CLEARFORCE Case Study

Preventing Insider Threat Helped Global Market Leader Halt Data Transgressions and Theft from Trusted Employees

Introduction

Protecting against insider threats is difficult for employers. No matter how stringent their internal security mechanisms are, vetting and hiring credible, trustworthy employees is a challenge. Internal, siloed security measures alone cannot entirely prevent rogue employees from acting against their interests. Insider threat is especially important to address in industries that deal with sensitive, confidential, and secret information that can compromise the company and/or even the U.S. government.

Still, many top-performing companies rely on inefficient or old-fashioned security measures, and in the case of one global service provider, this reliance led to an outcome they were trying to avoid. Prior to partnering with ClearForce, the company's employee vetting process consisted of an initial point-in-time background check and, for cleared employees, a U.S. government-sanctioned security clearance at the start of employment – with no standardized continuous vetting of their employees with or without a clearance. In effect, they assumed the individuals they initially vetted would self-report if they no longer met the terms of employment or required compliance to hold a U.S. government clearance. This clearance process costs the firm between $60,000-$100,000 per employee and typically takes an average of three to four months to complete.

The sheer financial and time investment of this hiring process is one major reason why it is vital for many organizations to apply thorough and comprehensible employee monitoring programs that continue beyond the date of hire. Discovering an employee who has become vulnerable to committing crime within the organization, susceptible to being exploited by outside bad actors or simply distracted because of compounding events at any time during their employment helps mitigate losses of money, proprietary data, and other key resources. It also reduces the risk of negative or destructive behaviors within the company.

This case study examines how one company's use of ClearForce's Resolve™ monitoring platform helped identify a trusted employee's long-standing theft and legally remove the employee before it – and possibly the U.S. government – suffered any further damage.

The Case

A few years ago, a global services company paid for a respected senior attorney to receive a U.S. government-sanctioned security clearance that granted him access to classified information, including top-secret government data. The firm then elevated the attorney to a higher position of trust for company- and U.S.-government classified information after the costly and time-consuming clearance process was adjudicated.

The attorney passed an initial organizational background check and was entrusted with not only the government data – which could have jeopardized U.S. governmental missions and the company itself if released – but also key confidential company information and the intellectual property of its customers.

Coworkers trusted and befriended the attorney, not suspecting any illegal or damaging activity. But over time, he continuously stole realms of data. The lawyer understood the firm's limited security measures, so he was easily able to circumvent them.

The firm did not initially have a continuous monitoring program in place, but then contracted with ClearForce to pilot an initiative seeking broader risk reduction for their cleared workforce. Because the firm worked with such sensitive information, management decided it needed to upgrade security to a fully compliant tool that protects privacy, removes bias, supports transparency and – most importantly – aligns with the known high-risk threats being monitored by the U.S. government.

Meanwhile the lawyer was enrolled in the government insider threat program (per U.S. government clearance policy), but government officials and his work colleagues, including leadership, remained unaware not only of his transgressions – but also thefts by three other employees. The firm had lacked an integrated employee monitoring platform designed to detect transgressions early.

Then the company purchased ClearForce to handle its monitoring with the Resolve™ platform, quickly integrating it within its human resources, security, legal, and compliance departments. Among other capabilities, the program sends push alerts to organizational leaders when employees have violated selected organizational policies and committed crimes. Additionally, ClearForce enabled the organization to set alert triggers below those of the U.S. government threshold. This allowed the company to pick up on behaviors and patterns before the government. This integrated system of company policy and government risk thresholds enabled the company to discover risk sooner.

One day the lawyer was arrested and charged with driving under the influence (DUI) during his personal time. Because alcohol misuse requires self-reporting due to his clearance and company policy, Resolve™ automatically identified the arrest and alerted management within hours. The platform also found a misdemeanor arrest for theft and fraud outside the workplace on his record, notifying the company of that as well.

Following Resolve™ protocol, management began investigating the DUI. During their review, leaders found that the lawyer and the other culpable employees were stealing from the company – due in large part to sharing critical information across departments while properly applying Resolve™ "tip and lead" data. They elevated the lawyer's case to a higher risk level, where senior leaders soon assessed the situation and fired the attorney and several other employees.

Because the Resolve™ protocol also accounts for legal challenges and compliance regulations, the firm's leaders uncovered the thefts and terminated the lawyer without any fear of recourse. They then notified the government before governmental systems even detected the DUI arrest.

Key Takeaways

While the company was compromised by the attorney's thievery, its investigation and termination likely saved millions of dollars in resources and avoidance of government inquiry. This employee maintained his security clearance after he was arrested for DUI because he did not report the arrest as required and manifested no signs of slowing down his internal crimes before being caught.

Without a sophisticated and integrated monitoring platform, it is likely the attorney would have continued to filch from the firm for at least a bit longer. Only when Resolve™ tipped off management regarding the arrest did the firm have a valid reason to investigate him and uncover the crimes.

ClearForce's Resolve™ is an advanced example of an effective monitoring platform, one that clients rely on for best-in-class insider risk deterrence, detection, and mitigation.

In a dynamic environment of evolving threats, organizations must not only guard against increasingly savvy and intelligent cyberattacks, but also understand how to synchronize technology, company policies, and best practices into an integrated human capital risk solution. By augmenting a behavioral monitoring system that tracks legally binding eligibility requirements in real time, defense companies can bolster their insider threat countermeasures to stay ahead of reporting requirements and ensure all staff follow

clearance guidelines. Taking these steps leads to a smoother adjudication process, higher staff retention, and preserving organizational and employee integrity. No matter how inside the threat lies.