info@dtexsystems.com | dtexsystems.com

SOLUTION OVERVIEW: Dtex for Federal Organizations

INTRODUCTION

It is particularly important for U.S. Government department and agencies to adhere to stringent cybersecurity policies, including instituting an effective and sustainable approach to protect against insider threats. Dtex's Enterprise User Intelligence provides an effective, scalable, and lightweight approach to user activity monitoring. Dtex collects user activity data through a lightweight endpoint collector, providing visibility wherever a user is connected to the internet. This data is then analyzed through machine learning and known-bad behavior patterns in order to detect anomalies, pinpoint risky behaviors, and elevate users for inspection.

This combination allows Dtex to effectively detect and investigate risks such as credential misuse, credential theft, lateral movement, creative data exfiltration methods, network sniffing and hacking tools, negligence, and much more.

Organizations struggle to stop data breaches and detect insider threats because don't have the right visibility into what users are doing on the endpoint, nor the intelligence to understand that data. This is especially true considering that insider threats can take on a wide variety of appearances.

Dtex has proven this ability in top organizations across the globe, including government agencies. The Defense Information Systems Agency (DISA) uses Dtex to proactively detect insider threats. The Department of Defense also granted Dtex a constitutional Authority to Operate, which allows Dtex to be deployed across DoD systems globally.

With Dtex, government agencies can build a modern approach to organization-wide user visibility, detect and investigate insider threats, and achieve greater coverage under cybersecurity frameworks (such as the MITRE ATT&CK Framework).

PRODUCT OVERVIEW

The Dtex Enterprise User Intelligence Platform provides user visibility and insights that allow organizations to quickly detect insider threats, elevate their highest areas of risk, find early warning signs, and conduct rapid in-house investigations. It does this through its four primary components:

Visibility

The Dtex collector captures user behavior metadata from the endpoint, both on and off the corporate network. This metadata provides information about how users interact with the file system, applications, peripheral devices, printing, clipboard activities, network and ports. Since the collector only gathers metadata, its impact on both the endpoint and the network is negligible.

HIGHLIGHTS

- Dtex provides lightweight, organization wide user visibility that is paired with machine learning and behavioral models to draw out actionable insights and detect & investigate insider threats.
- Dtex has been granted an Authority to Operate by the DoD.
- A 2-year project with DISA is currently underway for insider threat detection.
- Dtex's modern approach to user visibility offers a more accurate, lightweight, and cost-effective solution for CNSSD 504 compliance.
- These insights also assist with MITRE ATT&CK Framework, NIST Cybersecurity Framework, and NSA Cyber Threat Framework coverage.

UNIQUE INSIGHTS

The uniqueness of Dtex's data set means that it sees activity other tools don't, including:

- Credential Misuse
- Credential Theft
- Data Exfiltration
- Lateral Movement

As well as additional use cases, including:

- Security Bypass
- Policy Violations
- Use of Personal Email to Transfer Corporate Data
- Publicly Accessible Documents in Online File Storage
- Pirated Software
- Obfuscation
- Print Activities
- Ransomware Indicators
- File Deletes

Intelligence

Dtex uses advanced behavioral models, collected from real-world investigations, to identify known threats and advanced risks, like credential theft. These patterns allow Dtex to quickly and effectively identify anomalous behavior (such as data exfiltration) from day one.

Analytics

Behavioral analysis baselines individuals' normal user behavior and alerts on suspicious anomalies or red flags. This allows Dtex to detect and alert on the "unknown unknowns" — never-before-seen suspicious behavior. Dtex generates risk scores by comparing a user's recent events in comparison to themselves (i.e. their own historical baseline), against their peer group (i.e. the baseline of users in similar departments or roles) and against the entire organization.

Answers

Alert stacking, risk scoring, and evolving anomaly detection mean that Dtex's prioritized alerts are highly targeted with little noise or false positives. The Dtex UI allows analysts to quickly sort, navigate, filter, and pivot as they triage alerts. Dtex is also a valuable endpoint forensics tool, since it offers a direct, complete audit trail of human behavior – including every stage of the insider threat kill chain.

Plus: Privacy Compliance & Anonymization

Dtex offers all of the above features without invading user privacy. Dtex does not by default perform keystroke logging, screen recording, screenshot capture or any other form of invasive information collection. (Note: Screen capture will soon be available as an optional add-on feature.) In addition, Dtex provides an optional anonymization feature that can encrypt sensitive information such as user IDs, machine names and IP addresses that might uniquely identify an individual.

DTEX IN FEDERAL ORGANIZATIONS

Authority to Operate Across DoD

Dtex has been granted a DoD Authority to Operate. This ATO allowed the Dtex Platform to be deployed on Department of Defense endpoints, serves and networks nationally and internationally, and indicates that Dtex has been evaluated and approved by DoD. Dtex is thus approved to be deployed across US Government agencies both in the United States and across the globe.

A More Effective Approach to CNSSD Compliance

Dtex can be used to fulfill CNSSD 504 directives, particularly in the significant gap where heavyweight traditional UAM solutions are not feasible or manageable. With a heavyweight user activity monitoring solution, storage costs alone can exceed hundreds of thousands of dollars per year. When one also factors in the cost of lost productivity through performance challenges, manpower to monitor/ingest this data, and server costs, heavyweight monitoring solutions have a high cost and a significant impact on end user experience.

Dtex, however, offers a lightweight alternative to user visibility for CNSSD 504 compliance. With a lightweight endpoint collector that records user activity metadata, Dtex was built to record only data that provides

DEPLOYMENT

Dtex offers flexible deployment options. It can be deployed on-prem, or hosted in the cloud. (Additional hosting fees may apply.)

PLATFORM COMPATIBILITY

The Dtex collector is compatible across the following platforms:

Microsoft

Windows 7

Windows 8/8.1

Windows 10

Windows Server 2008 R2, 2012, 2012 R2, 2016

Apple

macOS 10.10 (Yosemite)

macOS 10.11 (El Capitan)

macOS 10.12 (Sierra)

macOS 10.13 (High Sierra)

Linux

Red Hat Enterprise Linux or CentOS 6.x 7.x actionable insights into user behavior, in the lightest possible package. This collector can be deployed across hundreds of thousands of endpoints to provide on and off network visibility that does not impact productivity, privacy, or performance. Dtex also offers screen capture in an additional add-on for high-risk users that require closer monitoring.

DTEX AND THE MITRE ATT&CK FRAMEWORK

Dtex offers dashboards and alerts mapped to the MITRE ATT&CK framework. Dtex's visibility provides critical coverage that spans several key areas of the matrix. A few particularly important areas of visibility include:

- Reconnaissance activity
- Screen capture tools
- Keylogging tools
- Network sniffing
- Removable devices
- Privilege escalation
- Exfiltration, including complex data exfiltration

These specific use cases, however, are only the beginning. Because Dtex offers comprehensive visibility into all user activity on the endpoint, Dtex's data can be used to enhance most aspects of the MITRE framework, as well as help federal organizations diagnose and understand their coverage levels.

DTEX AND THE NIST FRAMEWORK

Dtex Enterprise User Intelligence offers unmatched insider threat detection and investigation capabilities. The visibility that Dtex provides has applications that span every silo of a well-rounded cybersecurity approach, such as those outlined in the NIST Cybersecurity Framework. Thus, Dtex enhances all five primary functions included in the framework:

IDENTIFY: The Identify function centers around knowledge — more specifically, knowledge of data, risks, and flaws. Dtex provides user-centric, enterprise-wide visibility at the endpoint through human-readable metadata. Achieve complete user visibility wherever users are connected to the internet. Proactively identify greatest areas of risk, such as which users come into contact with the highest number of sensitive files.

PROTECT: Dtex enables federal organizations to develop and enhance stronger ongoing security policies. Dtex has visibility that solutions such as DLP, SIEM, EDR, and CASB solutions lack, allowing it to close the gaps in other tools and identify weaknesses (such as, for example, identifying where DLP rules are misconfigured or failing). Dtex also allows federal organizations to detect negligent insiders, and see how users are interacting with files, allowing them to verify whether users are accessing files that they shouldn't have access to.

DETECT: Dtex offers unparalleled insider threat detection by combining its visibility data with machine learning, anomaly detection, and alert staking. Dtex elevates users for inspection that either match known-bad behavior patterns or exhibit troubling behavioral anomalies, all in near-real-time.

RESPOND: Dtex is an invaluable investigations tool. It captures the full audit trail of an event, allowing security teams to instantly see every action leading up to and after a suspicious security incident. This timeline makes it easy to determine the context and intent of an incident, revealing not just what happened, but how and why.

RECOVER: With all of the insights provided above, Dtex enables federal organizations to fully understand what users are doing with technology and data, allowing for more informed incident recovery and a organization-wide, proactive insight into the effectiveness of security approaches.

DTEX IN ACTION AT DISA

This lightweight approach to proactive monitoring has been used by top organizations globally, including government agencies. The Defense Information Systems Agency (DISA), for example, utilizes Dtex to proactively detect insider threats. With this approach, they are able to automate the detection of threats like abnormal lateral movement, unusual or malicious activity by users with legitimate credentials, execution of simultaneous logins, and other critical insider threats.

Below are some examples of Insider Threat use cases that Dtex is solving currently for DISA as part of the 2 year RIF project. This project specifically focuses on several Credential Misuse Use Cases such as:

- Unauthorized changes to: administrative rights of users or groups, security groups (like creation, deletion or modification), accounts (creation, deletion or modification), database or admin roles, file permissions, event logs or any logs, application settings and application execution.
- Failed Login to: Active or Disabled or Expired or Vendor Accounts (both Local & Domain Accounts)
- Anomalous behavior: Remote administrative actions, after-hour administrative actions, off-network actions
- Trying to Access/Delete Files that users don't have access to
- File/Directory Reconnaissance
- Data Exfiltration via webmail, social media, USB, Printing etc.
- Use of shared accounts
- Account login from multiple geo locations