

Behavioral DLP & Workforce Visibility for CrowdStrike Falcon

Next-Gen Human Intelligence, Endpoint Telemetry & Digital Forensics



Prevent Data Loss
with behavioral intent intelligence.



Detect Insider Threats
with dynamic risk scoring.



Maintain Privacy & Compliance
with human telemetry.

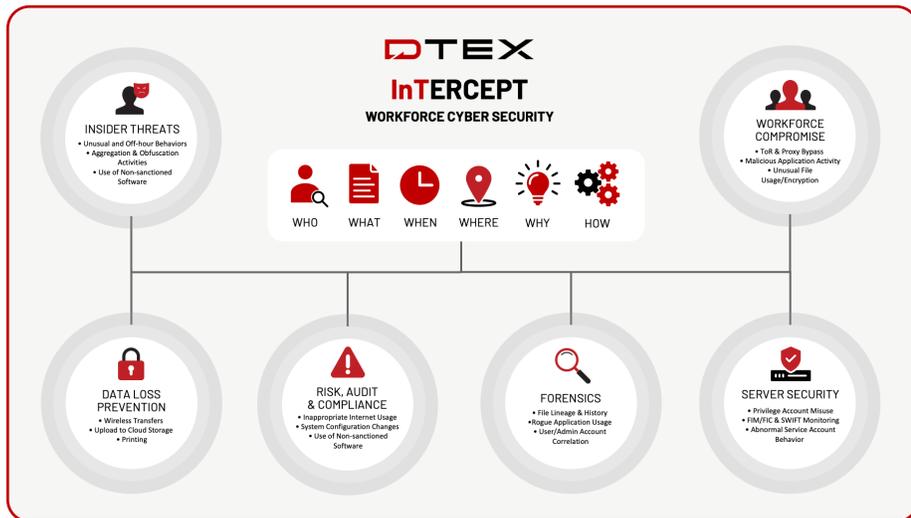


Accelerate Incident Response
with real-time forensics.

The most valuable assets for every enterprise are its employees. Those same employees, and their digital identities, represent the greatest risk to data, IP and operational resiliency yet most cybersecurity solutions do nothing to address human risks because they focus solely on machines, applications, and networks. They are blind to genuine human behavioral history, trends, and context.

Understanding human **'intent'** directly from the endpoint is the most important element of a Zero Trust DLP strategy that will work in today's and tomorrow's virtual economy driven by a distributed workforce no longer dependent on the network perimeter.

As part of the CrowdStrike Store, customers can seamlessly deploy DTEX InTERCEPT Behavioral DLP capabilities within the CrowdStrike Falcon platform to gain real-time, contextual visibility into human activity and data usage telemetry. This behavioral intent intelligence answers **How, When, Why, Where** and **What** sensitive IP and other data files every employee and third party is interacting with, aggregating, archiving, modifying, obfuscating, and may be attempting to exfiltrate. Customers also gain access to DTEX Systems' digital forensics intelligence to enable on-demand compilation of an evidentiary quality audit trail of user activities to enrich incident response investigations.



DTEX InTERCEPT is a first-of-its-kind Workforce Cyber Security solution that focuses on human intent and activity at its core. It brings together the capabilities of Behavioral Data Loss Prevention, Digital Forensics, Insider Risk Management, Remote Worker Security, and User and Entity Behavior Analytics in an easy-to-deploy, extremely lightweight cloud-native platform.

With DTEX InTERCEPT, employees are ensured non-intrusive, privacy-compliant intelligence gathering that recognizes them as partners in enterprise security and operational efficiency initiatives. Likewise, enterprise security and IT teams benefit from real-time, metadata human behavioral intelligence that detects anomalies, automates peer group profiling, correlates user logic and behavioral risk scoring to enrich Falcon.



With DTEX InTERCEPT, we understand what is happening to our data, who is using it and where it is going because we can truly evaluate behavior. If important data is being used or replicated in ways that seem abnormal or unnecessary, such as attempts to copy to external drives or uploads to non-corporate cloud storage sites, this signals a risk. If this behavior is negligent, we can take steps to educate the user. If it is malicious, we can take appropriate action to ensure that data meant for our organization stays within our organization."

Bruce Moore
Chief Information Officer,
Victorian Rail Track Corporation

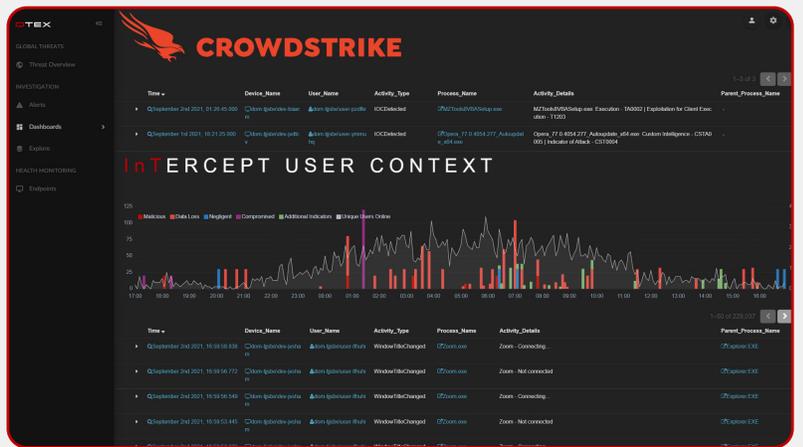
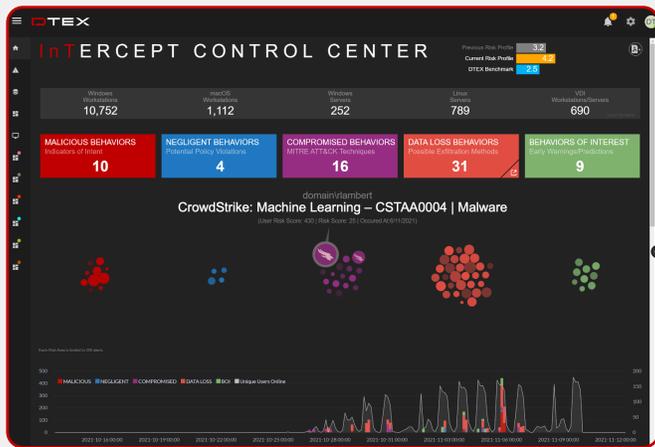


KEY FEATURES:

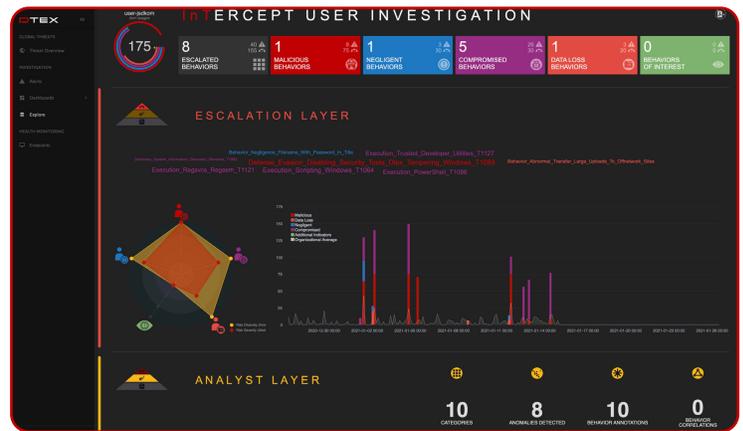
- Lightweight Collector & Forwarder
- Real-Time Cloud Analytics
- Dynamic Activity Risk Scoring
- Digital Forensics & Audit Reports
- Live, Interactive Dashboards
- Executive Reports

How Organizations Are Utilizing DTEX InTERCEPT with CrowdStrike Falcon®

- **Behavioral Data Loss Prevention:** Highly actionable, user behavior-focused data utilization intelligence protects regulatory-mandated and valuable IP data movement on and off-network in use, at rest, in transit from leaving the organization.
- **Digital Forensics & Incident Response:** Human telemetry compliments Falcon Forensics to provide user-centric, pre-incident behavioral evidence that fills in gaps in context and ‘intent.’



- **Insider Threat Detection & User Lockout:** This anonymously identifies which users are engaging in malicious, negligent and compromised behaviors, offers real-time contextual investigation and escalation, and allows for immediate user lockout to prevent data exfiltration.
- **Work-from-Home (WFH) Engagement Monitoring:** Easily understand and compare the processes of team members alongside one another to evaluate productivity, balance workloads, spot abnormal activities and support team members to enable increased productivity.
- **Shadow IT/Unwanted Applications:** Identify the most used and least used apps in an environment, evaluate necessity and risk, and identify potential licensing issues.



SUPPORTED PLATFORMS



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.