Impact of Cyber Attacks on Healthcare

Using Threat Intelligence to Protect Healthcare

Cyber attacks in the healthcare industry damage much more than reputations and bottom lines. A single ransomware attack can shut down critical care systems, creating dire consequences for patients. With the rise in this class of cyberattack, healthcare organizations are once again challenged to not only protect their patients and their data, maintain HIPAA compliance, maintain and merge old systems with new technology, protect their remote users, but protect the entire healthcare network from complete failure and lockout—resulting in loss of reputation, potential lawsuit, huge payouts, and in extreme cases, loss of life.

- **93% of Healthcare Orgs Experienced a Data Breach**
- **$10.9M = Average Cost of a Healthcare Data Breach**
- **385M = Number of patient records exposed since 2010**

Key Risk Factors

Mounting Cyber Threats

Cyber attacks against healthcare are growing exponentially and having a devastating impact. Ransomware in particular has become a common attack facing healthcare resulting in loss of patients personal identifiable information (PII), costly financial loss, and potentially severe system lockout repercussions.

Regulatory Compliance

HIPAA regulatory compliance is top of mind for the healthcare industry. Healthcare organizations find themselves at risk for both major cyberattacks, as well as financial and criminal penalties under HIPAA regulation when they do not have the appropriate tools in place.

Third-Party, IoT, and Supply Chain Weaknesses

As our healthcare networks and systems have become more interconnected, threat actors are targeting systems and networks that leverage third-party software to attack healthcare systems' networks. To make matters worse, many healthcare devices and proprietary software needed for patient care are left unpatched and vulnerable for threat actors to exploit.

Challenges Incorporating Threat Intelligence

Proprietary Vendor Perspective

Threat Intelligence from NGFW vendors is proprietary and offers to narrow a 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 (H-ISAC), to commercial sources (DomainTools). The ability to incorporate multiple, trusted sources and then grow as needed, is key.

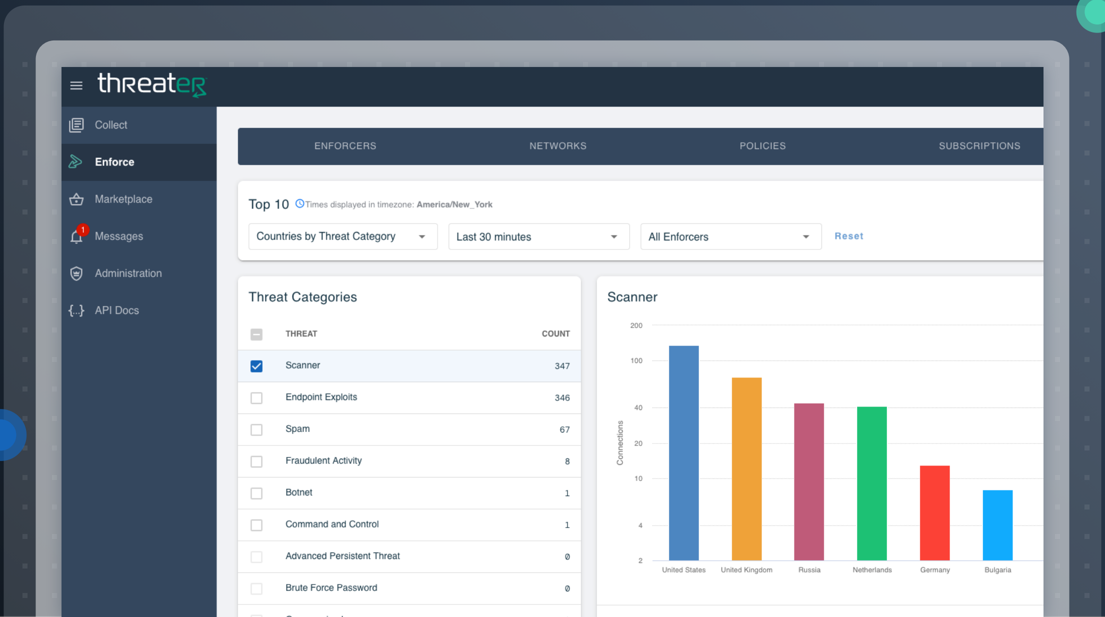
Operationalizing Threat Intelligence

Managing threat intelligence can be challenging, expensive and time consuming. How much threat intelligence is enough? Is there the resources or security maturity to use it? How well does the threat intelligence play with NGFWs? Selecting the right solution is critical.

SOLUTION

Fortunately, for healthcare organizations, there is a simpler way. Threater Enforce uses simple, innovative technology and best-in-class threat intelligence to secure your networks, data and and users in real time, wherever they are. Whether it’s using data we provide out of the box, data from one of 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.

At Threater, we believe nothing scales like simplicity. Healthcare organizations can use Enforce to block known threats in a smart, simple way—at scale—everywhere.



Top 10 Times displayed in timezone: **America/New_York**

Countries by Threat Category ▾ | Last 30 minutes ▾ | All Enforcers ▾

Threat Categories

	THREAT	COUNT
☑	Scanner	347
□	Endpoint Exploits	346
□	Spam	67
□	Fraudulent Activity	8
□	Botnet	1
□	Command and Control	1
□	Advanced Persistent Threat	0
□	Brute Force Password	0

Large Healthcare Systems

With greater resources, budget, and staff, large firms typically have a more mature security practice. They are most likely 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, Threater Enforce:

- Blocks up to 150 million IP and domain indicators, far outpacing the capabilities of next-generation firewalls.
- Easily integrates threat indicators from any source including Threat Intelligence Platforms (TIPs), SIEMs, SOAR, and other systems.
- Maximize 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 aren't.
- Improving the efficiency and effectiveness of next-generation firewalls by using threat intelligence to block known threats before they hit the firewall freeing the firewall to focus on more advanced threats.

Medium Sized/Regional Hospital Systems

Due to HIPAA regulations, Information Systems, and the very present danger of cyber threats, these healthcare organizations will have more resources dedicated to cybersecurity budgets than other sector organizations of this size. However, they may still be challenged with operationalizing large volumes oforganizations of this size. However, they may still be challenged with operationalizing large volumes of threat intelligence. These organizations need a threat intelligence solution that is smart, simple, scalable, and everywhere.

With over 20 small and mid-sized healthcare clients, Threater Enforce:

- Provides powerful, day-one protection with over 30 million "out of the box" threat intelligence indicators from best-in-class providers (DomainTools, Proofpoint, open source, government (DHS), and industry (H-ISAC).
- Easily integrates threat intelligence from any source: custom Deny List, open source threat feed, SIEM. Saves time by eliminating the need to manually manage threat feeds and external blocklists.
- Delivers an automated, easy to deploy and manage solution on-prem and in the cloud.
- Complements and increases the ROI of existing firewall investments.

Contact Threater for a Free Risk Assessment

TRY FOR FREE