threater

An MSP's Guide to Threater

Threater.com

The Opportunity

Cybersecurity is one of the largest growing areas in IT investment. In fact, a recent study found that 91% of IT and business decision makers will place cybersecurity as a high priority for their organization over the next two years. And it's no wonder: threat actors have become more sophisticated and relentless in their attacks, with every breach costing an organization millions of dollars and reputational damage. Cybercrime-as-a-Service has created an underground industry worth billions of dollars, and these cybercriminals have no intention of letting up.

As organizations look to secure their most valuable digital assets, hiring in-house cybersecurity professionals has become almost impossible.

A chronic industry staffing shortage means there are too few security professionals to fill open positions, astronomical costs of full-time employees (when you can find them), and a notoriously high turnover rate of industry employees who report extremely high levels of burnout. Finally, companies have been tasked with securing a complex and increasing attack surface with the rise of permanent hybrid/remote work for their workforce.

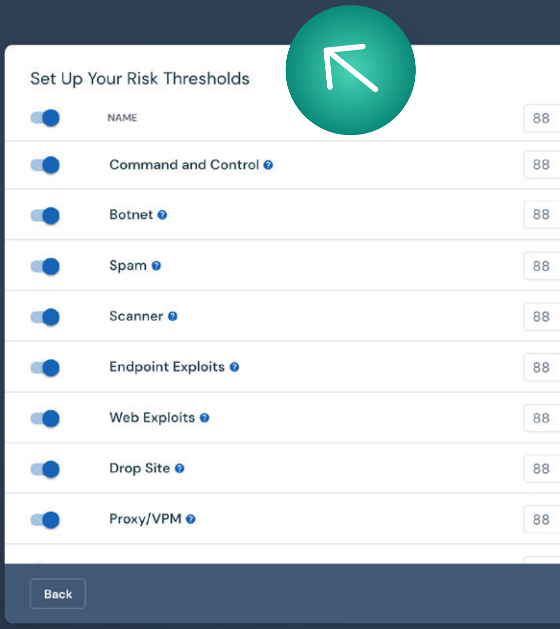
All of these conditions have led to organizations increasingly turning to one place for their cybersecurity needs: managed service providers (MSPs) and managed security service providers (MSSPs).

THE TIME IS NOW!

The cybersecurity market for MSPs is growing exponentially, even through economic downturns. Now is the time to start a cybersecurity portfolio.

Find out why MSPs are partnering with Threater as their first step to building out a multi-layered cyber security solution. A strong cybersecurity strategy begins with keeping out all known threat actors.

https://www.Threater.com/msps/



Set Up Your Risk Thresholds

	NAME	
●	Command and Control	88
●	Botnet	88
●	Spam	88
●	Scanner	88
●	Endpoint Exploits	88
●	Web Exploits	88
●	Drop Site	88
●	Proxy/VPM	88

Why Are Security Stacks Failing?

By now, the idea of a multilayered security stack is ubiquitous in the cybersecurity world. The basic premise of this is that one technology's "holes" can be filled by the others' protections. A common way to describe this is the "Swiss cheese" model, where one solution fills the "holes" left by another, like a block of Swiss cheese.

But as we have seen news of breach after breach after breach, it has become clear the modern security stack still needs help. Why?

Security stacks are too reactive.

By now, most organizations have adopted a multilayered security stack model with various specialized tools. A typical security stack most likely includes a combination of these technologies:

- (Next-generation) Firewall
- SIEM
- SOAR
- Detection and response tools (e.g., MDR, EDR, XDR, etc.)
- TIP

All of these tools are of course valuable and serve important functions in and of themselves. However, outside the firewall, **modern cybersecurity tools are all fundamentally reactive by design**. Or in cybersecurity language: almost all security stack tools sit "right of boom", trying to detect and fix problems after they're already in the network.

Worse yet, integrating these tools with each other often proves challenging at best and impossible at worst. This leaves cybersecurity teams managing too many tools throwing too many alerts, and they are unable to parse the real threats from the false or duplicate flags.

Firewalls can’t keep up with the modern day Threat Actor.

Every organization has a firewall. They are an essential piece of any security stack, but they are also tasked with too many requests they were never designed to handle. And while next-generation firewalls (NGFWs) have made great strides, they are still limited. Some of the challenges of firewalls and NGFWs include:

- Limited threat intelligence
- Challenging integrations with additional threat intelligence and other deployed security stack technologies
- Limited block lists
- Cannot efficiently process the amount of malicious internet traffic thrown at it
- Lack of outbound threat blocking
- Network latency caused by encrypted traffic

Threater Fills the Gaps

Managing an organization’s security stack has become untenable. Security teams, security operations centers (SOCs), and MSPs have been left to manage multitudes of cybersecurity tools, logs, and alerts, yet are still left vulnerable.

Unfortunately the cybersecurity world has been asking the wrong questions. For too long we have asked, “How do we stop threat actors in the network?”

Threater is instead asking, “Why not start by eliminating the known threat actors?”

This is a cybersecurity paradigm shift, and an important one. Here’s how Threater’s solution fills the gaps left open by modern security stacks by sitting “left of boom.”

Here’s how.

Reduce the noise.

Threater's Enforce product sits at the network layer, eliminating traffic to and from known threat actors on all ports and protocols. By leveraging many different threat intelligence feeds (described below), this technology can **block up to 150 million known malicious IP addresses** moving both inbound and outbound with no impact on network performance.

This large-scale threat blocking results in a **30-50% reduction in traffic hitting the security stack.** The benefits of this type of noise reduction are substantial:

- **Increased firewall efficiency.** Firewalls require massive amounts of resources to decrypt and analyze large amounts of internet traffic. Reducing the amount of traffic it has to parse allows it to work more efficiently as well as ease performance issues caused by the firewall.
- **Fewer alerts.** By blocking known malicious traffic, the rest of the security stack's alerts become more manageable and fewer alerts slip through the cracks.
- **Increased security posture.** Any organization's security posture is automatically improved for a rapidly expanding threat surface when known threat actors are no longer in the network nor have a way to call back if they do get in via phishing, password breach, etc.

Threat intelligence at scale.

The ability to block known threat actors is only as good as the intelligence of who and where the threat actors are. Most firewalls will market their own proprietary threat intelligence as a selling point, which results in organizations relying on one vendor's view of the threat landscape. And while threat intelligence platforms (TIPs) are valuable, they do not actively block the threats they know about and can be difficult to integrate with the existing tools in the security stack.

Threater's solution turns the idea of proprietary threat intelligence on its head by aggregating 50+ cyberintelligence feeds and leveraging them to block threats at scale.
Even better: this technology automatically updates and stays current with up-to-the-minute information.

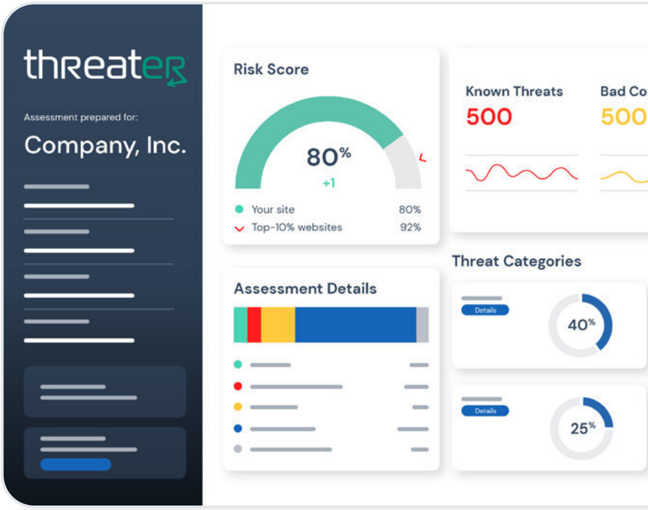
Many of the intelligence feeds Threater leverages are from vendors who might ordinarily compete with each other, which provides an unparalleled view of the threat landscape. By pulling in all these intelligence sources, utilizing the threat intelligence to block known threat actors, and delivering threat intelligence to the existing security stack, the Threater solution is uniquely positioned to **secure networks.**

Active defense for all traffic.

Outbound threat blocking remains one of the largest security weaknesses in modern security stacks. Threater solves this, too.

When threat actors do manage to penetrate the network, either via hacking, phishing, etc., the malicious software typically has a "phone home" feature that sends data back to the threat actor who deployed it. Threater's solution blocks these outbound calls back to malicious IPs and stops the threat actors from compromising the network. This outbound "left-of-boom" blocking mechanism is not only unique, but can be the difference between protecting an organization's data and a breach.

Why Threater for MSPs



Threater's active defense is an essential component to keep up with today's modern threat actor and can fit into any MSP's portfolio whether they are just dipping their toes into security or have a robust security portfolio for their clients.

Let's explore some of the benefits of Threater for MSPs specifically.

Identify blind spots.

Cybersecurity blind spots are where threat actors flourish. Until now, identifying those blind spots has been a perennial challenge. Threater solves this by removing the blinders to give organizations crucial insights about the malicious traffic hitting their networks.

Threater offers a **complimentary threat risk assessment** that analyzes firewall logs and shows organizations what is happening behind their firewall today. This report demonstrates the malicious traffic Threater would have stopped but instead passed through the current firewall's protections. This type of data has proven invaluable to both organizations looking to secure their network as well as MSPs wanting to show quantifiable results and value in this solution. In short: **MSPs can show their clients what they couldn't see before.**

When the full picture is clear, the question naturally unfolds: can organizations really afford to keep the blinders on?

Low touch and high value.

Like everyone, MSPs are looking for security solutions that not only work for their customers, but are easy to maintain and update post-deployment. In other words: they need solutions that are low touch yet provide high value. Fortunately, Threater is one of those rare "easy win" technologies.

Here are a few reasons MSPs find Threater a low touch/high value solution:

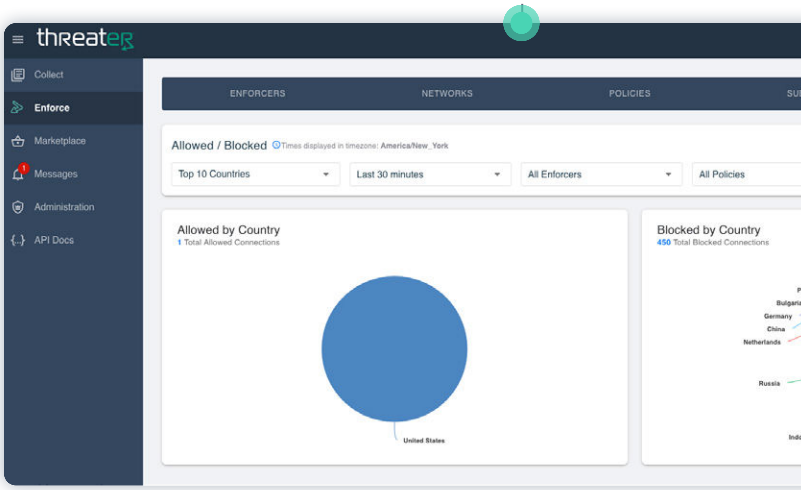
- **Easy to deploy.** Threater's solution can go to market within 60 days and begins protecting customers' assets immediately.
- **Does not require "unselling" current software.** Threater is not meant to replace other previously-sold security solutions and does not erode trust in existing sales solutions.
- **Autonomous.** Once deployed and configured, Threater automatically updates and blocks malicious IPs without the need for employees to babysit the software.

Complementary security technology.

Threater is not just the "latest version" of an existing cybersecurity solution. Instead, this solution makes each part of an organization's security stack better and work more efficiently as it blocks the known threat actors from ever hitting network assets.

Large-scale rip-and-replace projects require extended sales cycles and capital investment project approval. However, Threater can provide threat blocking services with unparalleled threat intelligence that can also deliver threat intelligence to a customer's MDR/SIEM platforms as well as any third-party system using RFC-compliant, standards-based formats and/or open REST APIs.

Threater's easy-to-use console can be adjusted to any organization's risk comfort level, and also reveals the malicious traffic hitting the network. This valuable data generated from the platform helps inform current and future cybersecurity decisions.



Allowed / Blocked Times displayed in timezone: America/New_York

Top 10 Countries | Last 30 minutes | All Enforcers | All Policies

Allowed by Country
1 Total Allowed Connections

Blocked by Country
450 Total Blocked Connections

Simply put: no matter the configuration of the security stack, Threater works.

Threater works with all security stack technologies regardless of configuration or location, making this a true complementary solution.

Sales wins for MSPs.

Customers trust MSPs to stay current on the best solutions for the best value. In this relationship, MSPs must also take their own interests into account by offering products that will work for their clients but also maintain their sales value. Threater is one of those rare solutions that does both.

Here are a few reasons MSPs love Threater in their sales cycles:

- **Wedge product.** Threat Blocking-as-a-Service provides exceptional protection while working with any existing security stack, making it an easy “in” for new clients or an easy “add-in” for existing customers.
- **Reduces load on security analysts and SOCs.** Because Threater blocks 30–50% of the internet traffic hitting the security stack, it also reduces the load on back-end security analysts and security operation centers (SOCs). For MSPs, this is another huge benefit post-deployment.
- **High margin.** This technology doesn’t require massive trainings or certifications for staff, nor does it require constant maintenance. This is one of the most effective, highest-margin cybersecurity products for MSPs to sell on the market today.
- **Builds credibility quickly.** When deployed, this technology enables MSPs to build trust with customers by recommending security software that provides outsize value immediately.

Conclusion

Leverage best-in-class intelligence and save your security stack with Threater

There are a few absolute truths in the cybersecurity world today. First, threat actors are relentless and growing more sophisticated every day. Second, the threat surface is rapidly expanding as companies are scrambling to secure more remote employees and more devices. Third, network and data breaches are expensive and potentially fatal to a company. Finally, **every single organization needs cybersecurity.**

And as more and more organizations turn to MSPs for their cybersecurity needs, MSPs are turning more and more to Threater as one of the most effective solutions on the market. No matter the existing security solutions or configurations, Threater **will** make any network more secure.