observe IT
a division of Proofpoint

CUSTOMER STORY

Besso Insurance Group Uses ObserveIT to Protect Data Assets

Company Gains Around-the-Clock Visibility into All User Activity to Detect, Manage, Investigate and Resolve Insider Threat Incidents

BESSO

THE CHALLENGE

- Protect sensitive and confidential customer data
- Monitor user activity and alert security teams to suspicious or out-of-policy behavior
- Investigate and evaluate the context and intent around a potential breach
- Manage volume of alerts and focus on priorities

THE SOLUTION

- ObserveIT Insider Threat Management Platform

THE RESULTS

- Achieved customized protection of data assets
- Created comprehensive visibility into day-to-day user activity
- Increased speed and precision of investigations
- Reduced time spent on security, with a core IT team handling cybersecurity globally

The Company

Besso offers insurance brokering services worldwide, across a number of divisions including Property, Casualty, International, Marine, Aviation, Professional and Financial Risks and Reinsurance. The firm covers global markets from its headquarters in London, with additional offices in Turkey, Brazil and Hong Kong. Besso also provides risk transfer services for reinsurance and capital markets, and is particularly noted for handling complex and unusual risks.

The Challenge

As an insurance company, Besso evaluates risk on a daily basis and, similar to the financial and legal sectors, handles a great deal of sensitive client information. Given the highly confidential nature of the data it processes, Besso was committed to protecting these valuable assets and set out to find a security solution that could be tailored to its specific needs, enabling it to take a proactive, rather than reactive, approach to data protection.

“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,” said Alex Money, head of information security and enterprise architecture at Besso.

Aware of the risks and far-reaching consequences of the insider threat, Besso required full visibility into its everyday users' activities and a solution that alerted security teams to suspicious or out-of-policy behaviour in real-time. Crucially, they needed a solution that enabled them to fully investigate and evaluate the context and intent around a potential breach and, by doing so, illustrate to senior management that robust and proactive steps were being taken to protect the business and its customers' data.

"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," said Alex Money, head of information security & enterprise architecture, Besso Insurance Group Ltd.

> "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 Solution

Fortem Information Technology introduced Besso to ObserveIT. Working in partnership, Besso deployed ObserveIT across its organization worldwide, and Fortem IT coordinated the relationship to ensure a seamless implementation.

"The IT security team can now rely on ObserveIT to provide full visibility into user activity 24/7, and no longer has to waste time reviewing copious amounts of logs in search of a potential problem or reverse engineering after something has already gone awry," said Tunji Oyedele, director of sales, Fortem Information Technology. "When there's an actual issue that requires further investigation, the team is alerted and immediately has all the details and context they need at their fingertips."

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 400+ 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 one 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 AlienVault 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.

LEARN MORE

For more information, visit **proofpoint.com**.

observe IT
a division of Proofpoint