Block. Every. Threat.

THREAT BLOCKR®

Impact of Cyber Attacks on Financial Services and Banks

- **300x** more likely to be targeted by cyber attacks
- Most attacked industry **3 years in a row**
- **50%** of ALL phishing attacks target banks and credit unions
- **$18.5M** = Annual cost of targeted attacks

Using Threat Intelligence to Protect Banks and Credit Unions

According to a report by Boston Consulting Group (BCG), banks and credit unions are 300 times more likely to be attacked by cyber criminals and hold the unwelcomed title of "most attacked industry" three years in a row. The reason for this is simple, the payoff for cyber criminals is unmatched. No other industry offers as rich a reward both in financial gain as well as user identity than banks and credit unions. With each successful attack making headlines, the pressure to ensure cyber defenses increases from customers, regulatory agencies, and shareholders.

Key Risk Factors

Financial Gain: From targeted phishing attacks and their associated ransomware attacks, to 3rd party supply chain attacks, the primary motivation is a financial one. Cybercriminals go where the money is.

Regulatory Compliance: More than any other industry, banks and credit unions are subject to very stringent and public regulations. From national acts such as GLBA and Sarbanes Oxley, to regional such as the California Consumer Privacy Act (CCPA), ensuring security and compliance during an audit is top of mind.

Damage to Business and Reputation: Cyber attacks can have devastating impact on banks and credit unions. From the obvious damage to reputation, to the expenses incurred responding and recovering from the attack, the consequences can be severe.

Challenges Incorporating Threat Intelligence

PROPRIETARY VENDOR PERSPECTIVE

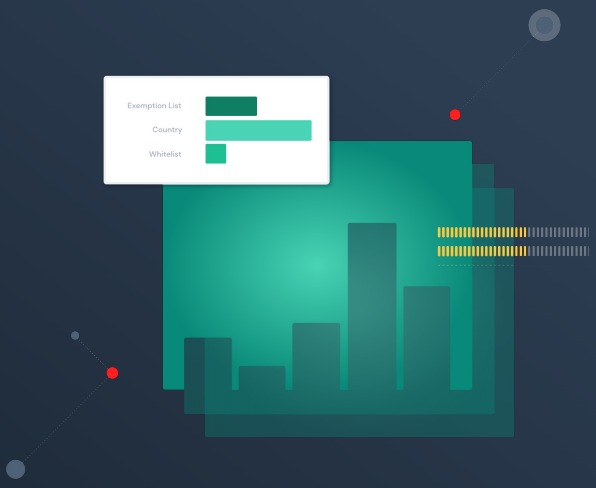
Threat Intelligence from NGFW vendors is proprietary and offers a narrow view of the threat landscape. The ability to take action on threat intelligence from multiple sources is paramount to protecting from today's targeted attacks.

ACCESSING THREAT INTELLIGENCE SOURCES

There are a plethora of threat intelligence sources including industry specific (FS-ISAC), to commercial sources (DomainTools). The ability to incorporate multiple, trusted sources and then grow as needed, is key.

OPERATIONALIZING THREAT INTELLIGENCE

Managing threat intelligence can be expensive and time consuming. How much threat intelligence is enough? Is there security "know-how" to use it? How well does threat intelligence play with NGFWs? Selecting the right solution is critical.



Solution: The ThreatBlockr Platform

ThreatBlockr uses simple, innovative technology and best-in-class threat intelligence to secure your networks, data and users in real time – wherever they are. Whether it's from data we provide out of the box, data from one of our Partner Integrations – or any other data source you have – we block attacks from up to 150 Million malicious IPs and domains in real-time, with no latency. At ThreatBlockr, we believe nothing scales like simplicity. We make blocking threats smart and simple – at scale – everywhere.

Use Cases

Medium Sized Banks and Credit Unions

Often operating regionally, medium sized banks and credit unions do not have the luxury of large cybersecurity budgets, staff, and resources at their disposal. These organizations need a threat intelligence solution that is smart, simple, scalable, and everywhere. With close to 50 small and mid sized bank and credit union clients, the ThreatBockr platform:

- Provides powerful, day-one protection with over 30 million "out of the box" threat intelligence indicators from leading commercial providers (DomainTools, Proofpoint), open source, government (DHS), and industry (FS-ISAC).
- Easily integrates threat intelligence from any source.
- Saves time by eliminating the need to manually manage threat feeds and external blocklists.
- Delivers an automated solution that is easy to deploy and manage, both on-prem and in the cloud.
- Complements and increases the ROI of existing firewall investments.

Large Banks and Credit Unions

With greater resources, budget, and staff, larger banks and credit unions typically have a more mature security practice. They are most likely using multiple sources of threat intelligence, a dedicated Threat Intelligence Platform (TIP), and a SIEM. The challenge for these organizations lies in their ability to efficiently integrate threat intelligence into security controls. In addition to the aforementioned benefits, the ThreatBlockr platform:

- Blocks 150 million IP and domain indicators, far outpacing the capabilities of NGFWs.
- Easily integrates threat indicators from Threat Intelligence Platforms (TIPs), SIEMs, and SOARs.
- Maximizes the ROI of threat intelligence investments by taking action, as well as gaining real-time visibility into which threat intelligence sources are adding value and which are not.
- Improves the efficiency and effectiveness of next generation firewalls by blocking known threats, freeing the NGFW to focus resources on more sophisticated attacks.

If you would like to know more about how you can use the **ThreatBlockr platform** to protect your business visit **threatblockr.com**

THREAT BLOCKR®