threatER

Using Threat Intelligence to Protect the Legal Industry

Law Firms and Legal Services have become a big business for targeted cyber attacks. Due to the confidential nature of their customer data, law firms present a tantalizing target for attackers, as they often also possess the wherewithal to pay the demanded ransoms. With each successful attack making headlines, the pressure to ensure cyber defenses increases from clients, state entities, and industry associations.

Impact of Cyber Attacks on Law Firms

- ✓ 26% of Law Firms Experienced a Data Breach
- ✓ $4.45 million = Average Cost of a Data Breach
- ✓ Cybercrime is now the world's 3rd largest economy

Key Risk Factors

Reducing 3rd Party Risk

Law firms interact with a multitude of 3rd parties on a daily basis. From file sharing with corporate networks and client devices, to connected service companies on the physical premises, each represents a threat vector that can be compromised.

Regulatory & Ethical Duties

While not currently subjected to regulatory and compliance requirements, state and industry associations are increasingly adding cybersecurity elements into ethics rules for law firms. Examples of these guidelines can be found in the American Bar Associations Rules of Conduct and ABA Formal Opinion 477.

Damage to Business and Reputation

Cyber attacks can have devastating impact on law firms and legal services. 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 (LS-ISAO), to commercial sources (DomainTools). The ability to incorporate multiple, trusted sources and then grow as needed, is key.

Operationalizing Threat Intelligence

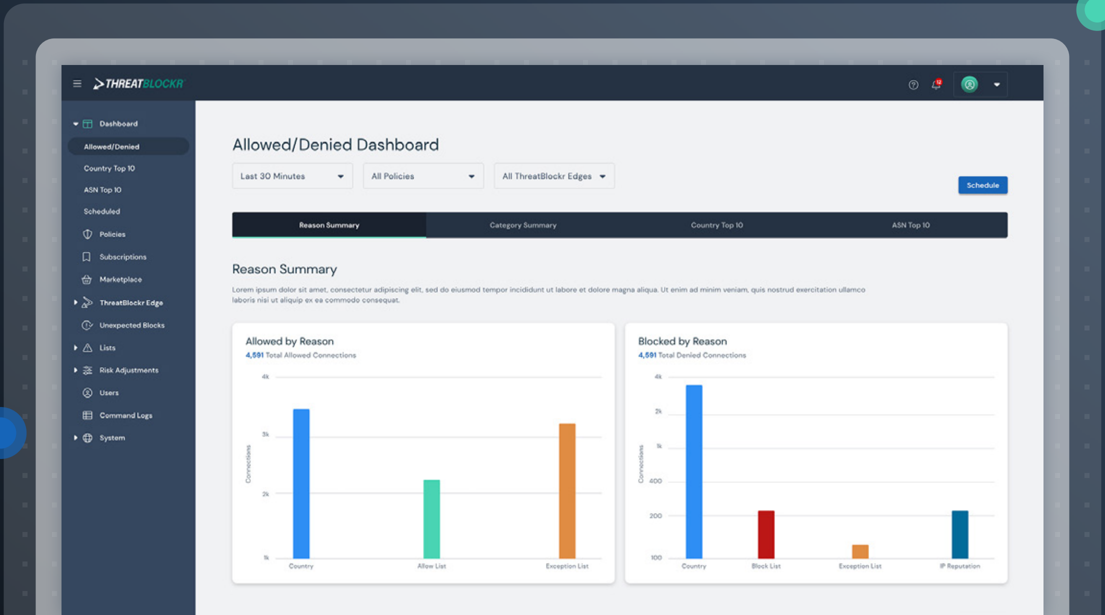
Managing threat intelligence can be expensive and time consuming. How much threat intelligence is enough? Is there security "know-how" to use it? How well does threat intelligence play with NGFWs? Selecting the right solution is critical.

SOLUTION

Threater

Fortunately, for law firms and legal services, there is a simpler way. Threater's platform 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 using data we provide out of the box, data from one our Partner Integrations—or any other data source you have, we block attacks from up to 150M malicious IPs and domains in real-time with no latency.

At Threater, we believe nothing scales like simplicity. Educational institutions can use Threater's platform to block threats in a smart, simple way—at scale—everywhere.



Allowed/Denied Dashboard

Reason Summary

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

Allowed by Reason

4,591 Total Allowed Connections

Blocked by Reason

4,591 Total Denied Connections

Use Cases

Small & Mid-Sized Law Firms

Smaller law firms often do not have the luxury of large budgets, teams, and resources at their disposal. From single-attorney firms to regional practices, these firms need a threat intelligence solution that is turnkey, automated, and affordable.

With over 20 small and mid-sized law firm clients, the Threater Enforce 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 (LS-ISAO).
- 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.
- Complements and increases the ROI of existing firewall investments.

Large and Multi-National Law Firms

With greater resources, budget, and staff, larger firms 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 Threater Enforce 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.