CASE STUDY

A Leading Multi-Asset Alternative Investment Firm

MONITORING USERS

observe it

www.observeit.com

CASE STUDY

Use Case

The security team of a leading multi-asset alternative investment firm sought a solution that would provide visibility into user activity. Their focus was on privileged users and high-risk business users (including those who had given their two-week notice) and their interactions with sensitive data residing on corporate network shares, web applications and repositories.

Customer Needs

The customer required visibility into print jobs, copy/paste operations, and USB insertions in order to:

- Identify early warning signs and detect data exfiltration attempts by users
- Establish daily reporting on which users have access to what content for sensitive IP
- Gain visibility into user actions before, during and after incidents for use by key compliance teams

Current Solution

The primary tool for addressing insider threat was Digital Guardian, a Data Loss Prevention (DLP) solution.

Challenges

Performance
Browser plug-ins resulted in Chrome and Firefox crashes which was the most frequent feedback received from end users.

Heavy on the endpoint
The content scanning engine caused slowness on user machines.

Lack of visibility
DLP only provided an inventory of the files that were removed using a USB. The customer required visibility into user activity prior to and following an incident for their compliance team.

Company
Leading Multi-Asset Alternative Investment Firm

Industry
Financial Services

Size
950+ Employees

observe it
observeit.com/tryitnow

Why ObserveIT

As a large financial services provider, it is important to know what the organization's privileged users are doing at all times both to guarantee security and to meet compliance regulations. With thousands of sessions to track, this can quickly become a major headache.

ObserveIT's unique, user-centric approach providing customers the ability to detect risky behavior, streamline the investigation process, and prevent data loss were some of the reasons ObserveIT was selected.

Visibility

ObserveIT provides a comprehensive context of user and data activity including user endpoint visibility, user login, user network access path, file activity (copy, rename, delete, move), file names, file sizes, and more.

Detection

ObserveIT's Insider Threat Library includes 200+ pre-configured, customizable user scenarios that triggered alerts to the security analyst when a user attempts to access data on the network shares providing financial services customers unmatched visibility into attempts to exfiltrate data.

Investigation

ObserveIT streamlines the investigation process by collecting irrefutable evidence via session recordings and rich metadata that can be shared with the incident response team to expedite their investigation of the incident.

Accuracy

ObserveIT's alerts are triggered based on the context of user behavior resulting in low false positives and ensuring the security and incident response teams focus their efforts on the truly high risk behavior.

> "ObserveIT has enabled me to tell a better security story. I no longer have to say 'I don't know.'"
>
> Chief Information Security Officer

observe it
observeit.com/tryitnow

RESULTS

- ObserveIT resolved the performance issues associated with Digital Guardian, the current DLP, reducing the cost of maintenance and the volume of help desk tickets, and improving user satisfaction and productivity
- The time to generate audit reports by the security operations team was reduced by 20% - 30%; the team achieved greater incident clarity and context
- User event incident response times were reduced from an average of 5 – 10 hours to less than 1 hour
- Enhanced visibility and reporting has allowed HR and internal audit teams to streamline their business processes for handling user terminations
- Insider threat prevention cost was reduced as the customer was able to replace a labor-intensive and costly DLP solution

observe it
observeit.com/tryitnow