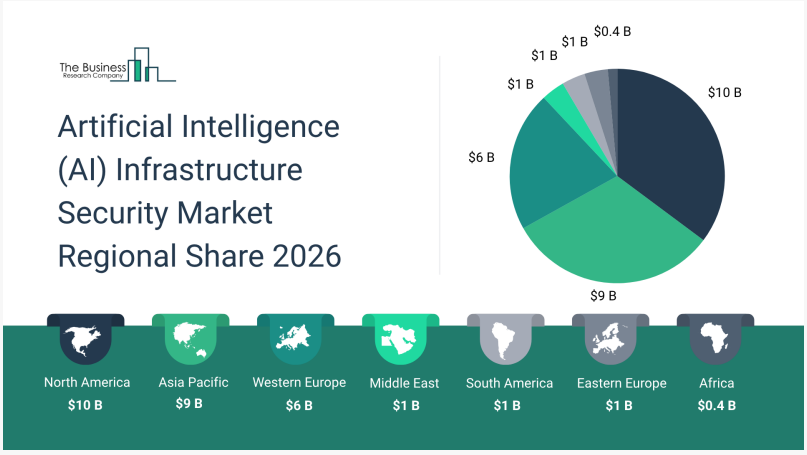
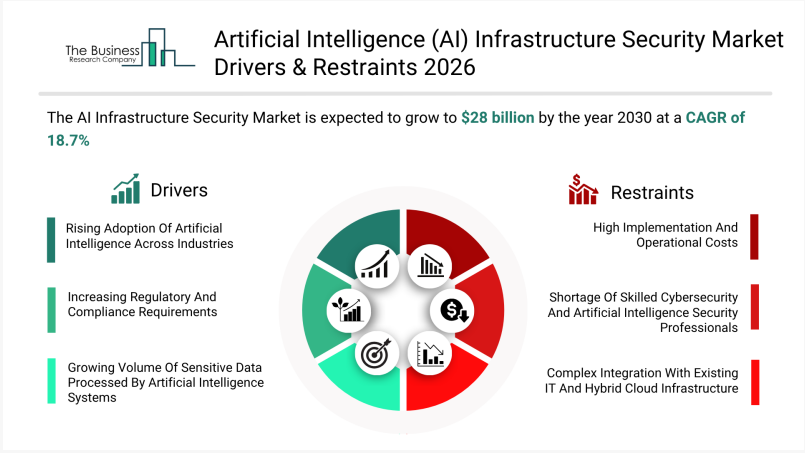
Trends and Forecast Analysis of the Artificial Intelligence (AI) Infrastructure Security Market Highlight Significant

The Business Research Company's Artificial Intelligence (AI) Infrastructure Security Global Market Report 2026 – Market Size, Trends, And Forecast 2026-2035

LONDON, GREATER LONDON, UNITED KINGDOM, October 26, 2026 /EINPresswire.com/ -- The landscape of artificial intelligence (AI) infrastructure security is evolving rapidly as organizations increasingly recognize the critical need to protect AI systems and data. This sector is emerging as a vital component within the broader managed security and information technology markets, with substantial growth expected over the coming years. Below, we explore the market's size, regional dynamics, key segments, and driving forces shaping this important industry.



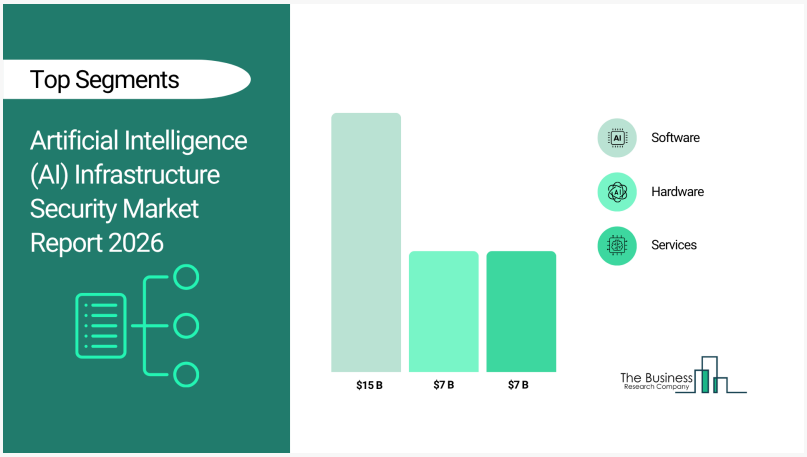
Artificial Intelligence (AI) Infrastructure Security Market



Artificial Intelligence (AI) Infrastructure Security Market analysis

Artificial Intelligence (AI) Infrastructure Security Market Size and Comparison Forecasts suggest the AI infrastructure security market will exceed $28 billion by 2030. When compared to the larger managed security services market, valued at roughly $80 billion in the same year, AI infrastructure security is set to represent about 35% of this parent market. Within the vast Information Technology sector, which is projected to reach $13,788 billion by 2030, the AI infrastructure security segment will make up close to 0.2% of the total market value, highlighting its growing significance but still niche status within IT.

Request A Free Sample Of The Artificial Intelligence (AI) Infrastructure Security Market Report
https://thebusinessresearchcompany.com/sample_request?id=45956926&type=smp&name=AI%20Infrastructure%20Security%20Market%20Report%202026&utm_source=EINPresswire&utm_medium=Paid&utm_campaign=Oct_PR



Artificial Intelligence (AI) Infrastructure Security Market size

North America Set to Lead the AI Infrastructure Security Market by 2030

North America is poised to maintain its dominance as the largest regional market for AI infrastructure security, with a valuation of $10 billion projected in 2030. This marks a substantial increase from $5 billion in 2025, reflecting a compound annual growth rate (CAGR) of 16%. The region's rapid expansion is driven by several factors including the swift development of AI data center infrastructure, the widespread adoption of generative AI workloads in enterprises, increased cybersecurity spending aimed at securing AI models, a strong presence of key cloud and AI technology providers, and heightened regulatory efforts focused on safeguarding critical AI-powered systems.

The United States as the Foremost National Market for AI Infrastructure Security
The USA is expected to be the top country within the global AI infrastructure security market, with its value reaching $9 billion by 2030. Growing from $4 billion in 2025, this growth mirrors a 16% CAGR. Key contributors include broad enterprise adoption of AI infrastructure, escalating investments in specialized AI threat detection and security platforms, expansion of high-performance computing clusters tailored for AI workloads, rising needs for secure AI model lifecycle management, and continuous innovation by cybersecurity firms to combat evolving threats targeting AI environments.

Access The Detailed Artificial Intelligence (AI) Infrastructure Security Market Report Here
https://thebusinessresearchcompany.com/report/ai-infrastructure-security-market-report?utm_source=EINPresswire&utm_medium=Paid&utm_campaign=Oct_PR

Software Segment to Dominate the AI Infrastructure Security Market
Among the core components of the AI infrastructure security market—software, hardware, and services—the software segment will hold the largest share. It is expected to account for 52% of the market, roughly $15 billion, by 2030. This dominance stems from the growing use of AI-driven security analytics, threat intelligence platforms, automated vulnerability management, continuous security monitoring, identity and access management solutions, and security orchestration and incident response tools. Ongoing software advancements focus on addressing emerging cyber risks specifically related to AI systems.

Market Segmentation by Deployment, Organization Size, Security Type, and End-User

The AI infrastructure security market is further divided by deployment modes—on-premises and cloud—to meet diverse organizational needs. It categorizes organizations by size into small and medium enterprises as well as large enterprises. Security types include network, endpoint, application, cloud, data security, and others, reflecting the multifaceted approach required to protect AI environments. Key end-users span several industries, such as banking, financial services, and insurance (BFSI), healthcare, IT and telecommunications, retail, government, manufacturing, and other sectors, indicating broad applicability of AI infrastructure security across the economy.

Projected Market Growth Rate Leading up to 2030

The AI infrastructure security market is expected to grow at a compound annual growth rate of 19% through 2030. This robust expansion underscores the increasing demand for advanced security measures tailored to AI technologies and infrastructure.

Primary Factors Accelerating AI Infrastructure Security Market Growth

The rapid adoption of AI across various industries is a major catalyst for market growth. Sectors like healthcare, finance, manufacturing, retail, and government agencies are leveraging AI to enhance efficiency and decision-making. As AI environments become more complex and integral to business operations, there is a heightened need for advanced security solutions to protect AI models, computing resources, and supporting infrastructure from sophisticated cyber threats. Vendors are thus broadening their AI-focused security offerings to protect these increasingly distributed environments, contributing about 2.0% annual growth to the market.

Another key driver is the tightening regulatory and compliance landscape. Governments and regulatory bodies worldwide are imposing stricter cybersecurity, privacy, and AI governance rules that require secure AI deployment and management. Organizations are intensifying their security measures to comply with these evolving requirements, ensuring transparency and accountability in AI operations. This regulatory pressure is expected to add approximately 1.5% annual growth to the market.

Additionally, the growing amounts of sensitive data processed by AI systems fuel demand for infrastructure security. AI workloads handle confidential enterprise data, customer information, financial transactions, and proprietary datasets that must be protected throughout the AI lifecycle. Security providers are developing specialized solutions to ensure data confidentiality, integrity, and controlled access, driving roughly 1.0% annual market growth.

Key Growth Opportunities Within AI Infrastructure Security Sectors

Significant growth prospects lie within the software, hardware, and services segments of the market. Collectively, these areas are anticipated to contribute more than $16 billion in value by 2030. This growth is propelled by the deployment of AI-native cybersecurity platforms, expanded investments in high-performance AI computing infrastructure, increased demand for managed

security and consulting services, and heightened enterprise focus on securing AI development and operations. The need for resilient AI infrastructure and proactive cyber defense strategies is accelerating growth throughout the AI ecosystem.

Between 2025 and 2030, the software segment is expected to grow by $9 billion, hardware by $3 billion, and services by $4 billion. The market is led by a combination of large cybersecurity firms and specialized AI security companies. These players emphasize advanced threat detection, AI-driven security tools, automated monitoring, and strong data protection frameworks to maintain secure AI infrastructures. Complying with data privacy laws, defending against evolving cyber threats, securing AI model deployment, and adopting adaptive security architectures remain central to competitive advantage.

Microsoft Corporation as the Leading AI Infrastructure Security Market Player
In 2025, Microsoft Corporation held the top position globally with a 1% market share. Its cybersecurity and cloud services segment offers a broad portfolio of AI security solutions, including cloud-based protection, threat intelligence, and identity management tools. These offerings are designed to support secure AI deployments, data protection, and enterprise-wide security applications.

Other Prominent Companies in the AI Infrastructure Security Market
The market includes major players such as Alphabet Inc. (Google LLC), Amazon Web Services Inc., NVIDIA Corporation, Snowflake Inc., SAP SE, Cisco Systems Inc., International Business Machines Corporation, Oracle Corporation, Dremio Corporation, CData Software Inc., Databricks Inc., Fivetran Inc., Matillion Limited, Denodo Technologies Inc., Teradata Corporation, SingleStore Inc., Yellowbrick Data Inc., Hevo Data Inc., Starburst Data Inc., and Airbyte Inc. These companies contribute diverse capabilities, from cloud infrastructure to data integration and AI security innovation.

Market Concentration and Competitive Dynamics
The AI infrastructure security market is relatively fragmented, with the top 10 players accounting for about 4% of total revenue in 2025. Moderate entry barriers arise from stringent cybersecurity requirements, regulatory compliance, AI-specific security needs, and the importance of reliability in protecting AI infrastructure and enterprise applications. Key players like Microsoft, Google, Amazon Web Services, NVIDIA, Snowflake, SAP, Cisco, IBM, Oracle, and Dremio maintain significant market shares through extensive security portfolios, integrated cloud and AI ecosystems, global networks, and continuous innovation. As demand grows for secure AI deployments and advanced threat detection, strategic partnerships, product development, and geographic expansion are expected to enhance their market positions.

Leading Raw Material Suppliers Essential to AI Infrastructure Security
Critical raw material suppliers feeding into this market include Intel Corporation, NVIDIA Corporation, Advanced Micro Devices Inc., Qualcomm Incorporated, Broadcom Inc., Cisco Systems Inc., Dell Technologies Inc., Hewlett Packard Enterprise Company, Lenovo Group

Limited, Super Micro Computer Inc., IBM Corporation, Oracle Corporation, Samsung Electronics Co. Ltd., Micron Technology Inc., Seagate Technology Holdings plc, Western Digital Corporation, NetApp Inc., Pure Storage Inc., Arista Networks Inc., Juniper Networks Inc., Palo Alto Networks Inc., Fortinet Inc., Check Point Software Technologies Ltd., CrowdStrike Holdings Inc., and Zscaler Inc. Their components and technologies form the backbone of AI infrastructure security solutions.

Key Wholesalers and Distributors Supporting the Market
Major wholesalers and distributors providing AI infrastructure security products include Arrow Electronics Inc., Avnet Inc., Ingram Micro Inc., TD SYNNEX Corporation, Tech Data Corporation, CDW Corporation, Insight Enterprises Inc., SHI International Corp., Softchoice Corporation, Bechtle AG, Computacenter plc, ALSO Holding AG, Esprinet S.p.A., ScanSource Inc., D&H Distributing Company, Exclusive Networks SA, Westcon Group, Redington Limited, Mindware FZ LLC, ASBIS Enterprises PLC, Macnica Inc., Future Electronics Inc., Mouser Electronics Inc., DigiKey Electronics, and RS Group plc.

Prominent End-Users Driving Demand Across Sectors
Significant end-users of AI infrastructure security solutions include Microsoft Corporation, Amazon Web Services Inc., Google LLC, Meta Platforms Inc., OpenAI, Anthropic PBC, Databricks Inc., Snowflake Inc., ServiceNow Inc., Salesforce Inc., SAP SE, VMware Inc., Red Hat Inc., HashiCorp Inc., Cloudflare Inc., Akamai Technologies Inc., Okta Inc., SentinelOne Inc., Gen Digital Inc., Sophos Limited, Trend Micro Incorporated, Trellix Inc., Elastic N.V., and Rapid7 Inc. Their adoption of AI security technologies helps set industry standards and drives further innovation.

Current Competitive Trends Shaping the AI Infrastructure Security Market
AI-powered infrastructure security platforms are revolutionizing the market by enhancing threat detection, protecting AI workloads, and improving governance across AI ecosystems. For example, in April 2025, Aqua Security Software Ltd. launched Secure AI, a comprehensive solution designed to protect AI applications throughout their lifecycle, including safeguarding the prompt layer. This product offers real-time AI threat detection, protection against prompt injections, prevention of model misuse, AI governance features, and extensive visibility over AI models, cloud environments, and application code. These capabilities boost security, ensure compliance, and enable secure enterprise AI deployment.

Strategies Companies Are Using to Maintain Market Leadership
To stay ahead, companies are focusing on advancing AI infrastructure security solutions that strengthen protection and resilience. They are increasingly leveraging AI security technologies to improve threat detection and response capabilities. Expanding secure AI infrastructure frameworks aims to enhance privacy and operational robustness, while integrating zero-trust architectures and strong encryption methods bolsters authentication and protection across AI environments.

New analytical features added to our 2026 market reports:

• Market attractiveness scoring and analysis
• Total addressable market (TAM) analysis
• Company scoring matrix graphics and tables
• Excel-based forecasting dashboards
• Market hotspots infographics
• Key technologies and future trend analysis
• Updated graphics and tables

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 30,000+ 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: marketing@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/951465280

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.
© 1995-2026 Newsmatics Inc. All Right Reserved.