SOLUTION BRIEF

DTEX USER AND ENTITY BEHAVIOR ANALYTICS

Uncover behavioral intent through data-driven science

Behavior analytics have become an integral part of modern security strategy. The value is based in the ability to use machine learning to recognize activity patterns. This is done by correlating a wide range of seemingly unrelated data points and summarizing them into easy-to-understand actionable intelligence to stop a security breach.

A huge benefit of behavioral monitoring and analysis is that it evolves with the threat landscape and significantly improves an organization's understanding of risk. Continuously comparing behavior patterns can quickly identify activities that can lead to a security incident.

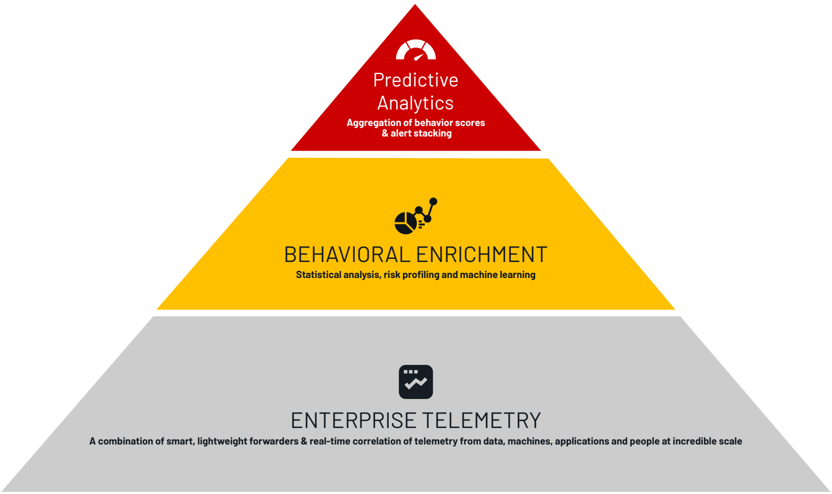
But the often-overlooked challenge is that to be effective, solutions are also highly dependent on the quality of the data being analyzed. Today's "good enough" security is often not good enough to protect your data, your employees, and your brand. A more successful approach involves more than simply layering UEBA on top of a security information and event management (SIEM) platform or adding a heavy, intrusive User Activity Monitoring tool to the network.

DTEX InTERCEPT

DTEX InTERCEPT™ is a purpose-built insider risk management platform that consolidates the essential capabilities of user and entity behavior analytics (UEBA), user activity monitoring (UAM) and data loss prevention (DLP) in a single solution to provide early detection and mitigation of insider risks. InTERCEPT employs continuous, behavioral monitoring, combining rich telemetry from across cyber, physical, and psycho-social sensors to detect and deter true insider risks at unmatched scale.

Minimize Collection, Maximize Accuracy

DTEX collects the minimum amount of data needed to build a forensic audit-trail, only 3-5 MB of data per user each day, with near zero endpoint or network impact. Data is captured from distributed devices, important for offering a comprehensive view of user behavior across the organization, and includes detailed information not provided by 3rd-party external log sources. DTEX metadata is the foundation for risk scoring algorithms to accurately identify deviations and indicate compromised, malicious and negligent behaviors.


Predictive Analytics
Aggregation of behavior scores & alert stacking
BEHAVIORAL ENRICHMENT
Statistical analysis, risk profiling and machine learning
ENTERPRISE TELEMETRY
A combination of smart, lightweight forwarders & real-time correlation of telemetry from data, machines, applications and people at incredible scale

Data Loss Protection for Endpoints and Servers

DTEX supports Windows and Mac workstations, Windows and Linux servers, and Citrix and VMware endpoints and servers that are deployed in the cloud, on-premises or as virtual servers. And they are monitored both on and off-network, providing real-time visibility into all user activity. Tracking relationships between entities in the system provides immediate insight into complex network interactions.

DTEX DMAP+ Technology

Powered by DMAP+ Technology™, InTERCEPT continuously collects unique elements of enterprise telemetry from data, machines, applications, and people to capture activity history, behavior trends, data utilization with situational context from across the enterprise to form a holistic understanding of insider risk and prevent data loss. Using behavioral enrichment, InTERCEPT identifies patterns or sequences of potentially related attributions. This enables teams to identify and correct risky activity sooner, while eliminating false positives.

DTEX does not rely on intrusive data collection and rules or violate employee privacy. DTEX patented Pseudonymization tokenizes personally identifiable information (PII) so organizations can apply the principle of proportionality to monitor employees based on the nature of the risk they pose.

AI-Driven Investigations

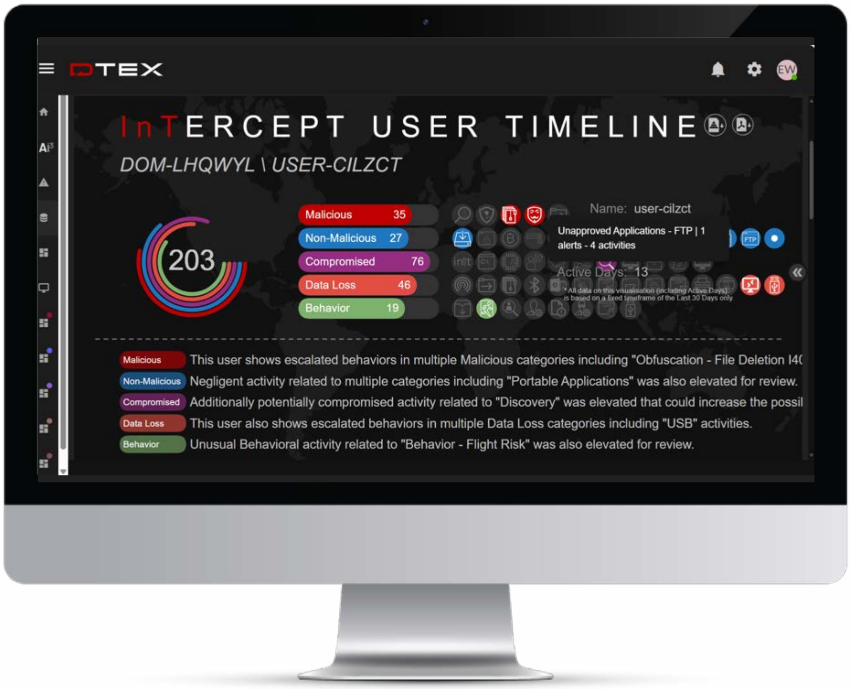
The DTEX Ai^3 Risk Assistant can help guide investigations that empower analysts to ask pointed questions about behavioral intent, who is risky, and most importantly, why.

HTTP inspection capabilities detect end user interactions with generative AI chat sites, cloud sign-ins, file uploads and downloads, and text translations to help prevent unauthorized use or sharing of sensitive information.

User Risk Modeling

Through AI-driven data science, InTERCEPT analyzes and baselines user behavior by role, department and geography and creates dynamic risk scores to accurately identify deviations. With high fidelity metadata and behavioral modeling, DTEX goes deeper than 'usual vs unusual' behavior to focus on activities truly associated with data loss like reconnaissance, obfuscation and circumvention. This forward-looking method pinpoints risk early in the kill chain before exfiltration can occur, enabling proactive defense strategies.

DTEX provides trigger notifications for abnormal activity and identifies elevated risks in interactive dashboards for forensic investigation, protective action, and cross-functional reporting. Information can also be exported to various 3rd party solutions like SIEM and Security Orchestration, Automation, and Response (SOAR) for subsequent action.



InTERCEPT USER TIMELINE

DOM-LHQWYL \ USER-CILZCT

203

Malicious	35
Non-Malicious	27
Compromised	76
Data Loss	46
Behavior	19

Name: user-cilzct

Unapproved Applications - FTP | 1 alerts - 4 activities

Active Days: 13

* All data on this visualisation (including Active Days) is based on a fixed timeframe of the Last 30 Days only

Malicious This user shows escalated behaviors in multiple Malicious categories including "Obfuscation - File Deletion I4(

Non-Malicious Negligent activity related to multiple categories including "Portable Applications" was also elevated for review.

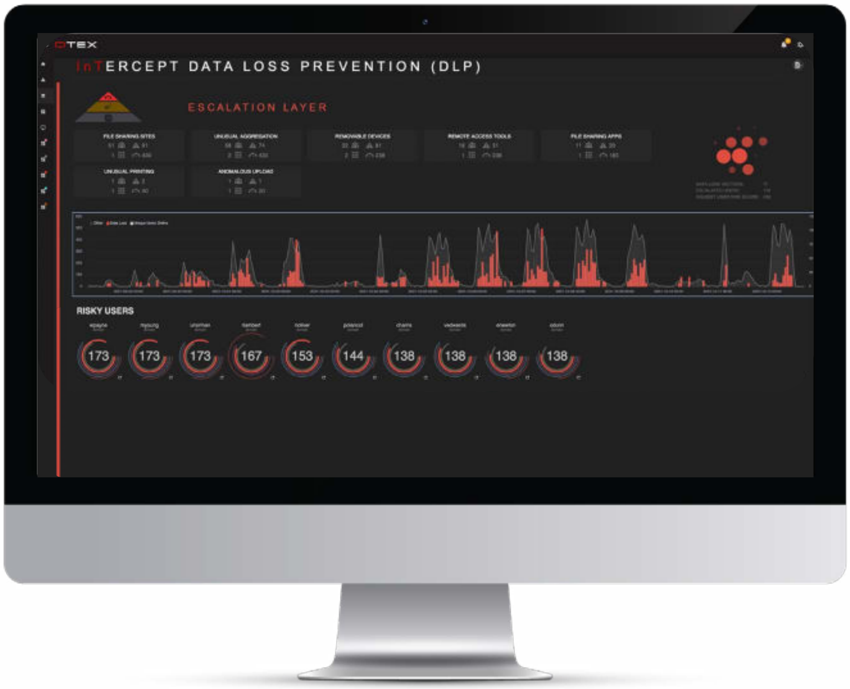
Compromised Additionally potentially compromised activity related to "Discovery" was elevated that could increase the possil

Data Loss This user also shows escalated behaviors in multiple Data Loss categories including "USB" activities.

Behavior Unusual Behavioral activity related to "Behavior - Flight Risk" was also elevated for review.

DTEX Behavioral DLP

DTEX behavioral DLP captures full file lineage to enable contextual understanding of data movement and behavioral intent including a complete audit trail of when every file is created, modified, aggregated, obfuscated, archived, encrypted, deleted, and by who. Data sensitivity is inferred based on file lineage, file location, creator, user role, file types and other file attributes. These data profiles are correlated with user behavior and leading data classification tools to detect the movement of sensitive and suspicious data without heavy content-aware rules.



Privacy by Design

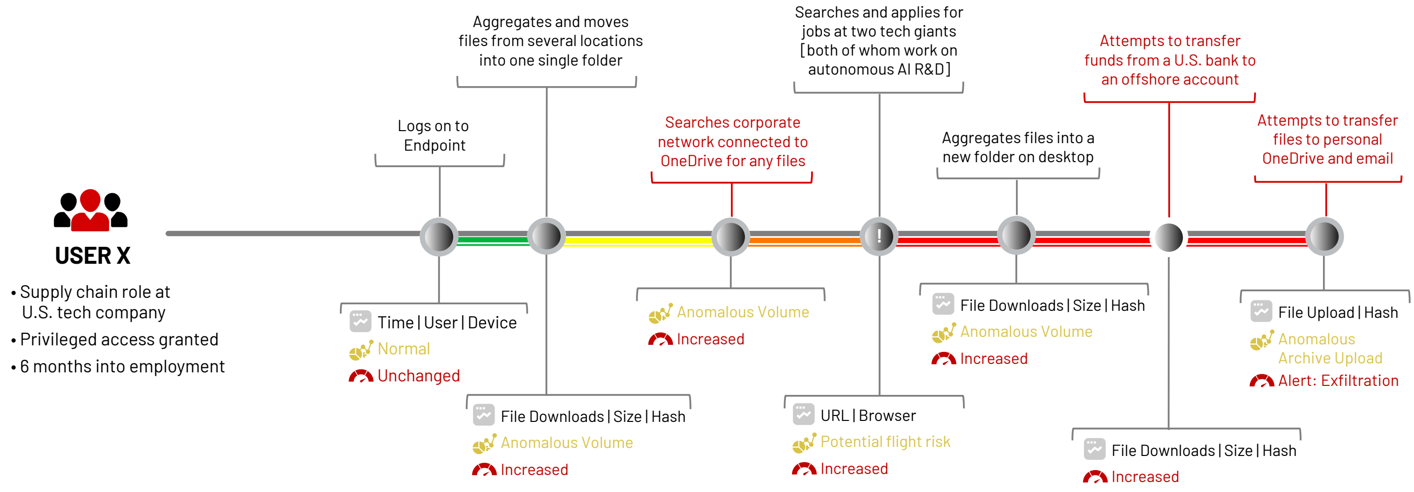
DTEX Pseudonymization™ ensures InTERCEPT can operate even under some of the strictest privacy regulations in the world like General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). DTEX applies Pseudonymization across raw data fields, including username, email, IP address, domain name, and device name, without affecting the underlying risk model or the ability to investigate suspicious behavior. Pseudonymization safeguards against identity theft, financial fraud, and other cybercrimes while providing the needed level of visibility to identify high risk events.

Improving on Zero Trust Strategy

The DTEX platform improves on a Zero Trust (ZT) security model by surfacing behavioral indicators of intent from individuals with permissions on the inside, defending ZT policies while keeping organizations aware of impending threats. With a continuous threat posture for every user based on behavioral risk scoring, DTEX enables organizations with risk-adaptive policy enforcement.

Behavioral Risk Modeling: A Timeline

The timeline below shows how behavioral analysis identifies indicators of intent and impacts user risk score.


USER X
• Supply chain role at U.S. tech company
• Privileged access granted
• 6 months into employment
Logs on to Endpoint
Time | User | Device
Normal
Unchanged
Aggregates and moves files from several locations into one single folder
File Downloads | Size | Hash
Anomalous Volume
Increased
Searches corporate network connected to OneDrive for any files
Anomalous Volume
Increased
Searches and applies for jobs at two tech giants [both of whom work on autonomous AI R&D]
URL | Browser
Potential flight risk
Increased
Aggregates files into a new folder on desktop
File Downloads | Size | Hash
Anomalous Volume
Increased
Attempts to transfer funds from a U.S. bank to an offshore account
File Downloads | Size | Hash
Increased
Attempts to transfer files to personal OneDrive and email
File Upload | Hash
Anomalous Archive Upload
Alert: Exfiltration

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 meta-data 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 dtexsystems.com.