threater™

EVANS & DIXON LLC
ATTORNEYS AT LAW

Evans & Dixon Law Firm Increases Protection from Cyber Threats

Founded in 1945, Evans & Dixon is a law firm representing corporate clients across a range of sizes and industries such as corporate, environmental, healthcare, intellectual property, and labor and employment law. Because of this, protecting the **sensitive client data**, intellectual property, and internal data in its network was one of the law firm's highest priorities.

In this effort to secure the network, the law firm outsourced a portion of its cybersecurity management to a Managed Security Service Provider (MSSP). This MSSP provides 24/7 monitoring and management of their IDS/IPS, while the firm's internal IT/Security teams manage their firewall, web filtering, virus protection, and email security. And because of the firm's position in both collections and divisions of Workers' Compensation, they must do so while **remaining compliant with PCI and HIPAA regulations.**

Once the CIO learned how Threater's Enforce technology could not only **aggregate cyber intelligence** from government, open-source, private, and industry-specific feeds and threat lists and enforce against known threat actors with no latency, they signed up for a **free, no-obligation** 30-day trial with Threater Enforce to see how this security product could help their overstretched security teams and technologies.

Challenges

- Ingest and enforce upon a massive volume of cyber intelligence at the network layer
- Increase productivity and efficiency of security staff and technologies
- Expand security protections without the need for additional full-time employees

BENEFITS:

- Reduced risk with increased cybersecurity **defense in depth.**
- Increased productivity by reducing alerts and **eliminating 30-50% of all traffic** hitting the security stack.
- Improved efficiency by **removing known threat actors** moving in and out of the network without the need for additional security staff.

Soution

Evans & Dixon deployed Threater Enforce to aggregate best-in-class cyber intelligence and autonomously remove traffic to and from known threat actors coming in or out of the network in real time with no latency.

Results

- **Elimination of known threat actors** *coming in and out of the network*
- **Increased protection from cyberattacks** such as ransomware and data exfiltration
- **Greater efficiency and visibility** into the law firm's security posture as Enforce removed unnecessary traffic from known threat actors in the network

The Value of the Threater Platform

Like almost all organizations, Evans & Dixon had deployed a firewall to protect against cyberattacks. While the firewall offered its own proprietary cyber intelligence it enforced upon, the law firm quickly ran against the firewall's limitations to ingest – and enforce against – additional sources of cyber intelligence. Evans & Dixon's CIO decided to test this and deployed Enforce behind the firewall to test just how much known malicious traffic was passing through the firewall into the network.

Immediately after deployment it was clear the amount of known malicious traffic passing in and out of the network past the firewall was immense. The law firm then re-deployed Enforce to the network's edge where it could eliminate traffic going to and coming from known threat actors, fully convinced of Threater's foundational position in their security posture.

"Instead of putting it outside the firewall where I'm sure I'd get lots of hits, I put it behind our current protection. Was eye-opening because the bad traffic went through the firewall, it went through other systems, and was still getting through to Threater. Kept it for 2-3 weeks, saw it worked, and then decided to put it in front of the firewall – why have someone come to my house to shake doors, just keep them at the street with Threater."

– JEFF SHELDON, CHIEF INFORMATION OFFICER, EVANS & DIXON LLC

Eliminate Threats And Increase Network Efficiency

The threat landscape is always changing. Threat actors are not only sending large amounts of encrypted traffic but also attempting “back door” entrances to the network such as stolen passwords, phishing, and other means.

Firewalls have physical limitations on how much additional cyber intelligence they can ingest, yet are often the only major left-of-boom technology in the modern security stack. Unfortunately this means they are enforcing on an extremely proprietary and limited view of the threat landscape while also bogged down by inspecting encrypted traffic they were never built to handle.

By removing this traffic going to and from known threat actors, Enforce eliminates up to 30-50% of internet traffic at line speed. Removing this known-bad traffic at scale also enhances the entire network and security technologies functionalities.

Increased Protection From the Modern Threat Actor

Law firms often find themselves the target of threat actors looking for easier ways to access their clients’ sensitive data. Evans & Dixon knew they were no exception and needed a **scalable, long-term security solution** that would help prevent a catastrophic breach from threat actors.

Because most successful cyberattacks are the result of threat actors entering the network via “back door” methods such as stolen credentials or phishing, the law firm knew they needed a way to protect against this **across every port and protocol** as well in order to protect against ransomware and data exfiltration.

By eliminating any traffic to and from known threat actors no matter the protocol (HTTP/HTTPS, FTP, RDP, etc.), threat actors are left without any ability to complete their attacks. This is why Threater is a*foundational layer* in any organization’s security posture.

“Why have your firewall do the deep (packet) inspection when you don’t need to have traffic from Russia in the first place?”

Greater Visibility and Control

Geo-blocking is yet another way Enforce customers can protect their networks and gain visibility into their traffic. While firewalls often claim they can geo-block, configuration and maintenance of these policies is often difficult and cumbersome. By aggregating threat intelligence in real time with up-to-the-minute data, Enforce can **protect against traffic coming from or going to hostile nation states.**

It's also simple to make exceptions to these policies through Enforce dashboard, giving you more visibility and control over who is coming and and out of the network and – more importantly – who isn't.

"We were surprised to discover that our blog was being hosted in Bulgaria. So we added an exception for that one IP address (for our company blog). We found a few cases like this where a third-party support system we use was located in Eastern Europe. It was simple to white-list those IP addresses, and block the rest."

"With the Threater platform, we can set it and forget it. It automatically updates and we know that everything that gets blocked is one less thing we have to worry about attacking us!"

Satisfied Customers Year After After

Since deploying Enforce, the Evans & Dixon team have loved the platform's reliability and just how easy it is to manage. Since his no-obligation, 30-day trial, the law firm has remained a **loyal and satisfied Threater customer.** Most recently, the firm upgraded to a higher throughput to accommodate their growing needs of their practice.

"I'm sure that our other security devices have features and functions, but making those changes would require weeks of learning how to configure a simple change... So any time I have to do anything on them, I have to call my outside engineer at $165 an hour. Versus, the Threater handles our needs and it's solid. No problems or support issues. And it's cost effective!"

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: Threater.com