

Prevent Data Loss with Data Loss Detection









Get the visibility you need to protect your data and align to compliance requirements

Traditional data loss prevention (DLP) technology is often mistaken for data loss prevention strategy; DLP technology is used by enterprises as a tool to protect company data and prevent it from getting lost or stolen. On the other hand DLP strategy focuses on a broader approach and frameworks that include policies and procedures, network controls and more technical pieces like tools and technology.

The Challenge





Companies use a combination of DLP strategy and DLP technology to mitigate data loss. Larger enterprises with a high level of security maturity are able to institute layers of policies and procedures, controls, technology, and dedicated in-house expertise to run it all. Smaller businesses lack the same level of security maturity and budget that their larger peers have, and often turn to large cloud service providers who offer some level of DLP controls as part of all-in-one licensing agreements. Yet without a DLP strategy, knowing how to implement those controls can be confusing, so teams won't use the controls at all – or worse, assume that their service providers are operating them on their behalf.

Risks of Data Loss Prevention Strategy and Technology Gaps:

-  Poorly protected data
-  Increased cyber risk
-  Increased operational risks
-  Breach liability
-  Data loss
-  Reputational risk
-  Regulatory non-compliance
-  Incomplete data inventory




The Solution

A data loss prevention strategy starts with knowing what data exists on every endpoint across the network. With full visibility, businesses can establish a comprehensive data inventory, and better identify the tools they need to encrypt and protect sensitive company data, all by data type. From an auditing perspective, an up-to-date data map helps businesses demonstrate alignment to data security, privacy policies and data protection controls. Data loss detection provides:

-  Visibility to data in motion, not just data at rest
-  Faster time to respond to data risk
-  Demonstratable actions, policies and controls to achieve compliance
-  Up-to-date data inventory supporting incident response requirements

Establish your DLP strategy with data loss detection from Cavelo.

Here's how:

-  Manage organizational data policies by defining access boundaries for your data.
-  Get alerts if your customer or employee data is found in a place it shouldn't be. Focus your training efforts on users who are openly discussing organizationally sensitive topics over email to personal email accounts.
-  Discover, track and define data boundaries to make sure you're alerted when action needs to be taken.

[Request a demo](#)