Block. Every. Threat.

THREAT BLOCKR®

Using Cyber Intel for K-12 and Higher Ed Orgs

Of all industries, the education sector faces the most daunting cyber security challenges. Already faced with budgetary cuts and mounting public regulation and scrutiny, the move to remote learning, hybrid classrooms, and lack of standard guidance, education has found itself in the crosshairs of opportunistic cyber threat actors. A 2018 report by SecurityScoreCard found that out of all 17 industries, education ranked last. Add to this an increase of over 30% in attacks targeting schools and institutions in the first quarter of 2020, and the devastating effects of both DDoS, Phishing, and Ransomware on vulnerable networks, and the potential damage, is catastrophic.

Impact of Cyber Attacks on K-12 and Higher Ed

- Attacks targeting education **increased by 33%**
- **Education ranks last** in cybersecurity preparedness
- Phishing and Ransomware **rank highest** attacks targeting education
- New remote learning **expands attack surface** and adds vulnerability

Challenges Incorporating Threat Intelligence

Proprietary Vendor Perspective

Threat Intelligence from NGFW vendors is proprietary and offers a narrow view of the threat landscape. The ability to take action on threat intelligence from multiple sources is paramount to protecting from today's targeted attacks.

Accessing Threat Intelligence Sources

There are a plethora of threat intelligence sources including industry specific (REN-ISAC), to commercial sources (DomainTools). The ability to incorporate multiple, trusted sources and then grow as needed, is key.

Operationalizing Threat Intelligence

Managing threat intelligence can be expensive and time consuming. How much threat intelligence is enough? Is there security "know-how" to use it? How well does threat intelligence play with NGFWs? Selecting the right solution is critical.

Solution: ThreatBlockr

Fortunately, for K-12 and Higher Education organizations, there is a simpler way. ThreatBlockr uses simple, innovative technology and best-in-class threat intelligence to secure your networks, data and users in real time, wherever they are. Whether it's using data we provide out of the box, data from one our Partner Integrations – or any other data source you have, we block attacks from up to 150M malicious IPs and domains in real-time with no latency.

Use Cases

Small and Mid-Sized K-12, Colleges and Universities

Always cognizant of budgetary restrictions and in-house expertise, these organizations do not have the luxury of large cybersecurity budgets, staff, and resources at their disposal. Therefore, having a threat intelligence solution that is turnkey, automated, and affordable, is key to tackling the new norm of remote learning and an overtaxed NGFW. With close to two dozen small and mid-sized school districts, colleges, and university clients, ThreatBlockr:

- Provides powerful, day-one protection with over 30 million "out of the box" threat intelligence indicators from leading commercial providers (DomainTools, Proofpoint), open source, government (DHS), and industry (MS/REN-ISAC).
- Easily integrates threat intelligence from any source.
- Saves time by eliminating the need to manually manage threat feeds and external blocklists.
- Delivers an automated solution that is easy to deploy and manage.
- Complements and increases the ROI of existing firewall investments.

Large K-12, Colleges and Universities

With greater resources, budget, and staff, these larger districts and institutions typically have more budget to work with. However, they are still faced with open networks and the "new norm" of an expanded attack surface due to remote learning. They might be using multiple sources of threat intelligence, a dedicated Threat Intelligence Platform (TIP), and a SIEM.
The challenge for these organizations lies in their ability to efficiently integrate threat intelligence into security controls. In addition to the aforementioned benefits, ThreatBlockr:

- Blocks 150 million IP and domain indicators, far outpacing the capabilities of NGFWs.
- Easily integrates threat indicators from Threat Intelligence Platforms (TIPs), SIEMs, and SOARs.
- Maximizes the ROI of threat intelligence investments by taking action, as well as gaining real-time visibility into which threat intelligence sources are adding value and which are not.
- Improves the efficiency and effectiveness of next generation firewalls by blocking known threats, freeing the NGFW to focus resources on more sophisticated attacks.

If you would like to know more about how you can use **ThreatBlockr** to protect your business visit **threatblockr.com**

THREAT BLOCKR®