WHY THREATER?

Why Now?

In today's rapidly evolving cybersecurity landscape, it can seem nearly impossible to keep up with the latest threats. Threater not only blocks you from millions of known bad actors—it keeps them from ever reaching your firewall. That gives your firewall more bandwidth to inspect incoming and outgoing data for unknown risks. Less malicious incoming data also dramatically lowers traffic to your SIEM, saving you money. Protect your network with Threater now. Your firewall (and the rest of your security stack) will thank you.

Block More Known Threats

Blocking known threats is the fundamental aspect of Threater's cybersecurity strategy. "But doesn't my firewall do that?" No, not at the scale that Threater can. We aggregate tens of millions of known threats from cybersecurity researchers and threat-intelligence feeds, then block these malicious entities—malware, viruses, phishing attempts, exploit kits, and more. Blocking them allows for immediate risk mitigation, a proactive defense posture, and resource optimization. And in addition to what we supply out-of-box, you can add as much of your own intelligence data from as many data sources as you want.

Ease the Load on Your Firewall

Firewalls can become overwhelmed by the sheer volume of incoming traffic, especially in environments with high network activity. By using Threater, organizations can identify and block malicious traffic before it reaches the firewall. This reduces its burden and allows it to allocate resources more efficiently and focus on inspecting legitimate traffic for potential threats. Organizations that use Threater see a total-traffic reduction of 30–50%—all known bad actors that can be blocked before they get to your firewall.

Your Firewall Gets Attacked Too

The most advanced attackers, including nation state attackers, are constantly looking to attack the next generation firewall itself, or its constituent components, such as VPNs, other secure tunnels, configuration, and more. By deploying Threater between your firewall and your ISP modem, you provide an extra layer of protection for the firewall itself, since no known malicious actor will be able to reach the firewall in the first place. In the era of zero-days targeting network security equipment at the edge of networks by nation state actors that have been called out in the headlines and further disseminated by organizations such as CISA as serious breaches (some with maximum scores of 10.0, meaning that simple network access is all a malicious actor needs to cause a breach), the security protection afforded by Threater is a must-have.

Reduce Traffic to Your SIEM

SIEM systems can be expensive to deploy and maintain, especially when they are processing large volumes of data from diverse sources. A 30–50% traffic reduction to your firewall also means a similar reduction in traffic directed to your SIEM. By using Threater, organizations can reduce the hardware, storage, and licensing costs associated with operating the SIEM infrastructure. Less traffic also streamlines the incident-response process, enabling security teams to allocate their resources more efficiently. By minimizing the noise and false positives within the SIEM, analysts can quickly identify genuine security incidents, investigate them thoroughly, and take appropriate remedial actions.

By embracing proactive threat detection and response strategies, organizations can fortify their defenses against evolving cyber threats, mitigate operational risks, and safeguard critical assets.

The time to act is now to increase resilience and security in an increasingly hostile digital landscape. Block more bad actors, ease the burden on your current security stack, and save money by reducing SIEM data volume when you choose Threater.