WORKFORCE CYBER INTELLIGENCE & SECURITY

MULTINATIONAL RETAILER
CASE STUDY

GAINING VISIBILITY TO RISK IN RETAIL STORES

Non-malicious Activity Also Presents Risk

The Customer – Multinational Retailer

This multi-brand retailer operates more than 2,500 stores in the North America, Asia, and Europe. In addition to Point of Sale devices, each retail outlet maintains one or more "back office" Windows PCs that are used by multiple retail Managers, Assistant Managers, and Regional Managers for employee shift scheduling, viewing and managing inventory, and other tasks.

All back office devices are connected to the corporate network and run Endpoint Detection and Response (EDR) software to protect the PCs and corporate network from malware and similar attacks.

The Challenge – No Visibility to In-Store Computers

According to the organization's Information Security Manager, the security team was concerned about their lack of visibility into activity on the back office endpoints. While they were satisfied with the protection their EDR solution provided against external malicious attacks, they had no idea how back office devices were used. While they had network-level visibility, they needed user-level visibility. In the Information Security Manager's words, "No EDR alert does not mean there is no risk."

In particular, they required better visibility into unauthorized use of external drives. A regional manager had recently traveled to several stores and printed documents from a thumb drive that contained malware, infecting back office devices in several stores. While the team was able to contain the infection, it highlighted the fact that their existing telemetry did not provide sufficient information to address risks to these endpoints. They required a solution that could provide them with data on exactly what was occurring across their retail environment and contextual information to understand whether activities were benign or potentially malicious. In short, a solution that would alert them to anomalies in authorized user behavior that signaled a potential risk of data loss.

The retailer also faced other challenges. The back-office endpoints varied in age and operating system, meaning that any solution to address the lack of visibility must have minimal computing overhead requirements. Additionally, technology enablement personnel would have to deploy it in stores around the world, thus simplicity in deployment and configuration was necessary.

The Solution – DTEX InTERCEPT

To meet these needs, the retailer brought in DTEX InTERCEPT. DTEX InTERCEPT™ is a Workforce Cyber intelligence and Security platform that brings together the capabilities of Insider Threat Management, User and Entity Behavior Analytics, Digital Forensics, and Endpoint DLP in an all-in-one lightweight, cloud-native platform. DTEX InTERCEPT delivers the context and intelligence that answers the Who, What, When, Where and How related to any potential insider threat situation, compromised account event or data loss scenario.

InTERCEPT is accurate, lightweight and easily scalable. It provides contextualized data accounting for actions and activities of data, machines, applications, and people (DMAP) in near-real-time, both on and off the corporate network to surface dynamic behavioral awareness indicators. It doesn't generate false positives that create confusion. It's smart enough to understand the difference between normal and malicious behavior, enabling you to quickly zero in on real threats. Finally, as a zero-impact, cloud-native solution, InTERCEPT collects only 3-5 MB of data per user each day with low CPU usage and zero impact on employee efficiency or performance. Importantly, InTERCEPT is a cross-platform solution, supporting Microsoft, Mac, Linux, and virtual environments.

The Results – Rapid Visibility to Previously Unknown Risks

Within the retail stores, DTEX InTERCEPT was deployed across all back office devices, within a few days, and provided the retailer's security team with a baseline of user activities — and some startling results.

Widespread unauthorized use of USB storage.

The retailer had a policy to limit the use of removable storage devices and had reinforced that policy after the earlier USB-based infection. To the team's surprise, DTEX InTERCEPT reported that almost a third of all authorized retail personnel used unauthorized USB flash drives multiple times each day! An order of magnitude of higher usage of USBs than any other group within the company.

An investigation by the internal security team determined that these activities were unauthorized, but not malicious. Instead of following company policy to use their OneDrive storage and other cloud-based tools, the regional managers, store managers, and assistant managers devised a "workaround" when sharing and printing schedules and other office work that needed to be moved between users and between shifts.

DTEX InTERCEPT quickly presented a picture of potential risks from these activities, allowing security teams to devise a roadmap to remediate risk that was efficient and actionable.

> "DTEX gave us a bird's eye view of the volume of USB activity, but also the ability to drill down, see details, determine intent, and build a plan for remediation."
>
> Information Security Manager at Multinational Retailer

> “We had no idea that these accounts existed or the potential liability from the loss of personal data. HR could not track these applicants because they were completely off network.”
>
> Information Security Manager at Multinational Retailer

Uncontrolled Webmail Accounts

Webmail accounts on corporate devices are an attack vector for malware and misuse that often introduce risk, including legal and reputational. Internal security was surprised to find dozens of unauthorized Gmail and Yahoo accounts incorporating the company’s brand. Since these were accessed through web browsers, the retailer’s security team had no visibility to the accounts or activity.

On investigation, the security team discovered that this too was a workaround that had spread between stores through word of mouth. The corporate email inboxes of store managers were inundated with messages from job applicants, making it easier to miss critical internal messages. The store manager’s solution was to establish webmail accounts for listing in local job postings, not recognizing the risk to the personal data of applicants or the possibility of former employees accessing this confidential data.

Visibility to these accounts was only possible through DTEX InTERCEPT. DTEX InTERCEPT also provided needed context to allow investigators to quickly discern between malicious and benign intent. The retailer quickly resolved the need for these accounts by establishing recruiting email addresses for each store.

WORKFORCE CYBER INTELLIGENCE & SECURITY

REQUEST A DEMO

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

ABOUT DTEX SYSTEMS

DTEX Systems helps hundreds of organizations worldwide better understand their workforce, protect their data and make human-centric operational investments. Its Workforce Cyber Intelligence & Security platform brings together next-generation DLP, UEBA, digital forensics, user activity monitoring and insider threat management in one scalable, cloud-native platform. Through its patented and privacy-compliant meta-data collection and analytics engine, the DTEX platform surfaces abnormal behavioral “indicators of intent” to mitigate risk of data and IP loss, enabling SOC enrichment with human sensors and empowering enterprises to make smarter business decisions quickly.

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