TATA

TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

ENSURING DATA PROTECTION IN TIMES OF COVID-19 USING DLP SOLUTIONS

@tataadvanced

contactcs@tataadvancedsystems.com | www.tataadvancedsystems.com

TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

Data security and privacy are no longer viewed as just a part of compliance or regulations. Remote working has shattered the situation as organizations are facing unusual hindrances in restricting malicious insiders and outsiders from exfiltrating company's data. Accordingly, businesses are compelled to adopt advanced security controls to prevent critical information from going outside the corporate perimeter. Data Leakage Prevention (DLP) solutions are one of those controls that are growing in popularity as organisations are looking to minimize the risk of data leaks. It can deal with problems, which fall out of the perimeter of conventional security measures like firewalls, intrusion detection systems, anti-viruses, etc. that aims at external threats only.

Let's inspect how DLP solutions help organisations to ensure the security and confidentiality of business-critical data.

Identify & Manage Critical Data

DLP solutions allow users/administrators to establish specific policies that help in identifying confidential information residing at different locations such as databases, repositories and endpoints throughout the organization. Then, customised policies can be applied against which identified data can be evaluated to detect and prevent data leaks.

Provide Improved Visibility

DLP solutions provide a comprehensive insight into how sensitive information within the organization is stored, utilized and shared. It helps in monitoring how the company's internal members deal with confidential information, which further allows administrators/privileged users to identify suspicious behaviour patterns (malicious insiders) that could put the organization's data security at risk.

Monitor Data Leakage Vectors

Emails are the most common channels of data leakage and widely exposed by threat actors to compromise legitimate accounts and gain access to sensitive information. DLP solutions apply specific policies (like content-aware policies) to identify and alert users while entering sensitive information in the mail body or attachments. Based on the configuration of policies, multiple actions can be taken to prevent data from leaving the organization, including creating alerts for risky behaviour, blocking such emails and quarantine email messages for further review. These solutions also allow users/administrators to apply controls to prevent other data leakage vectors such as portable storage devices and web communications (like file upload and Web mails).

Reporting

DLP solutions also provide reports to meet internal or external auditing requirements and determine areas of improvement, which further helps in taking corrective measures. These solutions can also be triggered to provide real-time incident reports in case of a suspicious event.

@tataadvanced

contactcs@tataadvancedsystems.com | www.tataadvancedsystems.com

TATA ADVANCED SYSTEMS

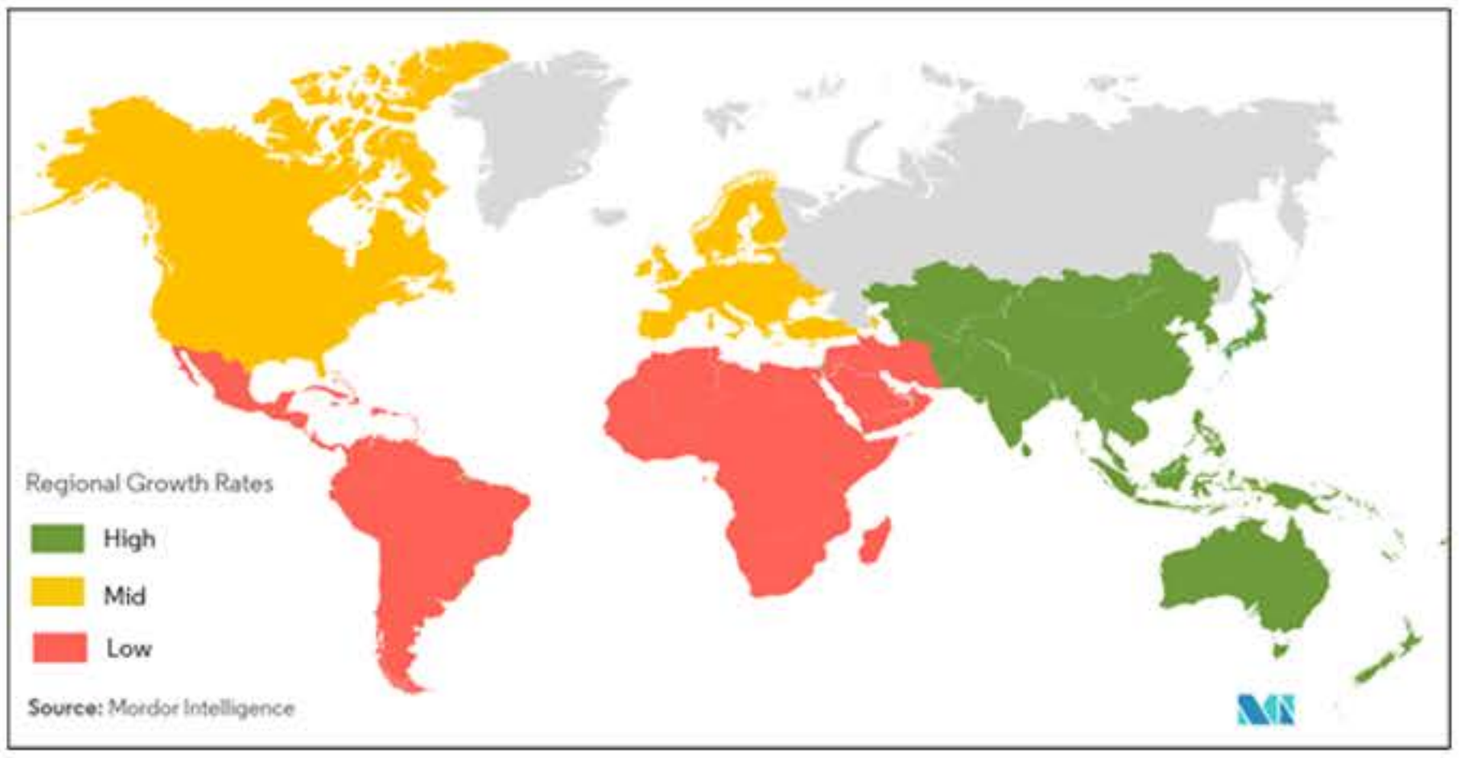
CYBER SECURITY PRACTICE

Achieve Compliance with Emerging Data Protection Regulations

Growing data breach incidents are getting the attention of regulatory bodies, pushing them to encourage organizations to embrace required data security controls. Organizations that store customers' data, including Personally Identifiable Information (PII), Protected Health Information and Payment Card Information (PCI) need to redefine policies and create a framework that secures the information being stored and processed throughout its lifecycle. DLP solutions assist enterprises to review and administer their compliance risks for multiple regulations including (but not limited to) GDPR, PCI, HIPAA, PDPA, etc.

DLP Solutions Getting Attention Globally

According to Mordor Intelligence report, the DLP solution market was estimated at USD 1.21 billion in 2019 and is likely to reach USD 3.75 billion by 2025, at a CAGR of 23.59% during the forecasted period. The contributing factors behind this tremendous growth rate include the rising crest of data breaches amid COVID-19 outbreak, sharing of data across cloud platforms, increasing volumes of data, etc. Asia-Pacific region is expected to receive the highest market share during the forecast period. Explore Image 1 for more details about other regions.



Embracing data protection is not a one-time activity. Threats originating from malicious insiders, nation-backed and independent cybercriminals groups will continue to evolve and target global businesses. Organizations need to remain vigilant and keep updating to advanced security practices, just like DLP, to ensure that their crown jewels (sensitive information and critical assets) are safe.

For more information on DLP solution, connect with our cybersecurity experts at
contactcs@tataadvancedsystems.com