# Departing Employee Monitoring

SERVICE OVERVIEW

## Protect valuable corporate assets against data theft and loss when employees depart

### Protect IP

Forensically image employee devices to retain data and preserve evidence around user behavior, not just ESI.

### Repeatable process

Utilize machine learning technology to automatically assess intellectual property (IP) theft risk per device with a composite risk score.

### Actionable insights

Understand aggregate risk trends for employees across regional offices, departments, and seniority rank.

### Expert testimony

Prioritize investigations and rely on our testifying forensic experts to achieve defensible findings.

Litigation as a result of corporate data theft and loss continues to rise, especially in high-stakes competitive industries, driven in part by today's increased remote workforce and mobility, as well as ubiquitous and ever-expanding consumer technology, such as external storage media, cloud storage accounts, and bring-your-own-device (BYOD) policies. These developments make it easier than ever for employees to copy, transfer, and reuse their employers' valuable and confidential information (whether nefariously across shadow IT environments or unknowingly via cloud synchronization agents).

Savvy corporations utilize digital forensics to proactively address risks related to the departure of employees who may possess and plan to use proprietary and confidential information by transferring documents from a work computer to a personal email account or thumb drive. Digital forensic analysis and expert testimony are powerful tools to prove and defend against trade secret misappropriation cases. The ability to get to the facts, distill them into actionable intelligence, and retain control throughout discovery can make the difference between winning and losing.

## Challenges We Address

- **Leaking of confidential information** – According to a global survey from Symantec, "Half of employees who left or lost their jobs in the last 12 months kept confidential corporate data, and 40 percent plan to use it in their new jobs." Employers need concrete, actionable evidence to effectively and quickly identify and address these risks.
- **Moving technical target** – Today's forensic investigations into departed employees regularly involve new and novel devices, data sources, and artifacts that must be diagnosed and understood.

- **Recreating the wheel** – Companies lacking a standard process for addressing departing employees must re-scoping investigations, incurring unnecessary time and cost. This is especially true where different outside counsel and/or forensic providers are used across multiple matters.
- **Lack of strategic interpretation** – Absent a skilled examiner, it can be challenging to meaningfully decipher nuanced forensic evidence, such as metadata time stamps, application/OS artifacts, deleted information, web browsing history, and more, to strategically understand what the evidence does or does not show.

## Departing Employee Monitoring Services

Lighthouse addresses data exfiltration risk by designing and implementing a defensible and repeatable process to guard against company data being copied to external USB hard drives, forwarded as email attachments, or uploaded to personal cloud storage accounts.

Our services consists of the following:

- Forensic preservation and immediate device hardware redeployment to other employees
- A phased forensic analysis of key computer artifacts
- Standardized reporting with risk scores per device and on aggregate per office, region, employee title, and product line
- High-quality, compelling testimony
- Fixed pricing for a standard red flag report and hourly fees for deep-dive investigative support

## Benefits:

Lighthouse provides industry-leading expertise and access to the latest tools and techniques for building a defensible, repeatable process to analyze the digital forensic evidence related to departing employees.

We deliver quick turnarounds and more actionable results, which subsequently helps to improve budget accuracy. In addition, we assist with deconstructing opposing experts' reporting and opinions, and can help prepare for the expert's deposition and/or cross-examination.

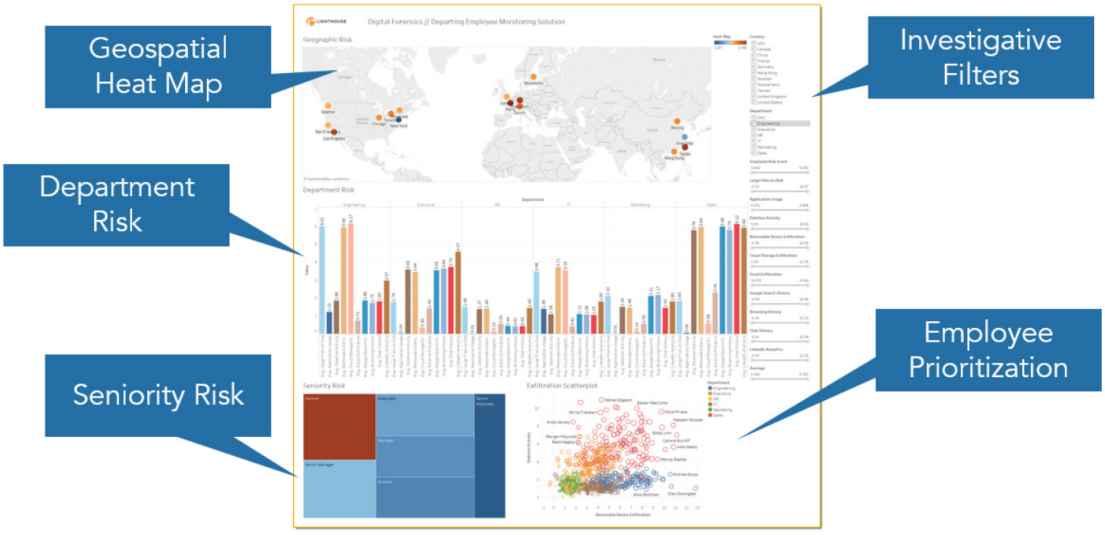
Our deep experience partnering with law firms and corporations enables us to design and implement defensible and repeatable processes to guard against the risk of departing employees who misappropriate confidential information. Benefits include:

- **Phased analysis** – We offer rolling insights based on priority/timing, first, an initial quick-turn, lower-cost layer for certain objective evidence (e.g., indicia a computer has been reformatted) and then a deeper, more comprehensive second layer as matters require.
- **Standardized reporting** – We empower stakeholders to more easily understand forensic results through repeatable reporting that summarizes key findings in a clear manner. Standardized reporting also drives effectiveness and efficiency where multiple outside counsel firms engage on different matters.

- **High-quality testimony** – We support our analysis and consulting results with high-quality written and oral testimony, based on years of experience.
- **Fixed pricing** – We also offer the ability to pay a flat rate for these types of investigations.

We offer a fully automated and objective scan of forensic images that outputs a composite risk score per device once completed. Results are presented on a visual interactive dashboard so clients can see the "big picture view" of their departing employee risk. Investigations can be prioritized accordingly, allowing for optimized resource deployment and budget accuracy.

## DEPARTING EMPLOYEE MONITORING SERVICES (DEMS)




# Summary

Partner with Lighthouse to build a bulletproof program that prevents the misappropriation of your company's data during employee departure or during a large-scale reduction-in-force (RIF) event.

Lighthouse helps protect your most valuable assets by taking proactive measures to keep data behind the corporate firewall, alerting you to the facts so you can mitigate the risk associated with departing employees, and remediating IP when it has propagated to unauthorized locations.

**Connect with us to see how Lighthouse can best support you.**

(206) 223–9690 | lighthouseglobal.com | info@lighthouseglobal.com



LIGHTHOUSE