BRING ENDPOINT TELEMETRY TOGETHER FOR EFFECTIVE INSIDER RISK MANAGEMENT

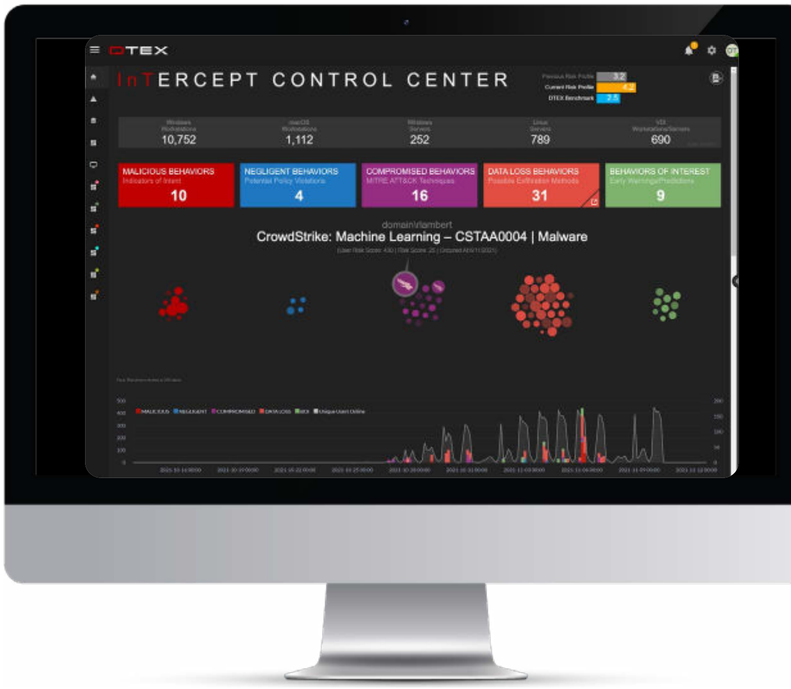
As the network perimeter has disappeared, telemetry from the endpoint is arguably the most important data source in threat detection and response. It is key to minimizing visibility blind spots and helps to ensure that malicious activity does not go unidentified. Endpoint data has proven to detect risky behavior sooner, despite evolving adversarial techniques. While endpoint data provides greater visibility to user activity than network security products, sufficient context remains challenging to identify insider risk and quickly determine malicious vs. non-malicious or careless behavior.

To solve this challenge, DTEX and CrowdStrike have partnered on integrations so customers can take advantage of rich behavioral context and deep endpoint telemetry to gain real-time visibility into human activity and data usage insights. DTEX behavioral intent data answers What, When, Where and Why sensitive IP and other data files are being aggregated, archived, modified, obfuscated, and may be exfiltrated. Customers gain access to DTEX digital forensics for an evidentiary quality audit trail of user activities to enrich incident response investigations.

DTEX InTERCEPT™

The most effective approach to insider risk management (IRM) converges the essential capabilities from data loss prevention (DLP), User Activity Monitoring (UAM), and User and Entity Behavior Analytics (UEBA). The key benefits are the ability to identify risks without impacting privacy or endpoint performance, and most importantly the capability to proactively detect and mitigate insider risk before a data breach occurs.

Through DTEX DMAP+ Technology™, InTERCEPT collects unique elements of enterprise telemetry from data, machines, applications, and people to capture activity history, behavior trends, data utilization with situational context from across the enterprise to identify indicators of intent and correct risky behavior sooner, while eliminating false positives.

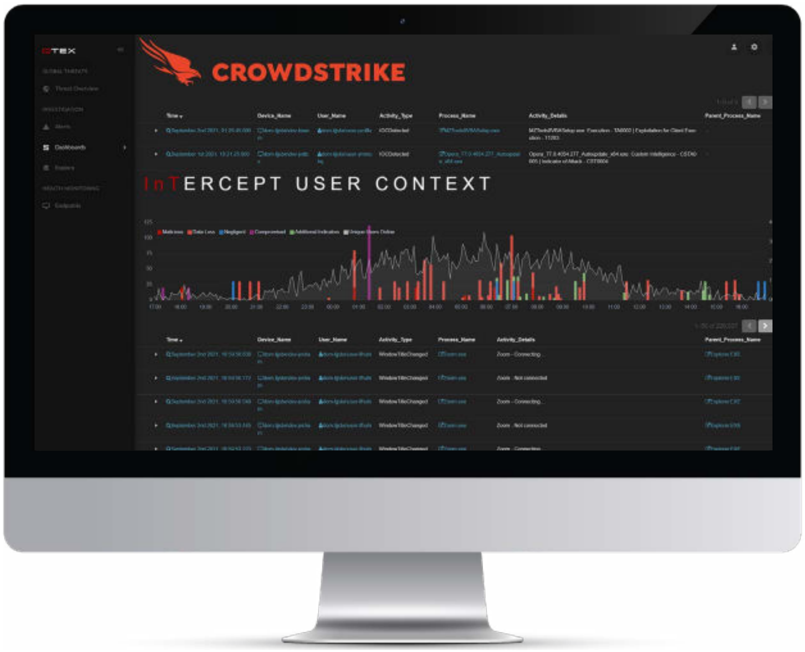


DTEX and CrowdStrike

DTEX and CrowdStrike work together to include critical user context for endpoint alerts, answering questions like, "What was the user doing? Did the user click on a link? Was it phishing, an ad, or a download?" The InTERCEPT platform identifies the root cause faster and details actions afterwards. DTEX complements endpoint detection and response (EDR) solutions because while EDRs capture system level activities, DTEX gives granular visibility into user sessions (which endpoint detection and response (EDR) do not).

More commonly seen external threat techniques, such as Discovery, Persistence, and Execution, may be ignored by endpoint solutions because of the volume of activities generated and the high number of false positives. Although EDR tools often capture the data, the log information is not robust enough to identify what is normal and what is a threat. DTEX also advances the Falcon platform with important behavioral DLP activity like file activity detection. And the audit trail DTEX captures not only gives insight into insider threats, but also validates whether a CrowdStrike alert is a true positive.

InTERCEPT dashboards provide visualizations that highlight CrowdStrike activity, work to validate alerts, and ultimately identify malicious and non-malicious behavior.



Additional benefits include:

- **Behavioral Data Loss Prevention:** File lineage and inferred file sensitivity information works to protect valuable IP both on and off-network, in use, at rest, in and transit.
- **Digital Forensics and Incident Response:** Behavior-based telemetry compliments Falcon Forensics to provide user-centric, pre-incident behavioral evidence that fills in gaps in context.
- **Insider Threat Detection & User Lockout:** Anonymously identify which users are engaging in malicious, negligent, and compromised behaviors, and escalate to immediate user lockout to prevent data exfiltration.

REQUEST A DEMO

Contact us today to schedule a demonstration at demo@dtexsystems.com

ABOUT DTEX SYSTEMS

DTEX Systems empowers organizations to prevent data loss and support a trusted workforce by proactively stopping insider risks from becoming insider threats. Its InTERCEPT™ platform consolidates the essential elements of Data Loss Prevention, User Activity Monitoring, and User Behavior Analytics in a single light-weight platform to detect and mitigate insider risks well before data loss occurs. Combining AI/ML with behavioral indicators, DTEX enables proactive insider risk management at scale without sacrificing employee privacy or network performance.

To learn more about DTEX Systems, visit www.dtexsystems.com.