

Security Assurance Market Growth Fueled by Rising Cybersecurity Threats Worldwide

Security Assurance Market is projected to reach \$14.8 billion by 2031, driven by rising cyber threats and cloud adoption.

WILMINGTON, DE, UNITED STATES,
June 4, 2026 /EINPresswire.com/ --

The global [security assurance market](#) is witnessing substantial growth as organizations across industries strengthen their cybersecurity frameworks to combat evolving digital threats. According to Allied Market Research, the market was valued at \$5.7 billion in 2021 and is projected to reach \$14.8 billion by 2031, registering a CAGR of 10.2% from 2022 to 2031.



As enterprises increasingly rely on digital infrastructure, cloud platforms, mobile applications, and connected devices, the importance of security assurance has become more critical than ever. Organizations are facing growing risks associated with cyberattacks, ransomware, phishing campaigns, malware infections, insider threats, and data breaches. These challenges are driving investments in advanced security assurance solutions designed to protect sensitive business information and ensure regulatory compliance.

“ Growing cybersecurity concerns, BYOD adoption, and digital transformation are accelerating security assurance market growth.”
Allied Market Research

Download PDF Brochure: <https://www.alliedmarketresearch.com/request-sample/A31446>

The growing adoption of digital transformation strategies across industries, combined with rising awareness regarding cyber resilience, is creating significant opportunities for the expansion of the security assurance market during the forecast period.

Understanding Security Assurance and Its Importance

Security assurance refers to a comprehensive approach for identifying, assessing, managing, and [mitigating cybersecurity risks](#) within an organization's technology ecosystem. It encompasses a wide range of tools, technologies, processes, and services designed to ensure that software applications, networks, databases, cloud environments, and connected systems remain secure against internal and external threats.

The primary objective of security assurance is to establish confidence that information systems can withstand unauthorized access, misuse, tampering, data loss, or operational disruptions. Modern security assurance frameworks enable businesses to proactively identify vulnerabilities before cybercriminals can exploit them.

Organizations increasingly depend on security assurance services to evaluate security posture, conduct vulnerability assessments, perform penetration testing, ensure compliance, and implement continuous monitoring mechanisms. As digital infrastructures become more complex, security assurance solutions play a crucial role in maintaining operational continuity and safeguarding valuable data assets.

Rising Cybersecurity Threats Driving Market Expansion

One of the most influential factors contributing to security assurance market growth is the increasing sophistication and frequency of cyberattacks worldwide. Businesses are facing unprecedented levels of cybercrime targeting critical information systems, customer data, financial assets, and intellectual property.

Attack methods have evolved significantly over the past decade. Cybercriminals now utilize advanced malware, ransomware, phishing campaigns, social engineering techniques, and artificial intelligence-driven attacks to infiltrate organizational networks. As a result, enterprises are investing heavily in security assurance technologies to detect vulnerabilities and strengthen their defense mechanisms.

Financial losses associated with cyber incidents continue to rise, encouraging organizations to adopt proactive security strategies. Security assurance enables businesses to identify weaknesses before attackers can exploit them, thereby reducing potential financial, operational, and reputational damage.

The increasing awareness of cyber risks among executives and decision-makers has further accelerated investments in comprehensive security assurance programs across multiple industries.

Growing Adoption of Cloud Computing Supports Market Growth

The rapid migration toward cloud-based infrastructure has significantly contributed to the expansion of the security assurance market. Organizations are increasingly moving critical

workloads, applications, and data to cloud environments to improve flexibility, scalability, and operational efficiency.

While cloud adoption delivers numerous benefits, it also introduces new security challenges. Businesses must address issues related to data privacy, identity management, access controls, and regulatory compliance. Consequently, demand for security assurance services has surged as organizations seek to secure cloud-based environments.

Cloud security assessments, configuration reviews, compliance audits, and continuous monitoring solutions have become essential components of modern cybersecurity strategies. Security assurance providers help organizations ensure that cloud deployments meet industry standards while minimizing vulnerabilities.

As cloud-native technologies continue to gain traction globally, the need for advanced security assurance solutions is expected to grow substantially over the coming years.

Impact of IoT and BYOD on Security Assurance Demand

The increasing adoption of [Internet of Things \(IoT\) devices](#) and Bring Your Own Device (BYOD) policies is creating new opportunities within the security assurance market. Businesses are connecting a growing number of devices to enterprise networks, including smartphones, tablets, sensors, wearables, and industrial equipment.

Although these technologies improve productivity and operational efficiency, they also expand the potential attack surface for cybercriminals. Each connected device represents a possible entry point into organizational systems if proper security controls are not implemented.

Security assurance services help organizations identify vulnerabilities associated with connected devices, evaluate network security, and establish effective risk management strategies. By implementing comprehensive security assurance frameworks, enterprises can safely embrace IoT and BYOD initiatives while minimizing exposure to cyber threats.

The continued proliferation of connected devices is expected to remain a major growth driver for the security assurance market throughout the forecast period.

Mobile Applications Creating New Security Requirements

The rapid growth of mobile platforms and applications has transformed how businesses interact with customers, employees, and partners. Mobile banking, e-commerce, healthcare applications, and enterprise mobility solutions have become integral components of modern business operations.

However, the increasing reliance on mobile technologies has created additional security

concerns. Mobile applications frequently process sensitive personal and financial information, making them attractive targets for cybercriminals.

Organizations are increasingly investing in security assurance services to identify vulnerabilities in mobile applications and ensure secure software development practices. Security testing, code analysis, threat modeling, and compliance assessments are becoming standard procedures within application development lifecycles.

The growing use of mobile applications across industries is expected to create substantial opportunities for the security assurance market over the next decade.

Procure This Report (345 Pages PDF with Insights, Charts, Tables, and Figures):

<https://www.alliedmarketresearch.com/security-assurance-market/purchase-options>

BFSI Sector Emerges as the Largest End User

The Banking, Financial Services, and Insurance (BFSI) sector accounted for the largest share of the security assurance market in 2021 and is expected to maintain its leadership position throughout the forecast period.

Financial institutions manage enormous volumes of sensitive customer information and monetary transactions every day. As digital banking services, mobile payment platforms, and online financial solutions continue to expand, cyber threats targeting the BFSI sector have become increasingly sophisticated.

Banks and financial organizations must maintain strict security standards to protect customer trust and comply with regulatory requirements. Security assurance solutions help these institutions evaluate vulnerabilities, strengthen cybersecurity frameworks, and safeguard critical assets.

The widespread adoption of cloud banking, digital wallets, and fintech platforms further reinforces the need for advanced security assurance services within the BFSI industry.

Manufacturing Sector Expected to Witness Rapid Growth

While BFSI currently dominates the market, the manufacturing sector is anticipated to experience significant growth during the forecast period. Industrial organizations are rapidly embracing digital technologies such as automation, smart factories, Industrial IoT, artificial intelligence, and predictive analytics.

The convergence of operational technology and information technology environments has created new cybersecurity challenges for manufacturers. Cyberattacks targeting industrial systems can disrupt production, damage equipment, and cause substantial financial losses.

Security assurance solutions help manufacturers identify vulnerabilities, secure connected systems, and ensure operational continuity. As Industry 4.0 adoption accelerates globally, demand for security assurance services within manufacturing environments is expected to rise significantly.

North America Leads the Global Market

North America emerged as the largest regional market for security assurance in 2021. The region's leadership can be attributed to strong technology adoption, advanced digital infrastructure, and high cybersecurity awareness among organizations.

Businesses across the United States and Canada are making substantial investments in cybersecurity technologies to protect digital assets and comply with evolving regulatory requirements. The presence of major technology providers and cybersecurity vendors further strengthens the region's market position.

Growing cloud adoption, increased mobile device usage, and rising incidents of cybercrime continue to support demand for security assurance solutions throughout North America.

Asia-Pacific Presents Strong Growth Opportunities

Asia-Pacific is expected to register the fastest growth during the forecast period. Rapid digitalization, expanding internet penetration, and increasing adoption of cloud-based services are creating favorable conditions for market expansion.

Countries such as India, China, Japan, South Korea, and Southeast Asian nations are witnessing significant investments in digital transformation initiatives. As organizations modernize their IT infrastructure, cybersecurity concerns are becoming a top priority.

The increasing number of connected devices, rising e-commerce activity, and expanding fintech ecosystems are further driving demand for security assurance services across the region. These factors position Asia-Pacific as a major growth engine for the global security assurance market.

COVID-19 Impact on the Security Assurance Market

The COVID-19 pandemic accelerated digital transformation efforts worldwide and significantly influenced the growth trajectory of the security assurance market. Remote work arrangements, online collaboration platforms, and digital business operations became essential during lockdown periods.

As organizations rapidly shifted to remote working models, cybercriminals exploited new vulnerabilities, leading to an increase in phishing attacks, ransomware incidents, and data

breaches. Consequently, businesses increased investments in cybersecurity and security assurance solutions to protect remote environments.

The pandemic also highlighted the importance of resilient digital infrastructure and effective risk management strategies. Organizations recognized the need for continuous security monitoring, vulnerability assessments, and compliance management to address evolving threats.

Even in the post-pandemic era, the heightened focus on cybersecurity remains a key factor driving continued growth within the security assurance market.

Competitive Landscape

The global security assurance market remains highly competitive, with major technology companies and cybersecurity providers continuously expanding their capabilities through innovation, partnerships, and strategic acquisitions.

Leading companies operating in the market include Accenture, Aura Information Security, Avaya Inc., BizCarta India, Cipher Security LLC, Capgemini, Happiest Minds, IBM, Infosys Ltd., Microsoft Corporation, Micro Focus, NETSCOUT, Radix Technologies, SAS Institute, Spirent Communications, Tenable Inc., and Telos Corporation.

These organizations are investing heavily in advanced security technologies, threat intelligence platforms, cloud security solutions, and managed security services to strengthen their market presence. Strategic collaborations and product innovations continue to shape competition within the industry.

Get a Customized Research Report: <https://www.alliedmarketresearch.com/request-for-customization/A31446>

Conclusion

The global security assurance market is poised for substantial growth as organizations increasingly prioritize cybersecurity in an era of digital transformation. Rising cyber threats, growing cloud adoption, expanding IoT ecosystems, and increasing reliance on mobile applications are driving demand for advanced security assurance solutions across industries.

With the market projected to grow from \$5.7 billion in 2021 to \$14.8 billion by 2031, businesses are expected to continue investing in comprehensive security frameworks that enhance resilience, protect critical assets, and ensure regulatory compliance. As digital technologies become more deeply integrated into everyday operations, security assurance will remain a cornerstone of modern enterprise risk management and cybersecurity strategy.

Trending Reports in Energy and Power Industry:

Security Assurance Market

<https://www.alliedmarketresearch.com/security-assurance-market-A31446>

Security Information and Event Management Market

<https://www.alliedmarketresearch.com/security-information-and-event-management-market>

Online/Virtual Fitness Market

<https://www.alliedmarketresearch.com/virtual-online-fitness-market>

Online Trading Platform Market

<https://www.alliedmarketresearch.com/online-trading-platform-market>

IoT Market

<https://www.alliedmarketresearch.com/internet-of-things-iot-market>

Deep Learning Market

<https://www.alliedmarketresearch.com/deep-learning-market>

E-Learning Market

<https://www.alliedmarketresearch.com/e-learning-market-A06253>

Brain Computer Interface Market

<https://www.alliedmarketresearch.com/brain-computer-interfaces-market>

Algorithmic Trading Market

<https://www.alliedmarketresearch.com/algorithmic-trading-market-A08567>

Customer Relationship Management Market

<https://www.alliedmarketresearch.com/crm-software-market>

video analytics market

<https://www.alliedmarketresearch.com/video-analytics-market>

fraud detection & prevention market

<https://www.alliedmarketresearch.com/fraud-detection-and-prevention-market>

About Us

Allied Market Research (AMR) is a full-service market research and business-consulting wing of Allied Analytics LLP based in Portland, Oregon. Allied Market Research provides global enterprises as well as medium and small businesses with unmatched quality of "Market Research Reports" and "Business Intelligence Solutions." AMR has a targeted view to provide business insights and consulting to assist its clients to make strategic business decisions and achieve sustainable growth in their respective market domain.

Pawan Kumar, the CEO of Allied Market Research, is leading the organization toward providing high-quality data and insights. We are in professional corporate relations with various companies and this helps us in digging out market data that helps us generate accurate research data tables and confirms utmost accuracy in our market forecasting. Each and every data presented in the reports published by us is extracted through primary interviews with top officials from leading companies of domain concerned. Our secondary data procurement methodology includes deep online and offline research and discussion with knowledgeable professionals and analysts in the industry.

David Correa

Allied Market Research

+ + + + + + + + + + +1 800-792-5285

[email us here](#)

Visit us on social media:

[LinkedIn](#)

[Facebook](#)

[YouTube](#)

[X](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/917236433>

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.