TOP 10 REASONS WHY ORGANIZATIONS DEPLOY DTEX

Dtex's User Behavior Intelligence is a new approach to fighting insider threat.

Dtex was built from the ground up specifically to detect insider threats. With Dtex's User Behavior Intelligence, organizations around the world are finally able to achieve actionable intelligence with context, accuracy, and genuine insights.

1 INSIDER THREAT

Dedicated User Behavior Intelligence

Organizations are struggling to fight insider threats. Many turn to heavy data loss prevention solutions, but those provide limited insight into user behavior, leaving significant blind spots. Some organizations install user behavior analytics or SIEM systems, but those have a critical gap rooted in their incomplete data, which provides limited endpoint visibility.

At Dtex, we've learned that any successful insider threat project starts with the right data set. Even if a tool has flawless math and a cutting edge UI, trying to reverse engineer a user's activities from disparate log data sources is a losing battle.

Instead of trying to pull insights out of existing flawed data, Dtex provides visibility specifically around insider threats from the point closest to the user: the endpoint. Dtex deploys a lightweight collector to create and collect metadata around user activities. Then, it feeds that data into analytics, which include thousands of patterns of known bad behavior, activity baselining, and alert stacking to identify strings of suspicious activity. Through this unique combination, Dtex provides intelligence that is currently unparalleled by any other security tool on the market.

2 INSIDER-FOCUSED DETECTION

Catch the threats that other tools miss

Dtex's unparalleled approach to threat detection outlined in Point 1 allows it to find insider threats that other tools struggle to see. Better yet, due to real time analytics, Dtex arrives at these answers faster than any other tool. The uniqueness of this dataset allows us to see some of the most elusive insider threats, including:

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

As well as additional use cases, including:

- Security Bypass
- Policy Violations
- Use of Personal Email
- Publicly Accessible Documents
- Pirated Software
- Obfuscation
- Print Activities
- Ransomware Indicators

3 USER INTENT

Understand the full context

Most solutions are unable to quickly and easily show you a user's intent because they don't have the dataset to back up those conclusions. Ultimately, determining intent is a matter of capturing:

1. Data related to user activities,
2. The sequence of user activities, and
3. Whether those activities are normal or abnormal for that particular user.

Dtex provides all of that information to give you a clear timeline of what happened before, during, and after an event. Just as importantly, Dtex's analytics reduce noise so that you can clearly see and understand the progression.

This contextual data around the type of activities performed allows organizations to determine whether the cause of an incident was malware, infiltration, a negligent mistake, or a truly malicious insider act – and adjust their response accordingly.

For example,:

- **Detection of a physical machine in the wrong location or logged in to multiple sessions at once may suggest more than one user with the same credentials (credential theft), or…**
- **A user downloading and renaming an abnormal number of files using Chrome's Incognito mode suggests an insider thief trying to cover their tracks, or…**
- **A publicly accessible Google Drive sharing link suggests that a user is *accidentally* leaving data unguarded.**

4 FORENSIC INVESTIGATION

Establish a clear forensic trail

The unmatched context that Dtex provides allows you to quickly understand how a security event occurred and progressed. This insight makes it easier than ever to establish a forensic trail and to simplify investigations.

What's more, by fully understanding a breach after the fact, your team is better able to truly grasp the consequences of a breach or other security incident.

In the wake of an event, Dtex has been used to quickly answer critical questions such as:

- **What files went missing?**
- **Which endpoints have opened this infected application?**
- **To which machines did an attacker move laterally?**
- **How long has this attack been in progress?**

The Dtex team also includes expert analysts who supplement your team with incident response and additional investigation after a security event.

5 CATCH THE EARLY SIGNS

Stop data theft before it happens

Many solutions focus either on preventing any potential threat completely (often via blocking, like DLP) or detecting only one particular moment in time. Dtex, on the other hand, looks for a full picture of what happened from the beginning stages of a potential threat. Through risk scoring and alert staking, Dtex is able to recognize suspicious sequences of events that may indicate an impending attack. For example:

Nearly all insider threat attacks follow some variation of the insider threat kill chain:

Reconnaissance

Investigation & research before attempting theft.

Circumvention

Disabling or avoiding security measures.

Aggregation

Collecting the data they intend to steal.

Obfuscation

Covering their tracks to avoid detection.

Exfiltration

The actual moment of data theft, when the data leaves the organization.

While many tools focus only on the single moment of data theft itself, Dtex watches for previous steps in the kill chain as well, especially in sequence. For example, a user downloading an unusually large number of files from SharePoint, then compressing and renaming them off-network is a strong indicator of aggregation and obfuscation.

6 PRIVACY & ANONYMIZATION

GDPR compliant, respects user privacy

Dtex was built with privacy in mind. Unlike heavier, more invasive employee monitoring solutions, it does not use screenshots, videos, or keylogging. Dtex also does not inspect the contents of emails or documents, instead collecting only activity metadata.

Dtex also includes optional anonymization, which can anonymize personally identifiable information such as user name, domain name, machine name, etc. This data can then only be unlocked only by a pre-determined specific keyholder within the organization.

7 IT POLICY VIOLATIONS

Enforce company policies

Because of the type of data that Dtex collects, it can be used to complement DLP and similar solutions. Dtex can help highlight corporate policy violations, including:

- Gambling
- Gaming
- Inappropriate Website Browsing
- Personal Webmail
- Cloud File Sharing
- Pirated Software
- ...And more

Policy violations are also highlighted in the regular User Threat Assessment reports provided by Dtex's expert analyst team.

8 OFF-NETWORK VISIBILITY

See what happens off the corporate network

In today's distributed enterprises, visibility can no longer be tethered to the corporate network alone. Many examples of data exfiltration have occurred when the user or employee was outside of the corporate network (such as at home, in a coffee shop, etc.). Due to its unique capability to collect data off-network, or offline and cache locally, Dtex is able to highlight and detect insider threats even when employees are off of the corporate network.

When the endpoint is outside the corporate network, Dtex will cache all activities locally. Those activities will then be sent back to the Dtex analytics server when the endpoint has connectivity, either by VPN or internet connection, depending on whether Dtex is deployed in the cloud or on-prem.

9 REDUCE FALSE POSITIVES

Maximize your team and tools

Due to the real user data that Dtex collects and analyzes, organizations can get to the answers faster than they ever have before – and, most importantly, they do it using the same number of security staff.

The data collected by many security tools, especially log file based systems, is extremely noisy. What's more, it's often difficult to understand, meaning that security employees need special training to quickly interpret and understand these logs. Dtex, on the other hand, collects metadata that provides more detailed information in a format that's human-readable and much less noisy.

Plus, Dtex's analytics and alert stacking reduce false positives, cutting through the noise to ensure that your team only spends time verifying legitimate alerts.

Organizations also have the option of viewing Dtex's data and alerts within their own preferred "pane of glass." Dtex can feed data into UBA platforms, SIEM systems, etc. It works with your current security tools, not against them.

Dtex also enhances your resources by providing world-class support from our analyst team. Our staff of insider threat experts provide regular User Threat Assessments that highlight key areas of risk, conduct ongoing support, and provide incident response & investigation services.

10 LIGHTWEIGHT

Fully scalable, no productivity impact

Dtex does not collect heavy data, like images, files contents, video files, and other similarly cumbersome data formats often captured by heavy employee monitoring tools. Instead, it only records metadata related to user activities, such as file activity, session activity, window titles, etc. As a result, the average amount of data collected by Dtex in a typical deployment is only around 2-3 MB of data per user per day.

The collector also has a negligible impact on CPU, with no hindrance to user productivity.

Dtex's lightweight nature makes it quick and easy to deploy. It can be hosted on-premise or in the cloud, and requires no other infrastructure beyond the tiny collector installed on each endpoint.

Contact Us to Learn More

Ready to find out more about how Dtex can help you within your organization? Contact us today to find out firsthand with a tailored demo. **Contact your sales representative or email us at info@dtexsystems.com.**