When we judge certain user activity to be especially risky to our cybersecurity, ObserveIT gives us the ability to write our own rules to protect against it. If someone then engages in malicious behaviour, we are immediately alerted, in real time, that they're doing something against policy — instead of finding out after the fact, when it's detected only because the damage has already been done. That's the real power of ObserveIT.”

— Alex Money, Head of Information Security & Enterprise Architecture, Besso Insurance Group Ltd
The Results

Besso was able to tailor ObserveIT’s rules and alerts to meet its particular business needs and make the most efficient use of the 350+ out-of-the-box indicators of insider threat ObserveIT provides.

By categorizing specific user activity to correspond with low, medium and high alerts, Besso was able to manage the volume of alerts it needed to focus on. The security team were then able to prioritize the investigations and responses, recording activity only when it was high priority and, in doing so, this helped to reduce its data storage requirements to 1 gigabit. This approach also meant the security team at Besso could take the right action as and when it was needed.

Shortly after ObserveIT was implemented, Besso was alerted to several cases of users logging in and using prohibited applications. The ability to integrate ObserveIT into their Alien Vault SIEM platform, ensured that Besso had continuous, around the clock visibility into user activity allowing them to quickly identify and manage insider threat incidents. This visibility removes uncertainty as to the ‘who, what, when, where, why and how’ of the policies broken, not only with respect to employees but also third-party vendors.

Likewise, ObserveIT has helped Besso simplify their auditing process, by enabling the organisation to generate reports that provide summary information with greater clarity and context. As a result, Besso’s executive team and board of directors are kept abreast of the company’s cybersecurity program and feel confident data protection is being handled proactively and comprehensively.

As the insurance industry becomes increasingly reliant on more and more data to assess risk, it’s becoming even more vital to confront the key threats to data security — and insider threat is clearly one of them. Whether it’s accidental or intentional, if someone breaches your system and data gets out in the world, there are serious consequences for both the individuals affected and the business. You need to know what’s happening in your organization 24/7, and technology that allows you to monitor and control user activity around the clock puts you in the best position to stop data leaving before it’s too late.”

~ Alex Money, Head of Information Security & Enterprise Architecture, Besso Insurance Group Ltd