threatER

Continuous Cybersecurity Improvement: A Necessity, Not a Luxury

Organizations must understand that cybersecurity is not a one-off project but a continual process. It's crucial to regularly assess defenses, identify potential weaknesses, and implement updates. This approach prevents complacency and ensures that your organization remains resilient against evolving threats. To avoid falling into the trap of "if it works, don't touch it," consider adopting a mindset of continuous improvement. Regularly review security protocols and vendor engagements, conduct vulnerability assessments, and engage in training sessions to keep staff informed about the latest threats and best practices. Remember, in cybersecurity, stagnation can be just as dangerous as active vulnerabilities.

MISCONCEPTION #1 Your firewall is "enough"

- Treating a firewall as a set-it-and-forget-it solution is a misconception. A great firewall requires ongoing monitoring, updating, and testing to adapt to evolving needs. The reality is that every successful cyberattack has breached a company's firewall, highlighting that it is insufficient on its own. Additionally, while many organizations collect threat intelligence from their firewalls, it is critical to proactively utilize this information rather than merely aggregating it in a SIEM (see the next bullet for more info), thereby falling into the trap of storing-and-forgetting-it.
- Firewalls perform deep packet inspection on all traffic, but struggle to keep up with the amount of double-or-triple-encrypted traffic arriving from threat actors. threatER eliminates known-bad traffic based on IP addresses attributable in real-time to threat actors, allowing it to scale and enforce without causing network latency.
- Firewalls are well intended but need help and that's where you need threatER to ensure you're stopping all threats before they infect your network.

MISCONCEPTION #2 I have enough threat intelligence already.

- While it's great that you're leveraging threat intelligence, the key question is: what are you doing with it? Many organizations mistakenly believe that simply collecting threat intel from their partners and firewalls is sufficient. Often, they find their firewalls can't effectively manage the influx of data and end up funneling it directly into their SIEM. However, if this is your approach, you're operating exclusively in a detect-and-respond capacity, and missing the opportunity to proactively utilize this valuable information to enforce in real-time.
- To truly benefit from threat intelligence, it's essential to enforce that data at the network level. This ensures that the rest of your security stack operates effectively and efficiently. Relying on a single source of threat intelligence is limiting; if you're using one source, why not tap into multiple? The challenge lies in the complexity of managing various sources of threat intel on your own. That's where threatER comes into play, enabling you to harness and integrate over 50 world-class cyber intelligence feeds that provide up to the minute threat intelligence data to inform enforcement and strengthen your overall security posture.

1.855.765.4925 | sales@threater.com

MISCONCEPTION #3 **I'm afraid to add something else to my network**

- In the nicest way possible - too bad. The fear of integrating new technologies should not hinder an organization's cybersecurity strategy. Embracing cutting-edge solutions can empower businesses to stay ahead of threats, improve efficiency, and enhance their overall security posture. Rather than viewing new tools as potential risks, organizations should recognize them as essential components of a robust cybersecurity framework. By fostering a culture of continuous improvement and innovation, organizations can better safeguard their assets in an ever-evolving threat landscape. Reiterating the first bullet above, every successful breach has breached a firewall - so you will need to add SOMETHING to strengthen it - let threatER show you what it can do to secure your network - without any added latency.

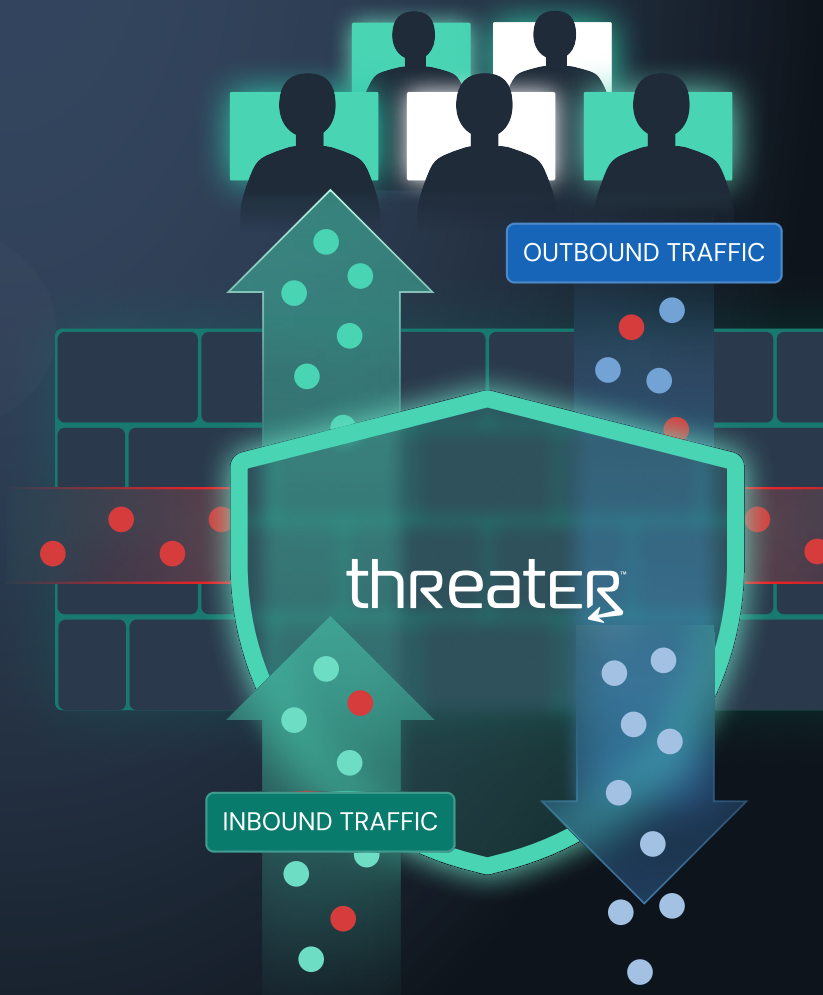
On average, threatER **blocks ~30,000 known threats** that your firewall is missing every 24 hours.

What Can You Do Now?

At a minimum - conduct a free firewall assessment
threatER looks at 24 hours of data from your firewall logs and we can show you the threats that sneak by.

The first step in onboarding a new solution is knowledge.

Learn more with threatER today.



1.855.765.4925 | sales@threater.com