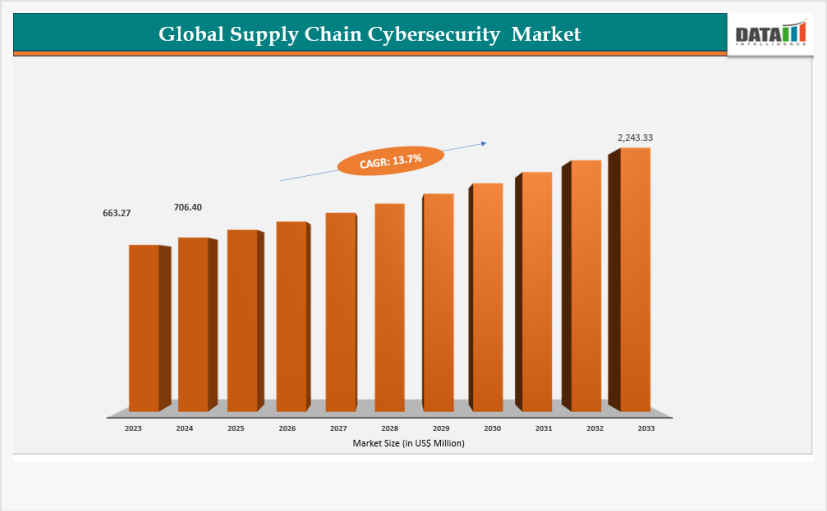
Supply Chain Cybersecurity Market to reach US$ 2,243.33 million by 2033, North America led 37.5% Share in Global Market

The Supply Chain Cybersecurity Market is growing rapidly as organizations strengthen defenses against rising third-party risks, cyberattacks.



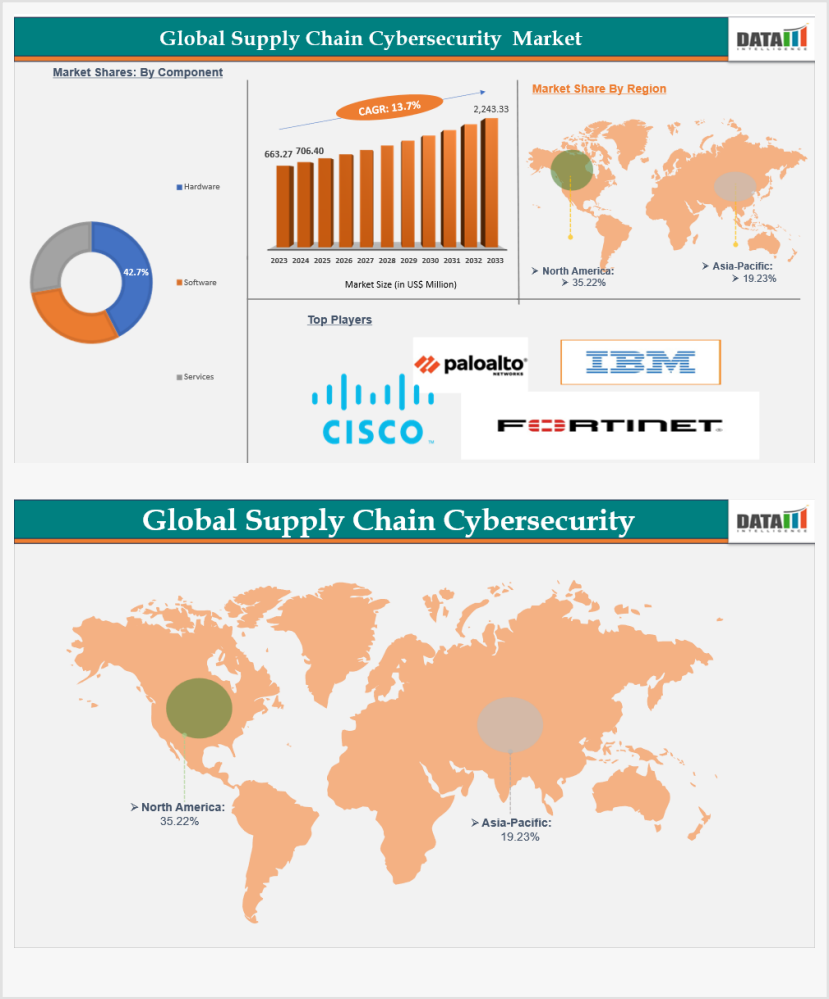
AUSTIN, TX, UNITED STATES, December 4, 2025 /EINPresswire.com/ -- The Global Supply Chain Cybersecurity Market was valued at US$ 663.27 million, which was followed by an increase to US$ 706.40 million in 2024, and the market is projected to grow up to US$ 2,243.33 million by 2033, thereby determining 13.7% as the CAGR in the forecast period of 2025-2033. This situation in the global supply chain cybersecurity market can be traced back to the rising number of cyber incidents that target critical infrastructures and vendor networks. The Cybersecurity and Infrastructure Security Agency (CISA) in the U.S. has released supply chain risk management advice, stating that third-party vendors were involved in more than 90% of the reported critical infrastructure breaches in 2022. Consequently, this scenario has been compelling large corporations and government bodies to incorporate security requirements more comprehensively into procurement and vendor management policies.

> As global supply chains digitalize, cybersecurity is no longer optional—it's mission-critical. Companies that invest early in end-to-end visibility, zero-trust frameworks."
>
> *DataM Intelligence*

Download your exclusive sample report today: (corporate email gets priority access):https://www.datamintelligence.com/download-sample/supply-chain-cyber-security-market

Exclusively for the United States: Major Industrial Changes
- October 2025: Microsoft delivered an upgraded Supply Chain Security Suite using AI for threat

prediction and quantum-resistant encryption that would give protection to vital vendor networks elevating the security of the supply chain against attacks from the software side aiming at the vendors.



- September 2025: The company Palo Alto Networks brought into existence a new zero-trust monitoring platform for the entire supply chain particularly for the use of manufacturers and logistics firms that could now detect irregularities in real-time across the entire ecosystem of suppliers on multiple tiers.

- August 2025: IBM by the deployment of an automatic SBOM (Software Bill of Materials) compliance system has increased its supply chain security measures. This system is meant to help enterprises become compliant with the new federal cybersecurity standards that govern third-party risk management.

Germany: Significant Industry Changes

- October 2025: SAP has launched a module for cyber-resilient supply chains as part of its ERP ecosystem, which provides predictive risk scoring and automated vendor compliance checks for German manufacturers in the industrial and automotive sectors.

- September 2025: In order to protect against attacks aimed at industrial suppliers and component manufacturers, Siemens expanded its supply chain security portfolio by introducing a new platform for cyber defense focusing on operational technology (OT) in factory networks.

- August 2025: The German Federal Office for Information Security (BSI) has published new guidelines for supply chain cybersecurity that are meant to be followed by the entire country and are basically urging businesses to implement universal vendor-risk frameworks as well as compulsory SBOM tracking.

Recent Mergers & acquisitions

- October 2025: Cisco's acquisition of SentinelVantage, a supply-chain-focused threat intelligence startup, was concluded to complete the company's end-to-end vendor risk monitoring and AI-

driven predictive analytics across global supplier ecosystems.

- September 2025: CrowdStrike's acquisition of Lockpath Cyber Systems, a provider of third-party and supply chain security automation tools, enabled the company to go deeper into SBOM compliance, vendor assessment workflows, and multi-tier supplier threat detection areas.

- September 2025: Fortinet's acquisition of TraceSecure Analytics, a cybersecurity analytics platform specializing in logistics and manufacturing supply chain vulnerability mapping, helped Fortinet's expansion in operational technology (OT) and supply ecosystem security.

- August 2025: Palo Alto Networks has finalized the acquisition of ChainDefend Technologies, which provides zero-trust validation for suppliers and software pipelines, and it is aimed at reinforcing the protection against the new software supply chain attacks.

- August 2025: IBM has acquired CyberRoute Solutions, a company specializing in blockchain-based supply chain integrity verification, with the goal of integrating tamper-proof supplier transaction monitoring into its supply chain security portfolio.

"Secure your 30% year-end discount - get this report before the offer expires."
:https://www.datamintelligence.com/buy-now-page?report=supply-chain-cyber-security-market
((Purchase 2 or more Repots and get 50% Discount)

Market Segmentation -
Segmentation by Component
 Software: The software segment includes cybersecurity solutions that are able to monitor, detect threats, and mitigate risks in supply chain networks, as well as offer scalable integration with the already existing systems. Its ease of deployment and multi-functionality make it the leader in the market with a projected share of 59.1%.

 Hardware: This segment consists of such physical equipment as IoT sensors, RFID tags, and endpoint protection hardware dedicated to securing the shipping of the supply chain assets and the data transmission. It is responsible for around 42.7% of the market share, which is mainly caused by the increasing demand for IoT and risk mitigation.

 Services: This is the case of consulting, managed security, and compliance services that are in fact aimed at vulnerability assessments and incident response in the supply chain. It is the third player on the market, but it is still quite an important one, as it provides the necessary support for the implementation of software and hardware.

Segmentation by Security Type
 Data Visibility and Governance: This category allows for real-time tracking, providing analytics, and having oversight of data flows in supply chains to ensure both transparency and control. The

segment is gaining importance due to stringent regulations surrounding data handling and processing.

 Data Locality and Protection: These are the solutions that are mainly focused on data storage security, encryption, and also compliance with regional data sovereignty laws across global supply chains. Affected by privacy risks are large international operations and hence that might be the reason for the existence of this category.

 Other Security Types: This is a combination of fraud prevention, third-party risk management, and network monitoring, which are capable of catering to a wide range of threats such as endpoint vulnerabilities.

Regional insights:-
 North America:-Market share estimates: 37.5% (2025).
North America is still the biggest regional market in the world, due to the presence of advanced digital infrastructure, strict regulatory requirements, and widespread use of supply-chain security solutions in logistics, manufacturing, healthcare, and other critical industries.

 Europe:-Market share estimates: 29%.
Europe possesses the second-largest share, largely due to strong regulatory frameworks (e.g. data protection laws, supply-chain compliance requirements), high industrial and manufacturing demand (particularly in Germany, UK, France), and increasing investment in supply-chain risk mitigation.

 Asia-Pacific (APAC):-Market share estimates: 21%
Asia-Pacific region is rapidly growing and becoming a very important region, as a result of fast industrialization, the growth of e-commerce and logistics networks, the increase of digitization, and the rising awareness of supply-chain cyber risks especially in countries like China, India, Japan, South Korea, and Southeast Asia.

Get Customization in the report as per your requirements:https://www.datamintelligence.com/customize/supply-chain-cyber-security-market

Competitive Landscape:-
 The global supply chain cybersecurity market is composed of various notable companies, such as International Business Machines Corporation (IBM), Cisco Systems, Inc., Palo Alto Networks, Inc., Check Point Software Technologies Ltd., Fortinet, Inc., Trellix Corporation, CrowdStrike Holdings, Inc., Broadcom Inc. (Symantec Enterprise Division), Trend Micro Incorporated, and Kaspersky Lab JSC., and others too.

Conclusion

The Supply Chain Cybersecurity Market is at a pivotal point in its growth trajectory as the global supply chains are increasingly digitized, interconnected, and susceptible to advanced cyber threats. All along the supply chain, from manufacturing to logistics, healthcare, retail, and critical infrastructure, the organizations are giving first priority to total security visibility, zero-trust models, and real-time threat intelligence in their operations. Deployment of supply chain cybersecurity solutions will be enhanced through the increase of geopolitical risks, vulnerabilities of third parties, and pressure from regulations. Enterprises deploying advanced technologies like AI-based risk scoring, automated compliance, and continuous vendor monitoring will position themselves for the future better than others in terms of building up resilience, having trust, and securing their digital ecosystems.

Related Reports-

Supply Chain Security Market
Artificial Intelligence in Manufacturing and Supply Chain Market

Sai Kiran
DataM Intelligence 4Market Research
877-441-4866
email us here
Visit us on social media:
LinkedIn
X

This press release can be viewed online at: https://www.einpresswire.com/article/872389349

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.