USE CASE

Data Loss Prevention

CAVELO

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 DLP software providers or large cloud service providers who offer some level of DLP controls as part of all-in-one licencing 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
- Breach Liability
- Regulatory Non-compliance
- Increased Cyber Risk
- Data Loss
- Incomplete Data Inventory
- Increased Operational Risks
- Reputational Risk

 | info@cavelo.com | www.cavelo.com

Achieve data loss prevention with data loss detection from Cavelo.

Here's how:

1. Manage organizational data policies by defining access boundaries for your data.

2. 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.

3. Discover, track and define data boundaries to make sure you're alerted when action needs to be taken.

LEARN MORE

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 prevention 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