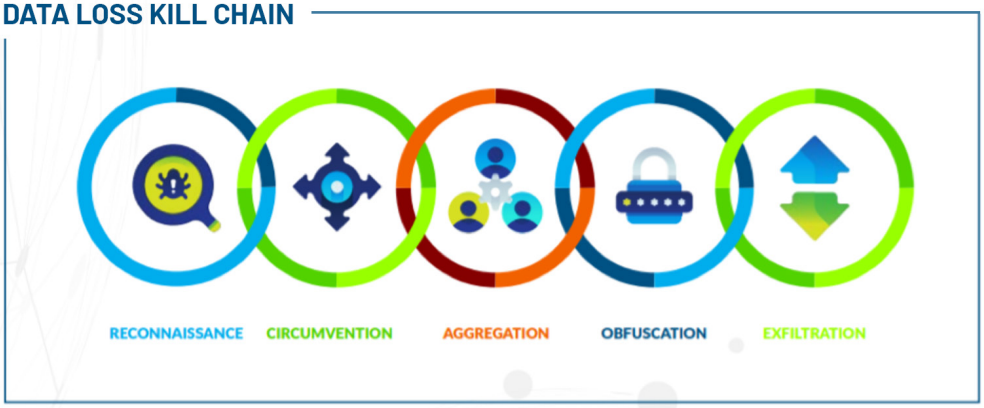
info@dtexsystems.com
dtexsystems.com

DTEX PREDICTIVE ENDPOINT DATA LOSS PREVENTION

TRADITIONAL ENDPOINT DLP ACTS TOO LATE

Intellectual property, trade secrets and sensitive data are highly sought after by external adversaries as well as malicious insiders. Perhaps even more precarious are the risks to these data sets by negligent users. Breaches that result in the loss of PII and PHI can trigger regulatory penalties under HIPAA, GDPR, PCI-DSS, Section 5 of the FTC Act, the California Consumer Privacy Act and dozens of other regulatory requirements. Trade secrets, customer lists, product designs and other corporate IP stolen by competitors and disgruntled or departing employees can eliminate competitive advantages.

Whether the attacker is a departing employee or an outsider using stolen credentials, attackers need to proceed through a "kill chain", specific steps in their attacks. This includes Reconnaissance (locating the data), Circumvention (testing and avoiding detection), Aggregation (collecting the data), Obfuscation (hiding malicious activity) and finally, Exfiltration. Blocking the attack at any point in the kill chain accomplishes the defender's goal. The earlier in the kill chain an attack is stopped, the lower the chances for potential damage.



Traditional Data Loss Prevention (DLP) solutions attempt to address this problem by stopping criminals at the very last step – data exfiltration. Due to high false positive rates that impede legitimate use of data and frustrate users, DLP blocking capabilities are rarely used. Instead, organizations using traditional DLP rely on data exfiltration alerts. Unfortunately, an alert that notifies an organization that an attack has already successfully executed (and that data has been lost) is of little practical use.

This occurs because traditional DLP only watches the data. To protect that data, organizations must build complex rules to cover every possible use (and misuse) case for the data, for each department, group and user in the organization. The rules for the CFO differ from the rules for the head of marketing or manufacturing, and may even differ from those of the CEO or VP of Finance.

This approach is complicated further as workforces migrate off the corporate network to a work-from-home (WFH) environment. In a WFH setting, unknown IP addresses become the rule. Attempting to rebuild rigid rulesets in a rapidly changing environment will result in denied access for legitimate use cases and missed alerts as rules are relaxed to accommodate the new reality.

A BETTER APPROACH – WATCH THE KILL CHAIN, STOP ATTACKS BEFORE EXFILTRATION

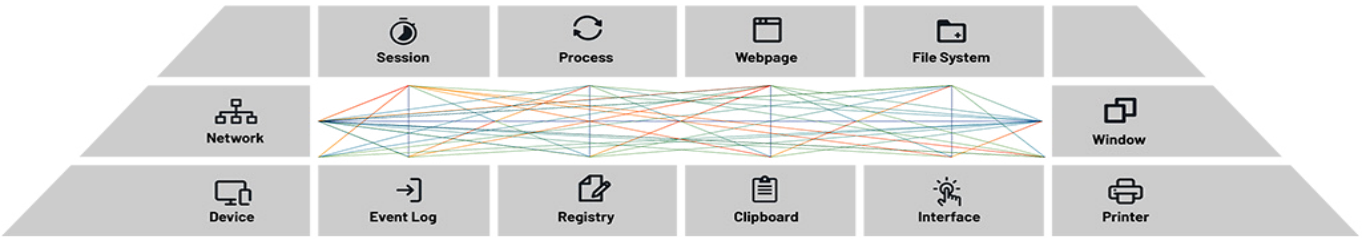
Network security professionals have long relied on "Indicators of Attack" and "Indicators of Compromise" to identify malicious attacks early. Likewise, with protecting organizational IP it is better to identify activities that are precursors to exfiltrating data. These "Indicators of Intent" are identified by observing and correlating activities associated with earlier stages in the kill chain.

Monitoring for "Indicators of Intent" simplifies an organization's defenses. Rather than attempting to classify every piece of data and role-based rules for legitimate use, organizations monitor all activities by all users (while protecting user privacy) to alert on suspicious, anomalous and known-bad activities before data exfiltration is attempted.

While the approach is simple in theory, it requires collecting, enriching and correlating hundreds of unique activities across thousands of users and applying statistical analysis and machine learning to execute properly.

STEP ONE: ENTERPRISE TELEMETRY

CAPTURE ALL USER ACTIVITIES



The DTEX InTERCEPT Platform™ delivers a 24x7x365 continuous audit trail of unique endpoint metadata to observe and record the actions and activities of data, machines, applications and people (DMAP) in near real-time, both on and off the corporate network. DTEX operates on the endpoint, where data is managed (and lost).

Note that while capturing machine, application and user actions is critical, more important is understanding the relationship beteen various activities. In Step Two the reader will see how DTEX enriches and correlates seemingly disparate activities to discern between legitimate and malicious actions.

User Session Activities – Each user session is logged and analyzed to identify anomalous, unsafe and malicious activities. This includes anomalous session access and shared logins that may indicate credential theft, unusual working hours, the use of decommissioned accounts or privileged accounts in abnormal ways.

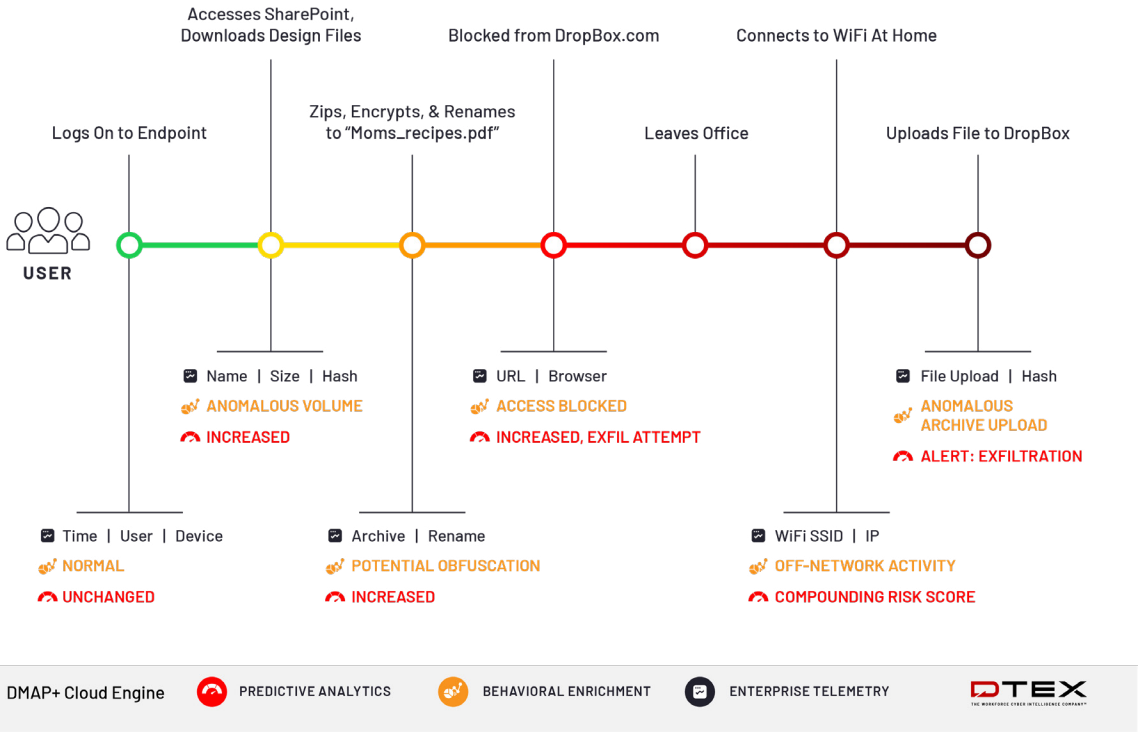
Process Activities – All activities on the endpoint trigger a process that can be recorded and analyzed, including process hash (MD5, SHA1 or SHA256), process parent and child relationships, application versions, execution paths and command line execution parameters.

DTEX uses this to identify 'Indicators of Intent' such as the unauthorized use of hacking tools (password crackers, network sniffers), attempts to bypass of security controls, the use of non-sanctioned software, unusual application behavior, and attempts to obfuscate activity by using ToR and Proxy Bypass applications.

DTEX uses this to identify "Indicators of Intent" such as the unauthorized use of hacking tools (password crackers, network sniffers), attempts to bypass security controls, the use of non-sanctioned software, unusual application behavior and attempts to obfuscate activity by using ToR and Proxy Bypass applications.

File System Activities – Attackers typically start by identifying sensitive data (Reconnaissance) followed by disguising (Obfuscation) and centralizing it (Aggregation) before attempting to exfiltrate data. Obfuscating data can include simply renaming a file or changing a file extension of a customer list from xslx to jpg. Data aggregation would involve large numbers of downloads or transfers between systems within the organizations (lateral movement). DTEX captures all relevant metadata about files such as ADS and document properties that include file classification markings, allowing it to focus on sensitive data. DTEX tracks the lineage of every file as it moves through the organization across different endpoints, effectively exposing attempts to disguise and aggregate data.

DTEX tracks all use of all data to identify actions that portend data theft. This includes creating, populating, moving and deleting files and directories, activities designed to inhibit tracing of data and forensics, and unauthorized system configuration changes.



Net-Flow Activities – While data can be exfiltrated by downloading to a portable drive or even printing the desired information, it is common for criminals to use network connections to remove data. Most traditional DLP solutions focus on the final step in the kill chain – exfiltration of large amounts of data, FTP and SCP file transfers, and uploads to cloud storage that can identify a completed attack. While DTEX also alerts on this action, it also focuses on activities required to prepare for exfiltration. This includes moving anomalous amounts of data laterally across the network, aggregating data to unsual network locations and the usage of rogue or unauthorized applications (e.g., anonymous proxies).

Webpage Activities – Searching recruiting websites and frequent updates to LinkedIn profiles can provide an early indication of employee flight risk, therefore warranting increased scrutiny on the use of sensitive data. Likewise large uploads to webmail or file sharing accounts can provide an "Indicator of Intent". DTEX tracks all web activity, including the full webpage URL for http and https websites, and domain and page title information correlated with web browser.

info@dtexsystems.com
dtexsystems.com

Network Interface Activities – DTEX tracks all network connections, on and off the corporate network. It captures Wi-Fi SSID and public IP information for geolocation to identify suspicious activity over public Wi-Fi, VPN disabling and all actions after logging on or off a network.

Device Activities – Removeable storage devices like SSD and thumb drives are popular exfiltration tools because they hold large amounts of data but still can be easily hidden in briefcases and pockets. DTEX identifies when these devices are attached to a system and all data activity associated with the devices. In addition, DTEX can alert on user actions that may precede data exfiltration, including connections to wireless Bluetooth or AirDrop devices.

Windows Event Log Activity – An attacker or compromised employee may create additional user accounts or change privileges for an individual or group. DTEX monitors all Windows event logs to identify indications of activity that could precede an exfiltration, including credential misuse, changed firewall or security settings and changes in privileges or group policies.

Windows Registry Activity – An attacker may attempt to bypass security controls by changing system configurations. DTEX captures all Windows Registry modifications (e.g., query, create, modify, delete) for configured registry directives as well as high-risk registry modifications and tampering with system settings.

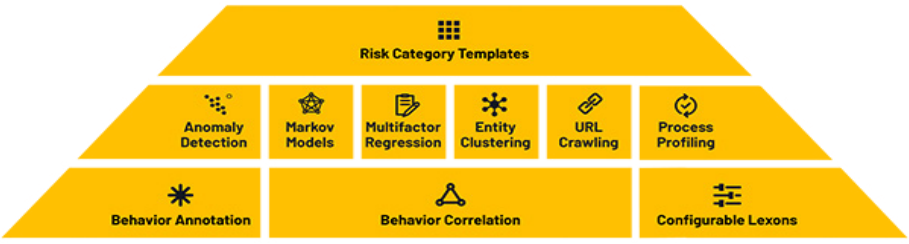
Clipboard Activities – Copy/paste is a simple way to capture data in preparation for an exfiltration attempt. DTEX has visibility into all endpoint activity, including any data copied to or pasted from the clipboard. By correlating the content hash with the user and source/destination processes, DTEX provides early indicators of malicious intent.

Print Job Activities – As previously noted, physical exfiltration of sensitive data can be just as damaging as electronic exfiltration. A user printing a large quantity of sensitive information on local or remote printers or printing during unusual hours can be an indicator of an attack in process.

Window Activities – When preparing to steal data, the attacker may need to continuously switch between applications, copying data from one into the other. DTEX observes task switching "window" behavior in context, and correlates this with the underlying user account and role, process and application (Webmail, file sharing or anomalous usage), and device to identify malicious "Indicators of Intent".

STEP TWO: BEHAVIORAL ENRICHMENT

DATA WITHOUT INTELLIGENCE IS NOISE



Security tools are notorious for verbose output that can obscure the results on which security analysts should focus. This is why many are simply left in "monitor mode". Unfortunately, this allows adversaries to continue their attacks until security sifts through results to (hopefully) identify indicators of an attack.

The second stage of DTEX InTERCEPT's approach to data loss prevention is to enrich the raw data from activity monitoring with behavior analytics, risk profiling and machine learning to expose Indicators of Intent; before an attack can be completed.

info@dtexsystems.com
dtexsystems.com

DTEX uses technicques including Markov Modeling, Entity Clustering and Multifactor Regression to enrich the raw data from activity monitoring and discern between legitimate activities and malicious intent. Two important stages of behavioral enrichment are Activity Annotation and Actitivity Correlation.

> **Activity Annotation** processes activities through known behavioral profiles. This tags activities that appear anomalous for a particular user, role, data set, device and other variables based on "known good" and "known bad" templates. Activities of interest will undergo additional behavioral analysis and anomaly detection routines.
>
> **Activity Correlation** applies "correlation logic" on a series of actions to cut through the noise and create a higher-level activity based on the expected sequence of activities, the expected time window, the linking data elements and a specified rule trigger.

Unlike traditional Endpoint DLP solutions, DTEX InTERCEPT does not require customized and complex policies to detect malicious activity. Its rules, patterns and logic codify DTEX's deep domain knowledge; similar to what a team of insider threat experts would bring to an organization. By applying this domain knowledge to raw activities, DTEX surfaces amonalous behavior relavent to data exfiltration attempts for further analysis in the Analytics Module.

STEP THREE: PREDICTIVE ANALYTICS

DON'T WAIT FOR DATA TO LEAVE

Armed with preprocessed behavioral data, DTEX's Predictive Analytics engine can focus quickly on those combinations of activities indicative of an attack – before the attack is completed. With DTEX's domain knowledge, false positives are minimized and legitimate use of data continues uninterrupted.

Waiting until an attacker has exfiltrated data to alert security makes security reactive. The data theft kill chain requires attackers to take a number of steps to find and aggregate data, test and bypass security controls, and hide their actions before exfiltration begins. Provided with complete activity information, behavioral context and predictive analytics, DTEX InTERCEPT processes and tracks the artifacts produced by these steps – in context with the users, roles, data and devices – to spot "Indicators of Intent" and stop attacks long before exfiltration attempts are practical.

To learn more about DTEX's approach, visit dtexsystems.com