

What is the Data Loss Prevention Managed Service?

IronTree Data Loss Prevention (DLP) is an additional layer of protection within the Prevent solution. Our solution helps you plan, implement, and secure your organisation with the most effective, next-generation technologies and expertise. The Data Loss Prevention Managed Service is a service that empowers your organisation 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 unauthorised use and transmission of your sensitive data.



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 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 unauthorised parties – both inside and outside the organisation. According to Verizon's 2021 Data Breach and Investigation Report, 44% of threat actors related to breaches in SMEs are internal employees.

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

HOW IT WORKS

How does it work?

1. Your user activities, connections and data flows are assessed. An initial DLP policy is created that is specific to your business – ensuring protection against the most common causes of data leaks to unauthorised persons.
2. Policies, specific to your business, will be created with a unique, behaviour-based approach, and will be presented in an easy-to-understand way, to be validated by your management teams.
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. These 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.

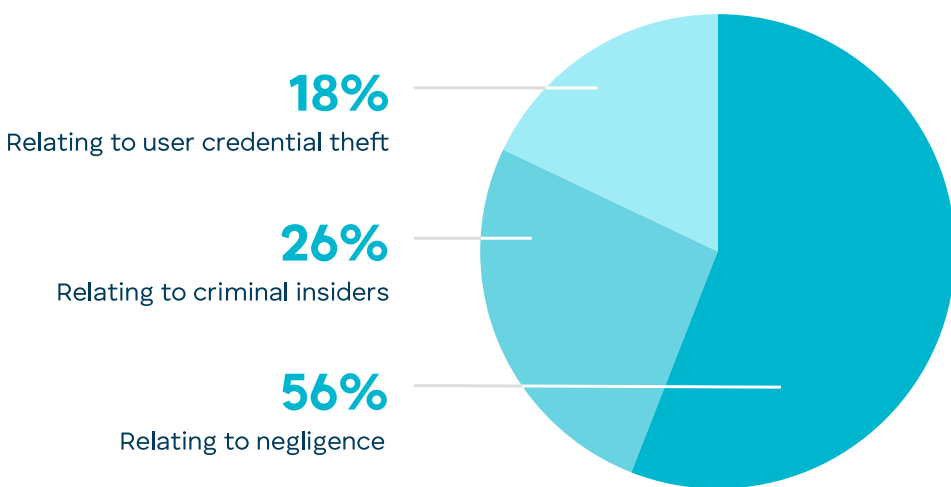
3 main uses of DLP Services

- ✓ **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 POPIA require you to protect your customers' sensitive data against leaking to unauthorised parties.
- ✓ **Sensitive information protection** – Does your company have important intellectual property and trade or state secrets that could put your organisation'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 organisation interact with data and how effectively DLP risks are remediated with this service.

DLP managed service benefits

- ✓ Minimise data leakage risk from accidental, compromised and malicious users.
- ✓ Strengthen regulatory compliance and protect sensitive data against unauthorised 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.

How data gets leaked:



Type of data leaked

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

What's at risk

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

To learn more about IronTree's Data Loss Prevention service, get in touch.

GET IN TOUCH →