

Enterprise Financial Services Institution

Multinational financial services institution chooses Forcepoint UEBA to prevent data exfiltration through sophisticated content analysis



Industry

Financial Services

Country

United States

Issue

Protect sensitive data and reduce people-based vulnerabilities

Product

Forcepoint UEBA

► Overview

This Enterprise Financial Services Institution, a multinational organization headquartered in the U.S., is one of the largest of its kind in the country. One of the top 10 largest banks in the world, it serves individual consumers, small and middle-market businesses, and large corporations with a full range of banking, investing, asset management, and other financial and risk management products and services. The institution is a global leader in wealth management, corporate and investment banking, and trading across a broad range of asset classes.

► Challenge

Protecting the company and its customers from malicious insiders ► Financial institutions house some of the most sensitive data in the world and are required to meet strict data security compliance requirements. Protecting those institutions from data breach is critical, and a vast number of today's most damaging breaches are rooted in people-based vulnerabilities.

Competitors in the financial services market had already fallen victim to insider breaches, which were widely publicized and had significant negative impact on those institutions' brand and reputation. This was just one of the factors that prompted this institution to take further steps to ensure protection of their customers, assets, and brand and reputation.



Get in touch with us.

Learn how Forcepoint can protect you. Contact us at forcepoint.com/contact.

Forcepoint UEBA outperformed its competitive vendors by demonstrating its sophisticated ability to both ingest log data from the institution's primary big data tools as well as unstructured data from within email and chat communication logs.

The Financial Services Institution's commitment to data security and compliance led to the search for a solution that would bolster its defenses against insider threats.

With a large employee base as well as sensitive customer data and intellectual property, the institution needed a more robust and holistic insider threat program with a faster, more effective path to uncovering vulnerabilities among a 150,000 employee workforce.

► Solution

Sophisticated content analysis capabilities with Forcepoint UEBA ► Though the Financial Services Institution had a number of cybersecurity measures in place, it did not have a user and entity behavior analytics (UEBA) product. One priority for the institution was to select a product that could ingest data from other data repositories, including Splunk and Cloudera, and analyze it for specific behaviors. The institution also wanted to be able to analyze the content of email and chat communication streams.

The institution chose to move forward with Forcepoint UEBA largely based on its sophisticated capabilities in content analysis. Forcepoint met with the institution's security team for two proofs of concept (POCs), demonstrating sophisticated capabilities in content analysis. These POCs proved Forcepoint's ability to ingest and examine content of email and chat logs as well as traditional security data sources.

With Forcepoint UEBA, the Financial Services Institution can implement an employee behavior-centric solution that will help them discover non-compliant behaviors, suspicious privileged user activity, and negative workplace conduct in network logs and electronic communications.

Where many competitive vendors log only metadata—who talked to whom and when—Forcepoint UEBA can perform a thorough analysis of unstructured data within email messages, chats, and web searches. The institution's main use case for this was identification of malicious users to prevent data exfiltration or deletion and unauthorized use of user credentials.

Going one step further, the institution wanted to use Forcepoint UEBA capabilities to analyze sentiment within communication streams. It aimed to reduce negative impacts by examining chat and email logs, discovering disgruntled employees at risk of leaving the company, exfiltrating proprietary information, or even harassing fellow colleagues or becoming violent. On the positive side, however, it also wanted to identify higher producing employees and those who receive praise from their colleagues.

This Enterprise Financial Services Institution is currently implementing Forcepoint UEBA with 150,000 users.

Summary

With Forcepoint UEBA, the Financial Services Institution ingests and analyzes data from other data repositories and analyzes the unstructured content of email and chat communications—in addition to metadata—to understand sentiment within communication streams.