

# **Data Protection Market - Global Industry Size, Share, Trends, Opportunity, and Forecast Segmented By Deployment Mode (Cloud and On-premise), By Organization Size (Small & Medium-sized Enterprises (SMEs) and Large Enterprises), By End-User (BFSI, Healthcare, IT & Telecom, Government and Others), By Region, and By Competition, 2019-2029F**

<https://marketpublishers.com/r/DA5022FDA536EN.html>

Date: May 2024

Pages: 186

Price: US\$ 4,900.00 (Single User License)

ID: DA5022FDA536EN

## **Abstracts**

Global Data Protection Market was valued at USD 73.29 billion in 2023 and is anticipated to project robust growth in the forecast period with a CAGR of 16.38% through 2029. The global landscape of data privacy regulations has become more stringent in response to the rising concerns about the misuse of personal information. Regulations such as the General Data Protection Regulation (GDPR) in Europe, the California Consumer Privacy Act (CCPA) in the United States, and similar laws worldwide mandate organizations to implement robust data protection measures. The need for compliance with these regulations acts as a significant driver for the adoption of comprehensive data protection solutions.

### **Key Market Drivers**

#### **Increasing Cybersecurity Threats and Data Breaches**

In recent years, the proliferation of digital technologies and the interconnected nature of global business operations have given rise to a significant increase in cybersecurity threats and data breaches. As organizations become more reliant on digital data for their day-to-day operations, the need to protect sensitive information from unauthorized access has become paramount. This escalating threat landscape has become a major

driver for the global data protection market.

Organizations across various industries are recognizing the critical importance of safeguarding their data assets, including customer information, intellectual property, and financial records. The financial and reputational repercussions of a data breach can be severe, leading to loss of customer trust, legal liabilities, and financial losses. Consequently, businesses are investing heavily in robust data protection solutions to mitigate the risks associated with cyber threats.

The global data protection market is witnessing a surge in demand for advanced security measures, such as encryption, multi-factor authentication, and threat intelligence, to fortify defenses against evolving cyber threats. As regulations governing data privacy become more stringent globally, organizations are compelled to adopt comprehensive data protection strategies to ensure compliance and avoid hefty fines. This increased focus on cybersecurity is propelling the growth of the global data protection market.

### Evolving Data Privacy Regulations and Compliance Requirements

Governments around the world are enacting and strengthening data protection and privacy regulations to address the growing concerns related to the misuse of personal information. Regulations such as the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA) in the United States are compelling organizations to adhere to strict data protection standards. The complex and evolving nature of these regulations is a significant driver for the global data protection market.

To comply with these regulations, businesses are required to implement robust data protection measures, including data encryption, access controls, and auditing capabilities. The need for comprehensive solutions that can adapt to evolving regulatory landscapes is fueling the demand for advanced data protection technologies and services. Organizations are seeking integrated solutions that not only provide compliance but also offer a holistic approach to data security and privacy.

The global data protection market is responding to this demand by offering solutions that not only meet current regulatory requirements but also anticipate future changes in data privacy laws. Companies providing data protection services are partnering with legal experts to stay abreast of regulatory developments, ensuring that their solutions align with the latest compliance standards. This alignment with evolving regulations is a

key driver propelling the growth of the global data protection market.

### Proliferation of Cloud Computing and Mobile Devices

The widespread adoption of cloud computing and the ubiquitous use of mobile devices have revolutionized the way businesses operate, providing increased flexibility and accessibility to data. However, this shift towards a more interconnected and mobile-centric work environment has also introduced new challenges related to data security. The need to secure data across diverse platforms and devices is a significant driver for the global data protection market.

Organizations are increasingly relying on cloud services to store and manage their data, making it imperative to implement robust data protection mechanisms in cloud environments. Additionally, the proliferation of mobile devices in the workplace introduces new vulnerabilities that can be exploited by malicious actors. As employees access corporate data from various locations and devices, the risk of data exposure and unauthorized access escalates.

To address these challenges, the global data protection market is witnessing a surge in demand for solutions that offer seamless integration with cloud platforms and provide comprehensive mobile device management features. Encryption, secure access controls, and data loss prevention technologies are becoming essential components of data protection strategies in the era of cloud computing and mobile workforces. The increasing adoption of these technologies to safeguard data across diverse environments is a key driver propelling the expansion of the global data protection market.

### Key Market Challenges

#### Rapidly Evolving Cyber Threat Landscape

One of the foremost challenge facing the Global Data Protection Market is the continuously evolving and sophisticated nature of the cyber threat landscape. As technology advances, cybercriminals are quick to adapt, employing increasingly sophisticated techniques to breach security measures. This dynamic environment poses a significant challenge for data protection solutions, requiring constant innovation and updates to stay ahead of emerging threats.

The rapid emergence of new cyber threats, such as ransomware, zero-day

vulnerabilities, and advanced persistent threats, presents an ongoing challenge for organizations seeking to safeguard their sensitive data. Traditional data protection methods may struggle to keep pace with the speed and complexity of these evolving threats. Consequently, companies investing in data protection solutions find themselves in a perpetual race to enhance their cybersecurity measures to effectively counter the latest tactics employed by malicious actors.

Addressing this challenge necessitates a proactive approach to cybersecurity, emphasizing threat intelligence, continuous monitoring, and real-time response mechanisms. The Global Data Protection Market must grapple with the need for solutions that not only offer robust protection against known threats but also possess the agility to adapt to novel and unforeseen cybersecurity risks.

### Regulatory Complexity and Global Variability

Another challenge confronting the Global Data Protection Market is the complex and varied landscape of data protection regulations worldwide. Different countries and regions have established distinct frameworks governing the collection, storage, and processing of personal data, imposing a significant compliance burden on organizations operating globally. This regulatory complexity is a formidable challenge for companies seeking to ensure comprehensive and consistent data protection practices across diverse jurisdictions.

The implementation of regulations such as the General Data Protection Regulation (GDPR) in Europe, the California Consumer Privacy Act (CCPA) in the United States, and various other regional data protection laws requires a nuanced understanding of specific requirements and mandates. Companies conducting business across borders must navigate a maze of legal intricacies to establish and maintain compliance with these regulations.

As the regulatory landscape continues to evolve, data protection solutions face the challenge of offering flexible and adaptable frameworks that can accommodate changes in legislation without causing significant disruptions to business operations. Achieving a balance between stringent compliance and operational efficiency is a delicate task for the Global Data Protection Market, necessitating continuous monitoring of regulatory developments and agile adjustments to ensure ongoing adherence to data protection standards.

### Balancing Security and Usability in an Interconnected World

The third challenge confronting the Global Data Protection Market revolves around finding the delicate balance between robust security measures and user-friendly experiences in an increasingly interconnected world. While enhancing security is paramount, overly complex or cumbersome data protection measures may hinder user productivity and adoption. Striking the right balance between security and usability is a perpetual challenge that requires careful consideration of user needs and preferences.

In today's interconnected business environment, where collaboration and data sharing are integral to operations, implementing security measures that do not impede the seamless flow of information is critical. Organizations face the challenge of implementing data protection solutions that are both effective in safeguarding sensitive information and user-friendly to encourage widespread adoption.

To address this challenge, data protection solutions need to integrate seamlessly into existing workflows, providing a frictionless experience for end-users. User education and awareness programs also play a crucial role in mitigating the challenges associated with balancing security and usability, ensuring that individuals within organizations understand the importance of adhering to data protection protocols without sacrificing productivity. The Global Data Protection Market must navigate this delicate equilibrium to deliver solutions that prioritize security without compromising the ease of use essential for today's interconnected digital landscape.

## Key Market Trends

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

A prominent trend shaping the Global Data Protection Market is the increasing integration of artificial intelligence (AI) and machine learning (ML) technologies. As the volume and complexity of data continue to grow exponentially, traditional data protection methods are facing limitations in effectively identifying and mitigating emerging threats. AI and ML offer a transformative solution by augmenting the capabilities of data protection systems to detect, analyze, and respond to evolving cybersecurity risks.

AI and ML algorithms empower data protection solutions to enhance threat detection and response capabilities in real-time. These technologies excel in identifying patterns, anomalies, and potential security breaches that may go unnoticed by conventional security measures. By continuously learning from historical data and adapting to new

threats, AI and ML-driven data protection solutions provide a proactive defense against a wide range of cyber threats, including sophisticated malware, phishing attacks, and insider threats.

One key application of AI and ML in data protection is in the development of predictive analytics for risk assessment. These technologies can analyze vast datasets to identify potential vulnerabilities and predict future security risks, allowing organizations to implement preemptive measures to safeguard their data. Additionally, AI and ML contribute to the automation of routine security tasks, freeing up cybersecurity professionals to focus on more complex and strategic aspects of data protection.

The integration of AI and ML in the Global Data Protection Market is expected to continue evolving, with an emphasis on improving accuracy, reducing false positives, and adapting to the dynamic nature of cyber threats. As organizations seek comprehensive and adaptive data protection solutions, the role of AI and ML technologies will become increasingly pivotal in fortifying defenses against emerging cybersecurity challenges.

#### Adoption of Zero Trust Security Frameworks

Another significant trend in the Global Data Protection Market is the widespread adoption of Zero Trust security frameworks. Traditionally, cybersecurity models relied on the concept of a perimeter-based defense, assuming that threats could be kept at bay by securing the network perimeter. However, the evolving threat landscape, characterized by advanced and persistent cyberattacks, has prompted a shift towards a Zero Trust approach, acknowledging that threats can originate from both external and internal sources.

Zero Trust security operates on the principle of 'never trust, always verify.' This model assumes that no user or device, whether inside or outside the corporate network, should be automatically trusted. Instead, every user and device must undergo continuous verification before being granted access to sensitive data or systems. This approach minimizes the risk of unauthorized access and lateral movement within the network, enhancing overall data protection.

Key components of the Zero Trust model include multifactor authentication, continuous monitoring, micro-segmentation, and least privilege access. Organizations implementing Zero Trust frameworks aim to establish granular control over access permissions, ensuring that users and devices have the minimum level of access necessary for their

specific roles. This not only enhances security but also helps in preventing the unauthorized exfiltration of sensitive data.

The adoption of Zero Trust security frameworks in the Global Data Protection Market is driven by the need for a more robust and adaptive security posture. As organizations recognize the limitations of traditional perimeter-based defenses, Zero Trust models offer a proactive and dynamic approach to data protection, aligning with the evolving nature of cybersecurity threats. This trend is expected to gain further momentum as companies prioritize comprehensive strategies that address both external and internal security challenges.

## Segmental Insights

### Deployment Mode Insights

The Cloud segment emerged as the dominating segment in 2023. The cloud segment of the Global Data Protection Market has witnessed substantial growth and transformation, driven by the increasing adoption of cloud computing services across industries. As organizations transition from traditional on-premises data storage to cloud-based solutions, the dynamics of data protection have evolved, presenting both opportunities and challenges within the cloud segment.

The shift toward cloud-native data protection solutions is a significant trend within the cloud segment of the Global Data Protection Market. Organizations are increasingly leveraging cloud-based technologies to optimize scalability, flexibility, and cost-effectiveness. In response to this trend, data protection providers are developing solutions specifically designed for cloud environments, offering seamless integration with popular cloud platforms such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform.

Cloud-native data protection solutions provide advantages such as automatic scalability, simplified management, and the ability to adapt to the dynamic nature of cloud workloads. These solutions often leverage containerization and microservices architectures, allowing organizations to deploy and manage data protection processes more efficiently in the cloud. The growing popularity of cloud-native solutions reflects a broader industry shift toward embracing cloud technologies for comprehensive data protection strategies.

## Regional Insights

North America emerged as the dominating region in 2023, holding the largest market share. Data protection solutions in North America need to align with these regulations to ensure compliance. As a result, there is a growing demand for solutions that offer features such as data encryption, access controls, and auditing capabilities to help organizations meet regulatory requirements and avoid potential legal liabilities.

North American enterprises are quick to adopt advanced technologies, and this holds true for the data protection market. The region has witnessed a surge in the adoption of cloud-based data protection solutions, leveraging the benefits of scalability, flexibility, and cost-effectiveness. The integration of artificial intelligence (AI) and machine learning (ML) in data protection strategies is also notable, with organizations seeking advanced threat detection and response capabilities.

The healthcare sector in North America, given its significance and the sensitivity of patient information, has become a focal point for data protection efforts. The healthcare industry is a major consumer of data protection solutions, with a focus on securing electronic health records (EHRs), ensuring compliance with healthcare regulations (such as HIPAA), and safeguarding patient privacy.

The demand for data protection solutions in the healthcare sector extends beyond traditional cybersecurity measures. There is a growing need for solutions that address the unique challenges of healthcare data, including interoperability, secure sharing of patient information among authorized entities, and protection against insider threats.

High-profile data breaches and cyberattacks have raised cybersecurity awareness in North America. Organizations across industries, from finance to critical infrastructure, are prioritizing cybersecurity and data protection. This increased awareness is translating into a growing market for comprehensive data protection solutions that offer not only robust security measures but also proactive threat intelligence and incident response capabilities.

Cybersecurity awareness is further amplified by collaboration between the public and private sectors. Government initiatives, industry collaborations, and information-sharing forums contribute to a collective effort to enhance the overall cybersecurity posture in North America.

The shift towards remote work, accelerated by global events, has prompted organizations in North America to reevaluate and reinforce their data protection



strategies. The increasing reliance on remote work infrastructure has led to a demand for solutions that secure endpoints, facilitate secure collaboration, and provide visibility into data access and usage outside traditional office environments.

The North American segment of the Global Data Protection Market is characterized by a stringent regulatory landscape, a focus on adopting advanced technologies, special attention to data protection in healthcare, increased cybersecurity awareness, and emerging trends related to remote work security. These factors collectively contribute to a dynamic and evolving market in the region, with organizations actively seeking innovative data protection solutions to secure their digital assets.

### Key Market Players

IBM Corporation

Gen Digital Inc.

Nextlabs Inc.

Oracle Corporation

McAfee Corporation

Hewlett-Packard Development Company LP

NetApp Inc.

Quest Software Inc.

Veeam Software Group GmbH

Acronis International GmbH

### Report Scope:

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

Data Protection Market, By Deployment Mode:

Cloud

On-premises

Data Protection Market, By Organization Size:

Small & Medium-sized Enterprises (SMEs)

Large Enterprises

Data Protection Market, By End-User:

BFSI

Government

IT & Telecom

Healthcare

Others

Data Protection Market, By Region:

North America

United States

Canada

Mexico

Europe

France

United Kingdom

Italy

Germany

Spain

Netherlands

Belgium

Asia-Pacific

China

India

Japan

Australia

South Korea

Thailand

Malaysia

South America

Brazil

Argentina

Colombia

Chile

Middle East & Africa

South Africa

Saudi Arabia

UAE

Turkey

### Competitive Landscape

Company Profiles: Detailed analysis of the major companies present in the Global Data Protection Market.

### Available Customizations:

Global Data Protection 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. SERVICES 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 DATA PROTECTION MARKET**

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

### **6. GLOBAL DATA PROTECTION MARKET OVERVIEW**

### **7. GLOBAL DATA PROTECTION MARKET OUTLOOK**

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

- 7.2.1.By Deployment Mode (Cloud and On-premise)
- 7.2.2.By Organization Size (Small & Medium-sized Enterprises (SMEs) and Large Enterprises)
- 7.2.3.By End-User (BFSI, Healthcare, IT & Telecom, Government and Others)
- 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 DATA PROTECTION MARKET OUTLOOK**

- 8.1. Market Size & Forecast
  - 8.1.1.By Value
- 8.2. Market Share & Forecast
  - 8.2.1.By Deployment Mode
  - 8.2.2.By Organization Size
  - 8.2.3.By End-User
  - 8.2.4.By Country
- 8.3. North America: Country Analysis
  - 8.3.1.United States Data Protection 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 Deployment Mode
      - 8.3.1.2.2. By Organization Size
      - 8.3.1.2.3. By End-User
  - 8.3.2.Canada Data Protection 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 Deployment Mode
      - 8.3.2.2.2. By Organization Size
      - 8.3.2.2.3. By End-User
  - 8.3.3.Mexico Data Protection 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 Deployment Mode
      - 8.3.3.2.2. By Organization Size

8.3.3.2.3. By End-User

## 9. EUROPE DATA PROTECTION MARKET OUTLOOK

9.1. Market Size & Forecast

9.1.1. By Value

9.2. Market Share & Forecast

9.2.1. By Deployment Mode

9.2.2. By Organization Size

9.2.3. By End-User

9.2.4. By Country

9.3. Europe: Country Analysis

9.3.1. Germany Data Protection 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 Deployment Mode

9.3.1.2.2. By Organization Size

9.3.1.2.3. By End-User

9.3.2. France Data Protection 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 Deployment Mode

9.3.2.2.2. By Organization Size

9.3.2.2.3. By End-User

9.3.3. United Kingdom Data Protection 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 Deployment Mode

9.3.3.2.2. By Organization Size

9.3.3.2.3. By End-User

9.3.4. Italy Data Protection 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 Deployment Mode

9.3.4.2.2. By Organization Size

- 9.3.4.2.3. By End-User
- 9.3.5. Spain Data Protection 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 Deployment Mode
    - 9.3.5.2.2. By Organization Size
    - 9.3.5.2.3. By End-User
- 9.3.6. Netherlands Data Protection 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 Deployment Mode
    - 9.3.6.2.2. By Organization Size
    - 9.3.6.2.3. By End-User
- 9.3.7. Belgium Data Protection Market Outlook
  - 9.3.7.1. Market Size & Forecast
    - 9.3.7.1.1. By Value
  - 9.3.7.2. Market Share & Forecast
    - 9.3.7.2.1. By Deployment Mode
    - 9.3.7.2.2. By Organization Size
    - 9.3.7.2.3. By End-User

## **10. SOUTH AMERICA DATA PROTECTION MARKET OUTLOOK**

- 10.1. Market Size & Forecast
  - 10.1.1. By Value
- 10.2. Market Share & Forecast
  - 10.2.1. By Deployment Mode
  - 10.2.2. By Organization Size
  - 10.2.3. By End-User
  - 10.2.4. By Country
- 10.3. South America: Country Analysis
  - 10.3.1. Brazil Data Protection 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 Deployment Mode
      - 10.3.1.2.2. By Organization Size



- 10.3.1.2.3. By End-User
- 10.3.2. Colombia Data Protection 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 Deployment Mode
    - 10.3.2.2.2. By Organization Size
    - 10.3.2.2.3. By End-User
- 10.3.3. Argentina Data Protection 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 Deployment Mode
    - 10.3.3.2.2. By Organization Size
    - 10.3.3.2.3. By End-User
- 10.3.4. Chile Data Protection 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 Deployment Mode
    - 10.3.4.2.2. By Organization Size
    - 10.3.4.2.3. By End-User

## **11. MIDDLE EAST & AFRICA DATA PROTECTION MARKET OUTLOOK**

- 11.1. Market Size & Forecast
  - 11.1.1. By Value
- 11.2. Market Share & Forecast
  - 11.2.1. By Deployment Mode
  - 11.2.2. By Organization Size
  - 11.2.3. By End-User
  - 11.2.4. By Country
- 11.3. Middle East & Africa: Country Analysis
  - 11.3.1. Saudi Arabia Data Protection 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 Deployment Mode
      - 11.3.1.2.2. By Organization Size

- 11.3.1.2.3. By End-User
- 11.3.2. UAE Data Protection 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 Deployment Mode
    - 11.3.2.2.2. By Organization Size
    - 11.3.2.2.3. By End-User
- 11.3.3. South Africa Data Protection 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 Deployment Mode
    - 11.3.3.2.2. By Organization Size
    - 11.3.3.2.3. By End-User
- 11.3.4. Turkey Data Protection 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 Deployment Mode
    - 11.3.4.2.2. By Organization Size
    - 11.3.4.2.3. By End-User

## **12. ASIA-PACIFIC DATA PROTECTION MARKET OUTLOOK**

- 12.1. Market Size & Forecast
  - 12.1.1. By Value
- 12.2. Market Share & Forecast
  - 12.2.1. By Deployment Mode
  - 12.2.2. By Organization Size
  - 12.2.3. By End-User
  - 12.2.4. By Country
- 12.3. Asia-Pacific: Country Analysis
  - 12.3.1. China Data Protection 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 Deployment Mode
      - 12.3.1.2.2. By Organization Size

- 12.3.1.2.3. By End-User
- 12.3.2. India Data Protection 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 Deployment Mode
    - 12.3.2.2.2. By Organization Size
    - 12.3.2.2.3. By End-User
- 12.3.3. Japan Data Protection 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 Deployment Mode
    - 12.3.3.2.2. By Organization Size
    - 12.3.3.2.3. By End-User
- 12.3.4. South Korea Data Protection 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 Deployment Mode
    - 12.3.4.2.2. By Organization Size
    - 12.3.4.2.3. By End-User
- 12.3.5. Australia Data Protection 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 Deployment Mode
    - 12.3.5.2.2. By Organization Size
    - 12.3.5.2.3. By End-User
- 12.3.6. Thailand Data Protection 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 Deployment Mode
    - 12.3.6.2.2. By Organization Size
    - 12.3.6.2.3. By End-User
- 12.3.7. Malaysia Data Protection 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 Deployment Mode

12.3.7.2.2. By Organization Size

12.3.7.2.3. By End-User

### **13. MARKET DYNAMICS**

13.1. Drivers

13.2. Challenges

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

### **15. COMPANY PROFILES**

15.1. IBM Corporation

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. Gen Digital Inc.

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. Nextlabs 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. Oracle Corporation

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. McAfee Corporation

- 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. Hewlett-Packard Development Company LP
  - 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. NetApp Inc.
  - 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. Quest Software Inc.
  - 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. Veeam Software Group GmbH
  - 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. Acronis International GmbH
  - 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: Data Protection Market - Global Industry Size, Share, Trends, Opportunity, and Forecast Segmented By Deployment Mode (Cloud and On-premise), By Organization Size (Small & Medium-sized Enterprises (SMEs) and Large Enterprises), By End-User (BFSI, Healthcare, IT & Telecom, Government and Others), By Region, and By Competition, 2019-2029F

Product link: <https://marketpublishers.com/r/DA5022FDA536EN.html>

Price: US\$ 4,900.00 (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/DA5022FDA536EN.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