SOLUTION OVERVIEW

Departing Employee Monitoring Solution

PROTECT VALUABLE CORPORATE ASSETS AGAINST DATA THEFT AND LOSS WHEN EMPLOYEES DEPART, AND MITIGATE RISK WHEN NEW EMPLOYEES ARE ONBOARDED

Protect IP

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

Repeatable Process

Employ Lighthouse's machine learning technology to automatically assess 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

Corporate data theft continues to rise, driven in part by today's increased workforce 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 employer's valuable confidential information (whether nefariously across shadow IT environments or unknowingly via cloud synchronization agents). Savvy corporations are using digital forensics to proactively address risks related to the onboarding and departure of employees who may possess and plan to use proprietary and confidential information by transferring documents from a personal email account or thumb drive to work computers. Digital forensic analysis and expert testimony are now one of the most 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 separate the successful from the unsuccessful.

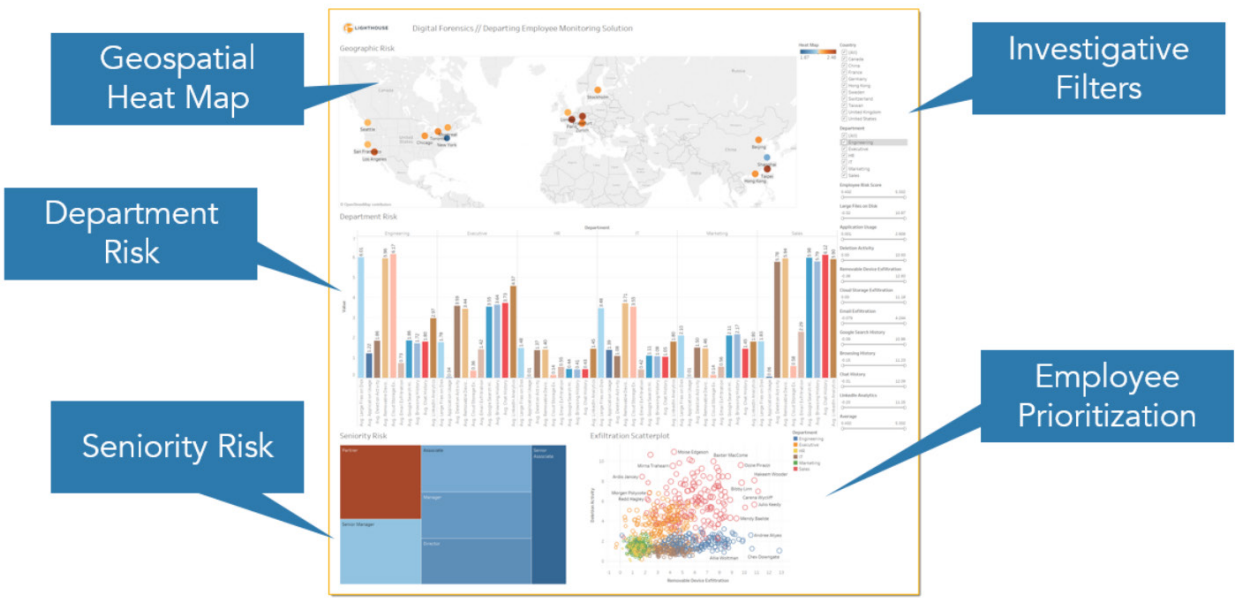
Challenges We Address

- 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, either through cease and desist measures, temporary restraining orders, and/or litigation.
- Risk of disputes with new hires — Despite advising new hires not to bring prior employer's information with them, companies continue to find themselves in the cross hairs of these disputes. Defending these cases (and remediating contested data) becomes much more complicated and expensive once a competitor's information makes it inside the enterprise, where it is then opened, modified, further disseminated, and saved.
- Moving technical target — Today's forensic investigations into departed/onboarded employees regularly involves new and novel devices, data sources, and artifacts that must be diagnosed and understood.
- Recreating the wheel — Companies lacking a standard process for addressing departed/onboarded employees must re-scope the investigation each time, 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.

Benefits We Provide

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 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 get a "big picture view" of their departing employee risk. Investigations can be prioritized accordingly, allowing for optimized resource deployment and budget accuracy.

Departing Employee Monitoring Solution (DEMS)



In addition, we assist with deconstructing opposing experts' reporting and opinions, and can help prepare for the expert's deposition and/or cross-examination.

Summary

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/onboarding employees, and remediating IP when it has propagated to unauthorized locations.

About Lighthouse

Lighthouse provides software and services to manage the increasingly complex landscape of enterprise data for compliance and legal teams. Lighthouse leads by developing proprietary technology that integrates with industry-leading third-party software, automating workflows, and creating an easy-to-use, end-to-end platform. Lighthouse also delivers unique proprietary applications and advisory services that are highly valuable for large, complex matters, and a new SaaS platform designed for in-house teams. Whether reacting to incidents like litigation or governmental investigations, or designing programs to proactively minimize the potential for future incidents, Lighthouse partners with multinational industry leaders, top global law firms, and the world's leading software provider as a channel partner.

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

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

LIGHTHOUSE