

Global Chemical Company Uses ObserveIT to Gain Visibility into Insider Threats

Case Study Summary

This global specialty chemical company recognized the importance of building a comprehensive insider threat program. They set out with the goal of increasing visibility into user behavior, while balancing the key priority of privacy. With ObserveIT, the team was able to dramatically improve visibility, increase efficiency of investigations, and exonerate innocent employees, all while preserving user privacy.

Their Challenges

This company seeks to prevent the intentional, accidental, and otherwise improper use of their technology systems. Previously, they lacked the necessary visibility into user activity to know when insider threat incidents took place, investigate them, and take appropriate action.

The Solution: ObserveIT

ObserveIT provides deep visibility into user behavior, without infringing upon privacy. The platform enables detailed investigations into potential insider threat incidents, including fraud and misuse, with the full context needed to understand what really happened.

Positive Business Outcomes

The team was able to achieve a number of key positive business outcomes, including:

- **Improved Efficiency:** ObserveIT enables more efficient investigations, as compared to forensic review and the use of logs.
- **No More Guesswork:** There's no need to guess what happened during a potential insider threat incident; it is immediately clear upon investigation.
- **Proactive Investigations:** Now, the team is able to take a more proactive approach to insider threat investigations, vs. relying on reactive forensics.
- **Identification of Specific Threat Vectors:** The team is now hyper-aware of activity around common threat vectors like USB device usage and exfiltration to cloud services.
- **Privacy Maintained:** The company can restrict investigations to likely infractions, and even uses ObserveIT to exonerate innocent employees.



ABOUT THE COMPANY

- Global specialty chemical company
- American Fortune 500
- 10,000+ employees

“We started out with some major blind spots around insider threat. With ObserveIT, we have dramatically improved visibility into user activity on our systems.”

~ IT Security Architect