Your Security Stack's Gaps & How To Close Them

Solution	What They Do	Solution's Limitations	How Threater Fills the Gaps
Firewall	• Sits left of boom, meant to inspect and filter traffic before it hits the network • Performs deep packet inspection (DPI) on the packets for malicious activity	• Limited threat intelligence: proprietary, solitary view, and limited in how much external intelligence they can ingest • Bogged down by encrypted traffic • Outbound traffic filtering is limited and difficult, if configured at all	✓ Ingests cyber intelligence from 50+ best-in-class intelligence feeds to enforce upon ✓ IP filtering through patented Bloom filter allows for removal of known bad traffic at line speed ✓ Inbound and outbound traffic checked and enforced with equal ease ✓ Can decrease utilization needs of firewalls
SIEM	• Monitoring and management tool • Provides alerts of suspected malicious activity already happening within the network	• Requires massive amounts of bandwidth to run and analyze the network traffic • Non-enforcement: only provides alerts for other tools • Need a lot of full-time, specialized resources to manage and run due to alerts, causing burnout and alert fatigue for staff • Expensive (software, hardware, storage, ingest, personnel) • Mostly focused on on-prem network configurations	✓ Decreases the amount of packets to monitor by removing known-bad traffic ✓ Reduces alerts as the SIEM is no longer tasked with unnecessary malicious traffic ✓ Enforcement of known-bad traffic before it hits the other network tools and technologies ✓ Does not require additional staff to manage
SOAR	• Orchestration tool that automates security rules and actions • A way to reduce alerts from the other tools and make sense of them	• Complex implementation • Cannot work without a SIEM • Configuration issues are common • Requires skilled and specialized full time employees (FTEs) to manage	✓ Does not require additional staff to manage ✓ Agnostic: does not require any specific brand or other technology to operate
TIP	• Stands for "Threat Intelligence Platform" • Feeds other tools threat intelligence	• Cannot enforce in and of itself, only provides intelligence • Still a limited, proprietary view of the threat landscape (curated by the TIP) • Can be difficult to integrate with other tools • Requires lots of maintenance and management by FTEs	✓ Can utilize intelligence from TIPs as well as other cyber intelligence feeds and sources ✓ Also enforces against bad traffic at the network level ✓ Integrates easily with other tools to receive and provide data ✓ Runs and updates autonomously without the need for monitoring by FTEs

threater

Your Security Stack's Gaps & How To Close Them

Solution	What They Do	Solution's Limitations	How Threater Fills the Gaps
XDR/EDR/ MDR	• Detect malicious activity based on signatures • Look at the threats themselves, not where they're going (i.e., the payload) • Provide forensics information in case of incident or breach • Throw alerts about suspected malicious activity in the network	• Reactive to threats already in the network • Requires teams of FTEs to manage • Expensive to manage (especially in the case of MDRs that are priced based on ingest) • Reliant on the level of human talent tasked with managing and investigating the alerts and logs • Produce large amounts of alerts (causing alert fatigue and mistakes from staff) • Bandwidth and latency issues	✓ Removes known bad traffic before it enters or leaves the network, reducing the amount of activity to monitor by these solutions ✓ Sits left of boom, preventing attacks instead of remediating them after they have happened ✓ Reduces bandwidth requirements of these solutions
DNS Filtering	• Web-based filtering of domains • Uses intelligence to figure out which domains are malicious • Covers from the POP (point of presence) to the customer's network	• Only looks at web traffic (HTTP) • Only one vendor's intelligence view of the threat landscape • There are a lot of other ports and protocols that can be exploited than just web traffic, even as the amount of web traffic is growing	✓ Utilizes DNS feeds as well as other lists, feeds, and sources ✓ Protects against all ports and protocols, not just HTTP, such as FTP (used in the MOVEit attacks) and RDP attacks
Secure Web Gateway	• Proxy that is mostly endpoint protection • Only ports 80 and 443 (internet) • Cloud firewall you can access anywhere	• Only looking at web traffic (which wouldn't have helped with MOVEit attacks that used FTP, not HTTP) • All DNS-based • Mostly signature-based • Looking for the threats, not the actor • Often not agnostic and requires integration with other brand-specific tools/technologies, limiting cyber intelligence intake	✓ Does not require monitoring of every single endpoint device to work since it protects at the network layer ✓ Focuses on the threat actor, not the quickly-changing threats themselves ✓ Protects against all ports and protocols both inbound and outbound, not just HTTP ✓ Can protect networks, on-prem, in the cloud, or hybrid configurations

threater