DTEX InTERCEPT for Behavioral DLP

Zero Trust People-Centric Data Loss Prevention

DTEX
WORKFORCE CYBER INTELLIGENCE & SECURITY

Prevent Data Loss
with behavioral intent intelligence.

Detect Insider Threats
with dynamic risk scoring.

Enrich SOC Operations
with human telemetry.

Accelerate Incident Response
with real-time forensics.

DTEX InTERCEPT for Behavioral DLP is the industry's first and only Zero Trust 'People-Centric' Endpoint DLP product explicitly designed to address the data protection and insider risk challenges of distributed and digital enterprises.

Data Loss Prevention solutions are an integral part of almost every public and private organization's cybersecurity framework. The data-centric approach of first-generation solutions, however, has failed to keep sensitive IP safe and prevent data exfiltration due in part to cumbersome rules and policy administration and management, lack of support for and visibility into Windows, Mac and Linux operating systems, and browser incompatibilities. Intrusive content scanning of files and applications has created additional performance issues that interfere with user workflows, block normal business processes and create non-compliance with regulatory mandates such as GDPR.

DTEX InTERCEPT for Behavioral Data Loss Prevention addresses the design, architectural and functional inadequacies of first-generation, data-centric Endpoint Data Loss Prevention solutions with seven unique and innovative capabilities that meet the dynamic needs of today's distributed organization.

Workforce Behavioral Intelligence & Analytics

DTEX InTERCEPT for Behavioral Data Loss Prevention demystifies the context and intent of human behaviors without violating the trust and privacy of employees. DTEX utilizes patent-pending artificial intelligence and machine learning data science to collect, analyze and baseline acceptable user behavior by role, department and geography. Alert stacking and activity scoring algorithms accurately detect deviations that precede data loss events and prevent data loss resulting from compromised, malicious and negligent behaviors.

360° Enterprise DMAP+ Visibility

DTEX InTERCEPT does not rely on rules to determine what it sees or doesn't see. Rather, it employs continuous, lightweight endpoint metadata capture and behavioral monitoring across every Windows, Mac, Linux and Citrix endpoint and server, on and off-network. More than 500 data elements are collected, analyzed and used to continuously update a forensic audit trail of scored user behaviors and made available to analysts in real time for response and investigations.

File Lineage Forensics & Auditing

DTEX InTERCEPT for Data Loss Prevention delivers a full audit history detailing file activity to enable a real-time, contextual understanding of the severity of 'indicators of intent' of a data loss event. Not only file movement but a full audit trail of by whom and when each file is created, modified, aggregated, obfuscated, archived, encrypted and deleted. These added attributes provide a clear distinction between normal activity and true data loss events.

Sensitive Data Profiling

Profiling data with a content-based approach using keywords, patterns and regular expressions create an abundance of false positives, which has limited the effectiveness of traditional DLP solutions. DTEX InTERCEPT's sensitive data profiles and analytics addresses this by inferring sensitivity based upon file lineage, file location, creation, user role, file types and many additional file attributes. This telemetry is correlated with a user's behavior profile, as well as leading data classification tools, to detect the potential loss of sensitive and suspicious data without the need for content-aware rules. This dramatically decreases false-positive events and the time needed for administrators to constantly tune rules and policies and an analyst's time to investigate data loss alerts.

Clean, easy-to-understand charts and graphs demonstrate key data loss metrics, including how data is handled on or off the network.

Quickly understand high-risk users and activities.

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

BEHAVIORAL DLP FROM DTEX IS:

ACCURATE
InTERCEPT doesn't deliver false positives that waste your security staff's time. It's smart enough to understand the difference between normal and malicious behavior, enabling you to quickly zero in on real threats - and deal with them.

BEHAVIOR-BASED
InTERCEPT's anomaly detection technology baselines user and device activities and can compare suspicious events to the behavior of a user, a department, or an entire organization.

EXTENSIBLE
InTERCEPT allows you to monitor your entire workforce, not just a few privileged insiders. That helps you catch the user negligence behind many insider incidents and take remedial action regardless of their geo-location, on- and off-network.

LIGHTWEIGHT
A zero-impact, cloud-native solution, InTERCEPT collects only 3-5MB of data per user each day with low CPU usage and zero impact on employee productivity or endpoint performance.

TRIGGER-FREE
InTERCEPT is focused on activities, not content. It continuously monitors all applications to spot suspicious events and empower the analyst with full context.

Risk-Adaptive Data Protection

DTEX InTERCEPT protects sensitive data and IP from leaving an organization with multiple, highly accurate and dynamic enforcement capabilities. Data loss is prevented intelligently when a user's behavioral risk score exceeds an organization's threshold by blocking specific application processes and network connections that are not part of normal or approved workflows. This includes blocking FTP, large files in email and access to certain cloud services. Additionally, SOC teams and analysts can remotely remove a user's credentials and lock them out of their device. These risk-based blocking features best meet the requirements of today's distributed workforce models, reduce operational overhead, and eliminate false positives.

Regulatory Data Loss Compliance

DTEX InTERCEPT supports a balanced and proportional approach to data loss prevention that exceeds the requirements of regulatory mandates with out-of-the-box compliance for HIPAA, CCPA, GDPR, SOX, PCI DSS, ITAR and others.

Cloud Architecture & Interoperability

DTEX InTERCEPT's SASE architecture introduces a lightweight forwarder that requires no more than 3–5MB of bandwidth per day per endpoint and utilizes less than 1% CPU. Data is collected and synchronized in near-real-time with DTEX's Cloud Analytics Engine for analysis, detection and prevention, eliminating the likelihood of user productivity issues and ensuring seamless interoperability with NGAV, IAM and UEBA solutions.

DTEX InTERCEPT™ is a first-of-its-kind Workforce Cyber Security solution that brings together the capabilities of Insider Threat Management, User and Entity Behavior Analytics, Digital Forensics and Endpoint DLP in an all-in-one lightweight, cloud-native platform.

Only DTEX InTERCEPT delivers the context and intelligence that answers the **Who, What, When, Where** and **How** related to any potential insider threat situation, compromised account event or data loss scenario.

DTEX InTERCEPT Zero Trust Behavioral DLP vs. Traditional Data-Centric Endpoint DLP Tools

Vendors		DTEX	Digital Guardian	Forcepoint	McAfee	Proofpoint	Symantec
DLP Use Case	Feature(s)						
Contextual Awareness	Behavioral Analytics and Machine Learning (native)	+++		+ (FBA/Requires 2nd agent)			
	File Lineage Forensics and Auditing	+++	+		+	+	
	MITRE ATT&CK and InT Kill Chain Framework Mapping	+++	+		++	+	+
Regulatory Compliance	Native Data Classification Integration	++	++	++	+	++	+++
	Compliance & Executive Report	+++	++	++	+	++	+
	Regulatory Data Loss Compliance	++	++	++	+++	++	+++
Theft of Intellectual Property	Sensitive Data Profiling with Inferred IP Sensitivity	+++					
Scalability	Lightweight Agent/Collector (near-zero impact to endpoint & network)	+++		+			
	Native Cloud Architecture (scalable to 100,000+ users)	+++	+	+		++	
	Breadth of Endpoints	++	+	++	+++	+	++
Automation	Risk-Adaptive Data Protection (e.g., Zero Trust DLP enforcement)	++	+	+ (FBA/Requires 2nd agent)	++	+	++
	Teachable-Moment Reporting	++		+		+	

ABOUT DTEX SYSTEMS

DTEX Systems helps hundreds of organizations worldwide better understand their workforce, protect their data and make human-centric operational investments. Its Workforce Cyber Intelligence & Security platform brings together next-generation DLP, UEBA, digital forensics, user activity monitoring and insider threat management in one scalable, cloud-native platform. Through its patented and privacy-compliant metadata collection and analytics engine, the DTEX platform surfaces abnormal behavioral "indicators of intent" to mitigate risk of data and IP loss, enabling SOC enrichment with human sensors and empowering enterprises to make smarter business decisions quickly. To learn more about DTEX Systems, please visit www.dtexsystems.com.