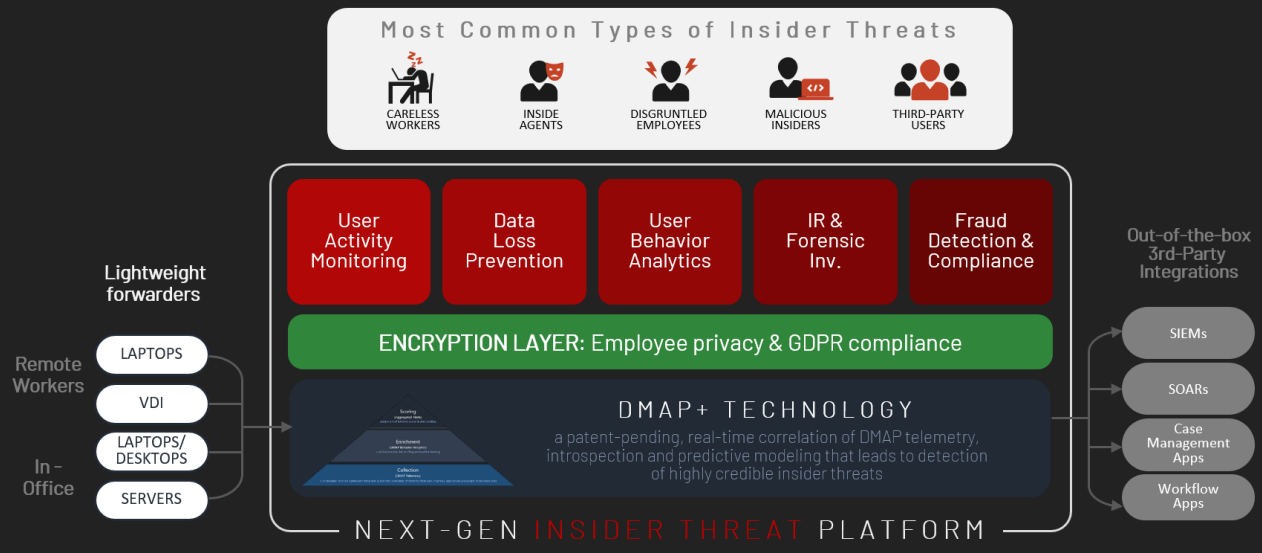
WHAT IS A NEXT GENERATION INSIDER THREAT PLATFORM?

Insider threats take many different forms in enterprise organizations, making them difficult to detect, investigate and mitigate. A modern Insider Threat (InT) platform must provide an integrated solution which replaces legacy point solutions.

A Next-Gen Insider Threat platform replaces the following legacy point solutions:

1. User Activity Monitoring (UAM)
2. Data Loss Prevention (DLP)
3. Internal Fraud & Forensics Tools
4. User Behavior Analytics (UBA)



DTEX InTERCEPT is a 'Next-Gen' Insider Threat platform which replaces legacy point solutions in a unified solution, while also delivering the following critical requirements:

- > Scales to the entire organization
- > Cloud-first & deploys in hours
- > Near-zero impact to endpoints & network
- > GDPR compliance out-of-the-box
- > Noise-free telemetry with 24x7 audit-trail

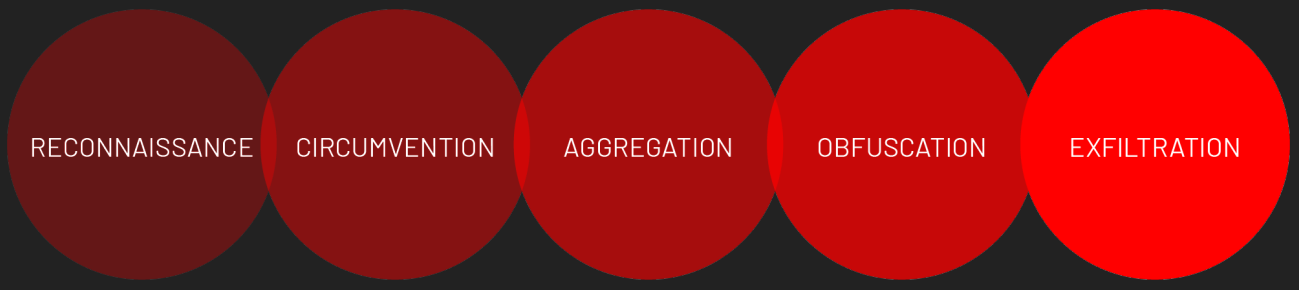
In the past year, many adjacent security vendors are claiming to solve insider threats, causing confusion amongst security teams who are new to the insider threat space. Some vendors in the following categories are claiming to have added insider threat capability as a 'new feature':

- Log-File-Based Behavior Analytics vendors who analyze aggregated log data (typically from a SIEM system populated by existing log data e.g. Windows Event Logs, OSquery etc.). Examples include Bay Dynamics, Securonix, Gurucul, Exabeam, and Interset.
- Network Detection & Response (NDR) vendors who analyze activity data gathered directly from network devices. Examples include DarkTrace and Vectra Networks.
- Endpoint Detection & Response (EDR) vendors who analyze malware and APT activity directly from endpoint devices. Examples include CrowdStrike, Cylance, Carbon Black, Cyber Reason, Microsoft Defender ATP, Sentinel One and many others.

While each of these approaches may have some overlaps to insider threat, none of them have been designed specifically as an insider threat platform.

This document is a checklist that organizations can use to measure how well your insider threat program is prepared to identify real-world attacks. All the attack vectors described on the following pages are taken from actual insider threat attacks discovered by DTEX customers using the proprietary DTEX Insider Threat Kill Chain.

INSIDER THREAT KILL CHAIN



RECONNAISSANCE

When preparing for data theft, the user typically begins with research. This is where they locate the data that they would like to steal, or, in the case of compromised credentials, where the insider will test the bounds of the stolen credentials' privileges.

	DTEX	NDR / EDR	Log File Analytics
Researching security bypass methods / tools	X		
Use of Network Scanning Tools	X	X	*Partial*
Anomalous Use of Network Scanning Tools in comparison to peer group	X		
Installation and Usage of Portable Applications	X		X
Unusual Usage of sysinternals Tools and Utilities	X		X
Network share enumeration	X	X	
File and Folder Access Denied Events	X	*Partial*	X
Unusual access to remote support tools	X		
Unusual rates of opening files	X		*Partial*
Unusual access to new file locations	X		X
Successful and failed attempts to mount USB drives or access cloud storage	X	*Partial*	
Commands issued through tools like cmd.exe, PowerShell, Terminal, etc.	X	X	
Suspicious internet search activities (e.g. google searches)	X		
Unusual login behaviors (e.g. outside of normal working hours)	X		*Partial*

CIRCUMVENTION

This is the stage where the insider attempts to get around existing security measures, such as web blocking, DLP tools, etc. It is particularly important to have visibility into this activity because it can shed light on intent: if a user is going through great lengths to get around company security, they are acting very deliberately.

This is also often where organizations can see where their security tools are failing. By capturing circumvention activity, Dtex shows analysts where and how users are able to bypass existing measures.

	DTEX	NDR / EDR	Log File Analytics
Usage of anonymous web browsers (e.g. ToR), including the actual sites visited during these anonymous sessions	X		
Disabling of corporate VPN	X	X	*Partial*
Research into tampering of corporate security tools	X		
Tampering of corporate security tools	X	*Partial*	
Suspicious off network activities (including detection of corporate and non-corporate networks, Wi-Fi SSID etc)	X		
Unusual usage of privileged admin accounts	X		*Partial*
Usage of vulnerability exploit tools	X	X	X
Unusual usage or creation of local accounts	X		*Partial*
Anomalous modification of configuration files	X	*Partial*	
Modification of file and directory permissions	X	X	*Partial*
Unusual privilege escalation activities	X	*Partial*	*Partial*

IMPORTANT NOTE:

Monitoring of super users and IT admins requires special consideration in the development of insider threat programs. It's important not to impose too many controls on these staff members as they're typically already overburdened, and often have to learn "on the job." Dtex customers use Dtex to get visibility into super user activity without slowing them down, opting for "trust but verify" instead of "locking and blocking."

AGGREGATION

This is when the insider assembles all of the data that they plan to steal, often moving it into one file directory or compressing it in a single location.

	DTEX	NDR / EDR	Log File Analytics
Download of sensitive files from corporate web portal	X		
Archive creation including correlation of files within the archive	X		
Unusual network file transfers (both from the file server and the endpoint)	X	X	*Partial*
Anomalous data aggregation behaviors based on file type, file size and other meta-data	X		
Unusual Clipboard Activity (e.g. excessive screenshots during a conference call or presentation)	X		
Anomalous mapped drive creation and data transfers	X		*Partial*
Automatic data collection (RPA)	X	*Partial*	
Anomalous email archive creation and transfers	X		
Administrative file copy utilities	X	X	
Unusual symbolic link creation	X		
Automated backup software (e.g. time machine)	X		

OBFUSCATION

In the Obfuscation step, the insider will cover their tracks in order to avoid detection, often by renaming files, changing file types, or by using more advanced tactics such as steganography. This is another important step to capture in order to prove malicious intent, as well as to understand where other security tools might be failing.

	DTEX	NDR / EDR	Log File Analytics
Use of private browsing modes (e.g. incognito)	X		
Data hidden within the Alternate Data Stream (ADS)	X		
Steganography use cases	X	*Partial*	
Unusual clearing of event viewer logs	X		X
Unusual clearing of browser history	X		
Suspicious file extension renaming	X		
Suspicious file renaming, especially sensitive files given innocuous file names	X		
Anomalous off-network activity (including device tethering)	X		
Unusual rates of file deletes	X		
Anomalous usage of disk erasing software	X		
Hidden Files & Attribute Changes	X	X	
Usage of anonymous web browsers (e.g. ToR), including the actual sites visited during these anonymous sessions	X		

EXFILTRATION

This is the final step in the process of stealing data: the moment that the data is actually transferred out of the organization. Many security tools focus only on this specific step, and often by way of blocking tools. Rigid rules, however, can't catch the hundreds of methods that can be used to get data out of the organization. Since DTEX sees all activity from the point closest to the user, it has visibility into less common exfiltration methods that other tools often miss.

	DTEX	NDR / EDR	Log File Analytics
Airdrop Exfiltration	X		
Bluetooth	X		
Encrypted USB	X	*Partial*	
Unencrypted USB	X	*Partial*	
FTP / sFTP Transfers	X		*Partial*
Online File Sharing	X		
Personal Webmail Uploads	X		
Printing	X		X
Anomalous Uploads	X		X
Network to Removable Device	X		*Partial*
Remote Support Tool Upload	X		
Messaging Tool Upload	X		
Automated Exfiltration / Scheduled Transfers	X	*Partial*	
Exfiltration over Alternative Protocol	X	X	*Partial*
Exfiltration over Command & Control	X	X	*Partial*
Exfiltration over Physical Medium	X	*Partial*	*Partial*
Data Transfer Size Limits	X		X
Exfiltration of High Sensitivity Score Documents	X		

IMPORTANT NOTE:
Employees leaving the company are significantly more likely to take sensitive data with them when they leave. Dtex customers use our endpoint visibility to look for signs of pending departure or disengagement.