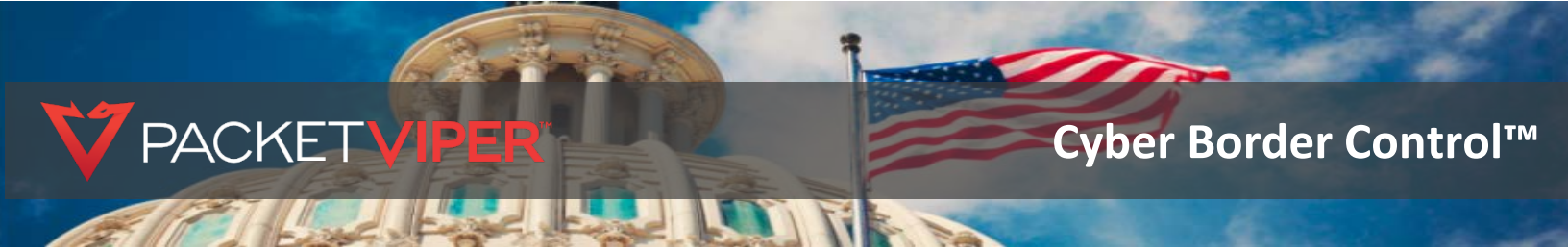


Proactive Cybersecurity Solutions for US Federal & SLED Organizations

PacketViper's dynamic threat defense platform allows users to continually deceive attackers, gather intelligence on threats and apply that intelligence to strengthen defense in a consistent and automated fashion.

PacketViper is a network security application that sits as an undetectable in-line bridge in front of the firewall and between network segments. This allows users to bring proactive cyber defense tactics to the network perimeter.

- **An in-line solution.** Deploying an integrated deception, defense and intelligence plan into a layered security approach provides a practical and cost-effective means to proactively strengthen cybersecurity.
- **Multiple deployment options.** Deploy PacketViper on-premise or in the cloud across the enterprise
- **Enterprise management.** Multiple instances of PacketViper can be centrally managed

Network modernization without the costly and disruptive 'Rip & Replace'

PacketViper is extremely cost effective and prolongs the useful life of firewalls, NGFWs, SIEM, IDS & IPS. Consumption and utilization based costs associated with these popular security solutions can be greatly reduced when PacketViper cuts as much as 70% of the illegitimate network traffic.

Fully Integrated Deception, Organic Intelligence and Dynamic Defense

With PacketViper, **dynamic network defense** and simplified IP traffic management is handled with 'point & click' simplicity both inbound and outbound. This greatly reduces the load on the firewall, IDS/IPS & SIEM and makes the network much harder to see for attackers.

- **Geo-targeting.** Easily geo-target and align IP traffic with the agency mission by performing precise filtering based on business intelligence, threat intelligence and custom rules.
- **Dynamic Perimeter.** The Virtual Minefield Zone™ (VMZ) can automatically change the access rules around any port or service and rotate when they are turned on or off, creating a dynamic perimeter. This is much different than the static front of typical firewalls an NGFWs.

PacketViper's **perimeter based deception** offers significant complementary benefits to interior deception. PacketViper offers deception in all directions, which we call Deception360. This includes internal and perimeter deception that we link together.

- **Recon Stage Deception**. PacketViper is extremely effective against reconnaissance type/NMAP scans because deception at the recon stage of the deceptive/response kill chain is highly effective.
- **Nothing to breach.** PacketViper Deception360 is very lightweight, easy to deploy and generates truly believable responses requiring no agents, workstations or honeypots.

PacketViper's deceptive efforts yield volumes of **organic threat intelligence**. Sources for threat intelligence are everywhere but applying it can be challenging. PacketViper makes threat intelligence easy to capture and operationalize.

- **Automated applied intelligence.** New intelligence is easily operationalized and applied in an automated, ongoing manner to consistently keep updating defense in real time.
- **Organic intelligence.** Harvest new intelligence based on what is actually happening within, and on the perimeter of, the networks while easily integrating it into their perimeter defense strategies.

Unique Benefits:

Deception

- Interior & perimeter focus
- Lightweight with no agents, workstations or honeypots
- Especially effective against reconnaissance scans

Defense

- 70% less traffic, logs & alerts
- 'Point & click' geo-targeting and country, company and network level filtering
- Works inbound & outbound

Intelligence

- Easily operationalized and applied
- Integrated with perimeter defense
- Forensics and reporting

Also featuring centralized enterprise management.

CONTACT US: 855.758.4737 | www.packetviper.com | PacketViper, LLC. 40 Center Ave. Pittsburgh, PA 15229

Compliance with FISMA and Specific NIST 800-53 Cybersecurity Control Recommendations

The Federal Information Security Management Act of 2002 (FISMA) requires organization-wide security programs for systems and data. Implementing PacketViper Cyber Border Control™ (CBC™) solutions is one of the most proactive, high-impact and cost-effective moves that federal & SLED agencies can make to improve network security and strengthen boundary defense in a manner that is consistent with NIST network security control guidelines.

PacketViper Cyber Border Control™ provides practical, easy to implement, high impact solutions that are well aligned with the NIST Framework Core Functions:

- **Identify** - CBC™ solutions make it easier to identify threats that are attempting to either enter or leave the network.
- **Protect** – Stop harmful connection based DDoS and flooding attacks using time and rate based sensors & bi-directional port level filters.
- **Detect** – Detect threats early by capturing and eliminating network scans and service probes.
- **Respond** – Respond to unconventional traffic patterns based on advanced analytics and edge intelligence.
- **Recover** – Reduce the time to recovery by identifying threats faster at border/network edge.

PacketViper CBC™ solutions provide particularly strong support of the following specific cybersecurity controls:

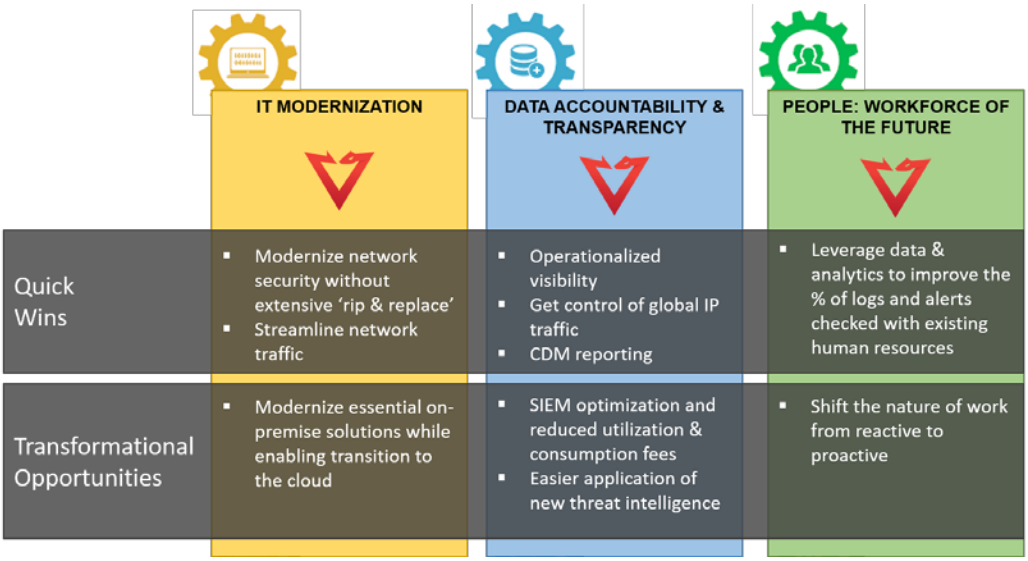
Limitation and Control of Network Ports, Protocols & Switches
(NIST Special Publication 800-53 r4 Controls: AT-1,2,3,4 | SA-11,16 | PM-13,14,16)

Boundary Defense
(NIST Special Publication 800-53 r4 Controls: AC-4,17,20 | CA-3,7,9 | CM-2 | SA-9 | SC-4,7 | SI-4)

Supporting the President's Management Agenda (PMA)

PacketViper can help US federal agencies and commissions support the President's Management Agenda.

Users can score both quick wins and transformational opportunities in the areas of IT Modernization, Data Accountability and Transparency and People.



A valuable Continuous Diagnostics and Mitigation (CDM) Phase 3 tool

PacketViper can be a valuable tool to US federal and civilian agencies leveraging CDM to better manage and secure their information systems. PacketViper's Virtual Minefield Zone (VMZ) can add particular value to boundary protection efforts.

About PacketViper

PacketViper is a leading provider of integrated cybersecurity deception, defense and intelligence solutions. Our threat defense platform & integrated approach to deception, defense and intelligence helps customers do more with existing resources while reducing cybersecurity related risks and costs. PacketViper customers are in both the public and private sector and cover multiple industries.