threater

AUTONOMOUS
CYBER DEFENSE

About Threater

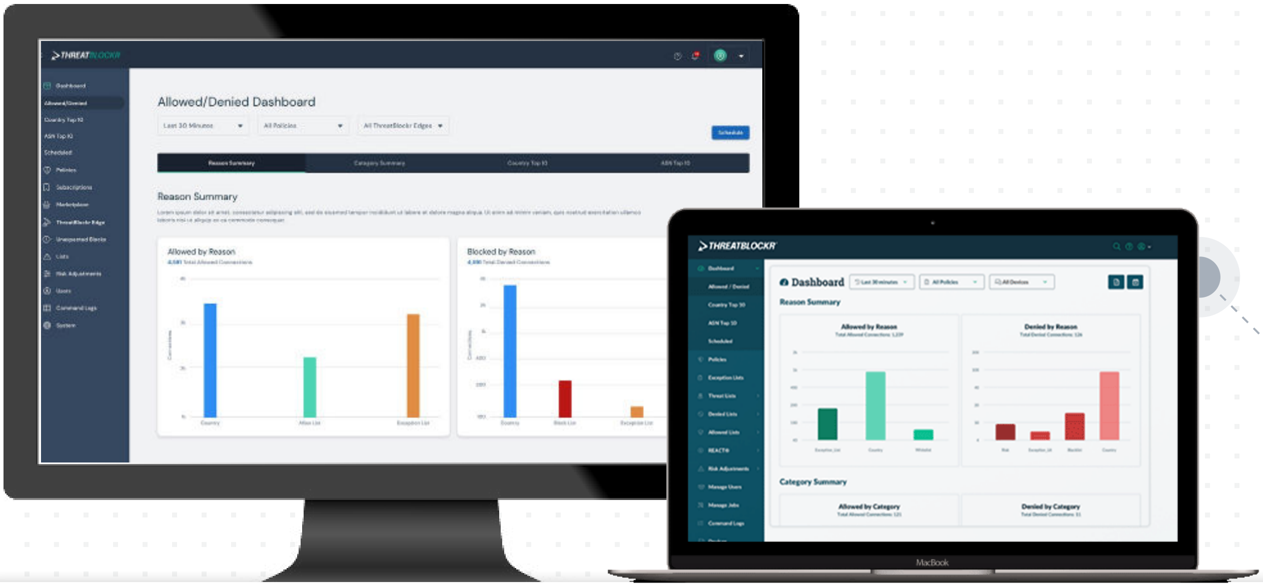
Threater® is the only active defense cybersecurity platform that fully automates the enforcement, deployment and analysis of cyber intelligence at a massive scale. As the foundational layer of an active defense strategy, Threater's patented solution blocks known threats from ever reaching customers' networks. Threater utilizes immense volumes of cyber intelligence from over 50 renown security vendors to provide unparalleled visibility over the threat landscape resulting in a more efficient and effective security posture. Security teams at companies of all sizes use Threater to deploy active security, gain real-time network visibility into threats and policy violations, ensure their network is protected and reduce manual work.

Threater vs. Firewalls

- Every cyber attack has gotten past a firewall at some point.
- Firewalls detect and block known threats using their own proprietary threat intelligence. This represents too narrow a view of the threat landscape - the view of a single vendor.
- Firewalls have limited ability to integrate additional intelligence., i.e. a typical high-end Palo Alto firewall can only handle 150,000 IP addresses in its external blocklist.ther systems.
- Threater uses massive volumes of threat intelligence from multiple sources - commercial, open source, industry, and gov't. Our platform can handle 150 Million third-party IP and domain indicators - 1000x what a firewall can handle under the same conditions.
- Threater makes it easy for organizations to add threat intelligence from any source, whereas it is notoriously complex to add even small amounts of third party intelligence to a "big three" (Palo Alto, Fortinet, Cisco) firewall.

Key Benefits / Features

- **Block up to 150 Million IP and domain indicators** - 1000x what a typical firewall can handle in external blocklists.
- **Immediately improve network protection** by using cyber intelligence from over 30 leading sources to block known-bad traffic that your current security stack is missing.
- **Easily add cyber intelligence from any source** with over 50 out-of-the-box connectors and integrations with industry threat intel sources (ISACs/ISAOs), Threat Intelligence Platforms, SIEMS, SOARs, and other systems.
- **Automation ensures threat intelligence is always up to date** and eliminates manual work and time spent managing firewall blocklists.
- **Rich log data provides visibility into threats** targeting your networks. Powerful syslog export capabilities enable easy integration with SIEMs and log management solutions.
- **Reduce traffic hitting your existing security stack** by 30%-50% enabling the entire stack to be more efficient and effective.
- **Our turnkey solution can be deployed in 30 minutes** or less and is easy to manage.
- **Seamlessly integrates** into and enhances the value of your existing security stack including firewalls, SIEMs, SOARs, NDR, and MDR.



Threater vs. Zscaler

- Zscaler only protects outbound traffic. Threater protects inbound and outbound traffic.
- Zscaler only protects web traffic incident from supported web browsers; Threater protects all traffic regardless of how it is generated or what software initiates it.
- Zscaler can only be consumed as a cloud-based service*; Threater can be deployed "Everywhere" on-prem, cloud, or "as-a-service."
- Threater inspects packet header only; Zscaler can do deep packet inspection and content inspection.
- Threater and Zscaler provide a complementary, layered security approach.
    - Threater provides network protection for both inbound and outbound connections and secures all traffic using massive volumes of best-in-class threat intelligence.
    - Zscaler provides additional deeper inspection for end user Internet web-browser traffic.

Threater vs. SIEM

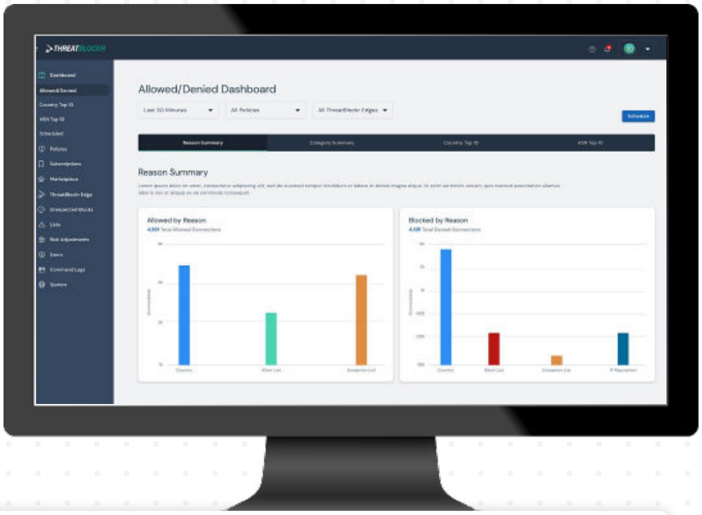
- While SIEMs add value, they are reactive in nature. By the time you detect and respond it can be too late. Threater is proactive. Threater blocks known bad traffic on the network in real time using massive volumes of threat intelligence.
- SIEMs aggregate log data from various cybersecurity controls and other IT systems and apply analytics to the log data to detect threats. Many organizations integrate threat intelligence data into SIEMs to improve their ability to detect threats and to prioritize alerts. This is reactive and too slow to protect against today's threats.
- Threater log data provides valuable visibility into threats targeting an organization's network. Threater has powerful syslog export capabilities making it easy to integrate Threater log data into SIEMs. Adding Threater log data into SIEMs, significantly improves organizations' detection and response efforts, to include triage and audit.

Threater vs. SASE

- SASE providers largely detect and block threats using their own proprietary threat intelligence. Threater significantly improves network protection by using massive volumes of threat intelligence from multiple sources to detect and block threats.
- Threater can be deployed at the network edge alongside SD-WAN and SASE network nodes adding a valuable layer of protection.

Threater vs. Managed Detection & Response (MDR)

- MDR is fundamentally a service where you outsource security monitoring to a third-party service provider. It's "eyes on glass."
- MDR effectively has the same challenge as integrating threat intel into a SIEM - it's reactive, not proactive. By the time you react it may be too late.
- In addition, the majority of MDR providers are focusing on detection ("telling you something is wrong") vs. response (actually doing something about it, or preventing it in the first place).
- Threater uses threat intelligence proactively to block threats before they hit your network.
- It's not necessarily Threater or MDR; many customers use Threater along with MDR.



Threater vs. Network Detection & Response (NDR)

- NDR is fundamentally reactive in nature while Threater is proactive in nature.
- Threater sits inline at the network perimeter detecting and blocking known threats using massive volumes of threat intelligence. NDR solutions sit inside the network and look at the behavior of network traffic to detect potential incidents after-the-fact.
- NDR is about detection not prevention. Detection has value, but prevention does too.
- NDR solutions tend to be significantly more expensive and harder to use compared to Threater.
- Because Threater and NDR solutions do different things, many customers will deploy both. In fact, Threater makes NDR solutions more effective and efficient by reducing the amount of noise they deal with.