PACKETVIPER®

Data Sheet

Deception360™ for OT & IT Focused Managed Security Service Providers (MSSP)

Turn the table on threats and delight your customers with provable security outcomes and differentiated services

We understand your struggle

MSSP teams go into service review meetings needing to articulate the value and outcomes they are providing the client. Proving a negative is impossible, and the fear that clients don't see a demonstrable difference between you and competitive alternatives always looms large. New security capabilities need to serve varying customer needs, be able to scale and provide measurable and meaningful security outcomes.

Deception. Threats use it to hurt. You can use it to help.

Decepton360 is the only active cyber threat detection, prevention and response solution that automates deception-powered attack protection from external and internal threats.

Cyber threats dynamically use deception to trick us into revealing information that they then use to increase the chances of attack success. In turn, we typically deploy static defenses that are necessary but insufficient. The active, nature of Deception360 cost-effectively turns the tables on attackers unlike anything else.

A solution for OT & IT

OT/IT convergence increases risk and creates new pathways into critical infrastructure for cyber terrorists and traditional IT cybersecurity solutions are often ineffective for OT.

The agentless, lightweight nature of our deceptive artifacts is ideal for OT. Networks can be passively monitored with virtually no false-positives. Our approach supports OT/IT alignment without creating the risk of unplanned downtime.

Deception360 is an adaptive network security solution that 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 both within a segment or across an enterprise.

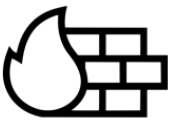
Measurable security outcomes

Every month you'll easily run reports to demonstrate the efficacy of your deception-based services to your clients. Expect to harvest thousands of new threats per month, see traffic reductions up to 70% while firewall and SIEM utilization stabilize.

Your clients will be impressed!

MSSP benefits

Highly differentiated new services & revenue streams



Firewall & SIEM complementary compensating control

Greatly improved SOC operating efficiency

Measurable outcomes and improvements to client security

Getting started is easy

Whether it is for you or your client, a proof-of-concept (POC) clearly demonstrates the measurable outcomes and benefits. We regularly support POCs in our efforts to demonstrate our commitment to our partner's success and keep the brand promise of Deception360. During a POC the PacketViper team works closely with the MSSP to ensure POC success.

The new, deception-based services your MSSP can offer around Deception360 are powerful.

Becoming a PacketViper MSSP partner

PacketViper offers a variety of options that align closely with our partners' go-to-market plan, up to and including white-label opportunities. The PacketViper team works with each MSSP to help identify new prospects and customers. We have excellent sales enablement and technical certification. The PacketViper's reseller agreement is well aligned and structured to reward the MSSP for its effort by offering aggressive discounts from the very first deal.

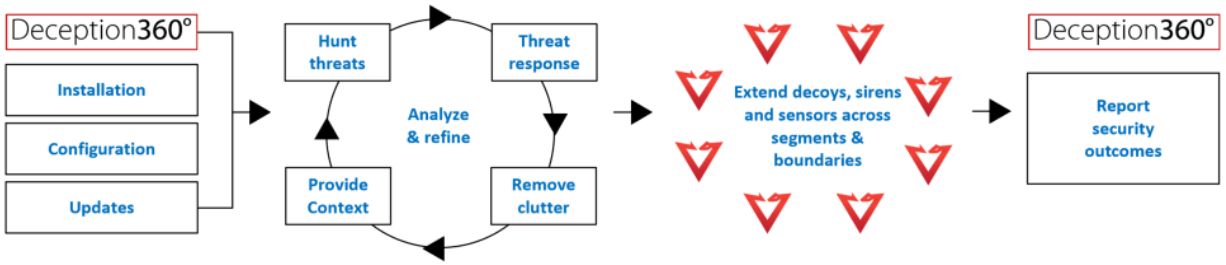
Deception-powered use cases

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

Building a service with recurring value demonstration

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 match the level of service to the desired outcomes.

Automated threat detection, prevention and response: How it works



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

About PacketViper

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