Midwest Bank Increases Protection to Gain Greater Visibility and Control

A locally owned, midwestern bank provides both personal and business banking services through its 7 locations. In operation since 1885, the bank has a vested interest in keeping both its organization and its members safe from the increasing volume of cyber threats. While faced with the same cybersecurity issues and regulatory compliance issues as larger financial institutions, the bank must protect its network and members while ensuring auditing and compliance with fewer resources—specifically, a 3-person IT team.

Upon learning about Threater, the bank CEO suggested the IT team deploy the Threater platform in front of the existing firewall, as part of an additional layer of protection for their defense-in-depth security strategy. With Enforce, he felt that he would be able to leverage Threater's 30M+ out-of-box threat indicators to prevent known bad actors from targeting them by stopping them before they hit the bank's firewall.

Benefits

- **Increased protection from cyber threats and third-party risks**
- **Less malicious traffic passing through firewalls**
- **Simplified ingestion of third-party FS- ISAC feeds**
- **Reduction in the time spent managing security devices**

Challenge

- Protect the bank and its customers from the massive amounts of threats that are unique to the financial industry by better utilizing FS-ISAC threat feeds
- Increase productivity and efficiency of on-site IT staff
- Expand security capabilities without increasing management overhead or complexity
- Increase the efficiency of audit

Solution

The bank deployed the Threater Enforce platform at its perimiter to block attacks from up to 150M malicious IPs and domains (including automated threat feeds such as FS-ISAC) in real-time with no latency.

Results

- Increased protection from cyber threats, including third-party risks, through the filtering of TI indicators, country IPs, and organization IPs
- Greater visibility and control of the bank's security posture as well as integration with current security stack
- Greater TCO and faster ROI through simplified deployment and management

The Value of the Threater Platform

With banks 300X more likely to be hit by a cyber attack, the CEO knew it was critical to address security head on. Operating as a regional, medium sized bank, they also did not have the luxury of large cybersecurity budgets, staff, and resources at their disposal. They needed a solution that was smart, easy, scalable, and everywhere. As such, they deployed the Threater platform and saw a substantial drop in the malicious traffic it sees on its network.

> "After finding that something has been blocked, it's easy to identify why it has been blocked (by the Threater platform). I like the fact that I can look through the reporting features and determine if I need to ease up on some of my rules. It's then a very simple configuration change. Or, if it's something that is getting through my firewall that shouldn't, I can simply strengthen the rule."

Simplified Compliance Auditing

As the bank is heavily regulated, they are regularly audited. After deploying the Threater platform, the bank has seen higher scoring due to the information sharing and use of their FS-ISAC feeds. By integrating the FS-ISAC feeds into the Threater platform, the bank is able to protect itself and its customers from the massive amounts of industry specific threats.

Greater Visibility and Control

In financial services, understanding ones security posture and maintaining security stack integration is critical. The bank undergoes regular PEN testing as part of its ongoing security validation practice. During the most recent annual Pentest, the third-party testing company complimented the bank on their security deployment.

Greater TCO and ROI through Simplified Deployment and Management

The Threater platform reduces the number of alerts to investigate and automates the management of threat intel feeds. The threat intelligence data in the platform is automatically updated eliminating the need to manually manage threat feeds. This allows the bank to expand security capabilities without increasing management overhead and complexity.

Since deploying the Threater, the bank's IT team has seen greater efficiency in how they feed logs into their other security products. Additionally, it has been delighted in the response times and personal interactions they've received from Threater.

After deploying three Threater Enforce's into their network, the bank has seen:

- **Increased protection from threats**
- **Less malicious traffic passing through their firewalls**
- **Simplified ingestion of their third-party FS-ISAC feeds**
- **A reduction in the time spent managing their security devices**

> "The set-up was really slick. It was very simple...and anytime I've ever needed anything, I've been able to call and it's been no problem. We've been able to figure everything out with a person to person call."

About Threater

Threater uses best-in-class threat intelligence to secure your networks, data and users in real-time—wherever they are—on-prem, cloud, remote, or all of the above. Our platform blocks attacks from up to 150M malicious IPs and domains in real-time with no latency. We provide out of the box threat intelligence and integrate data from any source. At Threater, we believe nothing scales like simplicity. We make blocking threats smart and simple—at scale—everywhere.

For more information visit: www.Threater.com