DTEX

DATASHEET

# DTEX InTERCEPT Insider Risk Management

*Proactively stop insider risks and prevent data loss*

The cost of an insider threat is the highest it's ever been, as the number of insider incidents continues to grow in both cost and frequency. Meanwhile organizations are spending more time and money on security solutions to stop these threats from happening. But insider risk management requires a nuanced approach to understand and proactively address behavioral indicators of risk.

## 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, light weight platform to provide early detection and mitigation of insider risks. Combining rich metadata across cyber, physical, and psycho-social sensors, InTERCEPT surfaces unique risk indicators to detect and deter true insider risks at unprecedented scale. It enables organizations to:

**Prevent Data Loss**
with behavioral intent intelligence.

**Detect Insider Threats**
with dynamic risk scoring.

**Fast-track Investigations**
with AI-driven insight.

**Maintain Privacy & Compliance**
with human telemetry.

### DTEX DMAP+ TECHNOLOGY

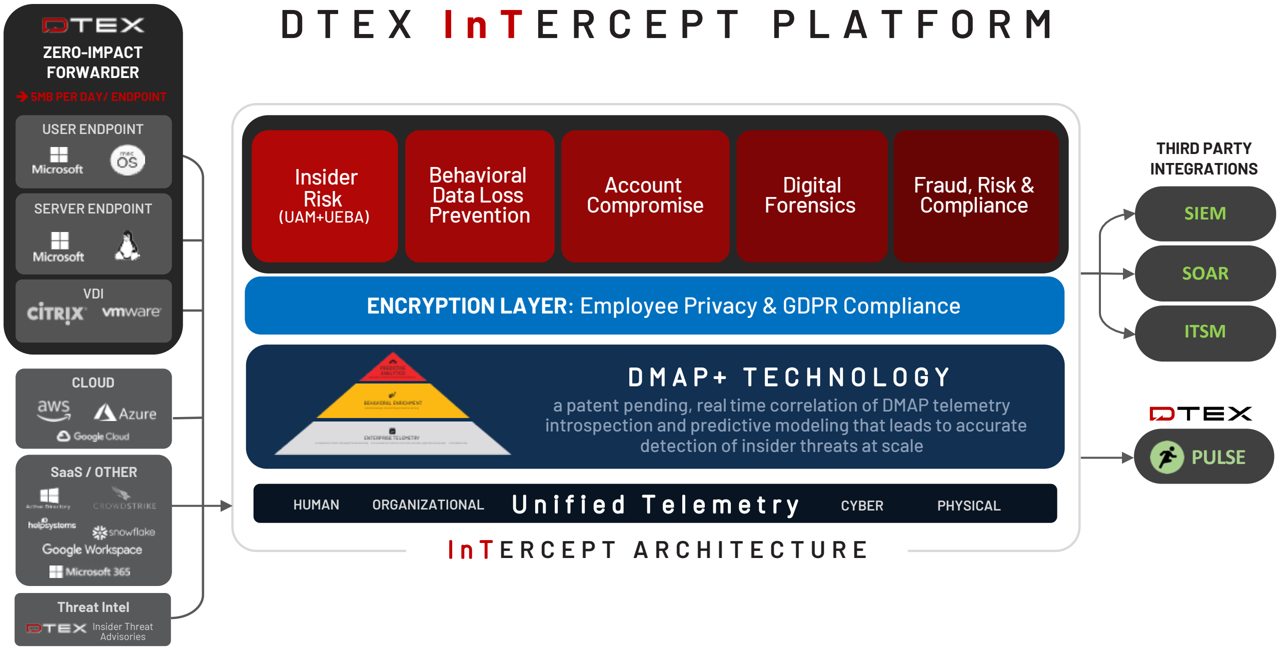
Powered by DMAP+ Technology™, InTERCEPT collects unique elements of enterprise telemetry from data, machines, applications, and people to capture activity history, behavior trends, data utilization with situational context from across the enterprise to form a holistic understanding of insider risk and prevent data loss. Using behavioral enrichment and backed by artificial intelligence and machine learning, InTERCEPT does not generate alerts for discrete events. Instead, it maintains a risk score for every user and activity to identify patterns or sequences of potentially related attributions. This enables teams to identify and correct risky activity sooner, while eliminating false positives.

## KEY FEATURES

- **Lightweight forwarder** collects 3-5 MB of metadata per user each day.
- Real-time threat posture for every user, both **on and off network**.
- **Behavioral risk scores** identify malicious, negligent, or compromised users.
- **Full file lineage** provides context for file changes and behavioral intent.
- **Patented Pseudonymization™** tokenizes personally identifiable information (PII).
- **AI-driven investigations** synthesize data into human-centric insights.
- **200+ out-of-the box dashboards** visually simplify threat-specific information.
- **Executive reports** summarize organizational risk with actionable recommendations.

## 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 INTERCEPT CORE CAPABILITIES

- **InTERCEPT Insider Threat**
  DTEX Insider Threat, with UEBA and UAM, supports thousands of pre-configured and customizable behavioral indicators. Automatic user baselining, anomaly detection, and risk scoring work together to accurately identify deviations. Out-of-the-box (OOTB) dashboards and reports are available for insider threat use cases.

  *Use cases: bypass of security controls, flight risk, and obfuscation and covering tracks.*

- **InTERCEPT Behavioral DLP**
  Behavioral DLP provides thousands of pre-configured DLP patterns of risky behavior. DTEX data sensitivity modelling identifies file sensitivity without the need for heavy content inspection. File lineage tracks interactions and changes to files, and data exfiltration analytics identifies behavioral indicators in advance of exfiltration. OOTB dashboards and reports are available for specific DLP use cases.

  *Use cases: uploads to cloud storage, USB device usage, and printing.*

- **InTERCEPT Account Compromise**
  MITRE ATT&CK$^{TM}$ profiling identifies lateral movement, privilege escalation, and other behaviors associated with malware. Through the collection of additional telemetry such as specific Windows Event Log IDs and Registry Change activity, credential misuse analytics help to identify account compromise.

  *Use cases: unusual privilege escalation, domain fronting, lateral movement.*

- **InTERCEPT Digital Forensics**
  Digital Forensics provides continuous activity audit trails that are captured directly from endpoints and servers as well as custom dashboard visualizations.

  *Use cases: file lineage, activity audit trail, abnormal internet activity.*

- **InTERCEPT Risk and Compliance**
  DTEX Risk and Compliance supports teachable moments detection and direct user communication for reminders of acceptable use policy. Automated reports support audit findings and adherence to policies with actionable recommendations.

  *Use cases: software license utilization, online file sharing, inappropriate internet usage.*

## AI-Driven Insights and Investigations

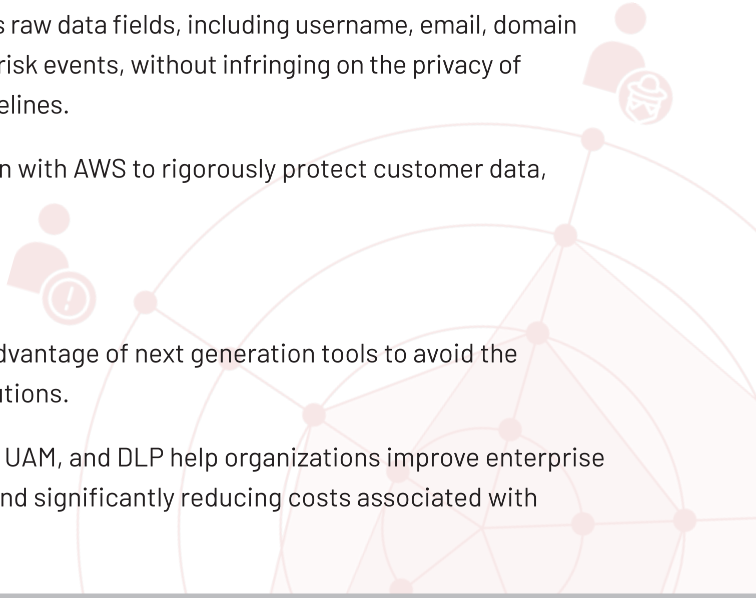
Insider risks are a human challenge that require an understanding of behavior through data-driven science. Based on behavioral risk modeling and DTEX metadata, InTERCEPT's human-centric detection capabilities baseline user and device activity to identify suspicious events and spot indicators of intent. No more false positives. A modern approach to insider risk management means intelligent context makes insights actionable.

With the DTEX Ai3 Risk Assistant, AI-assisted insider investigations provide greater awareness and an interpretation of user intent to identify and respond to insider risks faster and more effectively.

## Privacy and Protection by Design

The DTEX InTERCEPT platform has been built with privacy by design. With this in mind, the platform collects the minimum amount of metadata - 5MB per user per day needed to build a forensic audit-trail, significantly reducing the number of data sources necessary for an effective insider risk investigation. The platform applies its patented Pseudonymization™ technique to tokenize personally identifiable information (PII) across raw data fields, including username, email, domain name, and device name. This enables organizations to identify high risk events, without infringing on the privacy of individuals, and comply with GDPR, CCPA, and other regulatory guidelines.

Hosted on Amazon Web Services (AWS), DTEX works in conjunction with AWS to rigorously protect customer data, encrypting data both in transit and at rest.



## Simplify the Security Stack

As platforms modernize, many organizations have begun to take advantage of next generation tools to avoid the cumbersome and intrusive nature of many traditional security solutions.

DTEX high fidelity metadata and the combined strengths of UEBA, UAM, and DLP help organizations improve enterprise security and modernize the security stack, optimizing workflows and significantly reducing costs associated with disparate point solutions.

DTEX

**To learn more about DTEX Systems, please visit dtexsystems.com.**

**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.