National Telecom Company Builds Data Lineage Program with Less Noise

CASE STUDY

Company Profile – A Public Telecom Company in the Midst of a National Roll-Out

A major telecommunications company based in the Asia-Pacific region was in the middle of a large-scale, publicly-funded project to upgrade telecommunications infrastructure.

This project put the organization in the center of the public eye, which meant that they needed to be especially careful to avoid mistakes or scandals. Cybersecurity was a top concern because a high profile breach or accident could have dire backlash.

Challenges – Wading Through a Sea of Noisy Data, Searching for Insights

As news reports of insider incidents became increasingly prevalent, company board members and executives realized that they needed to build a dedicated insider threat program. However, this endeavor meant they were forging a new path as one of the first Australian companies to build a program specifically to address insider threats.

The security team understood that protecting against insider threats in a large, distributed organization was not a straightforward task – and most importantly of all, they understood that such a program's success hinged upon detecting threats based on not just a large ***quantity*** of data, but the ***quality*** of user behavior data. This was particularly important for the Chief Data Office, who has determined that a data lineage program would be required to determine the origins of sensitive data and track its path through the organization. In order to do that , they needed high-fidelity user behavior data.

The organization's first attempt was the implementation of a leading SIEM tool, filled with large amounts of log data. It produced a massive noise and false positives. They quickly realized that they were trying to digest too much data, and that the data was poor-quality, making it nearly impossible to efficiently detect threats or conduct post incident investigations.

INDUSTRY
Telecommunications

REGION
Asia-Paci ic

COMPANY SIZE
5,000 Employees

DTEX DEPLOYMENT
8,500 Endpoints

PRIMARY USE CASES
Data Lineage – Getting the big-picture data view to understand and validate data usage and the associated risks

PRIMARY CHALLENGE
Finding the right data, instead of just a larger quantity of data

Solution — Finding the Right Data is the Backbone of Insider Threat Security

When the security team investigated DTEX, they quickly realized that it provided the user behavior data at scale that would enable them to evolve their strategy, producing better results with less data and less human effort.

- **High-fidelity user visibility from the endpoint.** The Insider Threat Team knew that the cornerstone of their success would be the quality of user visibility data provided by their chosen security tool. DTEX was the only solution that offered a high-fidelity signal tailored specifically around insider threats (unlike network or log file based visibility solutions, which attempt to reverse-engineer user behavior insights from other existing data). DTEX provided targeted user data instead of a huge quantity of noisy data, allowing them to do more with less. This was the immediate selling point for their team.
- **Lightweight and scalable.** After poor experiences with heavier solutions, like the bulky SIEM deployment, it was important that their chosen solution be easy to scale across the entire organization – which included thousands of endpoints. DTEX's lightweight nature allowed for quick deployment and scalability.
- **A complete audit trail.** DTEX provides an easy to understand audit trail that quickly and simply illustrates user activity. This enabled the organization to answer their pressing questions, like: Who opened this file in the past two days? Which users frequently access this server? Where are those files stored? Most importantly, DTEX collects important data like clipboard activities, file activities, print activities, etc. These data points, and more, provided the insights the security team needed to launch their data lineage program.

Ultimately, it didn't take long for the organization to choose DTEX as the cornerstone to their insider threat program. Once they made that decision, they began building a unique, top-down approach to insider threat detection and prevention.

INCIDENT TIMELINE

- High-fidelity data that allows them to **do more with less data.**
- User visibility that allows the insider threat team to integrate with their 12 visualizations to **show high-level "hot spots" of concentrated risk** at a glance.
- **Lightweight** and can be easily deployed and scaled.
- **Actionable user behavior intelligence** with visibility coming directly from the user and tailored to insider threat.
- **A full audit trail** that allows analysts to answer all the important questions.

Top Use Case: Data Lineage — An Innovative Approach to Data Security

Once installing DTEX, the organization quickly launched a new Data Lineage Initiative, which was a top priority borne of several unsuccessful attempts over the years.

Several years ago, the Chief Data Office was tasked a daunting job: to identify and tag all organizational data in a massive data classification project.

While the company reviewed several data classification tools, they weren't able to find any that were suitable at their scale. Ultimately, they hired a major consultancy to classify the data manually. After years passed, however, they were forced to determine that it simply was not feasible to tag all files in the organization at scale.

Although the project was technically unfinished, there was a positive outcome: during the course of the project, the organization identified all of their most important assets as "Crown Jewels" — and once DTEX was installed to track data lineage across the organization, they could put that work to use.

The Next Step: Using DTEX to Track User Interaction

Armed with the high-fidelity user data that DTEX provided, they were finally equipped to evolve their former data classification project into a data lineage program.

Instead of manually attempting to tag and categorize every piece of data in the organization, they now have the visibility to see how people and locations interact with that data. As a result of their previous attempted classification project, they had already identified the most critical pieces of data within the company. Using DTEX, they now track all the interaction with that key data. DTEX collects meta data on all confidential files — along with their hashes — and then feeds that audit trail into their visualization tool of choice, IBM's 12 solution.

With this combination, they can now visualize data lineage as sensitive data moves through the organization. This allows them to identify the highest risk people and locations in the company — meaning, the people and locations who most frequently come into contact with sensitive data. This way, they can pinpoint the people, files, or locations that inherently have the highest risk of data loss.

They now can categorize data in a business context by answering the critical question: What is the risk that this file will be lost or compromised, based on how many people touch this file and what they do with it?

This single question now underpins the organization's entire approach to insider threat and data protection. Once they can get that answer at a glance across the organization, they can easily prioritize their security measures around the high-value data that is most vulnerable.

The Results — An Innovative Data-Lineage-Focused Approach

For years, this organization struggled to get the data that they needed to effectively protect their IP — even as they tested solutions that devoured huge amounts of data. DTEX, however, provided the highly-focused signal that they needed to create an intelligent insider threat program.

This data lineage program allows the insider threat team to see "the big picture" at a glance instead of getting bogged down on an overwhelming number of specific alerts or minutiae. In a large organization like this, insider threat teams need to proactively identify the greatest areas of risk and strategize accordingly.

What's more, DTEX gives them the high-quality data that they need to drill down into these "hot spots" and easily answer the important questions around each risk.

The end result is a security program based on clear business context, which ultimately delivers greater visibility and a holistic, actionable understanding of the entire organization.

DTEX

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

ABOUT DTEX SYSTEMS

As the trusted leader of insider risk management, DTEX transforms enterprise security by displacing reactive tools with a proactive solution that stops insider risks from becoming data breaches. DTEX InTERCEPT™ consolidates Data Loss Prevention, User Activity Monitoring, and User Behavior Analytics in one lightweight platform to enable organizations to achieve a trusted and protected workforce. Backed by behavioral science, powered by AI, and used by governments and organizations around the world, DTEX is the trusted authority for protecting data and people at scale with privacy by design.