AT-A-GLANCE

Stop your business sensitive data from leakage

Data loss prevention – managed service

Can your business risk data leakage?

Are you losing data without even knowing it? As your business grows, the risk of sensitive data being breached increases at an alarming pace. Small and medium businesses need to remove the risk of sensitive and / or regulatory-protected information from leaving their company. The perpetrators may not only be hackers — they could also be your own employees who leak data, unknowingly. Whether accidental or malicious, data loss can occur through many channels such as email, web, USB drives, and via uploading to the cloud — potentially costing you millions.

The problem:

Data leakage is the exfiltration / transfer of data to unauthorized parties — both inside and outside the organization. According to Verizon's 2021 Data Breach and Investigation Report, 44% of threat actors related to breaches in small SMBs are internal employees.

How data gets leaked:

56% Relating to negligence

26% Relating to criminal insiders

18% Relating to user credential theft

Type of data leaked:

- Customer personal information
- Intellectual property and trade secrets
- Financial data
- Personnel files
- Patient health info

What's at stake:

- Your company's brand reputation
- Business and revenue loss
- Noncompliance risks and fines
- Embarrassing headlines and customer churn

BRT IT for Healthcare Simplified

DLP managed service benefits

Minimize data leakage risk from accidental, compromised and malicious users

Strengthen regulatory compliance and protect sensitive data against unauthorized usage

Benefit from continuous adjustment of DLP policies to your changing business specifics that only require validation from your end

Keep process disturbances to a minimum due to misconfigured policies or new business procedures / needs

What are three main use cases for DLP Services?

Compliance:
Does your company collect and store personally identifiable information (PII), protected health information (PHI) or payment card information (PCI)? Other compliance regulations, such as HIPAA, and GDPR (for E.U. residents) require you protect your customers' sensitive data against leaking to unauthorized parties.

Sensitive information protection:
Does your company have important intellectual property and trade or state secrets that could put your organization's financial health and brand image at risk if lost or stolen? Context-based classification of intellectual property can protect against unwanted exfiltration of this data

Data visibility:
Is your company looking to gain additional visibility into data movement? Understand how users in your organization interact with data and how effectively DLP risks are remediated with this service.

Next steps

To learn more about our Managed Advanced Data Loss Protection Service, contact us:

Alex Siow 9855 5036, Alex@brt.com.sg

1003 Bukit Merah Central #04-12 Inno Centre S(159836)

Data Loss Prevention (DLP) Managed Service explained:

What is the Advanced DLP Managed Service?

Our services help you plan, implement and secure your organization with the most effective, next-generation technologies and expertise. The Data Loss Prevention Managed Service is a service that empowers your organization with unmatched protection against data leakage risks by preventing data flows that are unnecessary or potentially harmful to your business. DLP strengthens compliance by preventing unauthorized use and transmission of your sensitive data.

How does it work?

1. Our technology and service delivery team will baseline and profile user activities, connections and data flows and create an initial DLP policy that's specific to your business — ensuring protection against the most common causes of data leaks to unauthorized persons.
2. Policies, specific to your business, will be created with a unique, behavior-based approach, and will be presented in an easy-to-understand graphical way to be validated by your business leads.
3. After the policies are validated, our team will enforce them and protect your sensitive data against leakage with 24/7/365 coverage across network channels and peripheral devices. Optimally, the enforced policies can be continuously adjusted to your ever-changing business processes with only periodic validation required from your end. This creates an effective barrier against both outsider and insider risks — now and in the future.

Our service strengthens regulatory compliance

Ensure access policies meet regulatory compliance including:

GDPR

Personally identifiable information (PII)

Prevent unauthorized disclosure of employees' PII name, email, address, SSN, passport number, drivers license, social media accounts, etc.

HIPAA
Health Insurance Portability & Accountability Act

Protected health information (PHI)

Block sending a patient's PHI from a medical center to external recipients or publishing PHI to social media.

PCI

Payment card information (PCI DSS)

Avoid accidental or deliberate sharing of clients' payment card data with contractors.

CONFIDENTIAL

Documents marked as confidential

Prevent uploads of sensitive business documents with the "Confidential" watermark to employees' private storage at file sharing services.