DTEX Insider Risk Management and the Department of Defense Zero Trust Strategy

Insider Risk Management and Zero Trust

Zero Trust (ZT) stands on a set of security principles that has evolved the focus of security from the network perimeter to users, devices, and data. But a limitation of ZT strategies lies in an inability to understand context behind actions.

DTEX improves on a Zero Trust security model by surfacing behavioral indicators of intent from individuals with permissions on the inside, defending ZT policies while keeping agencies left of boom. With a continuous threat posture for every user based on behavioral risk scoring, DTEX can enable agencies with risk-adaptive policy enforcement.

Aligned with the Department of Defense's (DoD) strategic goals to achieve its vision for Zero Trust through culture, adoption and practice, DTEX partners with agency programs on the journey to Zero Trust-based security and ultimately provides better outcomes as adversaries evolve.

DTEX AND THE SECURITY ECOSYSTEM

A well-connected technology ecosystem helps to create a comprehensive and proactive security strategy that leverages the strengths of individual products and provides a more holistic, business-oriented approach to problem solving. It can result in increases in productivity, lower costs, and the overall reduced risk of a security incident. Zero Trust as a framework relies on a connected ecosystem of technology integrations to support effective policies.

DTEX InTERCEPT integrates with a wide range of technologies, from next generation antivirus (NGAV), endpoint detection and response products (EDR), and cloud access security brokers (CASB) to security information and event management (SIEM), security orchestration, automation, and response (SOAR), and IT service management (ITSM) platforms. This approach assists in unifying policies across domains and helps organizations to more effectively manage risk.

The DTEX InTERCEPT™ Platform

DTEX InTERCEPT is a purpose-built insider risk management platform that consolidates the essential capabilities of UEBA, UAM and DLP to provide early detection and mitigation of insider risks. InTERCEPT complies with the National Insider Threat Taskforce (NITTF) minimum requirements for UAM while leveraging AI to form an aggregate, anonymized risk profile for every user in an organization. While InTERCEPT integrates with other security solutions like EDR, SIEM, and SOAR, the DTEX platform relies on a unique dataset from human, organizational, cyber, and physical sources to produce a holistic view of behavioral risk and facilitate mitigation well before a data loss event occurs.

Collaborative research partnerships with the U.S. Defense Information Systems Agency (DISA) and the MITRE Corporation have led to the development of key behavioral indicators that differentiate malicious behavior from benign. These DTEX partnerships have also led to integrations with additional data sets like the Open-Source Intelligence data sources and other insider threat frameworks, empowering InTERCEPT to deliver the most effective and accurate characterization of insider risk in the industry.

DTEX Coverage of DoD Zero Trust

DTEX provides extensive support for the DoD ZT strategy, capability and activity matrix. The heat map below summarizes support.

DTEX Heat Map for DoD Zero Trust Capabilities

User	Device	Application & Workload	Data	Network & Environment	Automation & Orchestration	Visibility & Analytics
1.1 User Inventory	**2.1** Device Inventory	**3.1** Application Inventory	**4.1** Data Catalog Risk Alignment	**5.1** Data Flow Mapping	**6.1** Policy Decision Point & Policy Orchestration	**7.1** Log All Traffic
1.2 Conditional User Access	**2.2** Device Detection and Compliance	**3.2** Secure Software Development & Integration	**4.2** DoD Enterprise Data Governance	**5.2** Software Defined Networking	**6.2** Critical Process Automation	**7.2** Security Information & Event Mgt'
1.3 Multi-Factor Authentication	**2.3** Device Authorization w/ Real Time Inspection	**3.3** Software Risk Mgt'	**4.3** Data Labeling and Tagging	**5.3** Macro Segmentation	**6.3** Machine Learning	**7.3** Common Security and Risk Analytics
1. 4 Privileged Access Mgt	**2.4** Remote Access	**3.4** Resource Authorization & Integration	**4.4** Data Monitoring and Sensing	**5.4** Micro Segmentation	**6.4** Artificial Intelligence	**7.4** User and Entity Behavior Analytics
1.5 Identity Federation & User Credentialing	**2.5** Automated Asset, Vulnerability and Patch Mgt	**3.5** Continuous Monitoring & Ongoing Authorizations	**4.5** Data Encryption & Rights Mgt		**6.5** Security Orchestration, Automation & Response	**7.5** Threat Intelligence Integration
1.6 Behavioral, Contextual ID, and Biometrics	**2.6** Unified Endpoint Mgt & Mobile Device Mgt		**4.6** Data Loss Prevention		**6.6** API Standardization	**7.6** Automated Dynamic Policies
1.7 Least Privileged Access	**2.7** Endpoint & Extended Detection & Response		**4.7** Data Access Control		**6.7** Security Operations Center & Incident Response	
1.8 Continuous Authentication						
1.9 Integrated ICAM Platform						

DoD Zero Trust Capabilities

User

DTEX InTERCEPT uses AI-driven data science to collect and baseline user behavior by role, department, and geography and accurately identify deviations that indicate compromised, malicious and negligent behaviors. DTEX identifies and tracks the activities of all users and provides full application visibility for all activities across the organization.

Combining behavioral rules and machine learning (ML), DTEX detects the use (or attempted use) of privileged admin accounts, as well as specific commands executed afterwards. Through continuous threat posture analysis, each user session is logged and analyzed as well as system account, service/local account and domain account activity to determine when a given account may be impersonated.

InTERCEPT is fully compliant with CNSSD 504 and NITTF minimum requirements for User Activity Monitoring.

DTEX can make dynamic access decisions based on risk and can export data to various 3rd party solutions for subsequent action.

Device

DTEX tracks an inventory of known assets and delivers a full audit history of file activity for a real-time, contextual understanding of data movement. Although the platform integrates across the security ecosystem to collect data from a variety of technologies to streamline security operations, DTEX InTERCEPT natively provides visibility beyond the endpoint, into application, network, and cloud activity.

Applications and Workloads

DTEX provides full application visibility of all activities. Through AI-driven data science, DTEX InTERCEPT continuously reviews users, devices and data security posture to accurately identify early indicators of malicious or compromised behavioral intent.

Data

With an emerging risk approach, DTEX unique metadata and behavioral enrichment work together to enable a real-time, contextual understanding of the 'indicators of intent' around a data event. DTEX behavioral DLP captures full file lineage to track all data changes and sensitive data profiles automatically infer data sensitivity. This is correlated with user behavior profiles and leading data classification tools to detect the movement of sensitive data without heavy content-aware rules. Data sensitivity can be used in rules to elevate the risk score of an individual and generate an alert.

Network and Environment

DTEX InTERCEPT monitors network traffic generated by endpoints via any application. Out-of-the-box rules are available to correlate file system activities with network activities, enabling effective profiling of data loss through webmail, file sharing sites, and other websites. These rules inform alerting and risk scoring.

Automation and Orchestration

The DTEX platform continuously collects and synthesizes unique elements of enterprise telemetry from data, machines, applications, and people to surface 'indicators of intent' that combine to deliver holistic, contextual awareness about user activity. DTEX provides trigger notifications of abnormal activity that deviate from baselines and indicate elevated risk to an interactive dashboard for forensic investigation, protective action, and cross-functional reporting.

Based on AI-driven automation, DTEX creates dynamic risk scores and captures full file lineage, enabling a more effective, contextual understanding of data movement and behavioral intent before a data loss event can occur. DTEX supports dynamic enforcement capabilities that can block FTP, large files in email and access to certain cloud services.

The DTEX Ai^3 Risk Assistant helps guide investigations that empower analysts with summarized user activity and to ask pointed questions like where sensitive data is going, who is accessing it, and most importantly, why. DTEX also detects end user interactions with Generative AI Chat sites, critical functionality to prevent unauthorized sharing, use, or transfer of sensitive information.

DTEX is based on Open Source Software, making integrations and API development quick and easy. Contact us for specific integration requirements.

Visibility and Analytics

DTEX dynamically updates InTERCEPT security profiles through continuous, organization-wide monitoring and risk scoring to surface early behavioral indicators of intent. DTEX unique metadata and behavioral enrichment underpin risk scoring algorithms to accurately identify deviations and indicate compromised, malicious and negligent behaviors.

InTERCEPT can act on data from integrations like NGAV, EDR and SWG, by blocking specific application processes and network connections that are not part of normal or approved workflows. To support a streamlined approach to data collection, the InTERCEPT platform can also export data to various solutions such as SIEM, SOAR, and ITSM for subsequent action.

DTEX i3 insider threat advisories, as well as external threat intelligence platforms, can be integrated into the DTEX platform and be exported to a SIEM or other 3rd party enterprise security tools.

Schedule a Demonstration

As an agency enabler for digital transformation and cultural change, DTEX provides the data to drive organization-wide decisions to protect data and strategically align to Zero Trust security principles.

Contact us at **dtexsystems.com/contact-us/** to learn more and to schedule a demo.

DTEX

To learn more 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.