Financial Services Solution Guide

Protect against data theft, fraud and privilege abuse from insider threats

THE PROBLEM

Financial services saw one of the highest cost per incident of insider threat, at $11.32 million, on average, according to the 2018 Ponemon Institute study.

Financial services security teams protect valuable assets that are more digitally accessible by a more distributed and agile workforce than ever. In today's world software developers, traders and executives can, accidentally or maliciously, leak data from the cloud, core banking mainframes, trading and processing platforms and employee endpoints.

Traditional Data Loss Prevention (DLP) tools are failing to detect, investigate and stop this new breed of insider threats causing data theft, fraud and privilege abuse.

WHAT IS AN INSIDER THREAT?

Someone inside the organization, such as an employee, contractor or vendor, who misuses authorized access to sensitive systems or data, either maliciously or accidentally, resulting in a negative outcome

DATA EXFILTRATION

Print, USB, Cloud Applications, Email

UNAUTHORIZED ACTIVITY

Bypassing security controls, Backdoor creation, Running malicious software

UNAUTHORIZED ACCESS

Remote access, Sharing accounts & passwords, privileged escalation

ACCIDENTAL ACTIONS

Unapproved application use, Configuration mistakes, Unauthorized web browsing

ObserveIT has earned the trust of more than 500 Banking and Financial Services organizations worldwide, including:

5 of the top 10 Financial Services organizations

3 of the top 5 banking institutions

2 of the top 5 Asset Management groups

Financial Services Solution Guide

Protect against data theft, fraud and privilege abuse from insider threats

OBSERVEIT vs INSIDER THREATS

Empower you to detect, investigate, and stop insider threats causing data theft, fraud and privilege abuse. Whether users are working on your core trading algorithms, processing client credit data, or accessing high net worth client PII, leading security teams trust our intelligence to safeguard core intellectual property, sensitive data and users.

Detect Data Theft, Fraud & Privilege Abuse

Rapidly detect potentially risky user actions and data movement, captured on UNIX/Linux, Windows, and Mac endpoints for employees and third-party contractors.

Investigate Incidents

When a potential insider threat incident is detected, you need answers fast. Don't judge an employee until the verdict is in with ObserveIT.

Prevent Insider Threats

Block out-of-policy activity and coach users in real-time as they are about to breach organizational guidelines.

COMMON RISKS IN FINANCIAL SERVICES

- Data theft, fraud and privilege abuse by insiders
- Data privacy for organizational and client data
- Mergers, acquisitions and significant reorganizations

KEY PRODUCT CAPABILITIES:

Insider Threat Detection Engine

More than 300 indicators of risk modeled on years of US-CERT and customer research. Financial services customers rely on our real-time alerts for data exfiltration such as from Office 365 or corporate network; unauthorized activity such as posting code on PasteBin; accidental actions such as modifying a root cron job.

Cybersecurity Incident Recreation

Insider threat investigations are fundamentally different – you need concrete, easy-to-understand metadata & visual evidence tying together multiple user actions to determine intent.

File Activity Monitoring

Track data across the file lifecycle, with the popularity of cloud software, from file creation, import and download to detection of potential data exfiltration.

Time to value & minimal endpoint impact

Get value immediately with silent installs, no reboot upgrades & 1% of endpoint CPU usage. Save yourself months of setup required with other tools.

Integration into existing cybersecurity tools

Correlate ObserveIT intelligence with your network, physical access and identity data through numerous integrations.

Data Privacy for organizational and client data

ObserveIT designed technical controls around lawful collection, usage and disposal of data. This includes data and user anonymization, intelligent monitoring and comprehensive self-auditing capabilities.