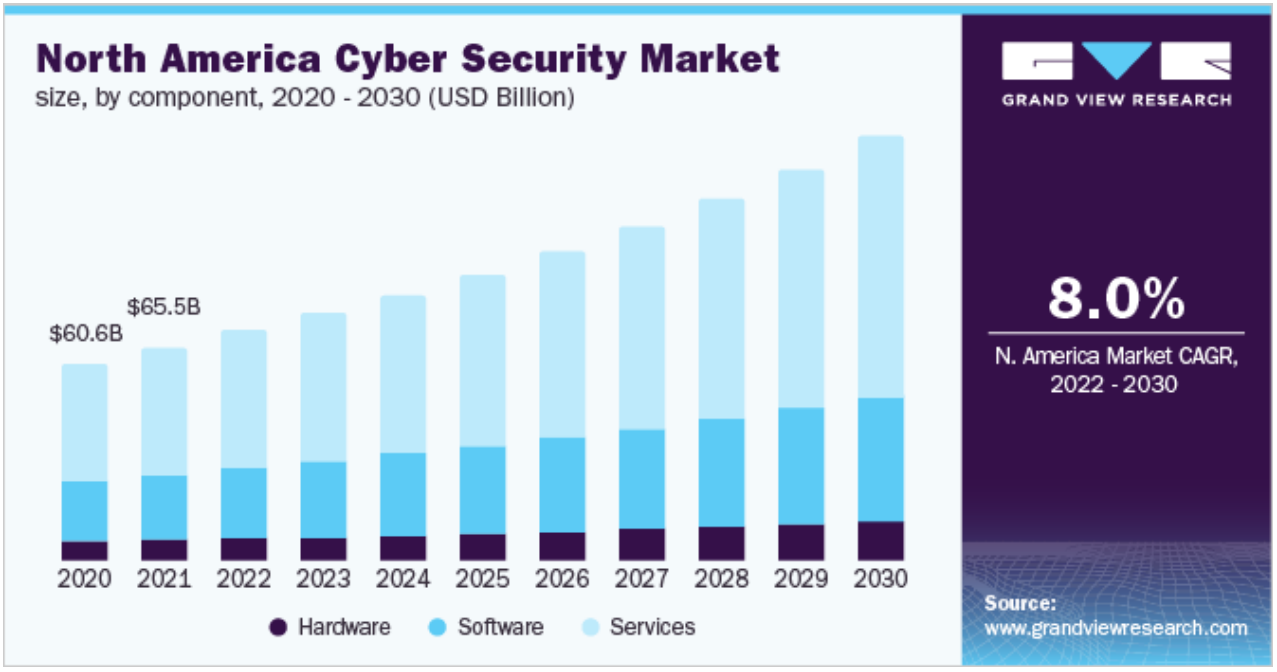
Cyber Security Market Size & Share Report, 2030

Report Overview

The global cyber security market size was valued at USD 184.93 billion in 2021 and is expected to expand at a compound annual growth rate (CAGR) of 12.0% from 2022 to 2030. The increasing number of cyber-attacks with the emergence of e-commerce platforms, deployment of cloud solutions, and proliferation of smart devices are some of the factors driving the market growth. Cyber threats are anticipated to evolve with the increase in usage of devices with intelligent and IoT technologies. As such, organizations are expected to adopt and deploy advanced cyber security solutions to detect, mitigate, and minimize the risk of cyber-attacks, thereby driving market growth.



To learn more about this report, request a free sample copy

Cyber security experienced a slight dip in 2020 due to the closure of several organizations during the first and second quarters of 2020. However, the market started recovering by the end of the second quarter owing to several firms deploying cyber security solutions with the implementation of remote working culture. Employees used personal devices for business work while connecting through private Wi-Fi or anonymous networks, putting the company's security at risk. As such, several organizations adopted cyber security solutions the manage and secure the increased number of endpoint devices while also getting protection from network threats.

The cyber security market is expected to continue its growth post-pandemic due to the hybrid working trend that is anticipated to stay over the future. Several employees are expected to continue working from home or remote premises with the increasing BYOD trend. According to data published by Nine2FiveJobSearch.com, before the pandemic, 29% of the U.S. workforce had an option of working from home on a part-time basis, which increased to 50% of the workforce working from home in 2020. The risk of cyber-attacks is expected to grow with the emerging BYOD and hybrid working trend, which is expected to drive the adoption of cyber security solutions and fuel market growth.

Several organizations incur significant losses in terms of loss of revenue, brand reputation, unplanned workforce reduction, and business disruptions due to data breaches. Companies have to spend a considerable amount of money to recover from these losses and mitigate the

risks evolving from data breaches. According to a report published by IBM in 2021, the average cost of data breaches for an organization amounted to USD 4.87 million, an increase of 10% over 2020. As such, organizations are engaged in deploying advanced cyber security solutions to detect cyber threats and provide a response, thereby helping in cutting down data breach costs.

Cyber security companies are engaged in developing security solutions with AI that helps organizations automate their IT security. Such solutions enable automated threat detection and remediation, allowing IT professionals to reduce the efforts and time required to track malicious activities, techniques, and tactics. These solutions offer real-time monitoring and identification of new threats while also responding autonomously. This helps the security teams analyze the filtered breach information and detect and remediate cyber-attacks faster, thereby reducing security incident costs.

Components Insights

The services segment accounted for the largest revenue share in 2021, contributing more than 50% of the overall revenue. This can be attributed to the increasing demand for consultation services and maintenance and upgrade services from small and medium enterprises. SMEs have a limited budget and small teams, owing to which these organizations often depend on consultations before implementing any solutions. Additionally, the pandemic outbreak led to a boost in the adoption of cyber security services owing to several organizations planning to strengthen their IT infrastructure and network security while also managing remote working employees and preventing threats from unknown networks and devices.

The hardware segment is expected to register the highest growth over the forecast period due to several organizations engaged in implementing cyber security platforms and also upgrading their existing ones. Security vendors are involved in developing cyber security solutions with artificial intelligence and machine learning-based capabilities, which require high-end IT infrastructure. With an increasing number of cyber-attacks from anonymous networks, internet service providers and large and small & medium organizations are anticipated to deploy next-generation security hardware such as Intrusion Prevention Systems (IPS), encrypted USB flash drives, and firewalls, among others. The hardware equipment is expected to help the organizations upgrade the IT security, enabling real-time monitoring of threats and protecting the systems by preventing the threats from entering computing systems.

Report Coverage & Deliverables

PDF report & online dashboard will help you understand:

- Competitive benchmarking
- Historical data & forecasts
- Company revenue shares
- Regional opportunities
- Latest trends & dynamics

Request a Free Sample Copy

Security Type Insights

The infrastructure protection segment accounted for the largest revenue share in 2021, contributing more than 25% of the overall revenue. The high market share is attributed to the rising number of data center constructions and the adoption of connected and IoT devices. Further, different programs introduced by governments across some regions, such as the Critical Infrastructure Protection Program in the U.S. and the European Programme for Critical Infrastructure Protection (EPCIP), are expected to contribute to market growth. For instance,

the National Critical Infrastructure Prioritization Program (NIPP), created by the Cybersecurity and Infrastructure Security Agency (CISA), helps in identifying the list of assets and systems vulnerable to cyber-attacks across various industries, including energy, manufacturing, transportation, oil & gas, chemicals, and others, which is damaged or destroyed would lead to national catastrophic effects.

The cloud security segment is expected to exhibit the highest growth in the forecast period owing to the increasing adoption of cloud-based solutions by enterprises due to its cost-effectiveness and the convenience of working with cloud-based platforms. However, cloud-based platforms are always vulnerable to data breaches and cyber-attacks. The growing risk of unauthorized access and the increasing number of threat actors across cloud layers coupled with the increasing malware infiltrations is expected to compel enterprises to adopt cloud security solutions. Further, with growing web traffic to access media content, the need for filtering this traffic is expected to drive the segment growth.

Solution Insights

The IAM segment accounted for the largest revenue share in 2021, contributing more than 25% of the overall revenue. The high market share is attributed to the increasing number of mobile endpoint devices subjecting the organization to data breaches and cyber-attacks. Further, the growing need to control user access to critical information during the pandemic is expected to contribute to market growth. Additionally, the need to automate and track end-user activities and security incidents are anticipated to drive IAM solutions adoption.

The IDS/IPS segment is expected to exhibit the highest growth in the forecast period due to the increasing need for real-time monitoring and identifying threats across the networks. An organization's network has numerous access points to both private and public networks. Although there are security systems in place, the sophisticated nature of cyberattacks can thwart the best security systems with encryptions or firewalls. As such, IDS/IPS solutions increase visibility across networks by identifying malicious content, thereby preventing cyber-attacks while also blocking unwanted traffic.

Service Insights

The managed services segment is expected to register the highest growth rate of more than 10% over the forecast period. The high growth can be attributed to the increasing demand for outsourcing IT security services to monitor and maintain security solutions and actions. Managed services provide a cost-effective way without requiring internal teams to manage the company's IT security workload. Further, managed service providers are entirely focused on observing threat patterns and enhancing security operations anticipated to mitigate cyber-attacks, thereby increasing the adoption of managed services.

The professional services segment held the highest market share of the overall market in 2021 and is expected to maintain its dominance over the forecast period. The increased adoption of these services is attributed to the growing demand for services such as enterprise risk assessment, penetration testing, physical security testing, and cyber security defense. Further, the lack of skilled IT security professionals is another reason driving the adoption of these services for employee training. Additionally, organizations depend on such professional service providers’ expertise and consultation who assess the business requirements and enterprise risks to ensure the implementation of cost-effective and suitable security solutions.

Deployment Insights

The cloud-based segment is expected to register the highest growth rate of more than 10% over the forecast period. The high growth can be attributed to the growing deployment of cloud computing infrastructure and migration of on-premises solutions to the cloud by

enterprises. Further, cloud-based security solutions are easy and cost-effective to deploy and manage as well as upgrade, which is a primary reason expected to contribute to market growth. Additionally, cloud deployment enables remote access to solutions across various devices, which is further expected to propel the segment growth.

The on-premises segment held the highest market share of the overall market in 2021 and is expected to maintain its dominance over the forecast period. Several large organizations prefer having complete ownership of the solutions and upgrades, thereby ensuring an optimum level of data security, as they possess critical business information databases. Further, on-premises deployment reduces dependency on third-party organizations providing explicit monitoring and data protection. The persistence of organizations in maintaining the confidentiality of in-house data is expected to upkeep the demand for on-premises deployment.

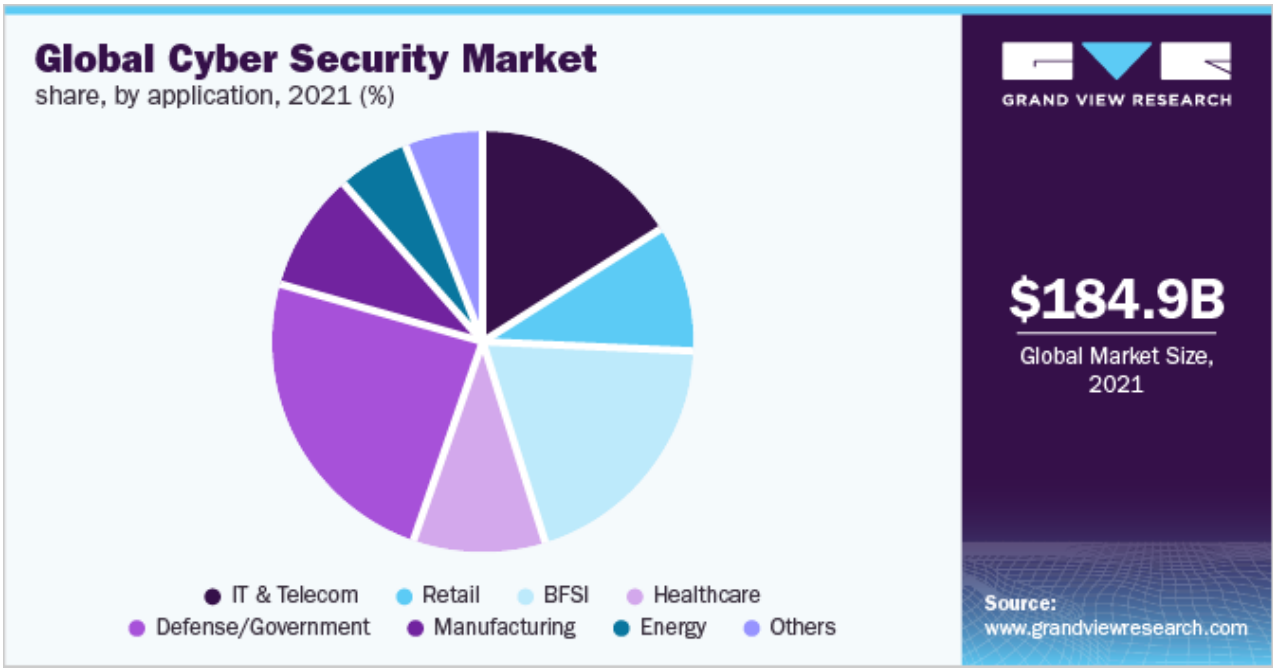
Organization Size Insights

The SMEs segment is expected to register the highest growth rate of more than 11% over the forecast period. Small and medium enterprises are more prone to cyber-attacks with a low level of security due to budget constraints. Additionally, lack of security policies and skills of employees are some of the critical factors responsible for increasing cyber-attack across SMEs. As such, the growing need to cut operational and data breach costs and secure IT assets is anticipated to drive the adoption in SMEs.

The large enterprise segment held the highest market share of the overall market in 2021 due to the increase in spending on IT infrastructure by these organizations. Large enterprises have a large volume of data storage, owing to which they are engaged in deploying AI and ML-based security solutions for automating their security platforms. Further, large enterprises possess several networks, servers, storage equipment, and endpoint devices, which puts them at high risk of substantial monetary losses in the wake of cyber-attacks. Additionally, with several firms adopting the hybrid working models, anonymous networks and usage of personal devices pose a high-security risk to large enterprises, which is another factor expected to drive the demand across this segment.

Application Insights

The defense/government segment held the highest market share of more than 20% of the overall market in 2021. Government and defense organizations are under a constant security threat from state-sponsored hacktivists due to the confidential nature of the information they possess. As such several governments worldwide are investing heavily in strengthening the cyber security of their nations, which is eventually contributing to the segment growth. For instance, the Japanese government is expected to increase its defense budget to USD 47.18 billion, out of which it plans to allot USD 298.2 million to strengthen its defense against cyber-attacks.



To learn more about this report, request a free sample copy

The healthcare segment held the highest revenue share of the overall market in 2021. Healthcare facilities have different types of information systems, including practice management support systems, e-prescribing systems, EHR systems, radiology information systems, and clinical decision support systems, among others, which hold a lot of sensitive patient and hospital data. Further, there are a lot of IoT-enabled systems that include smart HVAC systems, remote patient monitoring devices, infusion pumps, smart elevators, and more, which are critical in maintaining daily patient-related activities. As such, healthcare facilities are expected to adopt cyber security solutions to safeguard electronic assets and information from unauthorized use, access and disclosure, thereby driving the market growth.

Regional Insights

Asia Pacific is expected to register the fastest growth, at a CAGR of more than 15%, over the forecast period. The growth of this region can be attributed to the high deployment of cloud technologies, the proliferation of IoT devices, and the increasing number of data center constructions. Further, the massive working population in the region possesses a large number of endpoint devices and generates a large volume of data owing to which several organizations are engaged in deploying cyber security solutions. Additionally, the increasing spending from the government and defense sectors across countries like China, India, Japan, South Korea, and others to safeguard themselves from cyber warfare is expected to drive market growth.

North America held the high market share, followed by Europe, in 2021. The early availability and adoption of new technologies have contributed to the growth of the North American market over the past years. Further, the high number of capital and IT market and their diversified businesses worldwide call for efficient management of endpoint devices and protection across unknown networks. Such factors are compelling large enterprises and SMEs across the region to increase their spending on cyber security solutions, which is expected to contribute to market growth.

Key Companies & Market Share Insights

The key market players in the global market in 2021 include Palo Alto Networks, Trend Micro Incorporated, VMware, Inc., Broadcom, McAfee, Inc., and others. The market is characterized by the presence of several players offering differentiated security solutions with advanced features. Players in the cyber security space are engaged in introducing products with artificial intelligence and machine learning capabilities, which help organizations automate their IT

security. For instance, in August 2021, Palo Alto Networks introduced an upgraded version of its Cortex XDR platform. The new version is expected to expand the investigation, monitoring, and detection capabilities, thereby offering broader and enhanced protection to the security operation center (SOC) teams. Further, companies are also adopting inorganic growth strategies by engaging in partnerships, acquiring smaller players to leverage their technology, and reducing the competitors in the market. Some prominent players in the global cyber security market include

- Cisco Systems, Inc.
- Palo Alto Networks
- McAfee, Inc.
- Broadcom
- Trend Micro Incorporated
- CrowdStrike
- Check Point Software Technology Ltd.

Report Attribute	**Details**
Market size value in 2022	USD 202.72 billion
Revenue forecast in 2030	USD 500.70 billion
Growth Rate	CAGR of 12.0% from 2022 to 2030
Base year for estimation	2021
Historical data	2018 - 2020
Forecast period	2022 - 2030
Quantitative units	Revenue in USD million and CAGR from 2022 to 2030
Report coverage	Revenue forecast, company ranking, competitive landscape, growth factors, and trends
Segments covered	Component, security type, solutions, services, deployment, organization size, applications, region
Regional scope	North America; Europe; Asia Pacific; Latin America; MEA
Country scope	U.S.; Canada; U.K.; Germany; China; India; Japan; Brazil; Mexico
Key companies profiled	Broadcom; Cisco Systems, Inc.; Check Point Software Technology Ltd.; IBM; McAfee, LLC; Palo Alto Networks, Inc.; Trend Micro Incorporated
Customization scope	Free report customization (equivalent to up to 8 analysts' working days) with purchase. Addition or alteration to country, regional & segment scope.
Pricing and purchase options	Avail customized purchase options to meet your exact research needs. Explore purchase options.

Segments Covered in the Report

The report forecasts revenue growth at the global, regional, and country levels and provides an analysis of the latest industry trends in each of the sub-segments from 2018 to 2030. For this study, Grand View Research has segmented the global cyber security market report based on component, security type, solution, services, deployment, organization, application, and region:

- **Component Outlook (Revenue, USD Million, 2018 - 2030)**
    - Hardware
    - Software
    - Services
- **Security Type Outlook (Revenue, USD Million, 2018 - 2030)**
    - Endpoint Security
    - Cloud Security
    - Network Security
    - Application Security
    - Infrastructure Protection
    - Data Security
    - Others
- **Solution Outlook (Revenue, USD Million, 2018 - 2030)**
    - Unified Threat Management (UTM)
    - IDS/IPS
    - DLP
    - IAM
    - SIEM
    - DDoS
    - Risk and Compliance Management
    - Others
- **Services Outlook (Revenue, USD Million, 2018 - 2030)**
    - Professional Services
    - Managed Services
- **Deployment Outlook (Revenue, USD Million, 2018 - 2030)**
    - Cloud-based
    - On-premises

- **Organization Size Outlook (Revenue, USD Million, 2018 - 2030)**
  - SMEs
  - Large Enterprises
- **Application Outlook (Revenue, USD Million, 2018 - 2030)**
  - IT & Telecom
  - Retail
  - BFSI
  - Healthcare
  - Defense/Government
  - Manufacturing
  - Energy
  - Others
- **Regional Outlook (Revenue, USD Million, 2018 - 2030)**
  - North America
    - U.S.
    - Canada
  - Europe
    - U.K.
    - Germany
    - Rest of Europe
  - Asia Pacific
    - China
    - India
    - Japan
    - Rest of Asia Pacific
  - Latin America
    - Brazil
    - Mexico
    - Rest of Latin America
  - Middle East & Africa

Frequently Asked Questions About This Report

b. The professional service segment dominated the global cyber security market in 2021 with a revenue share of over 72%.

b. The global cyber security market size was estimated at USD 184.93 billion in 2021 and is expected to reach USD 202.72 billion in 2022.

b. The global cyber security market is expected to grow at a compound annual growth rate of 12.0% from 2022 to 2030 to reach USD 500.70 billion by 2030.

b. The services segment dominated the global cyber security market in 2021 and accounted for a revenue share of over 54%.

b. The infrastructure protection segment dominated the global cyber security market in 2021 with a revenue share of more than 27%.