

Global Data Protection as a Service (DPaaS) Market Segmented by Service Type (Storage-as-a-Service, Backup-as-a-Service, and Disaster Recovery-as-a-Service), By Deployment Model (Private Cloud, Hybrid Cloud and Public Cloud), By Organization Size (SMEs, Large Enterprises), By End User (BFSI, Healthcare, Government & Defense, IT & Telecom, and Others), By Region, Competition, Forecast & Opportunities, 2018-2028F

<https://marketpublishers.com/r/GCDA1383FDAEEN.html>

Date: November 2023

Pages: 181

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

ID: GCDA1383FDAEEN

Abstracts

The Global Data Protection as a Service (DPaaS) market was valued at USD 13.62 billion in 2022 and is anticipated to project robust growth at a CAGR of 31.57% during the forecast period. The global data protection as a service (DPaaS) market is at the forefront of the digital revolution, redefining how organizations safeguard their sensitive data and ensure business continuity in an era of unprecedented data growth and evolving cybersecurity threats. DPaaS represents a cloud-based service model that provides a comprehensive suite of data protection solutions, including backup, disaster recovery, data encryption, and security, all offered as a service. This innovative approach to data protection has gained substantial momentum in recent years, driven by a convergence of factors that underline its crucial role in the modern business landscape.

One of the central drivers propelling the growth of the DPaaS market is the explosive proliferation of data across industries. With the advent of digital technologies, the Internet of Things (IoT), and the widespread adoption of cloud-based applications, organizations are generating and managing vast volumes of data like never before. This

data deluge poses a multifaceted challenge, encompassing the secure storage, management, and protection of data. DPaaS addresses these challenges head-on by offering scalable, cost-effective, and flexible solutions for data protection. Scalability is a core advantage of DPaaS, allowing organizations to adapt their data protection strategies as their data volumes grow. Traditional on-premises solutions often struggle to keep pace with the exponential growth of data, requiring significant capital investments in hardware and infrastructure. In contrast, DPaaS providers offer scalable solutions that seamlessly accommodate increased data volumes without the need for major upfront investments. This scalability ensures that organizations can effectively manage and safeguard their data as their business needs evolve.

Moreover, the pay-as-you-go pricing model inherent to DPaaS eliminates the need for substantial upfront capital expenditures, making data protection accessible to organizations of all sizes. This democratization of data protection technology enables smaller businesses and startups to access enterprise-grade solutions without straining their budgets. It fosters a level playing field where organizations, regardless of their financial resources, can prioritize data protection and business continuity. The ever-evolving threat landscape of cybersecurity is another critical driver behind the DPaaS market's growth. Cyberattacks, data breaches, and ransomware attacks have become increasingly sophisticated and pervasive, posing significant risks to organizations' data and operations. DPaaS providers leverage advanced security measures, including data encryption, threat detection, and real-time monitoring, to safeguard data against a wide array of cyber threats. These security features fortify organizations' defenses and provide peace of mind, knowing that their critical data is shielded from malicious actors.

In a world where remote work and distributed workforces have become the norm, the importance of data protection has reached new heights. The COVID-19 pandemic accelerated the shift toward remote work arrangements, compelling organizations to rethink their data protection strategies. DPaaS solutions enable organizations to extend data protection to remote employees, ensuring that data remains secure whether accessed from the office, home, or other remote locations. This level of flexibility and adaptability has been instrumental in maintaining business continuity during times of crisis. Furthermore, data protection regulations and privacy laws, such as the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA) in the United States, have placed data privacy and compliance at the forefront of organizations' priorities. Non-compliance with these regulations can result in substantial fines and reputational damage. DPaaS providers offer features like data encryption, access controls, and audit trails, assisting organizations in meeting regulatory requirements and maintaining data privacy. DPaaS not only provides

organizations with the tools to comply with these stringent regulations but also offers a streamlined and automated approach to data governance and compliance management.

The global nature of business operations and data flows further drives the demand for DPaaS. Organizations with a global footprint must navigate complex data protection challenges, including data sovereignty requirements and cross-border data transfers. DPaaS providers offer geo-redundant data centers, ensuring that data is stored and managed in compliance with regional data protection laws. This global reach enables organizations to seamlessly expand their operations and maintain consistent data protection standards across borders. In conclusion, the global Data Protection as a Service (DPaaS) market is witnessing exponential growth and transformation, fueled by the escalating data volumes, evolving cybersecurity threats, the rise of remote work, and the imperative of regulatory compliance. DPaaS has emerged as an indispensable solution for organizations seeking to fortify their data defenses and ensure business continuity in an increasingly digital and data-centric world. As businesses across industries continue to recognize the paramount importance of data protection, the DPaaS market is poised for sustained growth, innovation, and adaptation, providing a lifeline for organizations navigating the intricate landscape of data security and privacy in the digital age.

Key Market Drivers

Escalating Data Volumes and Digital Transformation

One of the primary drivers propelling the global data protection as a service (DPaaS) market is the relentless escalation of data volumes across industries. In today's digital age, data has become the lifeblood of organizations, generated at an unprecedented rate from various sources, including IoT devices, social media, cloud applications, and business transactions. This explosion of data presents a multifaceted challenge for organizations, encompassing data storage, management, and, most critically, data protection. To effectively manage and safeguard this surging tide of data, organizations are increasingly turning to DPaaS solutions. DPaaS provides a scalable, flexible, and cost-effective approach to data protection. It allows organizations to adapt their data protection strategies in lockstep with their data growth, without requiring substantial upfront investments in hardware and infrastructure. This scalability ensures that organizations can not only store and manage their data effectively but also ensure its security and availability, regardless of its volume.

Moreover, the ongoing digital transformation journey undertaken by businesses and governments worldwide is a significant driver of the DPaaS market. Digitalization has become synonymous with modernization, streamlining processes, enhancing customer experiences, and improving decision-making through data-driven insights. However, this digital transformation also necessitates robust data protection measures to safeguard sensitive information and intellectual property. As organizations increasingly rely on digital technologies to drive innovation and competitiveness, DPaaS emerges as a critical enabler. It provides the data protection foundation needed to support digital transformation initiatives, ensuring that organizations can harness the power of their data while mitigating the risks associated with its exponential growth.

Evolving Cybersecurity Threat Landscape

The evolving and increasingly sophisticated cybersecurity threat landscape stands as a potent driver behind the global Data Protection as a Service (DPaaS) market's rapid growth. Cyberattacks, data breaches, and ransomware attacks have become omnipresent and ever more damaging in recent years, posing substantial risks to organizations' data and operations. These threats come in various forms, from phishing attacks and malware to zero-day vulnerabilities and insider threats. DPaaS providers are at the forefront of defense against these cyber threats, leveraging advanced security measures to fortify organizations' data protection strategies. Data encryption, one of the core features of DPaaS, ensures that data remains unreadable to unauthorized users, even if it falls into the wrong hands. Threat detection and real-time monitoring capabilities allow organizations to identify and respond to potential security breaches swiftly.

In addition to reactive measures, DPaaS solutions also focus on proactive security practices. Continuous data monitoring, automated backups, and multi-factor authentication contribute to a robust cybersecurity posture. Furthermore, DPaaS providers often maintain robust incident response and disaster recovery capabilities, allowing organizations to recover quickly and minimize downtime in the event of a cyber incident. As the cybersecurity threat landscape continues to evolve with increasing sophistication, DPaaS becomes an indispensable component of organizations' cybersecurity strategies. It not only provides a layer of defense against cyber threats but also offers peace of mind, knowing that sensitive data is shielded from malicious actors, while enabling organizations to focus on their core operations and digital transformation initiatives.

Remote Work and Distributed Workforces

The global shift toward remote work and distributed workforces, accelerated by the COVID-19 pandemic, is a significant driver behind the growth of the Data Protection as a Service (DPaaS) market. Remote work has become the new norm for organizations across various industries, and the trend is expected to persist well into the future. This seismic shift in work arrangements brings with it a multitude of data protection challenges. Organizations must ensure that their employees can securely access and share sensitive data from remote locations, whether working from home, satellite offices, or while traveling. DPaaS solutions offer a flexible and adaptable approach to data protection, enabling organizations to extend data protection to remote employees seamlessly.

DPaaS providers ensure that data remains secure, whether accessed from the office or remote locations, by offering robust security features such as data encryption, access controls, and audit trails. This level of security and flexibility fosters an environment where employees can work productively without compromising the organization's data protection standards. Moreover, the widespread adoption of remote work also underscores the importance of data availability and business continuity. Organizations cannot afford disruptions to their operations, and DPaaS providers typically offer comprehensive disaster recovery solutions. These solutions ensure that data can be quickly restored in the event of data loss or system downtime, minimizing disruptions, and enabling remote workers to remain productive.

The shift toward remote work is not limited to the pandemic era; it represents a broader transformation in the way businesses operate. DPaaS solutions are well-positioned to meet the needs of organizations seeking to maintain data security and business continuity in an increasingly remote and distributed work environment.

Regulatory Compliance and Data Privacy Mandates

Stringent regulatory compliance and data privacy mandates are compelling organizations to prioritize data protection, driving the adoption of Data Protection as a Service (DPaaS) solutions. Governments and regulatory bodies worldwide have implemented comprehensive data protection regulations such as the General Data Protection Regulation (GDPR) in Europe, the California Consumer Privacy Act (CCPA) in the United States, and similar laws in various regions. Non-compliance with these regulations can result in substantial fines, legal liabilities, and reputational damage. To navigate this complex regulatory landscape, organizations turn to DPaaS providers, which offer features and capabilities designed to facilitate compliance with data

protection regulations. DPaaS solutions typically incorporate data encryption, access controls, and audit trails, all of which are essential for maintaining data privacy and ensuring compliance with regulatory requirements. Encryption plays a crucial role in protecting sensitive data, both at rest and in transit, in accordance with regulatory mandates.

Furthermore, DPaaS providers often offer features that support data governance and compliance management, such as data classification, retention policies, and data discovery tools. These capabilities enable organizations to identify, classify, and manage sensitive data, ensuring that it is handled in accordance with regulatory guidelines. As the regulatory landscape continues to evolve and new data protection laws are enacted, DPaaS remains a critical component of organizations' compliance strategies. It provides the necessary tools and capabilities to navigate the complex terrain of data privacy regulations while simultaneously enhancing data protection and security measures. The imperative of regulatory compliance serves as a compelling driver for the continued growth of the DPaaS market, as organizations strive to meet their legal obligations and maintain the trust of their customers and stakeholders.

Key Market Challenges

Data Sovereignty and Compliance Complexity

One of the significant challenges facing the global Data Protection as a Service (DPaaS) market is the intricate web of data sovereignty requirements and compliance complexities that organizations must navigate. Data sovereignty refers to the concept that data is subject to the laws and regulations of the country where it is located, often requiring organizations to store and process data within specific geographic boundaries. These requirements can vary significantly from one country to another, adding layers of complexity to DPaaS implementation. For multinational organizations or those with a global customer base, complying with diverse data sovereignty regulations is a formidable challenge. Organizations need to ensure that data is stored and managed in accordance with the legal requirements of each jurisdiction where they operate or where their customers are located. This entails establishing a network of data centers and infrastructure that can accommodate data residency requirements, leading to increased operational costs and complexity.

Furthermore, the landscape of data protection regulations is constantly evolving. New laws are enacted, existing regulations are updated, and the interpretation and enforcement of these rules can vary. GDPR, for instance, introduced stringent

requirements for organizations handling the personal data of European Union citizens, while other regions have implemented their own data protection laws with unique stipulations. Staying up to date with these regulations and adapting DPaaS solutions to ensure compliance is an ongoing challenge. Additionally, the enforcement of data protection regulations carries substantial consequences for non-compliance, including hefty fines and legal liabilities. This makes it imperative for organizations to have a comprehensive understanding of the regulatory environment and to invest in DPaaS solutions that can adapt to changing compliance requirements.

Data Security and Privacy Concerns

Data security and privacy concerns represent an enduring challenge for the global Data Protection as a Service (DPaaS) market. As organizations increasingly rely on DPaaS solutions to safeguard their sensitive data, they must grapple with the ever-evolving threat landscape and the intricacies of protecting data in a digital world. These concerns are multifaceted, encompassing data breaches, cyberattacks, insider threats, and the ethical and legal aspects of data privacy. One of the primary data security concerns centers around the rising sophistication of cyber threats. Cyberattacks are becoming increasingly sophisticated and diverse, with threat actors continuously evolving their tactics to circumvent security measures. Ransomware attacks, in which attackers encrypt an organization's data and demand a ransom for its release, have gained notoriety for their destructive potential. DPaaS providers must continually innovate and invest in advanced security technologies to stay one step ahead of cyber threats.

Insider threats, whether intentional or unintentional, pose another significant challenge. Employees, contractors, or partners with access to an organization's data can inadvertently or deliberately compromise data security. DPaaS solutions must provide robust access controls, data monitoring, and user activity tracking to mitigate the risk of insider threats. Data privacy concerns are also paramount, with data protection regulations such as GDPR and CCPA requiring organizations to safeguard individuals' personal information and adhere to stringent privacy principles. Organizations must implement strong data encryption, access controls, and privacy-by-design practices to ensure compliance. The challenge lies in balancing data security with data accessibility, as stringent security measures can sometimes impede legitimate data access. Furthermore, the ethical and legal aspects of data privacy extend to data collection, storage, and usage practices. Organizations must be transparent about how they collect and use data, obtain consent where necessary, and provide individuals with the ability to manage their data. DPaaS providers must support these efforts by offering data governance features, such as data discovery and classification, and enabling

organizations to demonstrate compliance with data privacy regulations.

Key Market Trends

Rapid Adoption of Cloud-Native DPaaS Solutions

One of the prominent trends in the global Data Protection as a Service (DPaaS) market is the rapid adoption of cloud native DPaaS solutions. As organizations continue their digital transformation journeys, they are increasingly embracing cloud-based data protection services to ensure the security, availability, and compliance of their critical data. Cloud-native DPaaS solutions offer several advantages over traditional on-premises data protection approaches. First and foremost is the agility and scalability they provide. Cloud-native solutions enable organizations to scale their data protection capabilities up or down in response to changing data volumes and business needs without the need for substantial upfront investments in hardware or infrastructure. This flexibility aligns perfectly with the dynamic and evolving nature of today's data landscape.

Another significant advantage is the ease of deployment and management. Cloud-native DPaaS solutions can be provisioned and configured quickly, often within a matter of minutes. This streamlined deployment process reduces the burden on IT teams and accelerates time to value. Additionally, cloud-native solutions typically come with centralized management consoles that provide a unified view of data protection activities across an organization's entire infrastructure, making it easier to monitor and manage data protection policies and compliance. Cost-efficiency is also a driving factor behind the adoption of cloud-native DPaaS solutions. Organizations can reduce their capital expenditures on data center infrastructure and instead leverage the pay-as-you-go pricing model offered by cloud providers. This cost model allows organizations to pay only for the resources they consume, resulting in potential cost savings.

Furthermore, cloud native DPaaS solutions are well-positioned to address the challenges associated with remote work and distributed workforces. They facilitate secure data access and backup for employees working from various locations, ensuring data protection remains effective regardless of where data is accessed or modified. The trend toward cloud-native DPaaS solutions is expected to continue growing as organizations increasingly recognize the benefits of agility, scalability, cost-efficiency, and centralized management. DPaaS providers are likely to invest in enhancing their cloud-native offerings, further driving the adoption of these solutions across industries.

Convergence of DPaaS with Data Analytics and Artificial Intelligence (AI)

A noteworthy trend in the global Data Protection as a Service (DPaaS) market is the convergence of DPaaS with data analytics and artificial intelligence (AI) technologies. As organizations accumulate vast amounts of data, they are seeking to derive more value from it, not only for data protection purposes but also for strategic decision-making and insights generation. DPaaS providers are increasingly integrating data analytics and AI capabilities into their offerings. These technologies allow organizations to gain deeper insights into their data, detect anomalies, and identify potential security threats more effectively. For example, AI-powered anomaly detection can help organizations identify unusual data access patterns that may indicate a security breach or unauthorized activity.

Data analytics and AI also play a crucial role in improving data recovery and backup processes. AI-driven algorithms can optimize data deduplication, compression, and backup scheduling, reducing storage costs and improving backup performance. Additionally, AI can assist in data classification and prioritization, helping organizations determine which data is most critical for backup and recovery. Furthermore, the convergence of DPaaS with data analytics and AI enhances compliance and governance efforts. Organizations can use AI-powered tools to automate data discovery, classification, and tagging, ensuring that sensitive data is appropriately protected and that compliance with data protection regulations is maintained.

In addition to security and compliance benefits, this trend opens opportunities for organizations to leverage their data for business intelligence and competitive advantage. By analyzing data within the context of DPaaS, organizations can uncover valuable insights, predict future trends, and make data-driven decisions. The trend toward convergence is expected to continue as DPaaS providers recognize the value of incorporating data analytics and AI capabilities into their offerings. As organizations seek to make better use of their data and enhance their data protection strategies, the integration of these technologies with DPaaS solutions will become increasingly critical.

Increased Focus on Cyber Resilience and Incident Response

A significant trend in the global Data Protection as a Service (DPaaS) market is the heightened emphasis on cyber resilience and incident response capabilities. As cyber threats continue to evolve in complexity and frequency, organizations are placing a greater emphasis on their ability to withstand and recover from cyberattacks and data breaches. Cyber resilience encompasses the ability to maintain business operations

and data protection in the face of cyber threats, ensuring that organizations can continue to function even when facing disruptions. DPaaS plays a crucial role in achieving cyber resilience by providing robust data protection, backup, and disaster recovery solutions.

Organizations are increasingly incorporating cyber resilience into their overall data protection strategies. This includes conducting risk assessments, identifying critical data and systems, and implementing measures to prevent, detect, and respond to cyber threats effectively. DPaaS providers are responding to this trend by enhancing their solutions to include features that support cyber resilience. One essential aspect of cyber resilience is incident response. Organizations are investing in incident response plans and capabilities to minimize the impact of cyber incidents. DPaaS providers are aligning their offerings with these needs by providing automated incident response workflows, rapid data recovery capabilities, and tools to help organizations investigate and mitigate the effects of data breaches and cyberattacks. Moreover, organizations are recognizing the importance of cyber resilience testing and simulations to evaluate their preparedness for cyber incidents. DPaaS solutions are increasingly offering the ability to simulate cyber incidents and test data recovery and incident response procedures, allowing organizations to identify vulnerabilities and weaknesses in their data protection strategies.

Segmental Insights

Service Type Insights

Based on service type, the Storage-as-a-Service segment in the global data protection as a service (DPaaS) market emerges as the predominant segment, exhibiting unwavering dominance projected throughout the forecast period. This preeminence is a testament to the critical role that storage plays in data protection strategies. Storage-as-a-Service addresses the fundamental need for secure and scalable data storage, catering to organizations' burgeoning data volumes and the imperative to safeguard this data against an evolving array of threats. In an era where data is often considered an organization's most asset, the Storage-as-a-Service segment offers a comprehensive solution. It provides organizations with the ability to securely store their data in cloud-based environments, reducing the dependency on on-premises infrastructure while ensuring data availability and durability. The scalability inherent in Storage-as-a-Service allows organizations to adapt to the ever-expanding data landscape without the constraints of traditional storage limitations. As data protection continues to gain prominence in the face of evolving cybersecurity challenges and regulatory compliance

requirements, the unwavering dominance of Storage-as-a-Service underscores its pivotal role in fortifying organizations' data protection strategies and ensuring the resilience of their critical data assets.

Organization Size Insights

Based on organization size, the large segment in the global data protection as a service (DPaaS) market emerges as a formidable frontrunner, exerting its dominance and shaping the market's trajectory throughout the forecast period. This dominance reflects the strategic imperative for large enterprises to fortify their data protection strategies in an era of escalating cyber threats and burgeoning data volumes. Large organizations possess extensive and complex data ecosystems, comprising sensitive information critical to their operations, customers, and regulatory compliance. As such, they require robust and scalable DPaaS solutions to ensure the security, availability, and integrity of their data assets.

The large organization segment's dominance also stems from its capacity for significant investment in cutting-edge data protection technologies and services. These organizations are keenly aware of the financial and reputational risks associated with data breaches and non-compliance with data protection regulations. As a result, they are inclined to adopt comprehensive DPaaS solutions that encompass data encryption, backup, disaster recovery, and advanced security measures. This proactive approach to data protection aligns with their commitment to maintaining operational continuity, safeguarding customer trust, and adhering to stringent regulatory requirements. In the evolving landscape of data protection, the large organization segment's unwavering influence underscores its pivotal role in driving the adoption and innovation of DPaaS solutions to address the intricate data protection needs of the modern enterprise.

Regional Insights

North America firmly establishes itself as a commanding presence within the global data protection as a service (DPaaS) market, affirming its preeminent position, and highlighting its pivotal role in shaping the industry's course. This regional dominance is a testament to North America's proactive approach to data protection and its commitment to staying at the forefront of technological innovation. With an ever-increasing volume of data generated across industries, North American organizations recognize the paramount importance of safeguarding their sensitive information. As such, they have been early adopters of DPaaS solutions, leveraging these advanced services to secure their data against an evolving array of cyber threats, ensure

regulatory compliance, and maintain business continuity.

North America's pivotal role in the DPaaS market is further accentuated by the presence of tech giants, cybersecurity innovators, and a robust ecosystem of cloud service providers. These industry leaders continually drive the development of cutting-edge DPaaS offerings, setting global standards for data protection practices. Additionally, the region's commitment to cybersecurity research and development fosters an environment of innovation and collaboration, enabling DPaaS providers to evolve their solutions in response to emerging threats and market demands. In this ever-evolving landscape, North America's commanding presence not only reaffirms its influence but also underscores its responsibility in shaping the future of data protection on a global scale.

Key Market Players

IBM Corporation

Amazon Web Services Inc.

Hewlett Packard Enterprise Company

Dell Inc.

Cisco Inc.

Oracle Corporation

VMware Inc.

Commvault Systems Inc.

Veritas Technologies LLC

Asigra Inc.

Report Scope:

In this report, the Global Data Protection as a Service (DPaaS) market has been segmented into the following categories, in addition to the industry trends which have

also been detailed below:

Global Data Protection as a Service (DPaaS) Market, By Service Type:

Storage-as-a-Service

Backup-as-a-Service

Disaster Recovery-as-a-Service

Global Data Protection as a Service (DPaaS) Market, By Deployment Model:

Private Cloud

Hybrid Cloud

Public Cloud

Global Data Protection as a Service (DPaaS) Market, By Organization Size:

SMEs

Large Enterprises

Global Data Protection as a Service (DPaaS) Market, By End User:

BFSI

Healthcare

Government & Defense

IT & Telecom

Others

Global Data Protection as a Service (DPaaS) Market, By Region:

North America

Europe

South America

Middle East & Africa

Asia Pacific

Competitive Landscape

Company Profiles: Detailed analysis of the major companies present in the Global Data Protection as a Service (DPaaS) Market.

Available Customizations:

Global Data Protection as a Service (DPaaS) market report with the given market data, Tech Sci 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. SERVICE 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. Key Industry Partners
- 2.4. Major Association and Secondary Sources
- 2.5. Forecasting Methodology
- 2.6. Data Triangulation & Validation
- 2.7. Assumptions and Limitations

3. EXECUTIVE SUMMARY

4. IMPACT OF COVID-19 ON GLOBAL DATA PROTECTION AS A SERVICE (DPAAS) MARKET

5. VOICE OF CUSTOMER

6. GLOBAL DATA PROTECTION AS A SERVICE (DPAAS) MARKET OVERVIEW

7. GLOBAL DATA PROTECTION AS A SERVICE (DPAAS) MARKET OUTLOOK

- 7.1. Market Size & Forecast
 - 7.1.1. By Value
- 7.2. Market Share & Forecast
 - 7.2.1. By Service Type (Storage-as-a-Service, Backup-as-a-Service, and Disaster

Recovery-as-a-Service)

7.2.2. By Deployment Model (Private Cloud, Hybrid Cloud and Public Cloud)

7.2.3. By Organization Size (SMEs, Large Enterprises)

7.2.4. By End User (BFSI, Healthcare, Government & Defense, IT & Telecom, and Others)

7.2.5. By Top 10 Country

7.2.6. By Company (2022)

7.3. Market Map

8. NORTH AMERICA DATA PROTECTION AS A SERVICE (DPAAS) MARKET OUTLOOK

8.1. Market Size & Forecast

8.1.1. By Value

8.2. Market Share & Forecast

8.2.1. By Service Type

8.2.2. By Deployment Model

8.2.3. By Organization Size

8.2.4. By End User

8.3. North America: Country Analysis

8.3.1. United States Data Protection as a Service (DPaaS) 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 Service Type

8.3.1.2.2. By Deployment Model

8.3.1.2.3. By Organization Size

8.3.1.2.4. By End User

8.3.2. Canada Data Protection as a Service (DPaaS) 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 Service Type

8.3.2.2.2. By Deployment Model

8.3.2.2.3. By Organization Size

8.3.2.2.4. By End User

8.3.3. Mexico Data Protection as a Service (DPaaS) 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 Service Type

8.3.3.2.2. By Deployment Model

8.3.3.2.3. By Organization Size

8.3.3.2.4. By End User

9. EUROPE DATA PROTECTION AS A SERVICE (DPaaS) MARKET OUTLOOK

9.1. Market Size & Forecast

9.1.1. By Value

9.2. Market Share & Forecast

9.2.1. By Service Type

9.2.2. By Deployment Model

9.2.3. By Organization Size

9.2.4. By End User

9.3. Europe: Country Analysis

9.3.1. Germany Data Protection as a Service (DPaaS) 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 Service Type

9.3.1.2.2. By Deployment Model

9.3.1.2.3. By Organization Size

9.3.1.2.4. By End User

9.3.2. United Kingdom Data Protection as a Service (DPaaS) 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 Service Type

9.3.2.2.2. By Deployment Model

9.3.2.2.3. By Organization Size

9.3.2.2.4. By End User

9.3.3. France Data Protection as a Service (DPaaS) 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 Service Type

9.3.3.2.2. By Deployment Model

9.3.3.2.3. By Organization Size

- 9.3.3.2.4. By End User
- 9.3.4. Spain Data Protection as a Service (DPaaS) 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 Service Type
 - 9.3.4.2.2. By Deployment Model
 - 9.3.4.2.3. By Organization Size
 - 9.3.4.2.4. By End User
- 9.3.5. Italy Data Protection as a Service (DPaaS) 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 Service Type
 - 9.3.5.2.2. By Deployment Model
 - 9.3.5.2.3. By Organization Size
 - 9.3.5.2.4. By End User

10. SOUTH AMERICA DATA PROTECTION AS A SERVICE (DPAAS) MARKET OUTLOOK

- 10.1. Market Size & Forecast
 - 10.1.1. By Value
- 10.2. Market Share & Forecast
 - 10.2.1. By Service Type
 - 10.2.2. By Deployment Model
 - 10.2.3. By Organization Size
 - 10.2.4. By End User
- 10.3. South America: Country Analysis
 - 10.3.1. Brazil Data Protection as a Service (DPaaS) 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 Service Type
 - 10.3.1.2.2. By Deployment Model
 - 10.3.1.2.3. By Organization Size
 - 10.3.1.2.4. By End User
 - 10.3.2. Argentina Data Protection as a Service (DPaaS) 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 Service Type
 - 10.3.2.2.2. By Deployment Model
 - 10.3.2.2.3. By Organization Size
 - 10.3.2.2.4. By End User
- 10.3.3. Colombia Data Protection as a Service (DPaaS) 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 Service Type
 - 10.3.3.2.2. By Deployment Model
 - 10.3.3.2.3. By Organization Size
 - 10.3.3.2.4. By End User

11. MIDDLE EAST & AFRICA DATA PROTECTION AS A SERVICE (DPAAS) MARKET OUTLOOK

- 11.1. Market Size & Forecast
 - 11.1.1. By Value
- 11.2. Market Share & Forecast
 - 11.2.1. By Service Type
 - 11.2.2. By Deployment Model
 - 11.2.3. By Organization Size
 - 11.2.4. By End User
- 11.3. Middle East & America: Country Analysis
 - 11.3.1. Israel Data Protection as a Service (DPaaS) 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 Service Type
 - 11.3.1.2.2. By Deployment Model
 - 11.3.1.2.3. By Organization Size
 - 11.3.1.2.4. By End User
 - 11.3.2. Qatar Data Protection as a Service (DPaaS) 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 Service Type

- 11.3.2.2.2. By Deployment Model
- 11.3.2.2.3. By Organization Size
- 11.3.2.2.4. By End User
- 11.3.3. UAE Data Protection as a Service (DPaaS) 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 Service Type
 - 11.3.3.2.2. By Deployment Model
 - 11.3.3.2.3. By Organization Size
 - 11.3.3.2.4. By End User
- 11.3.4. Saudi Arabia Data Protection as a Service (DPaaS) 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 Service Type
 - 11.3.4.2.2. By Deployment Model
 - 11.3.4.2.3. By Organization Size
 - 11.3.4.2.4. By End User

12. ASIA PACIFIC DATA PROTECTION AS A SERVICE (DPAAS) MARKET OUTLOOK

- 12.1. Market Size & Forecast
 - 12.1.1. By Value
- 12.2. Market Share & Forecast
 - 12.2.1. By Service Type
 - 12.2.2. By Deployment Model
 - 12.2.3. By Organization Size
 - 12.2.4. By End User
- 12.3. Asia Pacific: Country Analysis
 - 12.3.1. China Data Protection as a Service (DPaaS) 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 Service Type
 - 12.3.1.2.2. By Deployment Model
 - 12.3.1.2.3. By Organization Size
 - 12.3.1.2.4. By End User

12.3.2. Japan Data Protection as a Service (DPaaS) 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 Service Type

12.3.2.2.2. By Deployment Model

12.3.2.2.3. By Organization Size

12.3.2.2.4. By End User

12.3.3. South Korea Data Protection as a Service (DPaaS) 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 Service Type

12.3.3.2.2. By Deployment Model

12.3.3.2.3. By Organization Size

12.3.3.2.4. By End User

12.3.4. India Data Protection as a Service (DPaaS) 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 Service Type

12.3.4.2.2. By Deployment Model

12.3.4.2.3. By Organization Size

12.3.4.2.4. By End User

12.3.5. Australia Data Protection as a Service (DPaaS) 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 Service Type

12.3.5.2.2. By Deployment Model

12.3.5.2.3. By Organization Size

12.3.5.2.4. 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 Financials & Revenue
- 15.1.3. Key Contact Person
- 15.1.4. Headquarters Address
- 15.1.5. Key Product/Service Offered

15.2. Amazon Web Services Inc.

- 15.2.1. Business Overview
- 15.2.2. Key Financials & Revenue
- 15.2.3. Key Contact Person
- 15.2.4. Headquarters Address
- 15.2.5. Key Product/Service Offered

15.3. Hewlett Packard Enterprise Company

- 15.3.1. Business Overview
- 15.3.2. Key Financials & Revenue
- 15.3.3. Key Contact Person
- 15.3.4. Headquarters Address
- 15.3.5. Key Product/Service Offered

15.4. Dell Inc.

- 15.4.1. Business Overview
- 15.4.2. Key Financials & Revenue
- 15.4.3. Key Contact Person
- 15.4.4. Headquarters Address
- 15.4.5. Key Product/Service Offered

15.5. Cisco Inc.

- 15.5.1. Business Overview
- 15.5.2. Key Financials & Revenue
- 15.5.3. Key Contact Person
- 15.5.4. Headquarters Address
- 15.5.5. Key Product/Service Offered

15.6. Oracle Corporation

- 15.6.1. Business Overview
- 15.6.2. Key Financials & Revenue
- 15.6.3. Key Contact Person
- 15.6.4. Headquarters Address

15.6.5. Key Product/Service Offered

15.7. VMware Inc.

15.7.1. Business Overview

15.7.2. Key Financials & Revenue

15.7.3. Key Contact Person

15.7.4. Headquarters Address

15.7.5. Key Product/Service Offered

15.8. Commvault Systems Inc.

15.8.1. Business Overview

15.8.2. Key Financials & Revenue

15.8.3. Key Contact Person

15.8.4. Headquarters Address

15.8.5. Key Product/Service Offered

15.9. Veritas Technologies LLC

15.9.1. Business Overview

15.9.2. Key Financials & Revenue

15.9.3. Key Contact Person

15.9.4. Headquarters Address

15.9.5. Key Product/Service Offered

15.10. Asigra Inc.

15.10.1. Business Overview

15.10.2. Key Financials & Revenue

15.10.3. Key Contact Person

15.10.4. Headquarters Address

15.10.5. Key Product/Service Offered

16. STRATEGIC RECOMMENDATIONS

17. ABOUT US & DISCLAIMER

I would like to order

Product name: Global Data Protection as a Service (DPaaS) Market Segmented by Service Type (Storage-as-a-Service, Backup-as-a-Service, and Disaster Recovery-as-a-Service), By Deployment Model (Private Cloud, Hybrid Cloud and Public Cloud), By Organization Size (SMEs, Large Enterprises), By End User (BFSI, Healthcare, Government & Defense, IT & Telecom, and Others), By Region, Competition, Forecast & Opportunities, 2018-2028F

Product link: <https://marketpublishers.com/r/GCDA1383FDAEEN.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

Payment

To pay by Credit Card (Visa, MasterCard, American Express, PayPal), please, click button on product page <https://marketpublishers.com/r/GCDA1383FDAEEN.html>