PACKETVIPER®

DATA SHEET

Cybersecurity Deception Technology

Lightweight deception. Heavyweight results.

Overcoming the practical limitations of deception

The historical goal for deception technologies has primarily been detection. The value of deception solutions focused on amplified detection and higher fidelity alerts has been questionable in this era of alert fatigue. These technologies have an unappealing prerequisite - that the attacker is already on your network.

PacketViper is a cybersecurity deception technology that overcomes the limitations of alternative deception solutions to solve critical cybersecurity problems.

Lightweight deception in all directions

PacketViper deception technology is a unique approach to security that changes the security paradigm towards more proactive cyber defense. PacketViper deploys believable, agentless, decoys and responses both at the perimeter and the interior of the network to lure and ultimately defeat attackers.

These software-based decoys and sensors are not services that can be exploited for use against the host. They perform a brief interaction and generate a quick revealing reaction from the attacker. This intelligence is automatically gathered and applied to strengthen defense. PacketViper can either be deployed out of band or in-line.

Start deceiving when attackers start scanning

All attacks start with an NMAP or reconnaissance scan. At this stage, while lurking and planning their approach, attackers have the advantage of anonymity. PacketViper deception at the perimeter proactively exhausts attacker's assets and kills the desired attack vector while stripping their anonymity. PacketViper does this by uniquely pushing deception to perimeter and mimicking applications response during the attacker's most vulnerable time, the reconnaissance stage of the attack.

Features & Benefits

Lightweight Deception

- Agentless
- Software based decoys and responses
- Not a honeypot
- Dynamic
- Believable responses
- Enterprise capable

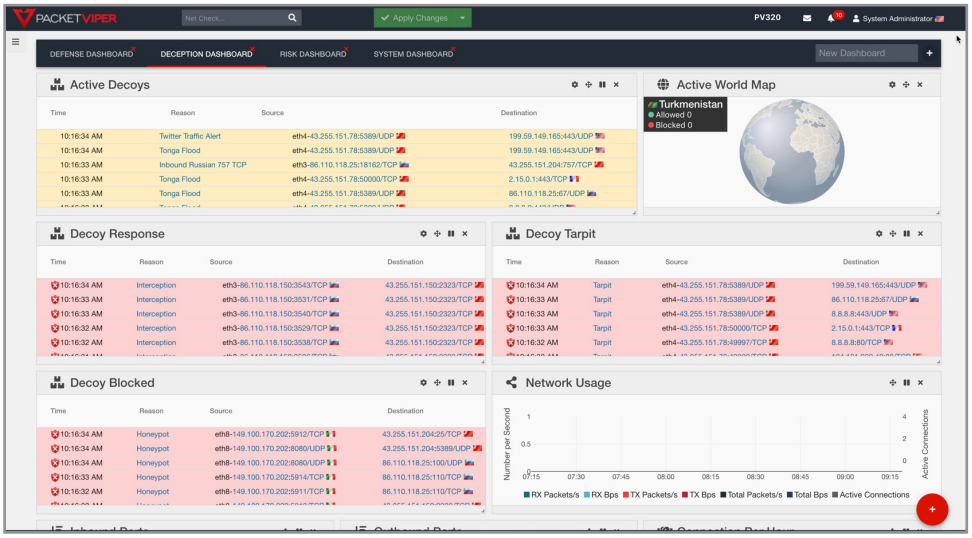
Heavyweight Results

- Solves critical problems
- Pushes deception to the network edge
- Produces intelligence
- Automated actions
- Policy enforcement

How it works

Deception dashboard

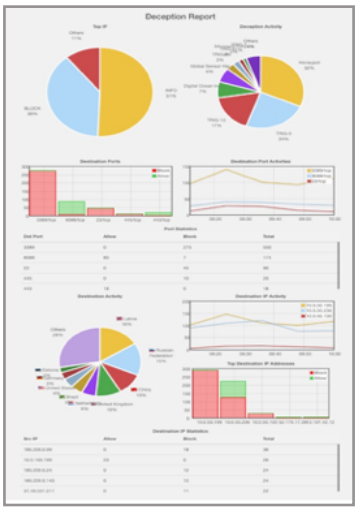
Network deception provides a better method for securing your infrastructure at the source rather than after a breach. We move the deception perimeter based on time, geo-target, business, protocol, or port to further confuse the attacker's plans, while at the same time blocking each new probe source in real-time. PacketViper also addresses the insider threat, curious employees, or malware that are exploring the inside of your environment.



With business and country granular control, PacketViper can eliminate as much as 70% of the volume of traffic entering the environment.

Reporting

A highly customizable report is available and key to your reporting structure. One of the most sought after details in security tools today, PacketViper delivers an easily digested visual for your executives.



Enhanced dynamic defense, relief of security operational costs and burdens, and 3rd party risk monitoring all in one.

30 DAY RISK-FREE TRIAL

No Money Down. RISK FREE Satisfaction Guaranteed

Try all the PacketViper features for thirty days risk free.

Get full functionality and see the difference deception can make for your organizaiton.

See for yourself.

About PacketViper

PacketViper is cybersecurity deception technology featuring a lightweight deception that produces heavyweight, practical results including dynamic network defense, relief of security related operational costs and burdens, and 3rd party risk monitoring with real-time policy enforcement.

Contact Us Today

Call: 855-758-4737

Email: info@packetviper.com