How Dtex Augments Data Loss Prevention (DLP)

Most Dtex customers also use DLP technology in some form. Here's an overview of how Dtex combined with DLP delivers a stronger security program.

DLP Misconfiguration

In nearly every installation we perform, we find DLP systems that are not performing as intended. DLP systems are incredibly powerful, but also require a significant amount of customization and configuration to perform properly. DLP systems will always tell you what they catch if told what to look for as or after an incident has happened, but don't have any capability in place to predict a data leakage incident.

Customers turn to Dtex to provide instant visibility into the places where DLP is unable to do its job, either because it is not fully deployed, is improperly configured or has been removed due to performance impact to the end-user hosts.

Answers to Simple Questions

Many DLP systems collect quite a lot of data, but make it very hard to get answers to simple questions. Customers find themselves turning to Dtex when they want simple answers to user behavioral questions like "what files were on a lost laptop" or "who inserted an unencrypted USB drive" or even "what files did an employee take on their last day?"

Dtex provides a clear, simple audit trail of a user's application, file, internet, and window activity so you can very quickly understand user activity without having to wade through extraneous noise.

User Risk Scores

DLP systems aren't looking for anomalous changes in user behavior that could signal that a user is preparing to bypass security or steal trade secrets.

Whether it's the user who searches for "how to disable DLP," or the employee who suddenly aggregates gigabytes of files onto their machine, or the user that suddenly changes their normal work patterns, Dtex builds profiles of normal user behavior and alerts staff to high risk users that require further scrutiny.

Performance Issues

Endpoint DLP systems are rich with blocking and lock-down capabilities, but this comes at the cost of system and network performance. Multiple Dtex customers report that endpoint DLP works fine in high performance environments with newer computers, but they struggle to get full enterprise protection due to performance impact.

Dtex is incredibly lightweight, and runs easily on older machines, slower networks, and small virtual endpoints. Dtex only generates 1MB per user per week of data, and has a 0.1% network impact.

Off-Network Visibility

Many companies start their DLP program with web filtering and email filtering. While effective, these perimeter DLP solutions lose visibility into end user behavior as soon as removable devices (like laptops) leave the office.

Dtex customers gain full visibility into user activity even when off the corporate network.

Trust But Verify - a People-Centric Approach to Security

Many companies are realizing that locking down the endpoint is not the best way to manage the insider threat. Locked down environments:

1. frustrate staff and reduce efficiency,
2. do little to stop someone intent on stealing information, and
3. actually encourage insiders to find less protected methods of data egress

By using Dtex's simple user visibility and risk scoring, Dtex customers find that they're able to relax lockdown controls in lieu of greater visibility. By increasing freedom, security teams spend less time managing rules and policies and can spend more time focusing on the small portion of the population that truly represents an insider threat.

Address Privacy Concerns

Content-aware DLP systems, by design, have access to all of the corporate *and* personal data that crosses corporate endpoints, firewalls, and email systems. Dtex only collects metadata, and can further protect employee privacy through anonymization of identifying details.