Onboarding Employee Monitoring

SERVICE OVERVIEW

Mitigate risk when new employees are onboarded

Proactively protect

Utilize machine learning technology to automatically assess infiltration risk per device with a composite risk score.

Repeatable process

Design a repeatable and defensible process to govern data use and handling at onboarding.

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.

If you've ever received a temporary restraining order (TRO) or preliminary injunction (PI) for a new employee due to their behavior as they left their previous employer, then you're well aware of the pain involved with tracking down and remediating documents originating from the former employer. It's critical for companies to have a plan to detect and prevent proprietary and confidential data belonging to a competitor from infiltrating your IT network through new hires.

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.
- **Risk of disputes with new hires** – Despite advising new hires not to bring prior employers' 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 re-saved.
- **Moving technical target** – Today's forensic investigations into onboarding 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 onboarding 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 program to analyze the digital forensic evidence related to onboarding 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.

Lighthouse helps companies proactively scan bring-your-own-device (BYOD) mobile devices, external USB hard drives, and personal cloud accounts belonging to new hires for data that might be considered intellectual property (IP) of another company. Documents may have been procured by new hires in an unauthorized and unlawful way, and the company can be held accountable for the material's reuse if appropriate measures aren't taken early in the onboarding process. It is not advisable to turn a blind eye toward data infiltration, especially when it might be considered a competitive benefit, because accusations of IP theft can extend from the new hire to the hiring company itself, and the costs of IP theft litigation can outweigh the perceived gain.

Summary

Lighthouse helps organizations take proactive measures to keep data behind the corporate firewall by arming organizations with the facts to mitigate the risk associated with onboarding employees, and to remediate 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