DTEX Data Privacy and Protection

Establishing Trust and Confidence

Insider Risk Management (IRM) and the monitoring of all activities in the workplace is now recognized as a core security requirement for many organizations. With the myriad of data privacy and protection laws in different states and across countries, navigating the ever-changing data landscape may seem like a daunting task. DTEX helps hundreds of organizations worldwide better understand their workforce, make effective security investments, and comply with regulatory requirements while keeping data private and protected.

Minimize Collection, Maximize Accuracy

A common challenge organizations face is striking the balance between employee privacy and insider risk monitoring. Enterprise security systems almost always collect more data than they need to, undertaking significant costs associated with excess data storage and processing that is unnecessary for improving security. The DTEX InTERCEPT™ platform has been uniquely designed to collect the minimum amount of metadata needed to build a forensic audit-trail, significantly reducing the number of intrusive data sources. The DTEX lightweight forwarder collects only 3-5 MB of metadata per user each day with near zero endpoint or network impact.

Visibility Without Intrusive Methods

Privacy laws vary drastically between different countries and industries. The DTEX collection method and anonymization ensure that InTERCEPT™ can operate even under some of the strictest privacy regulations in the world. DTEX applies its patented Pseudonymization technique to tokenize PII 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. Removing personal identifiers eliminates inherent bias, protects workers from undue surveillance, and complies with privacy regulations like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).

Pseudonymization also safeguards against identity theft, financial fraud, and other cybercrimes while providing the needed level of visibility to identify high risk events. Using this patented process, organizations can apply the principle of proportionality to monitor employees based on the nature of the risk they pose.

Additionally, DTEX behavioral DLP uses a unique approach designed to identify sensitive information in unstructured data, without having to inspect the data itself. A digital fingerprint is used to classify data, not the contents. For this reason, InTERCEPT is a valuable complement to email security solutions and network based DLP products.

Secure Data Handling

DTEX handles all data in a secure manner with written policies detailing security measures. Customers are given a choice, from a set of AWS regions, on where they would like their data to reside. Once chosen, the data does not leave that region. DTEX logs all data processing.

DTEX is experienced in working on Privacy Impact Assessments (PIAs).

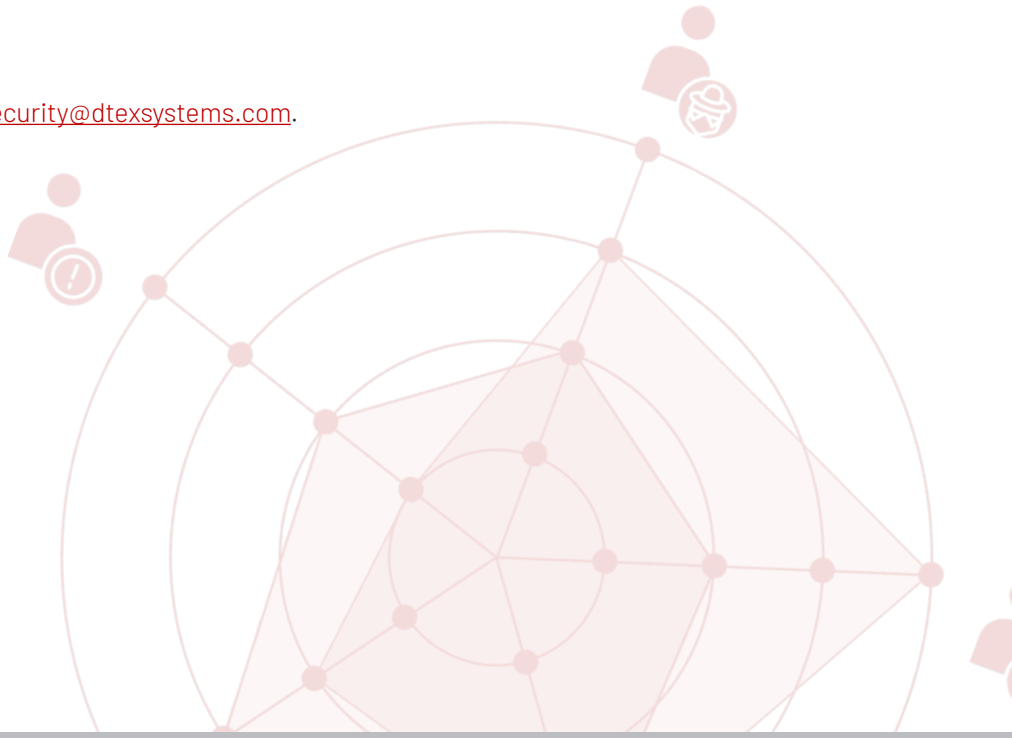
Ensuring Data Protection

Data protection is based on tools and policies that prevent data breaches and misuse. It works to secure data with techniques like encryption and access controls, mitigating risks of financial loss and reputational damage.

The DTEX architecture is based on Amazon Web Services. Amazon rigorously protects customers resources with its own methods and practices as described in https://aws.amazon.com/security. DTEX follows Amazon's Shared Responsibility Model to ensure end-to-end security of services. All unique tenant datasets are separated through AWS VPCs and S3 buckets. DTEX manages data in a separate AWS account from DTEX corporate workloads.

All DTEX data is encrypted both at rest and in transit.

For additional information please contact security@dtexsystems.com.



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.