

# **Cyber Security Services Market – Global Industry Size, Share, Trends, Opportunity, and Forecast, Segmented By Size of Organization (Small & Medium Enterprises, Large Enterprises), By Security Type (Vulnerability & Security Assessment, Threat Intelligence & Business Analytics, Auditing & Logging, Continuous Monitoring & Encryption, Identity & Access Management), By End-user Industry (Healthcare, BFSI, IT & Telecom, Government, Energy & Utilities), By Region & Competition, 2019-2029F**

<https://marketpublishers.com/r/C58617AF2BB4EN.html>

Date: October 2024

Pages: 181

Price: US\$ 4,500.00 (Single User License)

ID: C58617AF2BB4EN

## **Abstracts**

Global Cyber Security Services Market was valued at USD 178 Billion in 2023 and is anticipated to project robust growth in the forecast period with a CAGR of 13.4% through 2029. The global cybersecurity services market is experiencing significant growth driven by escalating cyber threats and the expanding digital landscape across industries. Organizations worldwide are increasingly vulnerable to sophisticated cyber attacks, prompting heightened investments in cybersecurity solutions and services. These services encompass a wide range of offerings, including threat detection and response, risk and compliance management, security consulting, and managed security services. Key factors propelling market expansion include the proliferation of cloud computing, IoT (Internet of Things) devices, and digital transformation initiatives, which amplify the attack surface and necessitate robust cybersecurity measures. Moreover, stringent regulatory requirements and data protection laws further compel organizations to bolster their cybersecurity posture through specialized services tailored to their needs. As businesses recognize the imperative of protecting sensitive data, maintaining

operational continuity, and safeguarding customer trust, the demand for cybersecurity services continues to surge. This trend is expected to persist as organizations prioritize proactive threat mitigation, resilience against cyber threats, and adherence to regulatory frameworks, driving further innovation and investment in the cybersecurity services sector globally.

## Key Market Drivers

### Rising Cyber Threat Landscape

The escalating frequency and sophistication of cyber threats globally are a significant driver for the cybersecurity services market. Cyber attacks continue to evolve, targeting critical infrastructure, businesses of all sizes, and individuals. Threat actors employ advanced techniques such as ransomware, phishing, and zero-day exploits to breach defenses and compromise sensitive data. As organizations face these persistent and evolving threats, there is a growing recognition of the need for robust cybersecurity measures and expertise. Cybersecurity services play a crucial role in helping organizations defend against, detect, and respond to these threats effectively. Services such as threat intelligence, incident response, and vulnerability management are in high demand as businesses seek to strengthen their cybersecurity postures. Moreover, the shift towards remote work and cloud adoption has expanded the attack surface, further driving the need for comprehensive cybersecurity services that can protect endpoints, networks, and cloud environments from a diverse range of threats.

Industries such as finance, healthcare, and government, which handle sensitive data and are prime targets for cyber attacks, are increasing their investments in cybersecurity services to safeguard critical assets and maintain operational resilience. The rising awareness of cyber risks among businesses and the proactive measures taken to mitigate these risks are key drivers shaping the growth trajectory of the cybersecurity services market globally.

### Stringent Regulatory Requirements

Stringent regulatory requirements and compliance mandates are compelling organizations across various sectors to invest in cybersecurity services. Governments worldwide have implemented regulations and standards to ensure the protection of personal data, secure critical infrastructure, and mitigate cyber threats. For instance, regulations like GDPR (General Data Protection Regulation) in Europe, HIPAA (Health Insurance Portability and Accountability Act) in the United States, and PCI DSS

(Payment Card Industry Data Security Standard) for payment card security impose strict requirements on data protection and cybersecurity practices.

To comply with these regulations, organizations are required to implement robust cybersecurity measures and demonstrate effective management of cybersecurity risks. This includes conducting regular risk assessments, implementing cybersecurity frameworks, and engaging cybersecurity services providers to ensure adherence to regulatory requirements. Cybersecurity services such as compliance audits, security assessments, and governance consulting help organizations navigate complex regulatory landscapes and achieve compliance effectively.

The penalties and reputational damage associated with non-compliance drive organizations to prioritize cybersecurity investments and seek specialized expertise to protect against potential breaches and data breaches. As regulatory frameworks continue to evolve and expand globally, the demand for cybersecurity services that facilitate compliance and enhance cybersecurity resilience is expected to grow, positioning regulatory requirements as a significant driver influencing the cybersecurity services market.

### Increasing Adoption of Cloud Computing

The rapid adoption of cloud computing is another major driver fueling the growth of the global cybersecurity services market. Cloud services offer organizations scalability, flexibility, and cost-efficiency, enabling them to streamline operations and enhance productivity. However, the shift to cloud environments introduces new security challenges related to data protection, identity management, and secure cloud adoption practices. As organizations migrate their data and applications to the cloud, there is a critical need for cybersecurity services that can address these challenges and ensure the security of cloud environments. Cloud security services such as cloud access security brokers (CASB), secure cloud migration, and continuous monitoring of cloud infrastructure are essential to protect against data breaches, insider threats, and unauthorized access.

Hybrid cloud environments, which combine on-premises infrastructure with cloud services, further complicate cybersecurity efforts by increasing the attack surface and requiring integrated security solutions. This trend has driven the demand for cybersecurity services that can provide holistic security coverage across hybrid and multi-cloud environments, ensuring consistent protection and compliance. The COVID-19 pandemic accelerated the adoption of remote work and cloud services,

prompting organizations to expedite their digital transformation initiatives. This rapid shift underscored the importance of cybersecurity services that can support remote workforce security, secure collaboration tools, and protect against emerging threats targeting remote access and cloud-based applications.

## Key Market Challenges

### Shortage of Skilled Cybersecurity Professionals

One of the primary challenges in the cybersecurity services market is the persistent shortage of skilled cybersecurity professionals. As the demand for cybersecurity services grows due to increasing cyber threats and digital transformation initiatives, the supply of qualified professionals capable of designing, implementing, and managing effective cybersecurity measures has not kept pace. This skills gap is exacerbated by the rapid evolution of cyber threats and the complexity of cybersecurity technologies and methodologies.

Organizations struggle to recruit and retain cybersecurity talent with expertise in areas such as threat detection and response, penetration testing, risk management, and compliance. The shortage of skilled professionals limits the ability of organizations to effectively manage cybersecurity risks and implement comprehensive security strategies. Furthermore, smaller organizations and those in less-developed regions often face greater challenges in accessing and affording skilled cybersecurity talent, which can leave them more vulnerable to cyber attacks.

Addressing the shortage of skilled cybersecurity professionals requires concerted efforts from educational institutions, governments, and industry stakeholders to promote cybersecurity education and training programs. Initiatives such as scholarships, apprenticeships, and partnerships between academia and industry can help build a pipeline of qualified cybersecurity professionals. Additionally, organizations can invest in upskilling existing IT staff and leveraging managed security services providers (MSSPs) to supplement internal capabilities and overcome resource constraints.

### Increasing Sophistication of Cyber Threats

The relentless evolution and increasing sophistication of cyber threats pose another significant challenge for the cybersecurity services market. Cybercriminals continuously develop new tactics, techniques, and procedures (TTPs) to circumvent traditional security measures and exploit vulnerabilities in IT infrastructures. Advanced persistent

threats (APTs), ransomware, phishing attacks, and supply chain compromises are among the complex threats that organizations must defend against. Traditional cybersecurity approaches based on signature-based detection and reactive responses are often insufficient to detect and mitigate sophisticated cyber attacks effectively. The ability of threat actors to adapt their techniques and evade detection requires cybersecurity services providers to employ advanced threat intelligence, behavioral analytics, and machine learning capabilities to detect anomalies and identify potential threats proactively.

The proliferation of interconnected devices and the Internet of Things (IoT) expands the attack surface, introducing new vulnerabilities that cybercriminals can exploit. Securing IoT devices and ensuring their integration into existing cybersecurity frameworks present additional challenges for organizations and cybersecurity services providers alike. Addressing the challenge of increasing cyber threat sophistication requires continuous innovation and investment in cybersecurity technologies and expertise. Collaborative efforts between cybersecurity vendors, researchers, and organizations can drive the development of next-generation security solutions that can detect, mitigate, and respond to advanced threats effectively. Additionally, organizations must adopt a proactive approach to cybersecurity, including regular security assessments, threat hunting, and incident response planning, to enhance resilience against evolving cyber threats.

### Complexity of Regulatory Compliance

Another significant challenge for the cybersecurity services market is the complexity of regulatory compliance requirements. Organizations across various industries are subject to a multitude of cybersecurity regulations, standards, and data protection laws aimed at safeguarding sensitive information, ensuring privacy, and mitigating cyber risks. Examples include GDPR (General Data Protection Regulation) in Europe, HIPAA (Health Insurance Portability and Accountability Act) in the United States, and PCI DSS (Payment Card Industry Data Security Standard) for payment card security. Compliance with these regulations requires organizations to implement specific cybersecurity measures, conduct regular audits, and demonstrate accountability for protecting personal and sensitive data. The complexity arises from the varying regulatory requirements across jurisdictions, industry sectors, and types of data handled, making it challenging for organizations to navigate and ensure comprehensive compliance. Regulatory frameworks are continually evolving in response to emerging cyber threats and changing technology landscapes, further complicating compliance efforts. Organizations may struggle to keep pace with regulatory updates, interpret complex



requirements, and allocate resources effectively to achieve and maintain compliance. Non-compliance can result in significant penalties, fines, reputational damage, and loss of customer trust, underscoring the importance of robust cybersecurity services that support regulatory adherence.

To address the challenge of regulatory complexity, cybersecurity services providers must offer specialized expertise in regulatory compliance, including knowledge of specific industry requirements and best practices for achieving compliance. This includes conducting thorough risk assessments, implementing appropriate security controls, and documenting compliance efforts to demonstrate adherence to regulatory standards. Leveraging technology solutions such as governance, risk, and compliance (GRC) platforms can streamline compliance management processes, automate compliance audits, and provide real-time visibility into compliance status. Collaboration with legal experts, regulatory bodies, and industry associations can also help organizations navigate regulatory landscapes effectively and proactively mitigate compliance risks.

### Budget Constraints and Cost Pressures

Budget constraints and cost pressures represent significant challenges for organizations seeking to invest in cybersecurity services. Effective cybersecurity requires substantial investments in technologies, skilled personnel, training, and ongoing maintenance to mitigate risks and protect against cyber threats effectively. However, many organizations, particularly small and medium-sized enterprises (SMEs) and nonprofit sectors, may have limited financial resources dedicated to cybersecurity initiatives.

The high cost of cybersecurity technologies, such as advanced threat detection systems, encryption tools, and security analytics platforms, can be prohibitive for organizations with constrained budgets. Moreover, recruiting and retaining qualified cybersecurity professionals often comes at a premium, exacerbating cost pressures for organizations seeking to build internal cybersecurity capabilities. The evolving nature of cyber threats necessitates continuous investment in cybersecurity measures and updates to security infrastructure, further straining organizational budgets. The challenge is compounded by the need to balance cybersecurity investments with other business priorities, such as innovation, growth initiatives, and operational efficiency improvements. To address budget constraints and cost pressures, organizations can consider leveraging managed security services providers (MSSPs) that offer cost-effective cybersecurity solutions tailored to their specific needs and budgetary constraints. MSSPs provide access to advanced cybersecurity technologies, expertise,

and round-the-clock monitoring and response capabilities without the upfront costs associated with internal deployments.

Adopting a risk-based approach to cybersecurity investment prioritization can help organizations allocate resources effectively by focusing on addressing high-priority risks and vulnerabilities. This approach involves conducting thorough risk assessments, identifying critical assets and potential impact scenarios, and aligning cybersecurity investments with business objectives and risk tolerance levels.

## Key Market Trends

### Rapid Adoption of Cloud-Based Security Solutions

The rapid adoption of cloud computing has transformed the cybersecurity landscape, driving organizations to embrace cloud-based security solutions. Cloud-based security services offer scalability, flexibility, and cost-effectiveness compared to traditional on-premises security solutions. Organizations are increasingly leveraging cloud security services such as Secure Access Service Edge (SASE), Cloud Access Security Brokers (CASB), and cloud-based identity and access management (IAM) to protect data and applications hosted in cloud environments.

The shift to remote work and hybrid cloud infrastructures further accelerates the demand for cloud security services that can secure endpoints, enforce data protection policies, and provide visibility and control over cloud-based assets. Moreover, cloud service providers (CSPs) are enhancing their security offerings with built-in security features, compliance certifications, and global reach, attracting organizations looking to simplify security management and enhance resilience against cyber threats.

As organizations continue to migrate critical workloads to the cloud, the adoption of cloud-based security solutions is expected to grow. This trend reflects a strategic shift towards leveraging scalable and integrated security architectures that can protect digital assets across distributed cloud environments while enabling business agility and innovation.

### Rise in Demand for Managed Security Services (MSS)

The increasing complexity and volume of cyber threats, coupled with the shortage of skilled cybersecurity professionals, are driving the adoption of Managed Security Services (MSS). MSS providers offer outsourced security operations, including threat

detection, incident response, vulnerability management, and 24/7 monitoring, to help organizations strengthen their cybersecurity postures without the need for extensive internal resources. MSSPs leverage advanced technologies such as Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR), and AI-driven analytics to detect and respond to threats in real-time, providing organizations with proactive threat hunting capabilities and actionable insights. This proactive approach is critical in mitigating risks and minimizing the impact of cyber attacks, particularly for organizations with limited cybersecurity expertise or resources. MSSPs offer scalable services tailored to the specific needs and risk profiles of organizations across various industries, from small businesses to large enterprises. By outsourcing security operations to MSSPs, organizations can benefit from access to specialized expertise, continuous threat intelligence updates, and compliance with industry regulations and standards.

The MSS market is expanding rapidly as organizations recognize the strategic advantages of partnering with MSSPs to enhance their cybersecurity defenses while optimizing operational efficiencies and reducing costs associated with managing cybersecurity internally. This trend is expected to continue as cybersecurity threats evolve and organizations prioritize proactive risk management and security resilience.

### Emphasis on Zero Trust Security Framework

There is a growing emphasis on implementing Zero Trust security frameworks across organizations as a proactive approach to mitigate cybersecurity risks. Zero Trust architecture assumes that threats may exist both inside and outside the network perimeter and requires strict identity verification and authorization for every person and device attempting to access resources. This approach minimizes the potential for breaches and lateral movement within networks by enforcing least privilege access controls and continuous monitoring of user and device behaviors.

Organizations are increasingly adopting Zero Trust principles to secure their digital assets, especially in response to the proliferation of remote workforces and cloud-based applications. Zero Trust frameworks help organizations achieve granular visibility and control over network traffic, applications, and data, reducing the attack surface and enhancing overall security posture. Key components of Zero Trust architecture include micro-segmentation, multifactor authentication (MFA), encryption, and continuous authentication, which collectively strengthen defenses against sophisticated cyber threats. Regulatory mandates and compliance requirements, such as GDPR and PCI DSS, are driving organizations to adopt Zero Trust principles to protect sensitive data



and ensure regulatory compliance. By implementing Zero Trust security models, organizations can align cybersecurity strategies with business objectives, enhance resilience against insider threats and external attacks, and improve overall risk management practices.

### Integration of Artificial Intelligence (AI) and Machine Learning (ML) in Cybersecurity

The integration of Artificial Intelligence (AI) and Machine Learning (ML) technologies is revolutionizing cybersecurity practices, enabling organizations to detect, analyze, and respond to cyber threats with greater speed and accuracy. AI and ML algorithms can analyze vast amounts of data in real-time to identify patterns, anomalies, and potential threats that may evade traditional security measures. This capability enhances threat detection capabilities, reduces response times, and enables proactive threat hunting and predictive analytics. AI-driven cybersecurity solutions encompass a range of applications, including behavior-based anomaly detection, predictive threat intelligence, automated incident response, and adaptive authentication. These technologies empower cybersecurity teams to prioritize and mitigate high-risk threats effectively while minimizing false positives and improving overall operational efficiency.

AI and ML algorithms can enhance cybersecurity resilience by continuously learning from new data and evolving threat landscapes, enabling adaptive security measures that can dynamically adjust defenses in response to emerging threats. This capability is particularly valuable in combating sophisticated cyber attacks such as zero-day exploits, polymorphic malware, and AI-driven social engineering attacks. As organizations embrace digital transformation and adopt increasingly complex IT infrastructures, the demand for AI-driven cybersecurity solutions is expected to grow. AI and ML technologies offer organizations the ability to augment human capabilities, improve threat detection and response capabilities, and strengthen defenses against evolving cyber threats. This trend underscores the transformative impact of AI and ML in shaping the future of cybersecurity services globally.

### Focus on Privacy and Data Protection

The heightened focus on privacy and data protection regulations worldwide is driving organizations to prioritize cybersecurity services that safeguard sensitive information and comply with stringent regulatory requirements. Regulations such as GDPR, CCPA (California Consumer Privacy Act), and the Personal Information Protection Law in China mandate organizations to implement robust security measures to protect personal data from unauthorized access, disclosure, and breaches. Cybersecurity

services providers are increasingly offering specialized solutions tailored to help organizations achieve and maintain compliance with data protection regulations. These solutions include data encryption, data masking, secure data storage, and privacy impact assessments (PIAs) to ensure that personal data is processed securely and in accordance with legal requirements.

Consumer awareness and expectations regarding data privacy have heightened, leading organizations to enhance transparency in data handling practices and strengthen customer trust through responsible data management. Cybersecurity services that emphasize privacy protection help organizations mitigate risks associated with data breaches, regulatory non-compliance, and reputational damage, thereby supporting sustainable business growth. The convergence of privacy regulations, evolving consumer expectations, and cybersecurity best practices is shaping the demand for comprehensive privacy-focused cybersecurity services. Organizations that prioritize privacy protection and adopt proactive measures to secure personal data are well-positioned to enhance customer loyalty, mitigate regulatory risks, and differentiate themselves in competitive markets.

## Segmental Insights

### Security Type Insights

Identity & Access Management (IAM) emerged as the dominant segment in the Global Cyber Security Services Market and is expected to maintain its leadership during the forecast period. IAM solutions play a critical role in enabling organizations to manage and control access to their networks, systems, applications, and data securely. With the proliferation of digital identities and the increasing complexity of IT environments, organizations are prioritizing IAM to strengthen security postures, ensure regulatory compliance, and mitigate insider threats. IAM solutions encompass functionalities such as single sign-on (SSO), multi-factor authentication (MFA), privileged access management (PAM), and identity governance and administration (IGA). These capabilities help organizations enforce least privilege access policies, authenticate user identities securely, and manage identities across diverse platforms and cloud environments. As businesses embrace digital transformation and adopt hybrid IT infrastructures, the demand for IAM solutions continues to grow, driven by the need to enhance operational efficiency, reduce security risks, and enable seamless access management across complex networks. IAM's ability to integrate with other cybersecurity technologies, such as cloud access security brokers (CASB) and security information and event management (SIEM) systems, further strengthens its position as

a cornerstone of comprehensive cybersecurity strategies. Moreover, IAM solutions contribute to cost savings by streamlining identity management processes, improving user productivity, and facilitating secure collaboration across distributed workforces. As organizations prioritize identity-centric security approaches to combat evolving cyber threats and address regulatory requirements, IAM is poised to remain a pivotal segment in the global cybersecurity services market, sustaining its dominance and driving innovation in identity and access management solutions.

### Size of Organization Insights

Large Enterprises emerged as the dominant segment in the Global Cyber Security Services Market and are expected to maintain their leadership during the forecast period. Large enterprises typically have extensive IT infrastructures, complex networks, and a higher risk profile due to their scale and industry presence. These organizations face sophisticated cyber threats, regulatory compliance requirements, and the need to protect vast amounts of sensitive data and intellectual property. As a result, large enterprises prioritize comprehensive cybersecurity services that encompass a wide range of solutions tailored to their specific needs. Key cybersecurity services favored by large enterprises include advanced threat detection and response, security consulting and advisory services, managed security services (MSS), and incident response planning. These services enable large enterprises to proactively detect and mitigate cyber threats, enhance resilience against cyber attacks, and maintain operational continuity. Moreover, large enterprises often allocate significant budgets for cybersecurity investments, allowing them to adopt cutting-edge technologies and solutions that integrate seamlessly with their existing IT environments. This strategic approach enables large enterprises to implement robust cybersecurity frameworks, enforce strict access controls, and ensure compliance with industry regulations and standards. Additionally, the scalability and customization offered by cybersecurity service providers cater to the complex needs of large enterprises, supporting their digital transformation initiatives while mitigating risks associated with evolving cyber threats. As large enterprises continue to prioritize cybersecurity as a critical aspect of their business strategies, the demand for specialized cybersecurity services tailored to their scale and operational requirements is expected to drive market growth and sustain their dominance in the global cybersecurity services market.

### Regional Insights

North America emerged as the dominant region in the Global Cyber Security Services Market and is expected to maintain its leadership during the forecast period. North

America's dominance can be attributed to several key factors, including a high concentration of technology-driven industries, stringent regulatory frameworks, and significant investments in cybersecurity initiatives. The region comprises leading cybersecurity service providers, innovative cybersecurity startups, and a mature market ecosystem that fosters continuous technological advancements and adoption of cybersecurity solutions. Industries such as finance, healthcare, government, and IT services in North America face sophisticated cyber threats due to their reliance on digital technologies, extensive data assets, and critical infrastructure. Consequently, there is a strong demand for cybersecurity services that offer comprehensive threat detection, incident response, compliance management, and risk mitigation strategies. Moreover, regulatory requirements such as GDPR in Europe and various privacy laws in the United States drive organizations to invest in robust cybersecurity measures to protect sensitive data and ensure regulatory compliance. North America's proactive approach to cybersecurity, coupled with strategic initiatives to enhance cybersecurity resilience across sectors, positions the region at the forefront of global cybersecurity services market growth. As cyber threats continue to evolve in complexity and frequency, North America's ongoing investment in cybersecurity innovation and collaboration between public and private sectors are expected to sustain its dominance and drive market expansion in the coming years.

### Key Market Players

Cisco Systems, Inc.

IBM Corporation

Palo Alto Networks, Inc.

Check Point Software Technologies Ltd.

Fortinet, Inc.

McAfee, LLC

Trend Micro, Incorporated.

Sophos Limited

CrowdStrike Inc.

Splunk Inc.

## Report Scope:

In this report, the Global Cyber Security Services Market has been segmented into the following categories, in addition to the industry trends which have also been detailed below:

Cyber Security Services Market, By Size of Organization:

Small & Medium Enterprises

Large Enterprises

Cyber Security Services Market, By Security Type:

Vulnerability & Security Assessment

Threat Intelligence & Business Analytics

Auditing & Logging

Continuous Monitoring & Encryption

Identity & Access Management

Cyber Security Services Market, By End-user Industry:

Healthcare

BFSI

IT & Telecom

Government

Energy & Utilities



## Cyber Security Services Market, By Region:

North America

United States

Canada

Mexico

Europe

France

United Kingdom

Italy

Germany

Spain

Belgium

Asia-Pacific

China

India

Japan

Australia

South Korea

Indonesia

Vietnam

South America

Brazil

Argentina

Colombia

Chile

Peru

Middle East & Africa

South Africa

Saudi Arabia

UAE

Turkey

Israel

## Competitive Landscape

**Company Profiles:** Detailed analysis of the major companies present in the Global Cyber Security Services Market.

## Available Customizations:

Global Cyber Security Services market report with the given market data, TechSci Research offers customizations according to a company's specific needs. The following customization options are available for the report:

## Company Information

Detailed analysis and profiling of additional market players (up to five).

## Contents

### **1. PRODUCT OVERVIEW**

- 1.1. Market Definition
- 1.2. Scope of the Market
  - 1.2.1. Markets Covered
  - 1.2.2. Years Considered for Study
  - 1.2.3. Key Market Segmentations

### **2. RESEARCH METHODOLOGY**

- 2.1. Objective of the Study
- 2.2. Baseline Methodology
- 2.3. Formulation of the Scope
- 2.4. Assumptions and Limitations
- 2.5. Sources of Research
  - 2.5.1. Secondary Research
  - 2.5.2. Primary Research
- 2.6. Approach for the Market Study
  - 2.6.1. The Bottom-Up Approach
  - 2.6.2. The Top-Down Approach
- 2.7. Methodology Followed for Calculation of Market Size & Market Shares
- 2.8. Forecasting Methodology
  - 2.8.1. Data Triangulation & Validation

### **3. EXECUTIVE SUMMARY**

### **4. IMPACT OF COVID-19 ON GLOBAL CYBER SECURITY SERVICES MARKET**

### **5. VOICE OF CUSTOMER**

### **6. GLOBAL CYBER SECURITY SERVICES MARKET OVERVIEW**

### **7. GLOBAL CYBER SECURITY SERVICES MARKET OUTLOOK**

- 7.1. Market Size & Forecast
  - 7.1.1. By Value
- 7.2. Market Share & Forecast

- 7.2.1. By Size of Organization (Small & Medium Enterprises, Large Enterprises)
- 7.2.2. By Security Type (Vulnerability & Security Assessment, Threat Intelligence & Business Analytics, Auditing & Logging, Continuous Monitoring & Encryption, Identity & Access Management)
- 7.2.3. By End-user Industry (Healthcare, BFSI, IT & Telecom, Government, Energy & Utilities)
- 7.2.4. By Region (North America, Europe, South America, Middle East & Africa, Asia Pacific)
- 7.3. By Company (2023)
- 7.4. Market Map

## **8. NORTH AMERICA CYBER SECURITY SERVICES MARKET OUTLOOK**

- 8.1. Market Size & Forecast
  - 8.1.1. By Value
- 8.2. Market Share & Forecast
  - 8.2.1. By Size of Organization
  - 8.2.2. By Security Type
  - 8.2.3. By End-user Industry
  - 8.2.4. By Country
- 8.3. North America: Country Analysis
  - 8.3.1. United States Cyber Security Services Market Outlook
    - 8.3.1.1. Market Size & Forecast
      - 8.3.1.1.1. By Value
    - 8.3.1.2. Market Share & Forecast
      - 8.3.1.2.1. By Size of Organization
      - 8.3.1.2.2. By Security Type
      - 8.3.1.2.3. By End-user Industry
  - 8.3.2. Canada Cyber Security Services Market Outlook
    - 8.3.2.1. Market Size & Forecast
      - 8.3.2.1.1. By Value
    - 8.3.2.2. Market Share & Forecast
      - 8.3.2.2.1. By Size of Organization
      - 8.3.2.2.2. By Security Type
      - 8.3.2.2.3. By End-user Industry
  - 8.3.3. Mexico Cyber Security Services Market Outlook
    - 8.3.3.1. Market Size & Forecast
      - 8.3.3.1.1. By Value
    - 8.3.3.2. Market Share & Forecast



- 8.3.3.2.1. By Size of Organization
- 8.3.3.2.2. By Security Type
- 8.3.3.2.3. By End-user Industry

## **9. EUROPE CYBER SECURITY SERVICES MARKET OUTLOOK**

### **9.1. Market Size & Forecast**

#### **9.1.1. By Value**

### **9.2. Market Share & Forecast**

#### **9.2.1. By Size of Organization**

#### **9.2.2. By Security Type**

#### **9.2.3. By End-user Industry**

#### **9.2.4. By Country**

### **9.3. Europe: Country Analysis**

#### **9.3.1. Germany Cyber Security Services Market Outlook**

##### **9.3.1.1. Market Size & Forecast**

###### **9.3.1.1.1. By Value**

##### **9.3.1.2. Market Share & Forecast**

###### **9.3.1.2.1. By Size of Organization**

###### **9.3.1.2.2. By Security Type**

###### **9.3.1.2.3. By End-user Industry**

#### **9.3.2. France Cyber Security Services Market Outlook**

##### **9.3.2.1. Market Size & Forecast**

###### **9.3.2.1.1. By Value**

##### **9.3.2.2. Market Share & Forecast**

###### **9.3.2.2.1. By Size of Organization**

###### **9.3.2.2.2. By Security Type**

###### **9.3.2.2.3. By End-user Industry**

#### **9.3.3. United Kingdom Cyber Security Services Market Outlook**

##### **9.3.3.1. Market Size & Forecast**

###### **9.3.3.1.1. By Value**

##### **9.3.3.2. Market Share & Forecast**

###### **9.3.3.2.1. By Size of Organization**

###### **9.3.3.2.2. By Security Type**

###### **9.3.3.2.3. By End-user Industry**

#### **9.3.4. Italy Cyber Security Services Market Outlook**

##### **9.3.4.1. Market Size & Forecast**

###### **9.3.4.1.1. By Value**

##### **9.3.4.2. Market Share & Forecast**

- 9.3.4.2.1. By Size of Organization
- 9.3.4.2.2. By Security Type
- 9.3.4.2.3. By End-user Industry
- 9.3.5. Spain Cyber Security Services Market Outlook
  - 9.3.5.1. Market Size & Forecast
    - 9.3.5.1.1. By Value
  - 9.3.5.2. Market Share & Forecast
    - 9.3.5.2.1. By Size of Organization
    - 9.3.5.2.2. By Security Type
    - 9.3.5.2.3. By End-user Industry
- 9.3.6. Belgium Cyber Security Services Market Outlook
  - 9.3.6.1. Market Size & Forecast
    - 9.3.6.1.1. By Value
  - 9.3.6.2. Market Share & Forecast
    - 9.3.6.2.1. By Size of Organization
    - 9.3.6.2.2. By Security Type
    - 9.3.6.2.3. By End-user Industry

## **10. SOUTH AMERICA CYBER SECURITY SERVICES MARKET OUTLOOK**

- 10.1. Market Size & Forecast
  - 10.1.1. By Value
- 10.2. Market Share & Forecast
  - 10.2.1. By Size of Organization
  - 10.2.2. By Security Type
  - 10.2.3. By End-user Industry
  - 10.2.4. By Country
- 10.3. South America: Country Analysis
  - 10.3.1. Brazil Cyber Security Services Market Outlook
    - 10.3.1.1. Market Size & Forecast
      - 10.3.1.1.1. By Value
    - 10.3.1.2. Market Share & Forecast
      - 10.3.1.2.1. By Size of Organization
      - 10.3.1.2.2. By Security Type
      - 10.3.1.2.3. By End-user Industry
  - 10.3.2. Colombia Cyber Security Services Market Outlook
    - 10.3.2.1. Market Size & Forecast
      - 10.3.2.1.1. By Value
    - 10.3.2.2. Market Share & Forecast

- 10.3.2.2.1. By Size of Organization
- 10.3.2.2.2. By Security Type
- 10.3.2.2.3. By End-user Industry
- 10.3.3. Argentina Cyber Security Services Market Outlook
  - 10.3.3.1. Market Size & Forecast
    - 10.3.3.1.1. By Value
  - 10.3.3.2. Market Share & Forecast
    - 10.3.3.2.1. By Size of Organization
    - 10.3.3.2.2. By Security Type
    - 10.3.3.2.3. By End-user Industry
- 10.3.4. Chile Cyber Security Services Market Outlook
  - 10.3.4.1. Market Size & Forecast
    - 10.3.4.1.1. By Value
  - 10.3.4.2. Market Share & Forecast
    - 10.3.4.2.1. By Size of Organization
    - 10.3.4.2.2. By Security Type
    - 10.3.4.2.3. By End-user Industry
- 10.3.5. Peru Cyber Security Services Market Outlook
  - 10.3.5.1. Market Size & Forecast
    - 10.3.5.1.1. By Value
  - 10.3.5.2. Market Share & Forecast
    - 10.3.5.2.1. By Size of Organization
    - 10.3.5.2.2. By Security Type
    - 10.3.5.2.3. By End-user Industry

## **11. MIDDLE EAST & AFRICA CYBER SECURITY SERVICES MARKET OUTLOOK**

- 11.1. Market Size & Forecast
  - 11.1.1. By Value
- 11.2. Market Share & Forecast
  - 11.2.1. By Size of Organization
  - 11.2.2. By Security Type
  - 11.2.3. By End-user Industry
  - 11.2.4. By Country
- 11.3. Middle East & Africa: Country Analysis
  - 11.3.1. Saudi Arabia Cyber Security Services Market Outlook
    - 11.3.1.1. Market Size & Forecast
      - 11.3.1.1.1. By Value
    - 11.3.1.2. Market Share & Forecast

- 11.3.1.2.1. By Size of Organization
- 11.3.1.2.2. By Security Type
- 11.3.1.2.3. By End-user Industry
- 11.3.2. UAE Cyber Security Services Market Outlook
  - 11.3.2.1. Market Size & Forecast
    - 11.3.2.1.1. By Value
  - 11.3.2.2. Market Share & Forecast
    - 11.3.2.2.1. By Size of Organization
    - 11.3.2.2.2. By Security Type
    - 11.3.2.2.3. By End-user Industry
- 11.3.3. South Africa Cyber Security Services Market Outlook
  - 11.3.3.1. Market Size & Forecast
    - 11.3.3.1.1. By Value
  - 11.3.3.2. Market Share & Forecast
    - 11.3.3.2.1. By Size of Organization
    - 11.3.3.2.2. By Security Type
    - 11.3.3.2.3. By End-user Industry
- 11.3.4. Turkey Cyber Security Services Market Outlook
  - 11.3.4.1. Market Size & Forecast
    - 11.3.4.1.1. By Value
  - 11.3.4.2. Market Share & Forecast
    - 11.3.4.2.1. By Size of Organization
    - 11.3.4.2.2. By Security Type
    - 11.3.4.2.3. By End-user Industry
- 11.3.5. Israel Cyber Security Services Market Outlook
  - 11.3.5.1. Market Size & Forecast
    - 11.3.5.1.1. By Value
  - 11.3.5.2. Market Share & Forecast
    - 11.3.5.2.1. By Size of Organization
    - 11.3.5.2.2. By Security Type
    - 11.3.5.2.3. By End-user Industry

## **12. ASIA PACIFIC CYBER SECURITY SERVICES MARKET OUTLOOK**

- 12.1. Market Size & Forecast
  - 12.1.1. By Value
- 12.2. Market Share & Forecast
  - 12.2.1. By Size of Organization
  - 12.2.2. By Security Type

12.2.3. By End-user Industry

12.2.4. By Country

12.3. Asia-Pacific: Country Analysis

12.3.1. China Cyber Security Services Market Outlook

12.3.1.1. Market Size & Forecast

12.3.1.1.1. By Value

12.3.1.2. Market Share & Forecast

12.3.1.2.1. By Size of Organization

12.3.1.2.2. By Security Type

12.3.1.2.3. By End-user Industry

12.3.2. India Cyber Security Services Market Outlook

12.3.2.1. Market Size & Forecast

12.3.2.1.1. By Value

12.3.2.2. Market Share & Forecast

12.3.2.2.1. By Size of Organization

12.3.2.2.2. By Security Type

12.3.2.2.3. By End-user Industry

12.3.3. Japan Cyber Security Services Market Outlook

12.3.3.1. Market Size & Forecast

12.3.3.1.1. By Value

12.3.3.2. Market Share & Forecast

12.3.3.2.1. By Size of Organization

12.3.3.2.2. By Security Type

12.3.3.2.3. By End-user Industry

12.3.4. South Korea Cyber Security Services Market Outlook

12.3.4.1. Market Size & Forecast

12.3.4.1.1. By Value

12.3.4.2. Market Share & Forecast

12.3.4.2.1. By Size of Organization

12.3.4.2.2. By Security Type

12.3.4.2.3. By End-user Industry

12.3.5. Australia Cyber Security Services Market Outlook

12.3.5.1. Market Size & Forecast

12.3.5.1.1. By Value

12.3.5.2. Market Share & Forecast

12.3.5.2.1. By Size of Organization

12.3.5.2.2. By Security Type

12.3.5.2.3. By End-user Industry

12.3.6. Indonesia Cyber Security Services Market Outlook



- 12.3.6.1. Market Size & Forecast
  - 12.3.6.1.1. By Value
- 12.3.6.2. Market Share & Forecast
  - 12.3.6.2.1. By Size of Organization
  - 12.3.6.2.2. By Security Type
  - 12.3.6.2.3. By End-user Industry
- 12.3.7. Vietnam Cyber Security Services Market Outlook
  - 12.3.7.1. Market Size & Forecast
    - 12.3.7.1.1. By Value
  - 12.3.7.2. Market Share & Forecast
    - 12.3.7.2.1. By Size of Organization
    - 12.3.7.2.2. By Security Type
    - 12.3.7.2.3. By End-user Industry

## **13. MARKET DYNAMICS**

- 13.1. Drivers
- 13.2. Challenges

## **14. MARKET TRENDS AND DEVELOPMENTS**

## **15. COMPANY PROFILES**

- 15.1. Cisco Systems, Inc.
  - 15.1.1. Business Overview
  - 15.1.2. Key Revenue and Financials
  - 15.1.3. Recent Developments
  - 15.1.4. Key Personnel/Key Contact Person
  - 15.1.5. Key Product/Services Offered
- 15.2. IBM Corporation
  - 15.2.1. Business Overview
  - 15.2.2. Key Revenue and Financials
  - 15.2.3. Recent Developments
  - 15.2.4. Key Personnel/Key Contact Person
  - 15.2.5. Key Product/Services Offered
- 15.3. Palo Alto Networks, Inc.
  - 15.3.1. Business Overview
  - 15.3.2. Key Revenue and Financials
  - 15.3.3. Recent Developments

- 15.3.4. Key Personnel/Key Contact Person
- 15.3.5. Key Product/Services Offered
- 15.4. Check Point Software Technologies Ltd.
  - 15.4.1. Business Overview
  - 15.4.2. Key Revenue and Financials
  - 15.4.3. Recent Developments
  - 15.4.4. Key Personnel/Key Contact Person
  - 15.4.5. Key Product/Services Offered
- 15.5. Fortinet, Inc.
  - 15.5.1. Business Overview
  - 15.5.2. Key Revenue and Financials
  - 15.5.3. Recent Developments
  - 15.5.4. Key Personnel/Key Contact Person
  - 15.5.5. Key Product/Services Offered
- 15.6. McAfee, LLC
  - 15.6.1. Business Overview
  - 15.6.2. Key Revenue and Financials
  - 15.6.3. Recent Developments
  - 15.6.4. Key Personnel/Key Contact Person
  - 15.6.5. Key Product/Services Offered
- 15.7. Trend Micro, Incorporated.
  - 15.7.1. Business Overview
  - 15.7.2. Key Revenue and Financials
  - 15.7.3. Recent Developments
  - 15.7.4. Key Personnel/Key Contact Person
  - 15.7.5. Key Product/Services Offered
- 15.8. Sophos Limited
  - 15.8.1. Business Overview
  - 15.8.2. Key Revenue and Financials
  - 15.8.3. Recent Developments
  - 15.8.4. Key Personnel/Key Contact Person
  - 15.8.5. Key Product/Services Offered
- 15.9. CrowdStrike Inc.
  - 15.9.1. Business Overview
  - 15.9.2. Key Revenue and Financials
  - 15.9.3. Recent Developments
  - 15.9.4. Key Personnel/Key Contact Person
  - 15.9.5. Key Product/Services Offered
- 15.10. Splunk Inc.

- 15.10.1. Business Overview
- 15.10.2. Key Revenue and Financials
- 15.10.3. Recent Developments
- 15.10.4. Key Personnel/Key Contact Person
- 15.10.5. Key Product/Services Offered

## **16. STRATEGIC RECOMMENDATIONS**

## **17. ABOUT US & DISCLAIMER**

## I would like to order

Product name: Cyber Security Services Market – Global Industry Size, Share, Trends, Opportunity, and Forecast, Segmented By Size of Organization (Small & Medium Enterprises, Large Enterprises), By Security Type (Vulnerability & Security Assessment, Threat Intelligence & Business Analytics, Auditing & Logging, Continuous Monitoring & Encryption, Identity & Access Management), By End-user Industry (Healthcare, BFSI, IT & Telecom, Government, Energy & Utilities), By Region & Competition, 2019-2029F

Product link: <https://marketpublishers.com/r/C58617AF2BB4EN.html>

Price: US\$ 4,500.00 (Single User License / Electronic Delivery)

If you want to order Corporate License or Hard Copy, please, contact our Customer Service:

[info@marketpublishers.com](mailto:info@marketpublishers.com)

## Payment

To pay by Credit Card (Visa, MasterCard, American Express, PayPal), please, click button on product page <https://marketpublishers.com/r/C58617AF2BB4EN.html>

To pay by Wire Transfer, please, fill in your contact details in the form below:

First name:

Last name:

Email:

Company:

Address:

City:

Zip code:

Country:

Tel:

Fax:

Your message:

**\*\*All fields are required**

Customer signature \_\_\_\_\_

Please, note that by ordering from marketpublishers.com you are agreeing to our Terms

& Conditions at <https://marketpublishers.com/docs/terms.html>

To place an order via fax simply print this form, fill in the information below  
and fax the completed form to +44 20 7900 3970