What Is Your DLP Software Not Protecting?

Introduction

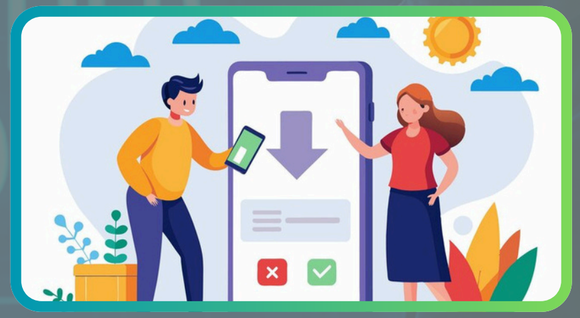
DLP software protects a lot, but not everything. It often misses insider risks, unmonitored devices, encrypted file transfers, and new threat patterns. While it's designed to safeguard sensitive data, gaps in configuration, coverage, and visibility can leave critical information exposed if not managed carefully.

EmpMonitor helps bridge these security gaps by offering detailed user activity tracking and early insider threat alerts. It provides deeper visibility across devices and workflows, ensuring sensitive data stays protected where traditional tools fall short.

What Your DLP Still Misses

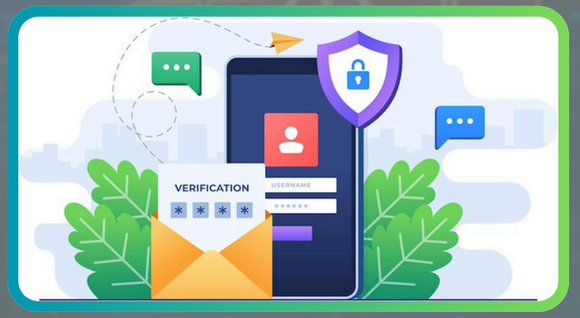
Insider Actions

DLP software may overlook subtle insider activities, especially when users exploit trusted access to move or misuse data quietly.



Shadow Devices

Unregistered or personal devices can bypass monitoring, making it harder for DLP systems to track sensitive data movement.



Encrypted Transfers

Encrypted channels, while secure, can hide unauthorized file transfers that the system may fail to detect or analyze.

The Final Verdict:

DLP software is essential, but it isn’t flawless. Its limitations often come from blind spots, not bad design. Strengthening policies, monitoring, and visibility tools can close these gaps and ensure more complete data protection.

EmpMonitor enhances this protection by offering real-time user activity insights and insider threat detection. It adds an extra layer of visibility, helping organizations spot risks that traditional tools often miss.

https://empmonitor.com/data-loss-prevention-software/