CXPONENT

POWER BRIEF *for* threatER

Executive Overview

- Headquarters: Tysons, VA

- Total Clients: 300+

Product & Service Offerings

- Cyber Security SaaS Platform

- Autonomous Cyber Defense

- Threat Intelligence

Key Features & Differentiators

- Immediately improve network protection by using cyber intelligence from over 30 leading sources to actively block known bad traffic that your current security controls are missing.

- Easily add cyber intelligence from any source with no limits. • Mitigate false positives quickly and intuitively using automated allowed lists.

- Automation reduces manual work, saves time, and ensures you are always protecting your network with the latest cyber intelligence...in real time.

- Improve layered security efficiency and effectiveness by eliminating 30%- 50% of the traffic hitting your existing security stack.

- Robust security without compromising network performance

- Seamlessly integrates into and enhances the value of your existing security stack including firewalls, SIEMs, SOARs, NDR, and MDR.

Top Industries Served

- Electronics
- Healthcare
- Education
- Hospitality (Hotels, Food, Beverage)

Ideal Customer Profile

- SME -- 100 to 499 employees

- Enterprise -- 500+ employees

- MDR, MSSP’s & MSP’s

- Target industries: Financial Services, Health Care, Energy, Legal Services, Manufacturing, Retail, Education, State & Local Gov’t

- Budget: Enforce is highly cost-effective for organizations of all sizes

Qualifying & Technical Questions

- What are your customers doing proactively to prevent attacks/breaches in their network?

- Reason I'm asking: Every 11mins there is an attack is taking place

- Are you using threat intelligence today and if so from what sources?

- Reason I'm asking: If they say they are using threat intelligence from existing security controls they are early in their threat intelligence journey and aren't really using threat intelligence.

- If you are using threat intelligence from multiple sources (commercial, open-source, industry, and gov't) how are they acting on it?

- Reason I'm asking: Most customers are not able to proactively block with threat intelligence because of the significant limits that firewalls have.

- If they are using threat intelligence, are they using a Threat Intelligence Platform (TIP) or a SOAR to aggregate and manage it?

- Reason I'm asking: ThreatBlockr easily integrates with leading TIP and SOAR platforms.

- Are your customers looking to gain more overall security in their infrastructure?

- Reason I'm asking: We are a foundational layer to the security solution that your customers should be looking to implement

- Are you considering a migration to the cloud?

- Reason I'm asking: We can be deployed practically anywhere. This includes cloud networks (AWS, Azure) and on-premises networks on dedicated hardware (ours or yours!) or virtually (VMware, KVM) • What tools are your customers using today to manage their security risk?

- Reason I'm asking: There is a huge hole in the security stack (Firewalls, SIEM's, MDR's, etc.) that we cover proactively without displacing anything in their current security environment!

Elevator Pitch

ThreatBlockr 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, ThreatBlockr's patented solution blocks known threats from ever reaching customers' networks. ThreatBlockr utilizes immense volumes of cyber intelligence from over 50 renowned security vendors to provide unparalleled visibility over the threat landscape resulting in a more efficient and effective security posture. Block. Every. Threat. at threatblockr.com.