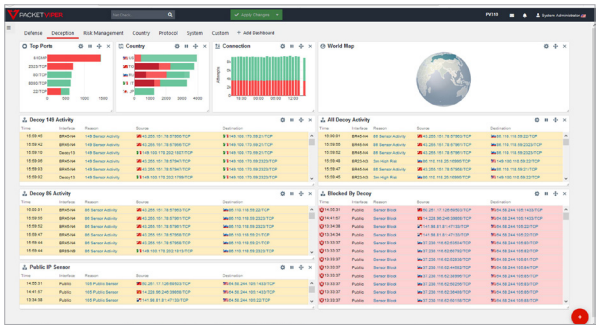
PacketViper
Deception360 v5.0



DETAILS

Vendor PacketViper, LLC

Price $20,000 MSRP annual subscription fees for a single standard deployment

Contact packetviper.com

Features	★★★★★
Documentation	★★★★★
Value for money	★★★★★
Performance	★★★★★
Support	★★★★★
Ease of use	★★★★★

OVERALL RATING ★★★★★

Strengths PacketViper works on the perimeter as well as inside the environment. This dynamic perimeter makes the network harder to size up and subsequently keeps threats off the network, functionally complementing the traditional security stack while eliminating the attacker's ability to operate anonymously.

Weaknesses None that we found.

Verdict PacketViper is an active, agentless deception solution combining internal deception with active exterior facing artifacts. Action taken early in the kill chain detects, prevents and responds to threats automatically without the need for complex orchestrations.

PACKETVIPER

https://www.packetviper.com
E: info@packetviper.us
PH: 855-758-4737

PacketViper is an active, agentless deception solution that combines internal deception with active, exterior-facing artifacts. It takes action early in the kill chain to detect, prevent and respond to threats automatically without the need for complex orchestrations. Decoys are lightweight, software-based and easily deployed. Internal decoys sit laterally within the network and yield virtually zero false positives.

The solution automatically stops threats from exfiltrating data or establishing command and control communications. External decoys create the illusion of moving a target at the edge of a network. PacketViper works on the perimeter as well as inside the environment. A dynamic perimeter makes the network harder to size up and subsequently keeps threats off the network, functionally complementing the traditional security stack while eliminating the attacker's ability to operate anonymously, which severely limits global attack vectors.

PacketViper sits in front of the firewall as well as between it and the switch. The deception traps act as devices on the network and detect traffic anonymously. The software configures decoys and sensors as it sees fit.

A deception solution needs a lot of points of interest inside an environment. Easy cabling deployment puts PacketViper at an advantage. Organizations can connect as frequently as they like. One PacketViper can handle multiple WAN interfaces and reduces traffic, helping to secure the number of blind spots and making it a truly comprehensive solution. PacketViper can communicate with one another as attacker hosts are identified.

It aims to identify and terminate connections to compromised systems as well as access outbound. The deception response uses low interaction haptics, with decoys detecting probes and responding in time with configured responses. Once detected, the source is immediately blocked.

PacketViper creates attractive false records. The goal is not to keep attackers there to understand them, but rather to identify the threat and take action. The solution can also place RDP and FTP services inside the environment. It uses key connection attributes to confuse attackers. Creating decoys and sensors based on attributes adds to the confusion. Deception, which keeps attackers on edge and prevents them from ever understanding the perimeter, is limited only by user creativity.

Resources can move decoys around to make the environment appear dynamic to confuse attackers. As attackers lose assets, they are blocked and repositioned to a different proxy, jeopardizing their anonymity. The tool batters and applies real-time intelligence to keep pace with the attackers, regardless of how quickly they are moving. We were impressed with this capability.

Dashboards offer insight into how defensive measures are working based on attributes to understand where the points of interest are and what their associations. PacketViper offers top-notch reporting and analytics. Security teams can select any decoy to view an associated traffic report.

PacketViper also can serve as a vendor risk management tool and wrap deception around known connections to determine any issue with a known vendor, allowing organizations to monitor vendors connecting to the network.

Starting price is $20,000 annual subscription fees for a single standard deployment. Standard and premium support options are available.

— Katelyn Dunn
Tested by Tom Weil