DTEX & User Behavior Analytics

How DTEX Replaces Legacy UEBA Tools

DATA BREACHES START WITH THE USER:
Malicious users, negligent users, and credential thieves are the primary culprits.

In recent years, organizations with sophisticated security programs have been forced to acknowledge the user threat. Malicious users, negligent users, and credential thieves pose more risk to the enterprise than ever before, especially since it's now harder than ever to control them with perimeter security. Today, enterprises need visibility into user behavior – whether that means seeing if a high profile employee is departing with sensitive data, or determining the risk of negligent users who may accidentally cause a data breach.

USER ENTITY BEHAVIOR ANALYTICS: AN INCOMPLETE SOLUTION
UEBA solutions are only as good as their data.

Many enterprises have turned to User Entity Behavior Analytics (UEBA to detect the user threats within their networks. UEBA solutions leverage expert system logic (rules and/or artificial intelligence (machine learning in an attempt to provide an out-of-the-box solution.

While UEBA solutions have developed useful models for analysis and alerting, there's one problem: their implementation relies on log files, which are a flawed data source for capturing user behavior. Firstly, log files are difficult to implement and manage. They require a significant amount of manpower to configure, collect, maintain, and interpret. Most importantly, even with all of this time investment, they simply do not provide enough visibility on their own to catch common user attacks quickly enough to prevent damage.

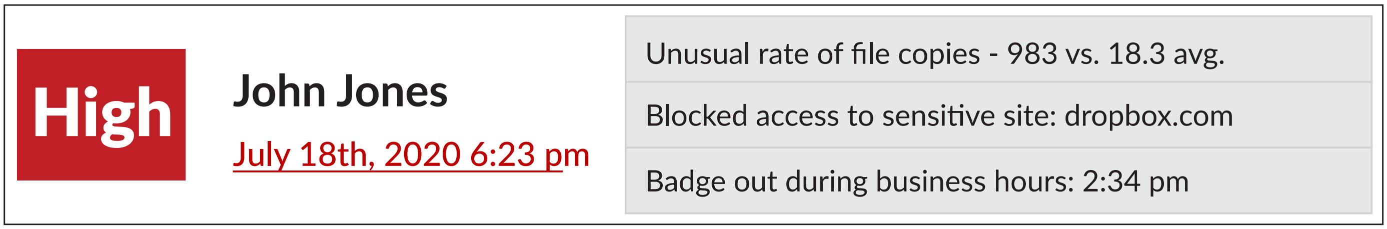
For example, most organizations allow for split tunneling also known as local network access to allow use of resources such as printers. This practice also allows for local access of network attached storage devices and other network devices that renders network based UEBA and other network tools blind to this activity. A similar gap in visibility for network-based UEBA tools occurs when Bluetooth access is allowed for computer peripherals, creating wireless access to storage devices that are invisible to these network tools.

ENHANCE YOUR UEBA IMPLEMENTATION WITH DTEX :
DTEX provides the context and visibility that log files alone can't.

DTEX doesn't rely on any Operating System or external logs. User visibility is achieved by monitoring the actions of the user – directly on the endpoint. This is accomplished by creating user-based metadata, from the users' interactions on the endpoint, which includes the detailed information that is not provided from external log sources. User-centric activity, collected in the form of metadata, provides real-time detection capabilities to identify actionable risks – regardless if the user is on/off the corporate network. DTEX then enriches the datasets to augment, corroborate, or potentially replace the requirement for additional log collection. This not only delivers faster time to value, but it also focuses on the highest risk: the user itself. DTEX can then integrate with UEBA solutions all in one single pane of glass. The result is full visibility into users behaviors, and less time trying to stitch together information from unreliable 3rd-party log sources.

A real world example:

Take a look at this alert, which you might get from a typical UEBA system:



High

John Jones

July 18th, 2020 6:23 pm

Unusual rate of file copies - 983 vs. 18.3 avg.

Blocked access to sensitive site: dropbox.com

Badge out during business hours: 2:34 pm

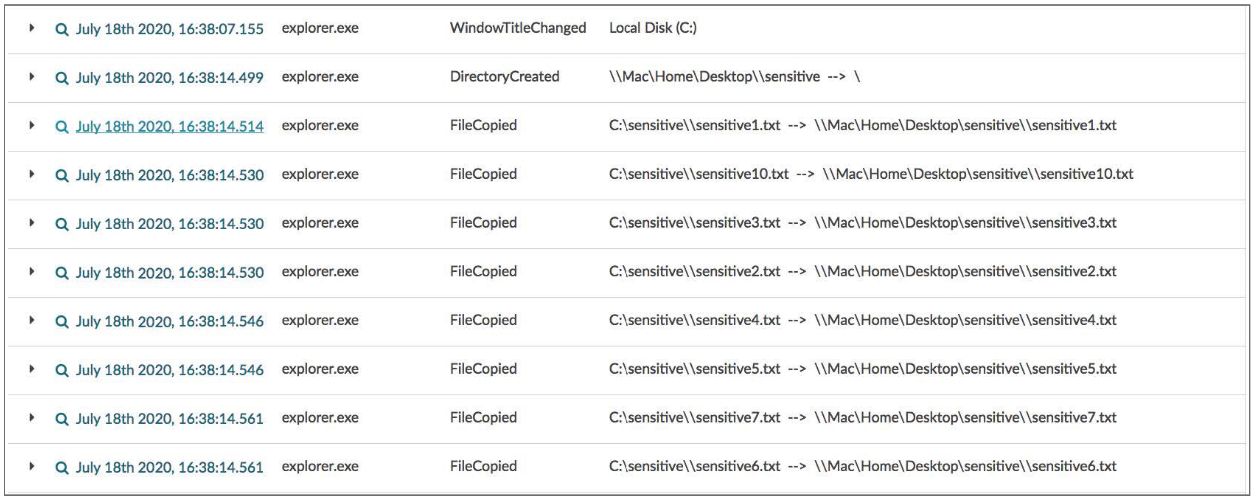
On the surface, this seems like a solid finding. John aggregated an unusual amount of data, and tried to get it out via Dropbox. Fortunately, he was blocked, so the analyst might be inclined to dismiss this alert.

However, this could be misleading. There's a lot of information missing here – **and UEBA alone completely misses that the user actually *did* successfully steal this data.** Let's dive deeper and look at what actually happened.

Finding the unusual rate of file copies with DTEX

Any UEBA system should trigger an alert for you when a user does an unusual number of file copies.

As you can see from the example below, DTEX doesn't require any integration with external data sources (like endpoint DLP or endpoint Windows Event logs to get visibility into file activity. Alerts on unusual file activity are included in an out-of-the-box algorithm that ships with DTEX.

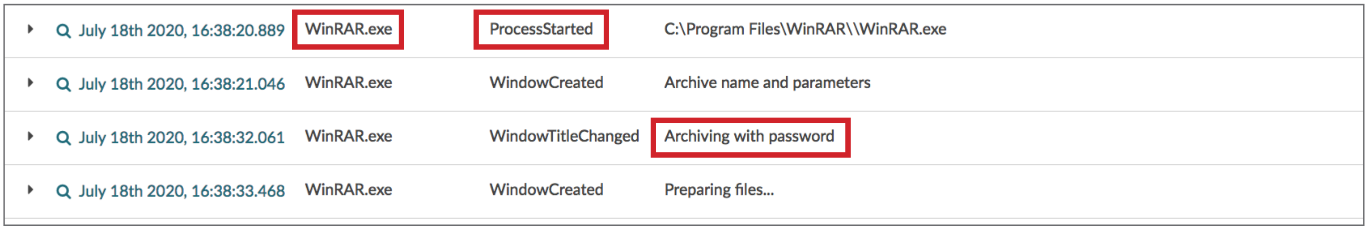


```
July 18th 2020, 16:38:07.155  explorer.exe  WindowTitleChanged  Local Disk (C:)
July 18th 2020, 16:38:14.499  explorer.exe  DirectoryCreated    \\Mac\Home\Desktop\\sensitive  -->  \
July 18th 2020, 16:38:14.514  explorer.exe  FileCopied          C:\sensitive\\sensitive1.txt  -->  \\Mac\Home\Desktop\sensitive\\sensitive1.txt
July 18th 2020, 16:38:14.530  explorer.exe  FileCopied          C:\sensitive\\sensitive10.txt  -->  \\Mac\Home\Desktop\sensitive\\sensitive10.txt
July 18th 2020, 16:38:14.530  explorer.exe  FileCopied          C:\sensitive\\sensitive3.txt  -->  \\Mac\Home\Desktop\sensitive\\sensitive3.txt
July 18th 2020, 16:38:14.530  explorer.exe  FileCopied          C:\sensitive\\sensitive2.txt  -->  \\Mac\Home\Desktop\sensitive\\sensitive2.txt
July 18th 2020, 16:38:14.546  explorer.exe  FileCopied          C:\sensitive\\sensitive4.txt  -->  \\Mac\Home\Desktop\sensitive\\sensitive4.txt
July 18th 2020, 16:38:14.546  explorer.exe  FileCopied          C:\sensitive\\sensitive5.txt  -->  \\Mac\Home\Desktop\sensitive\\sensitive5.txt
July 18th 2020, 16:38:14.561  explorer.exe  FileCopied          C:\sensitive\\sensitive7.txt  -->  \\Mac\Home\Desktop\sensitive\\sensitive7.txt
July 18th 2020, 16:38:14.561  explorer.exe  FileCopied          C:\sensitive\\sensitive6.txt  -->  \\Mac\Home\Desktop\sensitive\\sensitive6.txt
```

Did the user cover his tracks?

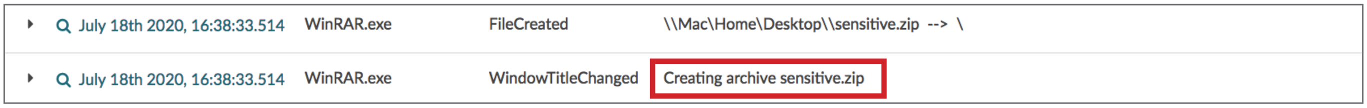
If you're looking at the UEBA alert, the next thing you'd see is the blocked attempt to access Dropbox.

But what you *don't* see with UEBA is that the user actually did something first to cover his tracks. He took those 983 files and zipped them up. Then, he encrypted them with a password to throw any content inspection off his tracks:



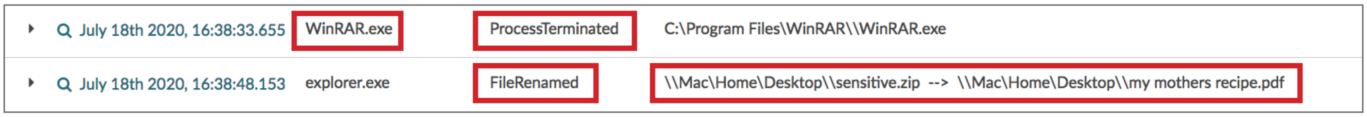
```
July 18th 2020, 16:38:20.889  WinRAR.exe  ProcessStarted       C:\Program Files\WinRAR\\WinRAR.exe
July 18th 2020, 16:38:21.046  WinRAR.exe  WindowCreated        Archive name and parameters
July 18th 2020, 16:38:32.061  WinRAR.exe  WindowTitleChanged   Archiving with password
July 18th 2020, 16:38:33.468  WinRAR.exe  WindowCreated        Preparing files...
```

DTEX even shows you the names of the new files from the compression, and ties them back to the original files.



```
July 18th 2020, 16:38:33.514  WinRAR.exe  FileCreated          \\Mac\Home\Desktop\\sensitive.zip  -->  \
July 18th 2020, 16:38:33.514  WinRAR.exe  WindowTitleChanged   Creating archive sensitive.zip
```

And even more importantly, you can see that the user renamed the file to take his obfuscation a step further:



```
July 18th 2020, 16:38:33.655  WinRAR.exe    ProcessTerminated  C:\Program Files\WinRAR\\WinRAR.exe
July 18th 2020, 16:38:48.153  explorer.exe  FileRenamed        \\Mac\Home\Desktop\\sensitive.zip  -->  \\Mac\Home\Desktop\\my mothers recipe.pdf
```

Log-based and network-based UEBA systems are completely blind to this activity.

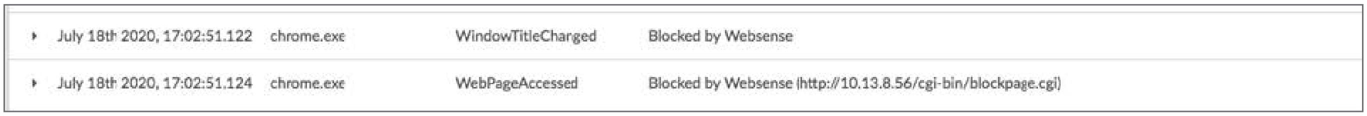
It's absolutely critical to have visibility into this, both to understand the user's actions and to prove that the user intended to steal data from his company. If an analyst was unable to see the archiving or the file rename, they would be relying on guesses to fill in the blanks and would have little-to-no proof as to the user's intent.

Even worse, the analyst might need to turn to forensic tools and disk image analysis in an attempt to recreate the user's actions, which is difficult and time consuming. With DTEX, the analyst gets that valuable intelligence in seconds.

The blocked Dropbox attempt

As you can see in the original UEBA alert, the user then attempted to access Dropbox. His company uses a proxy, so he was blocked.

The UEBA system gets this information from proxy logs. DTEX sees the same activity, with no need for integration with proxy logs:



```
July 18th 2020, 17:02:51.122  chrome.exe  WindowTitleChanged  Blocked by Websense
July 18th 2020, 17:02:51.124  chrome.exe  WebPageAccessed     Blocked by Websense (http://10.13.8.56/cgi-bin/blockpage.cgi)
```

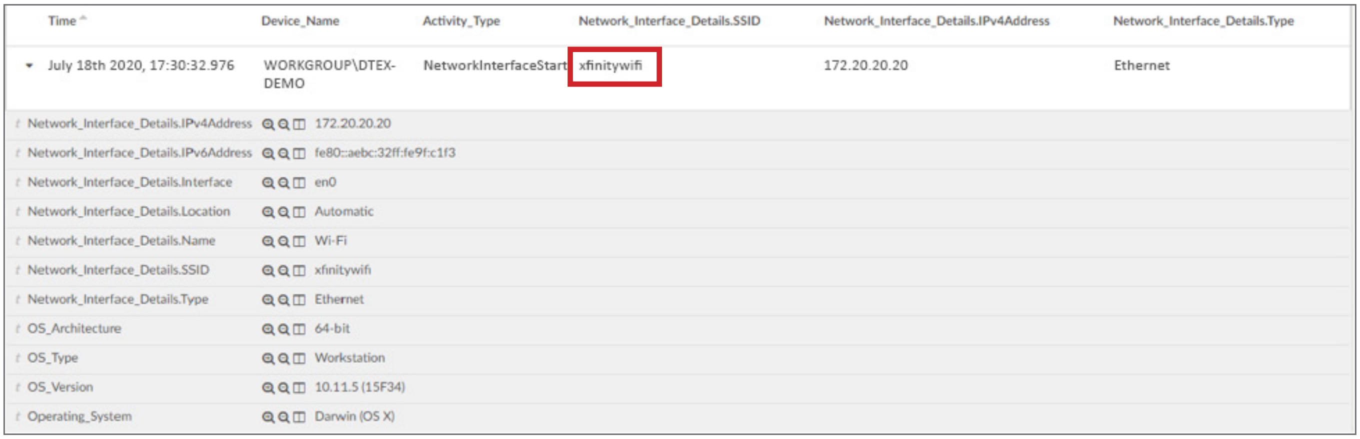
UEBA alone misses the full story, but DTEX catches the user steal data off-network.

According to the access logs analyzed by the UEBA system, the last step the user took was using his badge to swipe out of the office building.

But that’s not where the story ends. **That’s just where log-file and network-based visibility end.**

DTEX however, gets data directly from the endpoint. This means that you get user visibility at all times, even when the user is off your corporate network (or isn’t connected to the Internet).

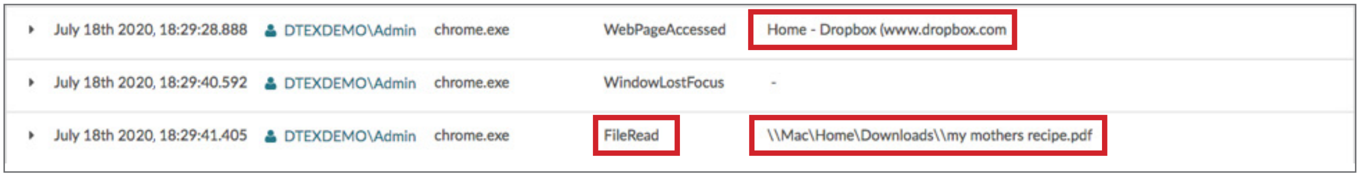
Here, DTEX sees the user log on to a private wifi network.



Time	Device_Name	Activity_Type	Network_Interface_Details.SSID	Network_Interface_Details.IPv4Address	Network_Interface_Details.Type
July 18th 2020, 17:30:32.976	WORKGROUP\DTEX-DEMO	NetworkInterfaceStart	xfinitywifi	172.20.20.20	Ethernet
Network_Interface_Details.IPv4Address	172.20.20.20				
Network_Interface_Details.IPv6Address	fe80::aebc:32ff:fe9f:c1f3				
Network_Interface_Details.Interface	en0				
Network_Interface_Details.Location	Automatic				
Network_Interface_Details.Name	Wi-Fi				
Network_Interface_Details.SSID	xfinitywifi				
Network_Interface_Details.Type	Ethernet				
OS_Architecture	64-bit				
OS_Type	Workstation				
OS_Version	10.11.5 (15F34)				
Operating_System	Darwin (OS X)				

Now, the user is on a network that your company doesn’t control. They are free to do whatever they want with corporate data. There is no proxy protection to keep them from going to unrestricted file sharing and webmail sites.

Next, DTEX shows that the user did, in fact, successfully upload the file to Dropbox.

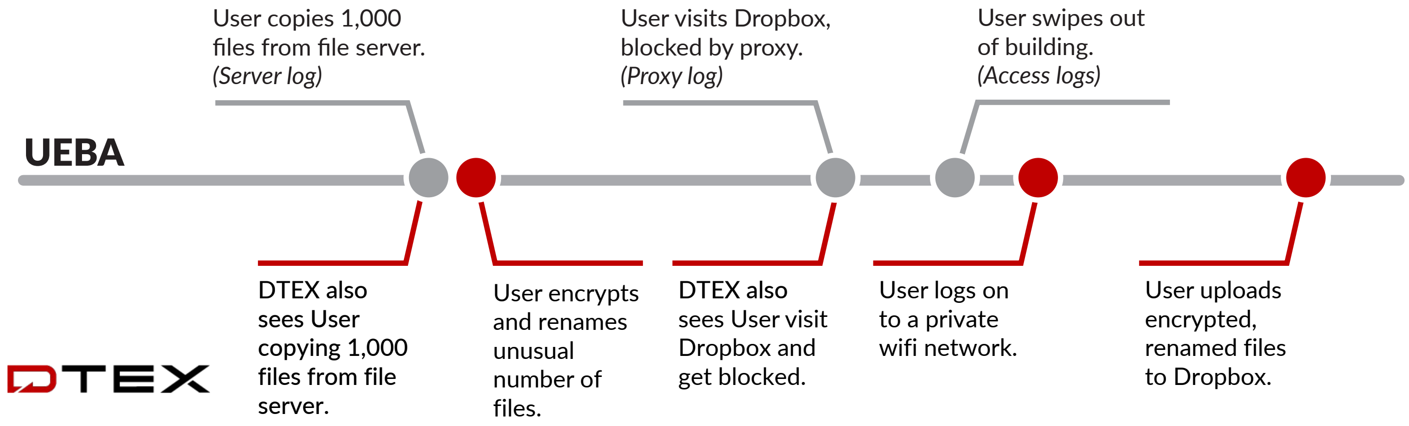


July 18th 2020, 18:29:28.888	DTEXDEMO\Admin	chrome.exe	WebPageAccessed	Home - Dropbox (www.dropbox.com
July 18th 2020, 18:29:40.592	DTEXDEMO\Admin	chrome.exe	WindowLostFocus	-
July 18th 2020, 18:29:41.405	DTEXDEMO\Admin	chrome.exe	FileRead	\\Mac\Home\Downloads\\my mothers recipe.pdf

As you can clearly see through this example, network logs alone don’t provide enough visibility to catch even common user breaches.

The only way to get the visibility necessary to see these attacks is to monitor the point closest to the user: the endpoint. DTEX provides an unmatched level of visibility into user activity. As a result, DTEX delivers higher quality alerts with fewer false positives.

The timeline below summarizes the full event, comparing data collected by log-based UEBA and visibility from DTEX.



UEBA

User copies 1,000 files from file server. *(Server log)*

User visits Dropbox, blocked by proxy. *(Proxy log)*

User swipes out of building. *(Access logs)*

DTEX

DTEX also sees User copying 1,000 files from file server.

User encrypts and renames unusual number of files.

DTEX also sees User visit Dropbox and get blocked.

User logs on to a private wifi network.

User uploads encrypted, renamed files to Dropbox.

In this simplified format, it's even more clear: in order to catch these events early, you need context and full user visibility from the endpoint. DTEX provides near-real-time events and visibility that gives analysts the full context they need to quickly dismiss or act on suspicious user activity.

FILL THE GAPS IN YOUR UEBA WITH DTEX

Integrate DTEX data into your UEBA solution for more complete visibility and analytics.

DTEX can integrate seamlessly with several UEBA vendors so that you can take advantage of all the benefits of DTEX's user visibility within your existing UEBA install. DTEX provides the data source that you need in order to fill the gaps in your security posture.

DTEX provides unparalleled insights into many risk factors across your organization, including but not limited to:

MALICIOUS USERS	NEGLIGENT USERS	CREDENTIAL THIEVES
Internal users that intentionally harm the enterprise.	*Internal users that accidentally harm the enterprise.*	*Outside attackers that infiltrate the organization.*
Creative Data Theft	Online File Sharing	Unusual Data Aggregation
Obfuscation & Covering Tracks	Webmail	Privilege Escalation
Bypassing Security Controls	Pirated Media & Applications	Lateral Movement Tools
Flight Risk	Gambling	Ransomware

LEARN MORE ABOUT DTEX AND ENTERPRISE USER INTELLIGENCE

DTEX's Enterprise User Intelligence Platform is purpose-built to provide intelligent, scalable, real-time, and privacy-conscious user insights. DTEX provides the visibility that you need in order to catch insider threats, utilizes machine learning to pinpoint critical insights, and prioritizes answers with alert stacking and intuitive risk scoring. Learn more at www.dtexsystems.com.