PACKETVIPER®

Product Brief

Deception360

Deception-based threat detection, prevention and response

Next-generation deception

PacketViper's Deception360™ is cybersecurity software that actively defends networks with deception-based threat detection and automated response to both external and internal cyber threats.

Deception360 is a transformative and trusted cybersecurity solution for organizations seeking to cost-effectively defend converging Operational Technology (OT) and Information Technology (IT) networks and modernize cybersecurity without a 'rip and replace'.

Deception360 provides measurable cybersecurity outcomes that improve OT/IT security, preserve OT process uptime and streamline security operations unlike anything else in the market.

Deception-powered use cases

Simply put, we use deception in a couple of powerful ways to drive security outcomes that make a difference.

First, we stop the threats outside your network from getting in. At the network boundaries Deception360 brings the principles of a moving target defense, making the network hard to understand during reconnaissance. This is true for both external gateways and OT/IT boundaries.

Then for threats on the network, we entice them to reveal themselves so that we can reduce their effective dwell time and take action to eradicate them.

A summary of our use cases includes the following:

- Internal threat detection
- Boundary defense & threat prevention
- Automated threat response
- Threat hunting
- Vendor risk management (VRM)
- Ransomware & DDoS prevention
- Firewall and SIEM optimization
- Compensating control/ critical asset fencing

Not a honeypot

Our deception-based approach is disruptive and makes practical sense. Deception is a dynamic mainstay for attackers who use it to trick us into revealing information that increases their probability of success. In turn, we respond with mostly static, insufficient defenses.

Deception360 turns the tables on threats at the earliest stages of their attack cycle, greatly increasing the difficulty of their attack at initial reconnaissance. Threat detection is equally effective against known and unknown threats.

Other deception solutions are costly and complex while only offering the single use of internal (on-network) threat detection. Alternative technologies like firewalls, SIEM and endpoint solutions are necessary but insufficient for keeping up with threats. Deception360 adds a much-needed layer to the security stack.

Aligning OT & IT security

The agentless nature of Deception360 makes it ideal for OT. Networks can be passively monitored with no false-positives and without unplanned downtime. The solution passively monitors the OT & IT networks without scanning.

This improves visibility while gathering intelligence on network threats performing reconnaissance and moving laterally, all while preserving options to respond to attacks at wire speeds within a segment or across the enterprise.

Measurable security outcomes

You will regularly see the measurable impact of the deception-based approach to network defense.

Expect to harvest thousands of new threats per month, see traffic reductions up to 70% while firewall and SIEM utilization stabilize.

How it works

Deception360 uses proprietary and agentless Decoys, Sirens and Sensors for network obfuscation, threat detection without false positives and the ability to automatically respond to threats.

Decoys are highly believable targets for threats actively scanning a network to potentially exploit or attack. Sirens emulate network traffic as if they were fully functioning systems to lure passively listening threats. Sensors provide a transparent mechanism to broadly monitor visible network traffic for anomalies and emerging patterns and support proactive threat hunting. All of our deceptive artifacts are entirely software-based and vendor agnostic. Decoys and sirens can be configured to match any type of OT or IT device.

The solution can evolve from mirror mode to in-line security. When inline customers can act on threats directly from the solution, up to and including blocking. Operating inline the solution also harvests and applies new machine-readable threat intelligence (MRTI) at wire-speed.

Deploy virtually, as an appliance, through AWS or Azure. Either way, from a basic initial setup and deploy service, to ongoing active threat hunting and dynamic deception campaigns, you can achieve the desired security outcomes.

Addressing security controls

Deception360 uniquely supports many important NIST and NERC CIP security controls that you may not have previously thought of addressing with a deceptive approach, but doing so will help achieve the actual intended goal of the control.

NIST Framework for Critical Infrastructure Cybersecurity	NIST 800-53 Security and Privacy Controls for Information Systems
Identify (ID) Protect (PR) Detect (DE) Respond (RS) **ID.RA.2**: Threat and vulnerability information is received from information sharing forum sources **ID.RA.3:** Internal and external threats are identified and documented **PR.DS.2:** Data in transit is protected **PR.DS.5:** Protections against data leaks are implemented **PR.IP.7:** Protection processes continuous improvement **DE.CM.1:** The network is monitored to detect potential cybersecurity events **DE.CM.7:** Monitoring for unauthorized personal, connections, devices and software is performed **DE.DP:** Detection Processes **RS.MI.1:** Incidents are contained **RS.MI.2:** Incidents are mitigated	**RA-3:** Dynamic threat awareness **RA-10:** Threat hunting **SC-5(3):** Detection and monitoring **SC-7:** Boundary protection **SC-7(9):** Restrict threatening outgoing traffic **SC-7(10):** Prevent exfiltration **SC-30:** Concealment and misdirection **SC-26:** Decoys **SI-4(1):** Systemwide intrusion detection **SI-4(5):** System generated alerts **SR-3:** Supply chain controls and processes **SR-3(2):** Limitation of harm
	NERC Critical Infrastructure Protection Standards (NERC CIP)
	CIP-003: Cyber Security Management Controls **CIP-005:** Electronic Security Perimeter(s) **CIP-007:** System Security Management **CIP-011:** Cyber Security – Information Protection

Getting started is easy

A proof-of-concept (POC) clearly demonstrates measurable outcomes and benefits. We regularly support POCs in our efforts to demonstrate our commitment to keeping the brand promise of Deception360.

About PacketViper

PacketViper has transformative and trusted cybersecurity solutions for organizations seeking better security outcomes across their converging OT & IT networks. Packetviper customers cover multiple public and private sector industries.