PACKETVIPER®

PRODUCT BRIEF

Deception360™

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.

Internal decoys detect and respond to threats moving laterally within the network with no false positives. Threats are automatically stopped from exfiltrating data or establishing command and control communications. External decoys create the appearance of a moving target at the network edge. A dynamic perimeter makes the network harder to size up and keeps threats off the network. This approach complements the traditional security stack while eliminating the attacker's ability to operate anonymously and severely limiting global attack vectors.

Start deceiving when attackers start scanning

Many 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 the perimeter and mimicking application responses 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

- Prevents threats
- Pushes deception to the network edge
- Produces intelligence
- Automated actions
- Policy enforcement

How Deception360™ Works

A Practical Approach to Deception

The PacketViper Deception360 solution uniquely blends the use of deception internally for threat detection with external deception for threat prevention. When threats hit a PacketViper decoy, either internally or externally, a series of adaptive responses can be automatically enacted straight from PacketViper and without complex orchestrations. 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. External threats are kept off of the network and internal threats are prevented from establishing command and control communications or exfiltrating data. This combination of internal and external deception produces practical results.

> Manager of IT
>
> **Outstanding and reliable!**
>
> "We've been extremely happy with the product and even more importantly, the support from the Packet Viper team! We know first hand how the product has helped to drastically reduce our risk and is key to our multi-layered security strategy."

Deception "flips-the-script" on attackers by using their own curiosity and capabilities against them. Rather than looking at "big data", deception is focused on gathering the "right data" to efficiently identify malicious actors. Zero-false-positive threat intelligence is applied in real-time to enable automated responses including the ability to stop attackers in their tracks.

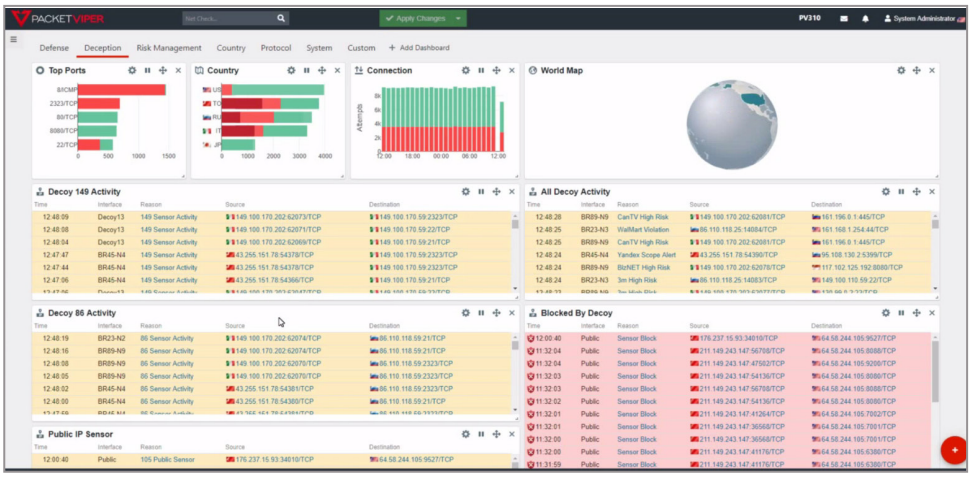

Figure 1. Deception dashboard sample from PacketViper.

Cyber Defense

The use of decoys along with environmental lures and honey tokens provides a proactive way of detecting and identifying threats to your external and internal networks before they become a full-fledged attack. Prevention of escalation through the Cyber Kill Chain® provides a robust defense for your critical assets.

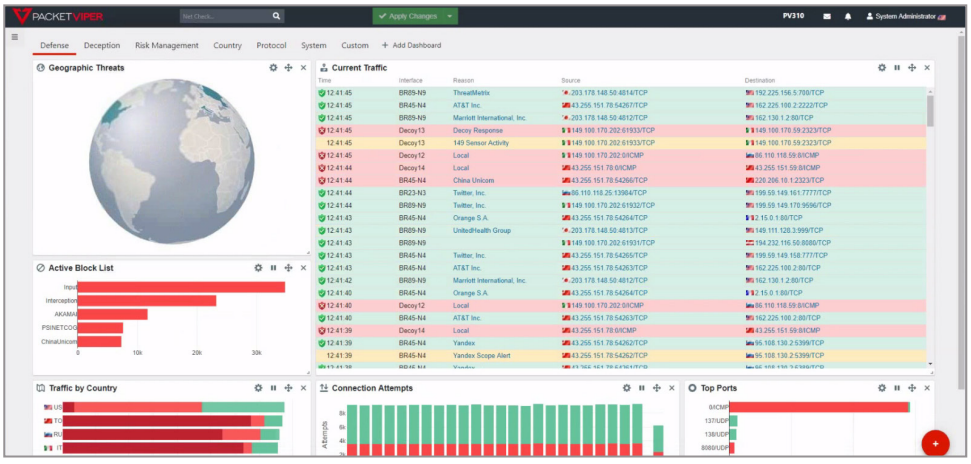

Figure 2. Defense dashboard sample from PacketViper.

Shortest Time to Greatest Value

PacketViper Deception360 allows people to derive immediate value from deception due to the unique combination of prevention, detection and the ability to respond without complex orchestrations. Figure 3 below compares PacketViper Deception360 to more traditional internal, detection only deception solutions. Traditional deception solutions tend to be costly, complex and require highly sophisticated teams to be effective. Even with all of that in place, the time to realize value is prolonged. Conversely, PacketViper Deception360 is extremely cost effective, lightweight in nature and delivers immediate, measurable benefits.

CTO Don Gray

"External threats are kept off of the network and internal threats are prevented from establishing command and control communications or exfiltrating data."

"Time to Greatest Value" Comparison of Deception Solutions and Use Cases

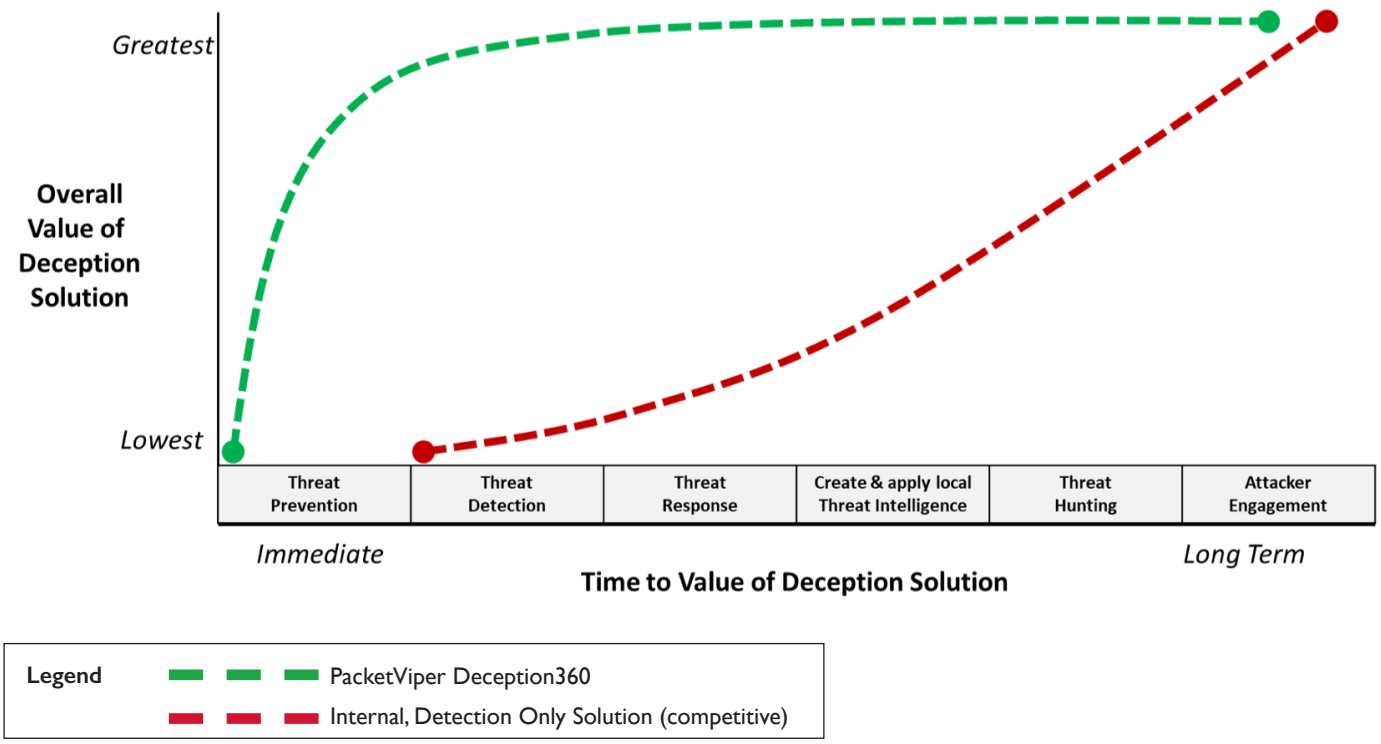

Figure 3. Time to greatest value deception comparison.

About PacketViper

PacketViper is a cybersecurity deception technology company 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