DTEX
THE WORKFORCE CYBER INTELLIGENCE COMPANY™

Prevent Data Loss without Operational Overhead

STOP

PREVENT DATA LOSS

REDUCE FALSE POSITIVES

NO RULES REQUIRED

Traditional Endpoint Data Loss Prevention (DLP) solutions rely on intrusive, resource intensive content inspection rules. These types of detection techniques are prone to high levels of false positives, require heavy endpoint agents that degrade performance, and must be constantly tuned by IT and security staff to remain effective.

The ever-changing dynamics of today's digital and distributed enterprises demand lightweight, easy-to-manage data loss prevention that doesn't rely on rules-based keywords, patterns, expressions, and hashing to detect and prevent user-initiated data loss. **Enterprises need a new approach.**

Data Loss Prevention from DTEX takes a behavioral approach to data loss by monitoring and auditing all user activities based upon "out of the box" policies. Using this method, DTEX InTERCEPT is able to see the full lifecycle of behavior activity and understand the who, what, when and how of a possible data loss incident. No false positives, simply a real-time, scoring-based audit trail of all events.

Unlike heavy Endpoint DLP tools, DTEX InTERCEPT is a lightweight forwarder that requires no more than 3-5MB of bandwidth per day per endpoint and utilizes less than 1% CPU. With DTEX InTERCEPT, processing of DLP policies is not performed on the endpoint. Instead, all data is streamed in real-time to the cloud for analysis and detection, thereby avoiding many of the endpoint interoperability issues associated with traditional endpoint agents.

DTEX InTERCEPT's modern architecture and design does not require "triggers" to determine when meta-data should be collected and supports continuous monitoring of all console and web-based applications. Likewise, DTEX's innovative human-centric scoring mechanism is based upon a series of activities, vs DLP's content focus, which means DTEX only notifies on truly suspicious events, saving time and empowering the analyst with full context about any given incident.

KEY FEATURES

- Lightweight Meta-Data Forwarder
- Real-time Cloud Analytics
- Dynamic Activity Risk Scoring
- Out-of-the-Box Policies
- No Invasive Content Inspection
- Digital Forensics & Audit Reports
- Live, Interactive Dashboards
- Executive Reports

KEY BENEFITS

- Prevent Data Exfiltration
- Identify Teachable Moments
- Eliminate Fales Positives
- Reduce Analyst Fatigue
- Maintain Regulatory Compliance

Quickly understand high risk users and activities through the interactive heatmap.

Easily spot when and how data loss is occurring across your organization.

Clean, easy to understand charts & graphs demonstrate key data loss metrics including how data is handled on or off the corporate network.
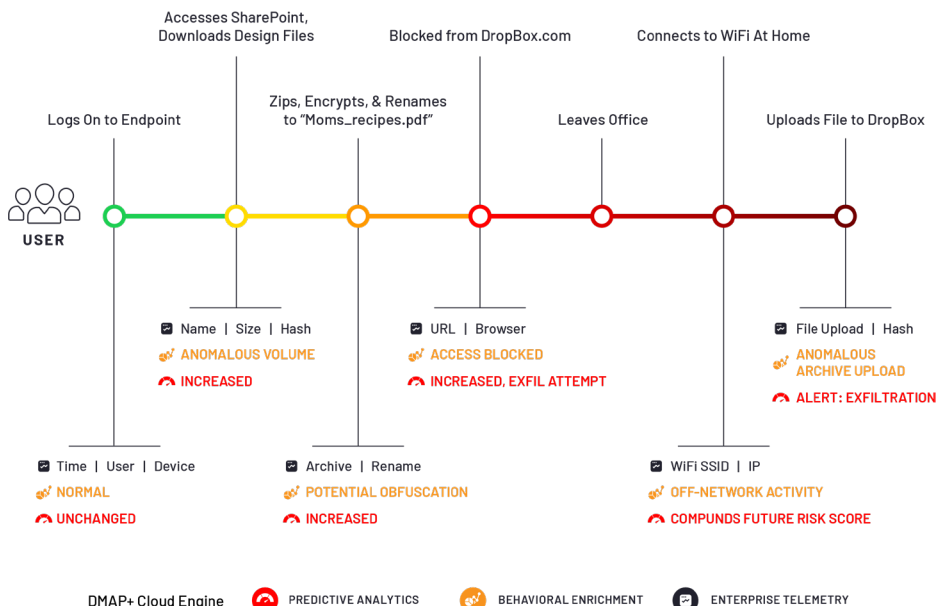
Prevent Data Loss without Operational Overhead
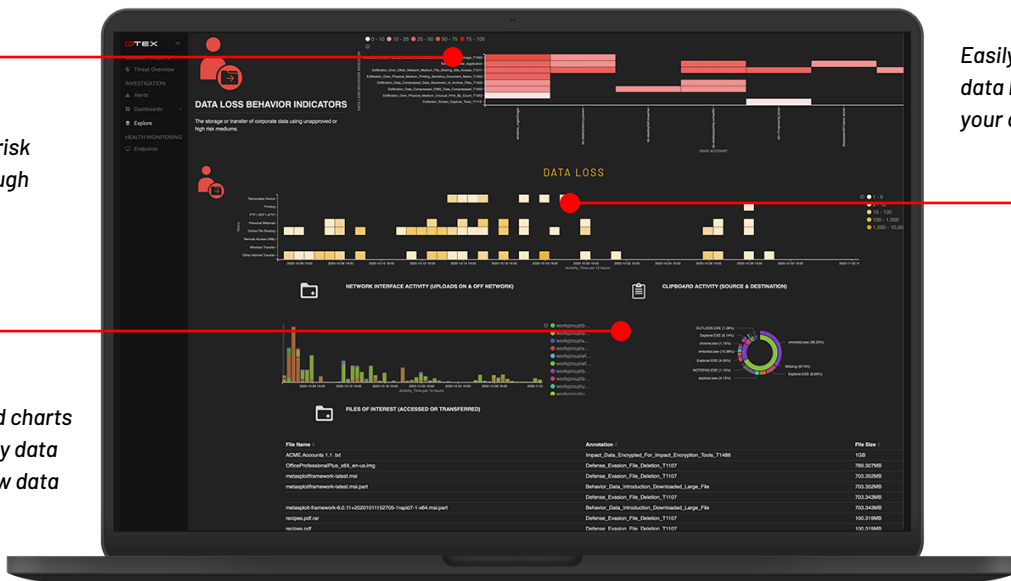
DTEX
THE WORKFORCE CYBER INTELLIGENCE COMPANY™

How **DTEX InTERCEPT** Detects and Stops Insider Threats

Insider Threat Management solutions are deployed to stop data exfiltration incidents including those initiated by a departing employee. The diagram below is a timeline representing common behaviors and actions involved in a data exfiltration incident.

In this scenario, an employee has decided it is time to leave her employer. After signing an offer letter from a competitor, she begins to search and download sensitive documents across SharePoint and accessible files shares. The employee archive and encrypts these files, obfuscates the data and attempts to exfiltrate via USB, drop-box and his/her personal Gmail account. Through continuous data lineage profiling of every file accessed, moved or renamed, DTEX InTERCEPT understands that the SharePoint design files and the obfuscated PDF file are one and the same, and also a key 'Indicator' of malicious intent. Many of these steps occur while off the company network or VPN. DTEX records every activity in this scenario and stitches this information together into one user incident report for an analyst to investigate. 'Indicators of Intent' present themselves well before the full scenario plays out and allows analysts and the organization to stop exfiltration.

SUPPORTED PLATFORMS

Microsoft   Linux   macOS®   CITRIX®

REQUEST A DEMO

Contact us today to schedule a demonstration
demo@dtexsystems.com

"

We evaluated five solutions against a weighted criteria of 13 must-have capabilities including user behavior monitoring within specialty engineering applications and a collector that was invisible to employees. DTEX InTERCEPT was the only solution that gave us those light-weight collection capabilities and the visibility we need to support our mission-critical operational requirements."

Graeme Hackland
Chief Information Officer, Williams Racing

WILLIAMS RACING