Silo
By Authentic8

CASE STUDY
FINANCIAL SERVICES

Case Study: Global Top Ten Financial Services Firm

Authentic8 Helps Identify Threats and Fraudsters Online

Banks, insurance companies, and financial service firms today use many different methods to gather intelligence from the open, deep, and dark web. For the financial industry, open source intelligence is a valuable resource to keep businesses up to date on existing, evolving and future threats, past breaches, or hidden caches of compromised, fraud-related data.

Introduction

A top ten financial institution with teams of investigators focused on different challenges, The firm relies on the Authentic8 Silo for Research (Toolbox) solution for their cyber-threat intelligence, financial fraud, and anti-money laundering investigations.

Thomas B. is tasked with gathering cyber-threat research from the far corners of the web. The information gathered helps to protect The firm from both targeted and indiscriminate attacks by malware and bad actors alike.

The Challenge

Prior to deploying Silo for Research, The firm was using a DIY approach to cyber-threat investigations by combining consumer browsers, plug-ins, and VPN solutions to perform their threat hunting activities. “We found that our existing perimeter security solutions were blocking where we needed to go on the web. There was no way to visit them without exposing the rest of the network to potentially malicious threats.” Thomas B. said. “In addition, we were using third-party vendors and business partners to outsource malware analysis, increasing costs and exposing sensitive information that we would prefer to keep in-house.”

One of the main business drivers for adopting the Authentic8 solution was maintaining the anonymity of online investigators. “Visiting a web page reveals a lot about the visitor, including the visitor’s IP address. That IP address can be traced back to the company and jeopardize future intelligence-gathering efforts, so maintaining anonymity is a top priority,” said Thomas B.

THE STORY

Previously used a high cost, resource intensive DIY investigation platform

DIY solution lacked anonymity, prone to tracking and compromise

Needed a cost effective, cyber-threat research solution to gather intelligence of targeted threats

Silo was an all-in-one solution to meet researcher requirements

Maintains anonymity and security of online investigations

Secure team storage for evidence sharing and collaboration

Another top concern for the organization was infection and compromise from the very same threats they were hunting for. “Cyber-threat investigations — without the proper safeguards and precautions — can significantly increase network risk,” Thomas B. continued. “We needed a solution that worked in our environment and provided the logical separation to mitigate just about any malware threat, and Silo’s cloud isolation provides that capability.”

The Implementation

In large organizations, getting approvals to implement a new application can sometimes be harder than implementing the solution itself. “As with any new solution, we had a number of internal departments to coordinate with, educate, and gain approval from, before the roll-out of the Silo Web Isolation Platform,” Thomas B. recalled. “Luckily, the solution was very straightforward to deploy across four to five different groups internally, and it is now utilized by multiple teams both inside and outside the security organization.”

Working in the highly regulated financial services industry, The firm is required to provide proof of compliance to both internal and external auditors. With integration into Splunk, The firm set up a log pipeline to capture all Silo for Research activity, storing the logs within a central repository to meet those compliance requirements.

“A number of key features in Silo for Research have been instrumental in helping us understand the threats that pose the most risk to the enterprise,” Thomas B. stated. “With thousands of alerts per month, time to intelligence is critical for making a determination and implementing an effective response. Silo is an all-in-one solution that helps us do that faster and more easily than our previous DIY solution.”

> A number of key features in Silo for Research have been instrumental in helping us understand the threats that pose the most risk to the enterprise.

The Result

Since the initial deployment, Authentic8 has been instrumental in helping The firm meet their goals. “Now with Silo for Research deployed, we can work around the IT restrictions and can go anywhere we need to go on the internet. We do all of the threat analysis in-house now and don’t have to outsource to anyone.

That reduces our cost, but more importantly it allows us to make a faster determination of risk to immediately verify the threat mitigation strategies we have in place," Thomas B. recollected. With DIY investigation solutions, bad actors and fraudsters are able to profile a researcher's web visits based on their resources, such as AWS S3 buckets used for storing evidence during collection. Non-attributable platforms such as Silo for Research can use multiple egress locations to protect the identity of The firm, enable encrypted storage in private cloud-based repositories, and keep counterintelligence efforts in the dark.

> **Silo has changed the way we approach cyber-threat hunting, fraud research, and other online investigations.**

"Silo has changed the way we approach cyber-threat hunting, fraud research, and other online investigations," concluded Thomas B. "The cloud-based management and policy framework allows control over Silos's features and functionality, while the isolation platform as a whole keeps our investigators safe and anonymous online."

Authentic8 enables anyone, anywhere, on any device to experience the web without risk. The Silo Web Isolation Platform by Authentic8 separates the things you care about like apps, data and devices, from the things you cannot trust like public websites, external users and unmanaged devices. Silo executes all web code in a secure, isolated environment that is managed by policy, to provide protection and oversight.

Today, the world's most at-risk organizations rely on Silo to deliver trust where it cannot be guaranteed.
Try Silo now: www.authentic8.com

Redwood City
333 Twin Dolphin Dr,
Suite 112
Redwood City, CA 94065

San Francisco
555 California St,
Suite 3360
San Francisco, CA 94104

Indianapolis
8888 Keystone Crossing,
Suite 675
Indianapolis, IN 46240

Washington, D.C.
1010 Vermont Ave NW,
Suite 816
Washington, DC 20005