cyberhaven

Departing Employees Pose *Significant* Data Risk

Valuable information can leave the organization before their departure is even noticed

When employees prepare to leave an organization, risk begins well before their final day. Some are actively job searching, others have already accepted new roles, but the behavior pattern is consistent. Access is still intact, oversight can be limited, and motivation shifts. In that window, employees frequently collect data they believe will be useful in their next role or valuable for personal use, creating data risks for their employer.

This data can include proprietary documents, source code, customer records, and regulated data such as personally identifiable information (PII). In some cases the intent is clearly malicious. In many others, however, it is rationalized as harmless or even deserved. Regardless of intent, the outcome is the same. Sensitive data leaves the organization without visibility or control.

This form of insider risk remains under-addressed despite its scale and impact. Malicious insider incidents now carry an average cost approaching $5 million*, rivaling or exceeding the global average cost of a breach. At the same time, most organizations have reported an increase in insider-driven activity over the past several years, yet fewer than a third believe they have the tools required to detect and stop it effectively.

Departing employees represent a predictable and recurring risk category. Unlike external threats, there is no need for intrusion. The access already exists and the data is already in their grasp.

* IBM Cost of a Data Breach Report 2025

Cyberhaven Sees Insider Threats in Action

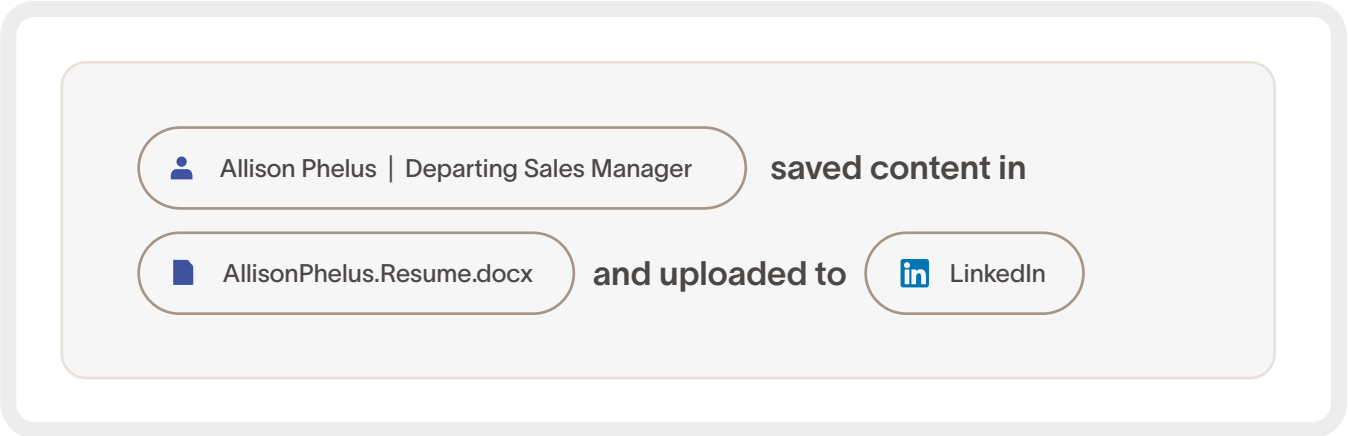
In a recent customer engagement, Cyberhaven worked with a security team to evaluate insider risk exposure during a policy development session. What surfaced was not a theoretical scenario, but an active data exfiltration event.

An employee had accepted a role at another company and began preparing for departure. Over the course of several days, they copied large portions of data from their local endpoint and exported email contents to a personal USB drive.

These actions didn't occur in isolation, as earlier signals provided critical context. The user had been uploading resumes to job platforms and receiving communications related to a new offer. These signals, combined with the subsequent data movement, created a clear narrative of intent and action.

Traditional tools would have struggled to connect these events. At best, they might log file transfers or flag large data movement in isolation. In many environments, this activity would not even be considered anomalous enough to trigger an investigation.

Cyberhaven identified the behavior as part of a broader pattern, enabling the security team to intervene before the employee exited the organization with sensitive data.



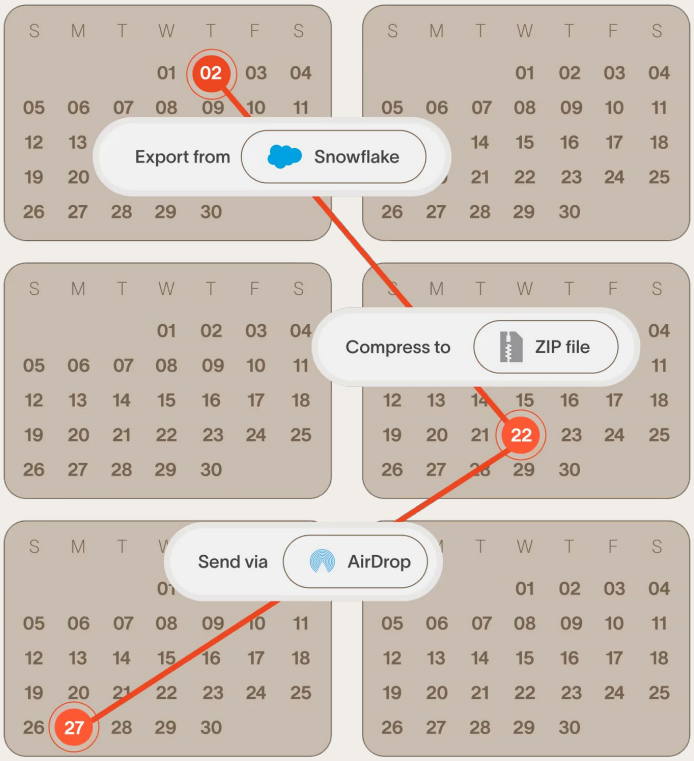
Cyberhaven is able to see data movement at a granular level, allowing teams to see exactly what occurred, where, when, and by whom.

Why Traditional Approaches Fall Short

Most data security tools operate within narrow boundaries. They rely on static classification, predefined policies, or visibility limited to specific parts of an environment such as cloud storage or email. This creates gaps in both detection and context.

Departing employee risk rarely manifests as a single, obvious event. It unfolds over time and across systems:

- Accessing sensitive files from endpoints
- Downloading data from SaaS applications
- Syncing or uploading data to personal cloud storage
- Copying files to removable media
- Forwarding information through personal email
- Interacting with external job platforms



When these actions are evaluated independently, they often appear benign. Security teams are left with fragmented signals and limited ability to distinguish normal work from risky behavior.

Without a unified understanding of how data moves and how user behavior evolves, organizations are forced into reactive detection. By the time an alert is generated, the data is often already outside the organization.

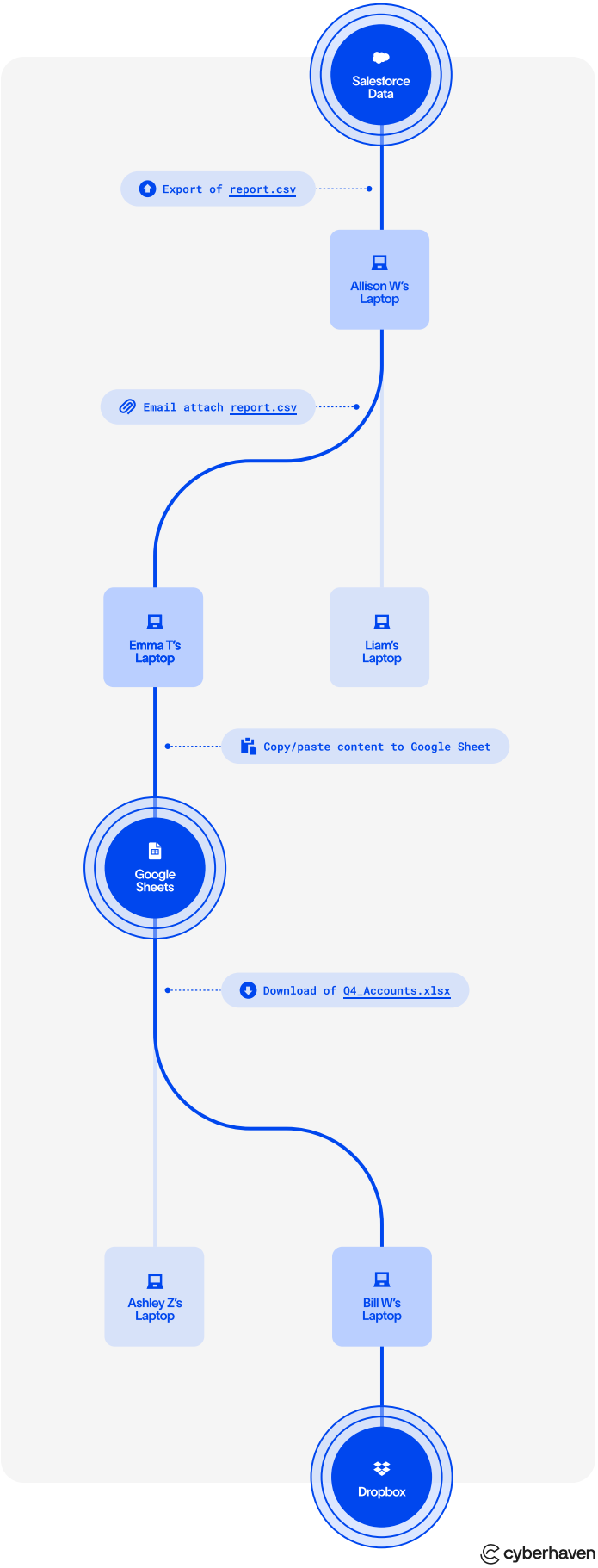
The Power of Data Lineage

Cyberhaven solves this visibility gap through data lineage, a fundamentally different approach to understanding data movement.

Rather than evaluating isolated events, Cyberhaven tracks the full lifecycle of data. Our unified AI & Data Security Platform understands where sensitive data resides, how it is transformed, where it moves, and who interacts with it along the way. Every action is connected into a continuous record, mapping data from source to destination.

In the context of departing employees, data lineage reveals when sensitive data is aggregated across systems and prepared for movement, surfacing risk before it reaches an external destination. It also preserves the connection to the original sensitive source even as data is copied, transformed, or renamed, ensuring context is not lost during exfiltration attempts.

If exfiltration does occur, Cyberhaven's data lineage adds critical context to separate low-level risk events from true insider risk by malicious users. It knows exactly what data moved, its sensitivity, its origin, and its downstream impact. This allows teams to prioritize real risk instead of chasing volume.



The Role of Linea AI

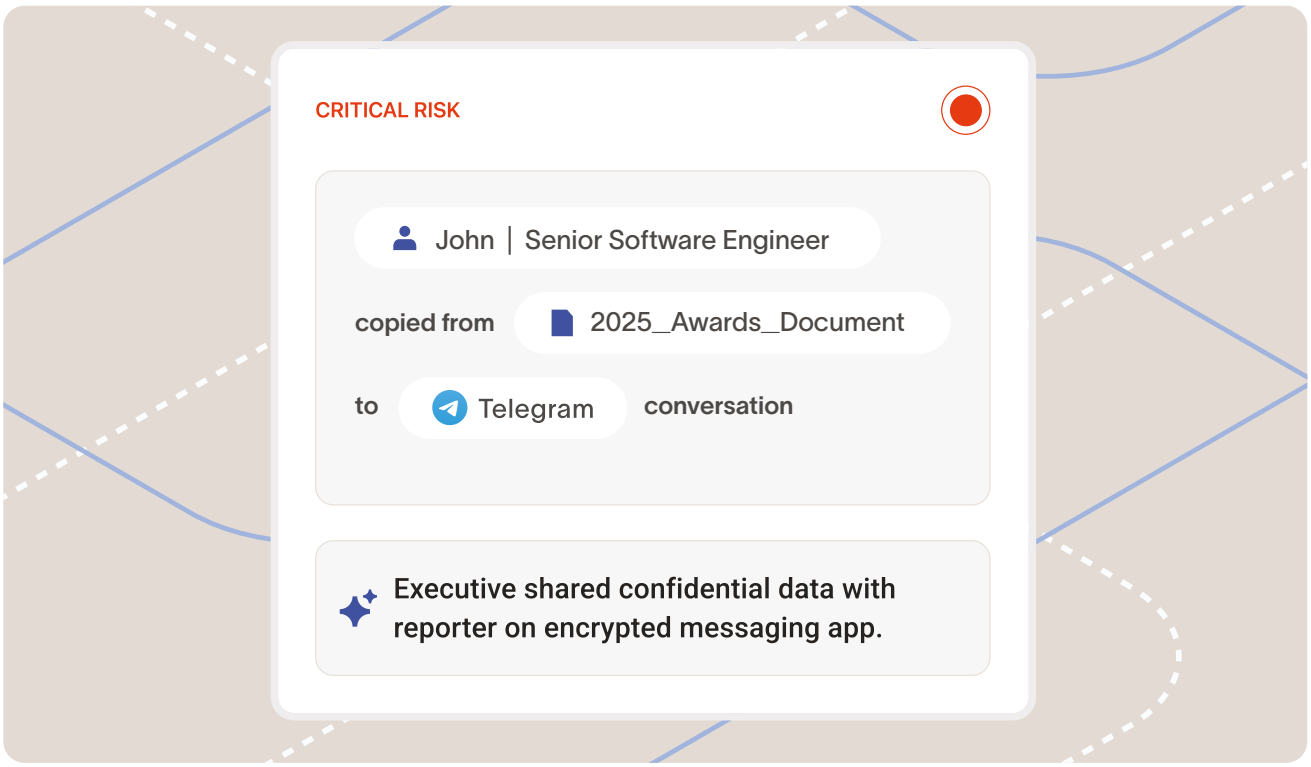
Cyberhaven extends its data lineage foundation with Linea AI, which brings intelligence and automation to insider risk detection and response.

Linea AI continuously analyzes data movement and user behavior to surface meaningful risk signals. It identifies patterns that indicate intent, such as staging data before transfer or accessing sensitive information outside normal workflows.

It also connects these signals into coherent narratives. Instead of presenting raw alerts, Linea AI explains what happened, how the data moved, and why it represents risk in plain, easy-to-understand language. This visualization allows analysts to move quickly from detection to decision.

In the context of departing employees, Linea AI is particularly effective at identifying the full sequence of events leading up to exfiltration. During employee transitions, Linea AI cuts through the noise to pinpoint high-risk data movement. It automatically surfaces early indicators, correlates them with later actions, and provides clear evidence for response.

This reduces investigation time and increases confidence, enabling security teams to intervene earlier — before sensitive data leaves the environment — especially in environments where insider activity can otherwise blend into normal operations.



Linea AI automatically traces and summarizes user and data behavior, creating easy to digest, actionable insights within minutes.

Detecting and Monitoring Departing Employees With Cyberhaven

Cyberhaven's insider risk management capabilities are built to identify and investigate users whose behavior indicates elevated risk, including those preparing to leave.

The platform provides visibility across:

- Endpoint activity, including file access, local storage, and removable media
- SaaS applications such as Microsoft 365 and Google Workspace
- Cloud and data platforms including storage systems, analytics environments, and code repositories
- Email and collaboration tools
- Custom and hybrid environments where sensitive data is frequently duplicated

This unified visibility enables security teams to follow data across environments without losing context.

Cyberhaven also delivers digestible metrics for potential data exfiltration. By prioritizing signals tied to sensitive data and correlating events across users, files, and systems, teams gain a clear understanding of risk without being overwhelmed by noise. Security teams can focus on actionable insights while maintaining maximum visibility across all environments.

Within the platform, teams can:

- **Identify users** exhibiting departure-related signals such as job search activity and unusual data access
- **Track insider risk** cohorts and monitor changes in behavior over time
- **Investigate activity** at the level of users, files, and datasets with full historical context
- **Build dashboards** that highlight active risks and emerging patterns

This approach aligns detection with how insider threats actually unfold, as a sequence of related actions rather than isolated events.

The Cyberhaven Difference

Departing employees represent one of the most consistent and preventable sources of data exfiltration. The challenge is not awareness, but visibility and context.

Organizations need to understand not just that data moved, but how and why it moved. They need to detect risk as it develops, while there is still time to act.

Cyberhaven delivers this through data lineage and AI-driven analysis. By connecting user behavior to data movement across every environment, security teams can identify departing employee risk early, investigate it with clarity, and prevent sensitive data from leaving the organization.

Request a demo