TerraFlow Intelligence Guard

Threat-Intelligence-Driven Perimeter Defense in the Age of Encryption

1. Defense in Depth and Perimeter Threat Detection

Enterprise security follows a defense-in-depth model. At the Internet perimeter, firewalls primarily enforce access policy based on IP addresses, ports, protocols and connection state, while IPS and next-generation firewall (NGFW) systems inspect allowed traffic for malicious content. If threats cross the perimeter, NDR, EDR and SOC operations provide additional detection and response.

Consider malware delivered over unencrypted HTTP. A firewall may see only an allowed web connection, while an IPS or NGFW can parse the HTTP session, reconstruct the file, compare its hash with known malware, or submit it to a sandbox.

When traffic content is visible, IPS and NGFW systems can therefore detect and block malware delivery, exploits and other malicious content at the network perimeter.

2. Encryption Weakens Content-Based Perimeter Detection

Content-based perimeter detection depends on the ability to inspect the original traffic content. Today, most Internet traffic is encrypted. HTTPS protects HTTP content with TLS, while HTTP/3 runs over QUIC.

When malware delivery moves from HTTP to HTTPS, IPS and NGFW systems can still observe IP addresses, ports and selected TLS or QUIC metadata, but they can no longer directly reconstruct the original file. File-hash matching, sandboxing and payload-based signatures are therefore limited, while exploit content, C2 commands and exfiltrated data become more difficult to identify.

TLS interception can restore visibility for selected traffic, but it introduces performance overhead, privacy concerns, certificate-management complexity and application-compatibility issues, making universal deployment difficult.

Encryption does not make IPS or NGFW systems ineffective, but it materially weakens threat-detection functions that depend on plaintext content. Threats that pass the perimeter must then be detected by downstream controls such as NDR, EDR and SIEM—often after malicious activity has already begun inside the enterprise.

3. Perimeter Defense: Containing Attacks Before Damage Escalates

Once attackers gain initial access, they may perform internal discovery, credential theft, privilege escalation, lateral movement and C2 communication while expanding control.

The best outcome is to stop malware delivery or exploitation before compromise. Even after malware lands, however, attackers typically still need C2 infrastructure to receive instructions, download additional tools or return results. Disrupting malware-delivery sites or C2 communication can therefore contain an attack before the damage escalates.

Enterprises consequently need perimeter controls that do not depend on plaintext traffic inspection, preserving an early intervention point during both Initial Access and Command and Control.

4. Why Reused Attack Infrastructure Makes IP and Domain IoCs Valuable

Attackers optimize their infrastructure for operational efficiency. As long as existing tools and resources remain effective, there is a strong incentive to reuse them.

IP addresses used for scanning, brute-force attempts, proxies, bots or C2 nodes may continue supporting multiple attacks. An IP previously associated with malicious activity is therefore more than a historical record; it may appear again in future attacks.

Domains provide even greater continuity. Internet services normally use domains as stable service names while backend IP addresses remain changeable. The same property benefits C2 infrastructure. If a C2 IP is blocked or a server is removed, the attacker can deploy a new backend and point the existing domain to it. Malware that already knows the domain can continue locating C2 without being modified simply because the IP address changed.

Attackers also prefer to change characteristics that are cheap to alter. A file hash can be changed by recompiling malware or making minor modifications. Replacing IP and domain infrastructure generally requires additional acquisition, DNS configuration and operational changes, making them less disposable than file hashes.

IP addresses and domains also remain observable under encryption. The remote IP address is directly visible, and domains are normally available through enterprise DNS activity. By contrast, obtaining the hash of a file delivered over HTTPS requires access to decrypted content.

IP and domain IoCs therefore combine operational persistence with visibility under encryption, making them particularly useful for network defense. When threat-intelligence providers identify and update these IoCs, one organization's attack experience can become another organization's preventive control.

5. From IoC Lists to Real-Time Defense

Many IPS and NGFW platforms already support IP reputation, domain filtering or external IoC lists. The challenge is not simply whether a device can import IoCs, but whether it can operationalize them at scale.

A production system must support millions of IP and domain IoCs, update them continuously, and perform real-time matching, alerting and blocking at high traffic rates. It must also manage allowlists, remove expired IoCs and maintain event records.

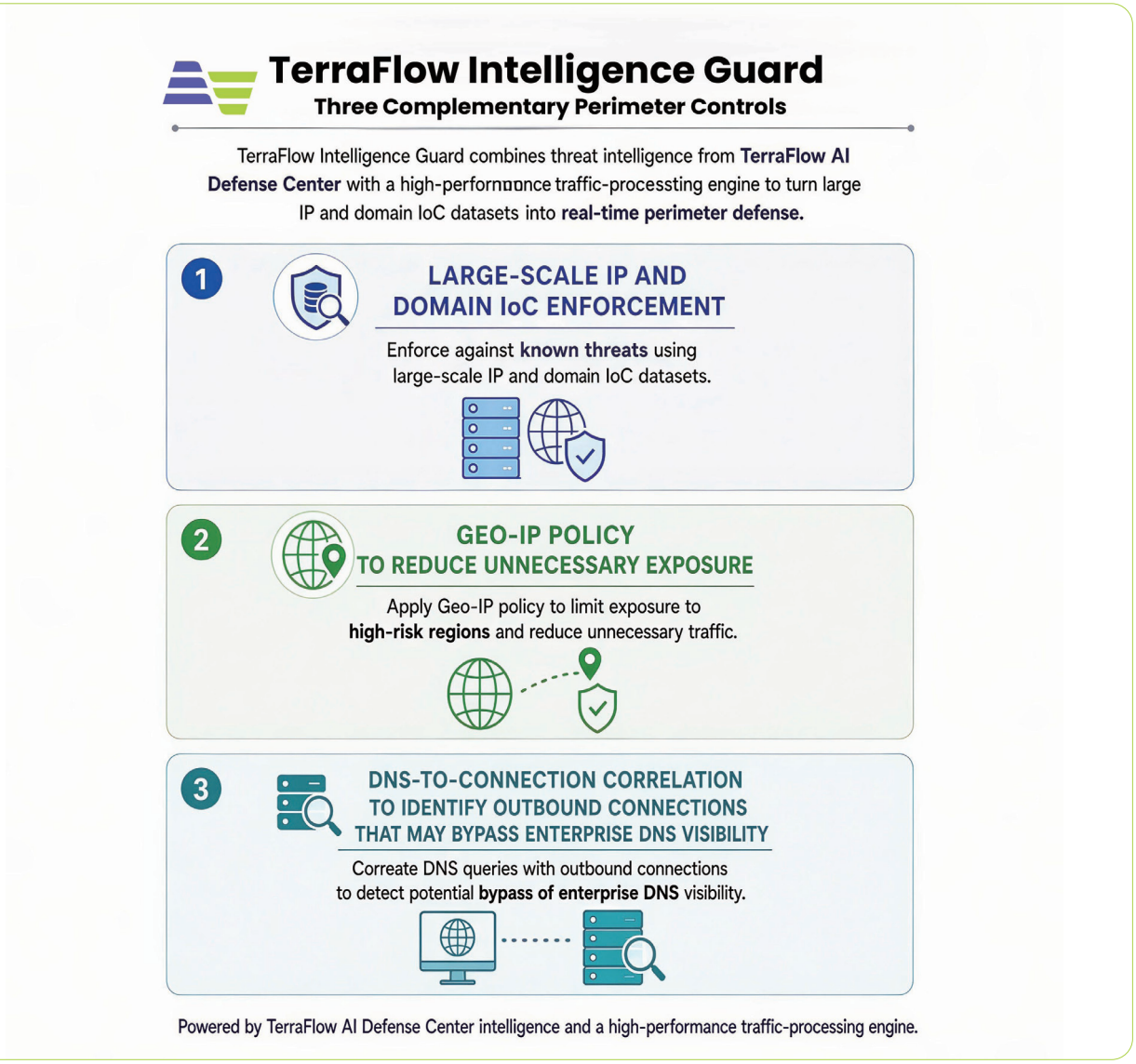
Limited capacity reduces threat coverage, while slow updates waste the period during which an IoC remains defensively useful. Large-scale threat-intelligence defense therefore requires a purpose-built mechanism that complements existing IPS and NGFW platforms.

TerraFlow Intelligence Guard: Three Complementary Perimeter Controls

TerraFlow Intelligence Guard combines threat intelligence from TerraFlow AI Defense Center with a high-performance traffic-processing engine to turn large IP and domain IoC datasets into real-time perimeter defense.

Its three core controls are:

- Large-scale IP and domain IoC enforcement against known threats
- Geo-IP policy to reduce unnecessary exposure
- DNS-to-connection correlation to identify outbound connections that may bypass enterprise DNS visibility



1. Blocking Known Threats with Threat Intelligence at Scale

TerraFlow supports millions of IP and domain IoCs and applies them to inbound and outbound traffic for real-time matching, alerting and blocking.

For inbound traffic, it can block source IPs associated with scanning, brute-force attempts, botnets and other malicious activity, reducing exposure of public-facing services to known hostile infrastructure.

For outbound traffic, it can prevent endpoints from reaching known malware-delivery sites, phishing sites and other malicious services, and cut communication between infected endpoints and known C2 infrastructure.

TerraFlow determines whether a connection involves a known IoC rather than attempting to identify the real-world attacker. Its value lies in turning continuously updated intelligence into enforceable perimeter controls without depending on plaintext traffic inspection.

2. Reducing Unnecessary Exposure with Geo-IP Policy

IoCs cover threats that have already been discovered and recorded; they cannot represent every unknown or unlisted source.

Where an enterprise has no business need to exchange traffic with a particular country or region, TerraFlow can apply allow, block, alert and exception policies based on source or destination geography, reducing unnecessary exposure beyond known IoCs.

Geo-IP is an attack-surface-reduction control, not a claim that a country, region or IP address is malicious. Policies should account for VPNs, proxies, cloud platforms, CDNs and legitimate international business, with appropriate allowlists and exceptions.

3. Using DNS-to-Connection Correlation to Expose Concealed Destination Domains

Advanced attacks may hide the true location of C2 infrastructure to evade IP or domain IoC matching. Fast Flux can rotate the IP addresses associated with a C2 domain, while encrypted DNS such as DoH or a Dead Drop Resolver can conceal how malware obtains the real C2 address, allowing the C2 domain to bypass enterprise DNS monitoring and domain-IoC controls.

TerraFlow builds relationships between observed domains and resolved IP addresses from DNS queries and responses that traverse the device. If an endpoint later connects to an IP that has not appeared in the observed DNS-resolution history, TerraFlow can alert or block according to policy. In an enterprise that requires endpoints to use designated DNS services, such a connection should be treated as a high-risk anomaly requiring priority investigation.

Traditional firewalls, and even IPS or NGFW platforms with anomaly-detection capabilities, do not typically correlate DNS-resolution results with subsequent IP connections on a per-connection basis. Malware that obtains a C2 address through DoH, a Dead Drop Resolver or another bypass method may therefore appear as an ordinary outbound IP connection. The organization may fail

to recognize that the true destination has moved outside its normal DNS monitoring and domain-IoC controls, increasing the risk that an infected endpoint can maintain C2 communication without detection.

By correlating DNS activity with subsequent IP connections, TerraFlow exposes these otherwise difficult-to-see connections at the enterprise perimeter and identifies the internal endpoint that initiated them, enabling earlier alerting, blocking and investigation.

Conclusion

Encryption has changed what security devices can observe at the network perimeter. Enterprises can no longer depend entirely on payload inspection, nor should they wait until an attack has spread internally before responding.

TerraFlow Intelligence Guard combines large-scale IP and domain IoC enforcement, Geo-IP exposure reduction and DNS-to-connection correlation to strengthen early detection and blocking at the perimeter without requiring universal traffic decryption.

Every disclosed attack should become defensive knowledge that the next organization can use—not simply a warning of the next attack to be repeated.

Technical Specification

Product	Terra 1G	Terra 10G
Network Interface	1G RJ-45 x 8	10/1G SFP+ x8
Hardware Bypass	1G RJ45 pair x2	10G MM pair x2
Management Interface	1GbE RJ45x1,HTTPS TLS 1.2/1.3,CLI,XML over sFTP	
System Console	SSH	
Network Management	SNMPv2c,SNMPv3	
Meta Extraction	DNS log/Netflow	
IoC(IP/Domain) Capacity	1M	3M
Power Supply	Single Power 100W100-240VAC	Dual Power 150W 100-240VAC
Operating	0~40°C	0~40°C

TERRAFLOW

www.terraflowtech.io

© 2026 Terraflow Networks. All rights reserved.
Terraflow Networks makes no representations or warranties regarding the accuracy or completeness of the information contained in this document and assumes no liability for any errors or omissions. Terraflow Networks reserves the right to update, modify, or revise this document at any time without prior notice.

Address
2nd Floor, No. 12, Zhouzi Street,
Neihu District, Taipei City

TEL
0952-393-228

Sales
contact@terraflowtech.io