REMOTE AND @RISK

TRUSTED INSIDER OR MALICIOUS THREAT?

How 2020 Changed Employee Behaviors and Put Organizations on High Alert

2020 Insider Threat Report

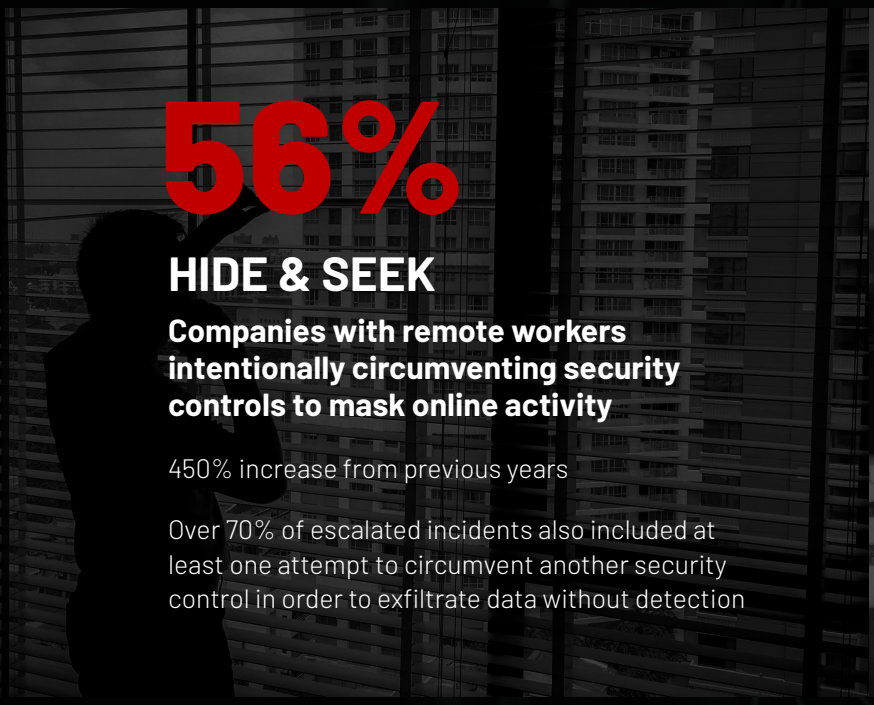
DTEX

THE WORKFORCE CYBER INTELLIGENCE COMPANY™

Executive Summary

For decades, the global workforce has been slowly shifting to a dispersed or "work from home" (WFH) model. In fact, WFH grew 173% from 2005 to 2018*, with companies such as Coinbase, Twitter, Upwork, Facebook and Shopify leading the way. The global political, environmental and infectious events that have defined the first nine months of 2020 accelerated this trend – creating operational and security challenges for every organization and causing disturbing changes in employee behaviors.

DTEX's analysis shows that the shift to a near 100% WFH workforce by the Global 5000 has significantly influenced and changed the behaviors of thought-to-be trusted insiders. Our customer stated that these changing employee behaviors are likely caused by several factors including an increase in employee separations and the need for security teams to augment security policies to improve the productivity of at-home workers. This research brief analyzes and plots these behaviors against the Insider Threat Kill Chain and offers specific indicators organizations can and should look for to identify elevated insider risks.



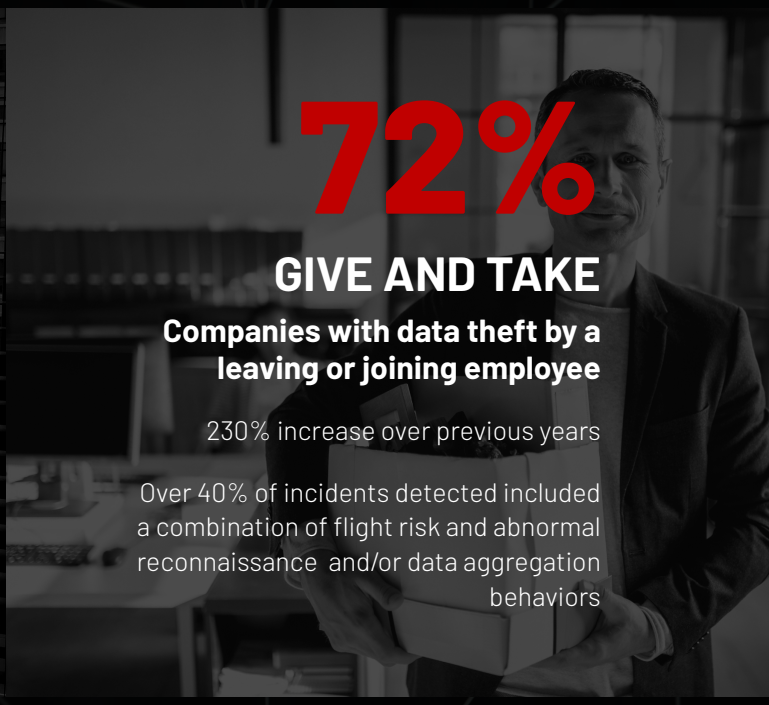
56%

HIDE & SEEK

Companies with remote workers intentionally circumventing security controls to mask online activity

450% increase from previous years

Over 70% of escalated incidents also included at least one attempt to circumvent another security control in order to exfiltrate data without detection



72%

GIVE AND TAKE

Companies with data theft by a leaving or joining employee

230% increase over previous years

Over 40% of incidents detected included a combination of flight risk and abnormal reconnaissance and/or data aggregation behaviors

These findings make it clear that the equilibrium between security posture and workforce productivity has been disrupted for almost all companies, regardless of size, industry, or geography. The question now facing the Global 5000 and every company is:

Are our trusted insiders changing their behaviors to put the company at risk and what must we do differently to drive high employee performance and positive sentiment, prioritize privacy and better protect regulated data and intellectual property?

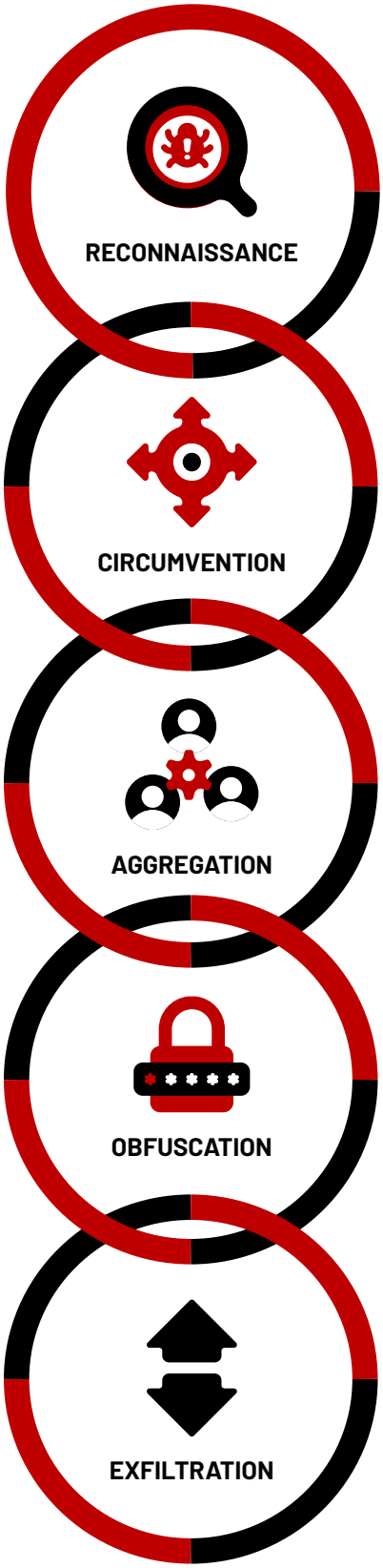
*GlobalWorkplaceAnalytics.com analysis of the 2005-2018 American Community Survey (ACS, a U.S. Census Bureau product).

The Insider Threat Kill Chain

The Insider Threat Kill Chain describes the pattern followed by malicious insiders and allows organizations to understand the entry-point and scope of an attack as well as the intent of the insider.

The data collected by the DTEX Counter-Insider Threat Research Team during interviews with hundreds of customers and Global 5000 organizations represents a diverse sample set of businesses that varied by size, industry, and geography. Based on these interviews, behaviors were plotted against the Insider Threat Kill Chain to properly identify the changing activity of trusted insiders in the first nine months of 2020 and the possible reasons based on the organization's identification as a compliance or innovation driven organization.

INSIDER THREAT KILL CHAIN



DEFINITIONS

When preparing for data theft, **a malicious insider** typically begins with research. This is where they locate the data that they would like to steal, test security controls, or, in the case of compromised credentials, where the insider will test the limits of the stolen credentials privilege.

Any attempts to bypass existing security controls provide an important **indication** that subsequent actions were intentional. Many organizations place too much reliance on the 'locks on their doors', however an insider typically has sufficient domain knowledge to know which doors are unlocked or simply has access to the key.

Whether it's **'low or slow'** or a **'smash & grab'**, most data exfiltration involves an aggregation step. Data is commonly aggregated on a local workstation or a server with internet access. Data compression is often leveraged for larger transfers.

The act of '**covering one's tracks'** is ultimately the strongest indicator of intent. While there's countless ways to get data out, there is a finite number of ways concealing malicious activity.

Many organizations make **the mistake of disproportionately investing in legacy endpoint DLP and UAM tools** which attempt to detect and prevent exfiltration routes. However, while rigid rules may stop malware detonation, they almost never stop an insider with malicious intention. InTERCEPT analyzes all activity from the point closest to the user, providing visibility into exfiltration routes that most other tools miss.

INDICATORS

- Suspicious research or innocuous file exfil
- Unusual network enumeration
- Anomalous file or device access

- Tampering with security controls
- Suspicious off-network activity
- Unusual privilege escalation

- Anomalous clipboard activity
- Sensitive data archival
- Anomalous drive mappings or symbolic link creation

- Suspicious file renaming
- Steganography & encryption
- Anonymous web browsing & disk erasing utilities

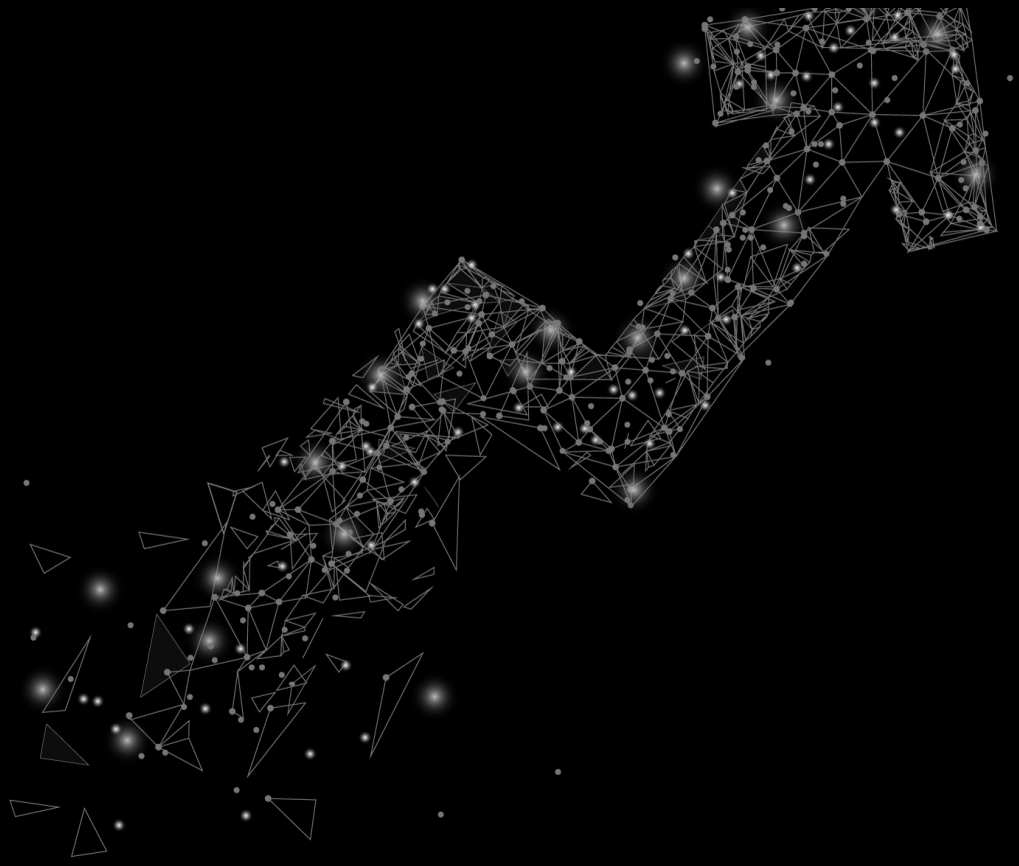
- Unencrypted USB drives
- Saving data to personal webmail drafts
- Airdrop or Bluetooth transfers

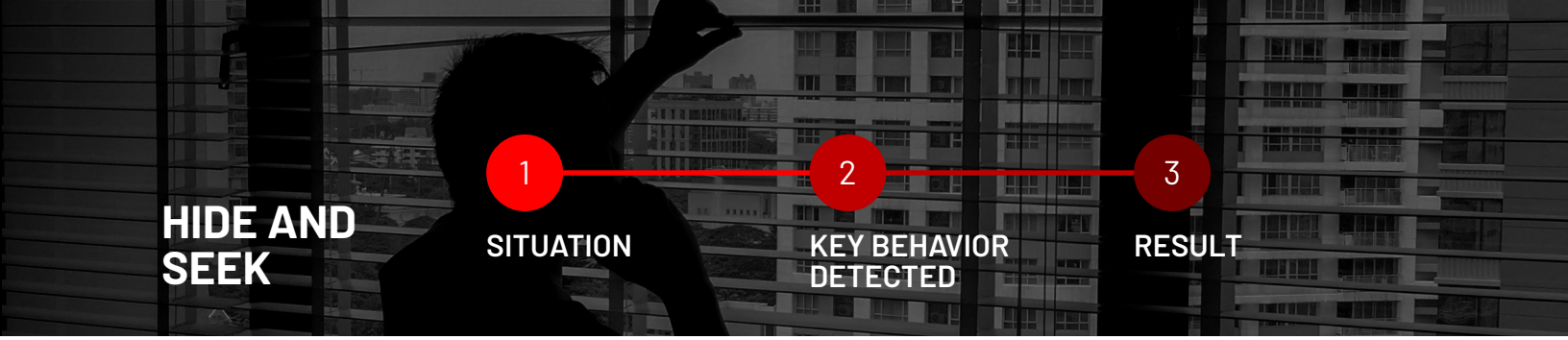
HIDE & SEEK

Employees Masking Online Activities Increases by 450%

DTEX's analysis shows that 56% of companies saw a dramatic increase in obfuscation behavior among employees in the first 9 months of 2020 compared to the full 12 months of 2019. This level of obfuscation behavior represents a 4.5x increase (450%) over 2019 findings.

Most commonly, these remote workers attempted to intentionally bypass the corporate VPN to mask their online activities. Within these incidents, DTEX also detected that 70% of the obfuscation behaviors visible to the security and HR teams included at least one attempt to circumvent another security control to exfiltrate data without detection.





HIDE AND SEEK

	1 SITUATION	2 KEY BEHAVIOR DETECTED	3 RESULT
Private Browsing Precedes Use of Personal Storage Devices	An employee at a global wealth management company browses job sites using incognito windows in Chrome or private windows in Firefox, puts corporate data onto an unauthorized USB device, and then attempts to leave the company.	Based on the employee's attempts to obfuscate browsing behavior, the employee was identified as flight risk. The employee was flagged as a 'person of interest' and subsequently detected downloading corporate email files and copying data to a personal USB drive. The specific files and information being copied was identified as well as the lack of encryption on the removable device.	The company was able to pursue legal proceedings to protect sensitive enterprise data.
Employee Hiding Illegal Internet Activity via the Tor Browser	An employee at a mid-size agriculture company who had recently transitioned to COVID related remote-work and was emboldened by the apparent lack of surveillance was able to disable the corporate VPN and use his device for personal activities outside of normal working hours. The user subsequently installed the Tor browser, which hides the users IP address and history, to order opiods, pirated media and other products on risky sites.	DTEX detected the disabling of VPN and the increasing trend of access to personal email and other personal websites in addition to the subsequent presence and use of the Tor browser, by which time the individual was already under focused-observation by the SOC team. The employee was observed hiding the browser in a folder named after a workrelated project. He would regularly install and uninstall the browser, as a further attempt to hide activity from the team.	The HR and Legal teams were provided with a detailed behavior audit which was escalated to line management using the appropriate channels. In addition, the historical alerts were provided as evidence that the 'focus-observation' feature was deployed in a proportionate way.
Unauthorized Employee Accesses Sensitive Financial Information in Log Files	An employee at a government agency in APAC requested access to payroll data but was denied. He then discovered that he could already access the same sensitive information in an unsecured log file. He reported the security weakness to the security team so the vulnerability could get eliminated.	A six-month review of the data to analyze access discovered that the employee who reported the vulnerability did in fact access the IP and potentially misused the data 6 days prior to the audit. It was detected that he had downloaded the file, obfuscated the data using an analytic tool, printed the data on a specific printer, and emailed a subset of the IP in a renamed CSV file to a recipient outside the company. It appeared that the employee was doing something malicious and trying to cover his tracks by reporting the vulnerability after he had already sent the data outside the company.	The six-month audit was completed within 24 hours and gave the senior executive team a comprehensive picture of the vulnerability created by this log file. The audit revealed that no one except for this individual had unauthorized access to this sensitive data, which meant that the agency could avoid the embarrassment of having to make a public announcement about a potentially broader breach. They were able to discipline the individual.

GIVE & TAKE

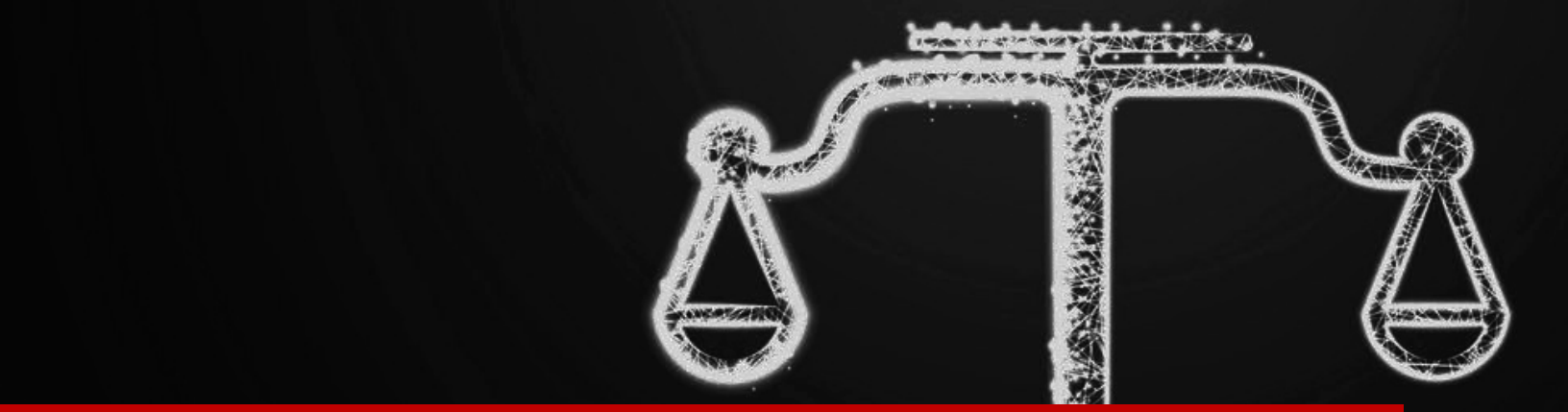
Data Theft by Leavers and Joiners Increases by 230%

The DTEX analysis shows that 72% of companies detected data reconnaissance or aggregation behavior either by an employee leaving the company and attempting to take protected IP with them or an employee joining the company and attempting to inject IP they have taken from prior employers into their new company. This analysis highlights a 2.3x increase (230%) in these reconnaissance and aggregation behaviors in the first nine months of 2020 versus similar behaviors detected by DTEX in 2019.

Of the organizations surveyed, those utilizing DTEX InTERCEPT – 40% of the 72% -- proactively identified employees as 'flight risks' and prevented data exfiltration attempts. The growth in premeditated data theft attempts by employees strongly suggests that companies are facing a heightened risk of data loss as work-from-home (WFH) continues and employees remain virtual.

GIVE AND TAKE

	1 SITUATION	2 KEY BEHAVIOR DETECTED	3 RESULT
Disgruntled Employee Creates Misleading Filenames in an Attempt to Exfiltrate Data	Employee was under investigation for violating security policy and suspected he was going to get terminated. He aggregated a significant number of sensitive/ confidential files, including applications, source code, specification documents, and certification IDs/keys to AWS servers. The files were aggregated into four compressed/encrypted files that were given inconspicuous names, such as "personal music", "personal docs", and "personal pictures", and copied to the corporate OneDrive's sync folder to exfiltrate files (likely to personal device with the corporate OneDrive installed). Finally the user deleted the files from the sync folder to cover their tracks.	The DTEX audit trail showed the specific files aggregated, the actions to rename the files, the actions to export the files through OneDrive and the actions to delete the contents of the sync folder to cover the tracks. While the transfer medium (OneDrive) was fully authorized along with access to the sensitive IP, the unusual aggregation behavior ultimately led to successful escalation of the incident.	The audit data was provided to the HR and legal teams to assist their investigation.
New Employee Captures Unauthorized Images of Products Prior to Release	A manufacturer of consumer products holds a virtual event to preview new products. To prevent images of the products from leaking to the public ahead of launch, they use an event URL that installs a watermark on the images. A new employees found a way to join the event using a public URL to avoid the watermark, raising the potential of unauthorized image leaks.	DTEX identified a new employee using screen capture tools and accessing the site through the public URL. Additional contextual behaviors related to large volumes of data transferred onto company systems by the new employee also revealed potentially sensitive data from the employees previous employer. As is often the case, a truly malicious user often exhibits multiple but unrelated high risk behaviors through the aggregation of these unrelated behaviors, the individual was escalated above all other employees at the organization.	Detailed behavior Information provided to the company's legal and HR team to investigate further
Employee Leaving Company Downloads 25GB of Data to a USB	An employee at a small financial services firm was leaving the company and transferred 25 GB of files regarding past projects onto a USB drive.	While flight risk was not predicted in this incident, upon resignation, DTEX alerted the company regarding the name, size, and date or the files being transferred. The files were a mix of personal and work-related files.	The employee was not being malicious, but the company issued a cease and desist order to stop the loss of sensitive files.



CONCLUSION

Enterprises Must Forge New Paths to Regain Equilibrium Between Security and Productivity

The equilibrium between security posture and workforce productivity is in chaos. Trusted insiders once thought to be reliable and responsible corporate citizens are changing their behaviors and increasing the risk of data loss, external attack and regulatory compliance violations for their employers.

What exactly is driving this drastic behavioral change? Is it fear of losing their job, dissatisfaction with their employer, a disregard for employer policies and their co-workers? In our interviews we found a massive and immediate uptick in employee separations along with a need loosen security controls to maintain data access for the virtual workforce are the leading causes. The question companies should be asking is there more to this increase in active, malicious obfuscation, reconnaissance and aggregation behaviors than layoffs and looser security policies on behalf of employers?

What is known is that enterprise workforce activity and user behavior telemetry remain a mystery to most enterprises and organizations. The global political, environmental and infectious events that have defined the first nine months of 2020 did not create this operational blind-spot. It has existed for decades.

The findings in this report highlight the lack of adoption and ineffectiveness of traditional cyber security and employee monitoring tools, and suggest that organizations need to prioritize the human-element and workforce behavior in relation to data, process and machines as a pillar of their next-generation security and IT technology strategies.

What remains to be decided is how organizations will respond to these changes in employee behavior and navigate the ethical, operational and technical challenges and requirements necessary to realize the visibility they need to protect their data and IP while also building a culture of trust and transparency amongst an increasingly privacy-conscience hybrid workforce.

About DTEX

We are the leading experts in Workforce Cyber Intelligence.

DTEX Systems is the world leader in Workforce Cyber Intelligence and committed to helping enterprises run safer and smarter. Only DTEX dynamically correlates data, application, machine, and human telemetry to stream context-rich user behavior and asset utilization analytics that deliver a first-of-its-kind human-centric approach to enterprise operational intelligence. Hundreds of the world's largest enterprises, governments and forward-thinking organizations leverage DTEX to prevent insider threats, stop data loss, maximize software investments and deployments, optimize workforce productivity, and protect remote workers. DTEX has offices in San Jose, California and Adelaide, South Australia and is backed by Northgate Capital, Norwest Venture Partners, Wing Ventures, and Four Rivers Group. To learn more visit: www.dtexsystems.com.