Global Data Loss Prevention Market - Growth, Trends, Covid-19 Impact, and Forecasts (2023 - 2028)

Market Report | 2023-01-23 | 100 pages | Mordor Intelligence

AVAILABLE LICENSES:

- Single User License $4750.00

- Team License (1-7 Users) $5250.00

- Site License $6500.00

- Corporate License $8750.00

Report description:

The data loss prevention market is likely to register a CAGR of 22.29% during the forecast period. Enterprises worldwide are increasingly adopting better security solutions as part of their digital transformation process, thereby augmenting the market's growth.

Key Highlights
The rapidly increasing instances of data breaches and other factors, such as DLP-as-a-service, DLP functionalities extending into the cloud, and advanced threat protection, have significantly increased the focus on data loss protection solutions worldwide. As the demand for digital assets increased, there was a massive growth in the amount of structured and unstructured data, driving the need for data protection services with a strategic focus on data-centric organizations. Multiple large enterprises in the Fortune Global 500 list have invested in the DLP market for over a decade. Currently, the market is emerging as a critical security strategy within reach of mid-sized enterprises.
Data loss prevention (DLP) tools are necessary for data protection strategies. DLP solutions can be tailored to various needs and support compliance efforts with the new data protection regulations, such as GDPR or the California Consumer Privacy Act (CCPA). They are helping organizations find, monitor, and control sensitive data travelling in and out of the company's network.
The increasing demand for BYOD is raising the concern among key enterprises regarding data security. According to the BYOD Security Report 2021 by Forcepoint, 82% of all businesses actively encourage employees to bring their own devices to work. BYOD is most associated with employees bringing unmanaged devices to work (70%), but it also applies to other groups such as contractors (26%), partners (21%), customers (18%), and suppliers (14%). However, information security issues (30%), employee privacy concerns (15%), and support cost concerns (9%) are the biggest impediments to BYOD adoption. Data leakage or loss is at the top of the list of security concerns (62%). Users installing hazardous apps or content (54%), lost or stolen devices (53%), and illegal access to the company data and systems are all significant worries (51%), according to the same report.

Data can still be viewed in a printable format even when access permission is restricted to confidential data. As these channels cannot be closed and are the foundation of business in terms of data interchange, channels like file sharing and online services related to data "in transit" have been one of the main challenges. Traffic must be heavily filtered to guarantee optimal security in these channels. The DLP system that would be implemented should constantly work to balance security and interconnectivity in these channels.

With the emergence of the COVID-19 pandemic, the market is anticipated to grow further as the total volume of data being generated worldwide is rising much faster. As a result of the COVID-19 lockdowns and work-from-home trends, an unprecedented number of people are now making use of mobile devices as their primary communication devices, thereby creating more endpoints for the organization to secure from the rising cyber threats.

Data Loss Prevention Market Trends

Rising Data Breaches and Cyber Attacks Worldwide to Drive the Market

The increasing instances of data breaches across multiple industries have leaked millions of consumer data records to hackers and led to the loss of millions of dollars for numerous companies, thus increasing the focus on security solutions across emerging economies.

As businesses worldwide grow, new threats such as zero-day malware, trojans, and advanced persistent threats have exposed critical data to risk. This trend has encouraged organizations to deploy DLP solutions to safeguard their data within endpoints and networks against potential attacks.?

The increasing adoption of BYOD trends in organizations has increased the influx of different laptops, desktops, and smartphones, thus creating other endpoints vulnerable to attacks. Security measures on their own are not enough to stop these threats. The massive growth in the adoption of mobile devices across the world is expected to create significant opportunities during the forecast period. According to the Cisco Annual Internet Report, there may be approximately 29.3 billion networked devices by 2023. Smart manufacturing and the smart industry are expected to augment the market with the increased adoption of 5G.

Ransomware threat actors target software supply chain businesses worldwide, compromising and extorting their clients. By focusing on software supply chains, ransomware threat actors can expand the scope of their assaults by gaining access to several victims through a single initial penetration. In recent years, technological advancements have increased cyberattacks in the telecom industry. Hence, it is becoming increasingly crucial for telecom companies to choose data security services to ensure that all operating systems on their network are secure.

There has been double-digit growth in the number of endpoints, primarily due to the rapidly increasing adoption of automation due to Industry 4.0, machine-to-machine communication, and the emergence of smart cities. The need to protect the vulnerability of data and devices and deploy tools to recognize attacks and minimize the damage is critically important.? Therefore, the increasing adoption of automation technology is expected to drive the market's growth during the forecast period.

North America is Expected to Account for the Largest Market Share

The United States is witnessing an increased number of data breaches. According to the Identity Theft Resource Center (ITRC), the average number of violations in the United States has increased marginally over the past few years, from 1,506 breaches in 2017 to 1,826 violations in 2021.

In 2021, the country's increasing number of data breaches impacted around 293.93 million individuals. These increasing data breaches in various industries are expected to be the primary factor driving the demand for data loss prevention solutions during the forecast period.

The US healthcare industry also witnesses many data breaches as the industry is moving to an electronic record base, thus requiring data loss prevention solutions.

As a growth strategy, companies heavily indulge in product launches as lucrative ways to maximize their market shares. For instance, in October 2022, Proofpoint Inc., a US-based cybersecurity and compliance company, declared an array of innovations across its Threat Protection Platform at the 2022 Microsoft Ignite Conference, allowing organizations to defend against today's most advanced and pervasive threats, including supply chain assaults and business email compromise (BEC). The enhancements provide companies with outstanding insight into email fraud detection, defense against third-party and supplier compromise, machine learning (ML), and behavioral analytics, all made available through a new, easy-to-deploy inline API model.

In March 2022, Quebec's Premier and Health Minister announced the reformation of Quebec's health system, including the management of health and social services information. The government introduced Bill 19, which aims to set up a new management system that modernizes and decentralizes the health network to enable a safer and more seamless flow of health and social services information.

Data Loss Prevention Market Competitor Analysis

The intensity of competitive rivalry in the data loss prevention market is high and is expected to increase during the forecast period. Major companies strongly influence the market in terms of R&D and consolidation activities. Conversely, the market can be characterized by high market penetration and increasing fragmentation levels.

April 2022 - McAfee Corp. launched Personal Data Cleanup in the United States, the company's newest privacy feature addition to its flagship product, McAfee Total Protection. Personal Data Cleanup provides consumers with visibility, guidance, and continuous monitoring to protect themselves from identity thieves, hackers, and spammers by removing their data from some of the web's riskiest data broker sites.

April 2022 - Broadcom Inc. announced "Day One" support for IBM's new z16, expanding opportunities for organizations to gain more value from the company's advanced AI, security, and hybrid cloud solutions. Broadcom's leading technology solutions, services, and innovative "beyond code" software give clients the competitive advantage required to succeed in an increasingly challenging business environment.

March 2021 - Proofpoint completed its acquisition of InteliSecure Inc., an innovator in data loss protection managed services. With this acquisition, Proofpoint strengthened its cloud-based people-centric security platform by enhancing customers' ability to protect critical data in diverse environments. Proofpoint acquired InteliSecure for USD 62.5 million in cash.

Additional Benefits:

 The market estimate (ME) sheet in Excel format
3 months of analyst support

Table of Contents:

4 MARKET INSIGHTS

4.1 Market Overview

4.2 Industry Attractiveness - Porter's Five Forces Analysis

4.2.1 Bargaining Power of Suppliers

4.2.2 Bargaining Power of Consumers

4.2.3 Threat of New Entrants

4.2.4 Threat of Substitute Products

4.2.5 Intensity of Competitive Rivalry

4.3 Assessment Of Covid-19 Impact On The Industry

5 MARKET DYNAMICS

5.1 Market Drivers

5.1.1 Rising Data Breaches and Cyber Attacks Worldwide to Drive the Market

5.1.2 Regulations and Compliances (GDPR, CCPA, PCI DSS, Etc.)

5.1.3 Increasing Data Criticality and Vulnerability

5.2 Market Restraints

5.2.1 Lack of Awareness About Complete Solution Adoption

5.2.2 Deployment Challenges Related to Access Rights, Encryption, Scalability, and Integration

6 MARKET SEGMENTATION

6.1 By Deployment

6.1.1 On-premise

6.1.2 Cloud-based

6.2 By Solution

6.2.1 Network DLP

6.2.2 Endpoint DLP

6.2.3 Datacenter/Storage-based DLP

6.3 By End-user Industry

6.3.1 IT and Telecommunication

6.3.2 BFSI

6.3.3 Government

6.3.4 Healthcare

6.3.5 Manufacturing

6.3.6 Retail and Logistics

6.3.7 Other End-user Industries

6.4 By Geography

6.4.1 North America

6.4.1.1 United States

6.4.1.2 Canada

6.4.2 Europe

6.4.2.1 Germany

6.4.2.2 United Kingdom

6.4.2.3 France

6.4.2.4 Rest of Europe

6.4.3 Asia-Pacific

6.4.3.1 China

Global Data Loss Prevention Market - Growth, Trends, Covid-19 Impact, and Forecasts (2023 - 2028)

Market Report | 2023-01-23 | 100 pages | Mordor Intelligence

To place an Order with Scotts International:

 - Print this form

 - Complete the relevant blank fields and sign

 - Send as a scanned email to support@scotts-international.com

ORDER FORM:

Select license	License	Price
	Single User License	$4750.00
	Team License (1-7 Users)	$5250.00
	Site License	$6500.00
	Corporate License	$8750.00
	VAT	
	Total	

*Please circle the relevant license option. For any questions please contact support@scotts-international.com or 0048 603 394 346.

** VAT will be added at 23% for Polish based companies, individuals and EU based companies who are unable to provide a valid EU Vat Numbers.

Email*

Phone*

First Name*

Last Name*

Job title*

Company Name*

EU Vat / Tax ID / NIP number*

Address*

City*

Zip Code*

Country*

Date   2026-02-27

Signature