observe it

Leading Independent Wealth Management Firm Implements ObserveIT to Protect its Clients from the Inside Out

Case Study Summary

The financial services industry faces a multitude of data security threats. Due to the sensitive and complex data they handle, the risks of cybercrime, corporate and state-sponsored espionage and monetary fraud are significant.

In 2014, Portcullis Group recognised that with the increasing sophistication of cybercrime it needed to strengthen its cyber security program with measures that both protected clients' valuable data and tackled the insider threat. Oyster Security, a subsidiary of the Portcullis Group of companies was then established to provide cybersecurity governance and technology risk management services across the board.

Challenge

Given the nature of services provided by Portcullis, it receives confidential and sensitive information about clients and/or their businesses, which are not normally publicly available. This increases their risk of experiencing insider threats.

Valuable Data at Risk

With much of their data stored digitally, Portcullis must ensure that the valuable and confidential data of all its customers is protected from risk at all times — whether from targeted cyber attacks to malicious or accidental compromise by employees or third-parties. Its broad customer base is made up of successful entrepreneurs, aspiring start-ups, private bankers, investment managers and financial advisors, as well as family offices.

A Lean Organisation

Oyster Security's ten-person IT department is tasked with a wide variety of responsibilities from technology implementation and management to data security and maintaining compliance and corporate governance. With a varied and growing customer base, the small, specialised team must uphold data security best practice.

ABOUT THE COMPANY

One of the largest Asian Independent Wealth Management Firms, Portcullis has been respected by its clients for its sterling reputation for integrity and professionalism since opening its doors in 1984.

Today Portcullis has offices in eight jurisdictions offering trustee, fund management, fund administration, corporate secretarial and administration services. Its more than 300 employees include lawyers, accountants, fiduciaries, fund managers and administrators to support its broad customer base of private bankers, investment managers and financial advisors. Its eight offices are located in Singapore, Hong Kong, Taiwan, New Zealand, Samoa and the Cook Islands.

> **" Insiders are the weakest link — ObserveIT helps us to address and manage this risk"**
> *~ Vincent Ang, Director of IT & Security at Oyster Security Pte Ltd.*

Compliance Requirements

Regulation and compliance are a key requirement in the financial services industry. This requires maintaining customer data confidentiality through secure data practices, detailed audit trails and breach notifications. Adhering to mandatory regulations and data protection rules can be difficult to follow without the robust tools to detect even the earliest indicators of an insider threat.

> **❝ We chose ObserveIT because it is easy to configure, intuitive to use and the comprehensive alert rules with playback enables us to stream and complete incident investigations faster"**
>
> *~ Vincent Ang, Director of IT & Security at Oyster Security Pte Ltd.*

The Solution: ObserveIT

ObserveIT provides comprehensive visibility into user and data activities, enabling the IT team at Oyster Security to detect and prevent attacks that could otherwise put its client's data in jeopardy.

Safeguarding Valuable Data

ObserveIT enables the IT team to monitor risky user activity across privileged and highly technical users as well as third parties that can open organisations up to potential vulnerabilities.

- Monitor third party vendors and contractors with system access
- Detection of high-risk users attempting to exfiltrate data
- Investigations with context enable faster incident response
- Use of Activity Replay as a deterrence/prevention tool

Running a Lean and Highly Automated Security Operation

With its powerful platform, ObserveIT empowers the IT team to monitor activities in real-time and verify any risky behaviours before they happen.

- Automated monitoring to quickly verify anomalous or risky behaviour
- Easy-to-use platform to give visibility to cross functional teams
- Reliable solution that helps IT deliver an effective cyber security program

Easily Meet Compliance and Governance

ObserveIT provides regulators and senior management with the assurance that Portcullis are meeting a range of compliance and governance regulations, including:

- Preserving data confidentiality
- Implementing protective measures
- Producing audit trails
- Managing insider threats

The Results

The primary benefit that Portcullis receives from ObserveIT is the ability to detect insider threats that would otherwise go unnoticed empowering the team to rapidly investigate and respond so incidents can be stopped in the earliest stages.

The IT team at Oyster Security benefit from the powerful ObserveIT platform which is easy to configure with its lightweight, intuitive-to-use user mode agent and the comprehensive alert rules with playback enabling them to streamline incident investigations.

With ObserveIT, Portcullis and Oyster Security can be confident in their ability to identify and prevent insider threats, streamline investigations, and maintain compliance and governance regulations — thereby serving as a trusted advisor protecting both their business and that of their valued customers.