PacketViper Extends Geographic Threat Intelligence to Organization-Level Filtering and Active Defense

PacketViper identifies the organization behind every IP, integrating geographic intelligence with inline enforcement and OFAC compliance.

Always on, Always Watching

PITTSBURGH, PA, UNITED STATES, April 8, 2026 /EINPresswire.com/ -- PacketViper announced expanded geographic threat intelligence capabilities that identify the organization behind an IP address, not just its country of origin, and integrate that intelligence directly with inline enforcement and automated deception.

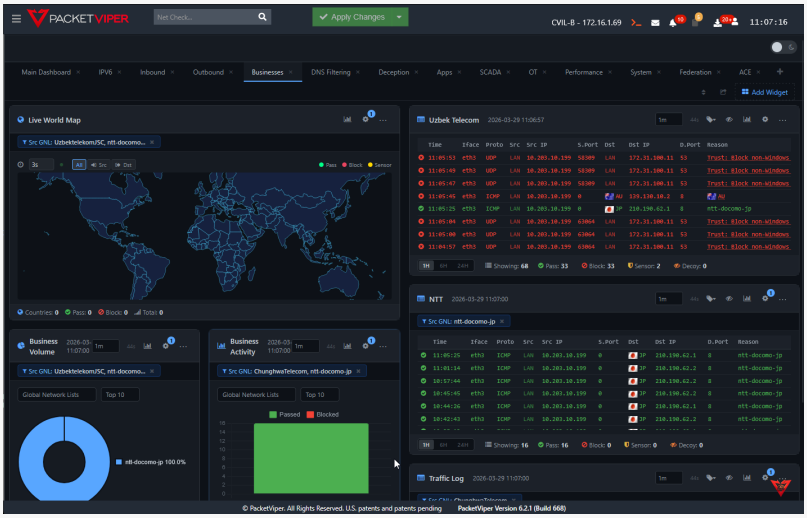
Traditional firewalls treat geography as a binary decision: block a country or allow it. That approach cannot distinguish between a trusted enterprise and a malicious hosting provider operating inside the same country. It also cannot address a practical reality most security teams face: the countries that represent the highest threat are often the same countries where cloud providers, business partners, and employees operate. In practice, most geographic policies restrict a handful of politically sensitive countries while leaving the majority open.

> Traditional firewalls see flags. PacketViper sees ownership."
>
> *Don Gray, CTO*

Attackers understand this. They route through infrastructure inside permitted regions and leverage cloud platforms in allowed countries specifically because country-level blocking stops at the flag.

PacketViper's Global Network List maps organizations to their IP ranges, business classifications, risk, network behavior profile and country presence. When traffic reaches a PacketViper-

protected network, the platform identifies the organization behind the address. Operators can block a specific hostile hosting network without blocking its entire country, allow trusted cloud providers within otherwise restricted regions, and filter VPN and proxy infrastructure independently of geography. The platform also detects businesses that move laterally through the environment from a boundary, tracking organizational identity as traffic shifts across addresses and network paths.



More than a Flag

Geographic policies in PacketViper apply inbound, outbound, or bidirectionally with port-level precision. Time-based controls support temporary restrictions during active incidents and revert automatically when the event window closes.

The platform integrates geographic intelligence directly with its Automated Moving Target Defense system. Deception strategies can be targeted at specific countries, organizations, or rotating geographic groups. When reconnaissance traffic interacts with a deceptive responder, PacketViper captures attacker behavior, identifies the originating organization, and can automatically block the source network.

OFAC-designated countries are automatically identified and flagged within the platform. Operators can apply bidirectional blocking, deploy monitoring sensors, and export geographic policy documentation for compliance audits.

The advisory issued this morning by the FBI, CISA, NSA, EPA, Department of Energy, and US Cyber Command confirming active Iranian attacks against water and wastewater infrastructure underscores why organization-level geographic intelligence matters. Country-level blocking alone would not have stopped infrastructure hosted inside permitted regions. Knowing the organization behind the address does.

All filtering, organization-level identification, deception integration, and enforcement operate inline on PacketViper's packet engine, validated at sustained rates exceeding 400 million packets per hour on standard x86 servers.

PacketViper is deployed across critical infrastructure, enterprise, and OT environments in the United States.

About PacketViper

PacketViper delivers automated moving target defense and inline network security for IT and OT environments. No agents. No cloud dependency. Learn more at packetviper.com.

Tim Jencka
PacketViper, LLC
+1 412-212-6348
email us here
Visit us on social media:
LinkedIn
X
