PACKETVIPER®

Product Brief

Deception360 for Operational Technology (OT) Networks

Trusted cybersecurity outcomes. No unplanned downtime.

OT is different

The purpose of operational technology (OT) is different than that of information technology (IT). IT focuses on the 'CIA Triad' of data. That breaks down to; confidentiality, integrity and availability. OT networks control our physical world and essential processes, so uptime and reliability are vital to OT

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

Deception360 helps organizations seeking to cost-effectively defend OT networks without unplanned downtime or a costly a 'rip and replace'.

Addressing OT specific issues

A deception-based approach to OT security can help owner/operators address OT security issues without threatening overall equipment effectiveness (OEE).

Deception360 addresses OT specific requirements in a manner that builds trust and delivers meaningful and measurable security outcomes.

The complex nature of OT networks and lack of tolerance for disruption requires OT cybersecurity solutions support the following key criteria:

- Provide compensating controls for dated systems
- Configurable to match any type of device
- Support asset discovery
- Provide a vendor-agnostic approach
- Segment-specific flexibility
- Function across both OT and IT environments
- Evolve from mirror mode to in-line security as teams develop trust and seek active threat response
- Cost-effectively scale throughout the enterprise

Agentless alignment of 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.

Next-gen OT cybersecurity

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 needed layer to the security stack.

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 across both OT and IT networks.

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 device.

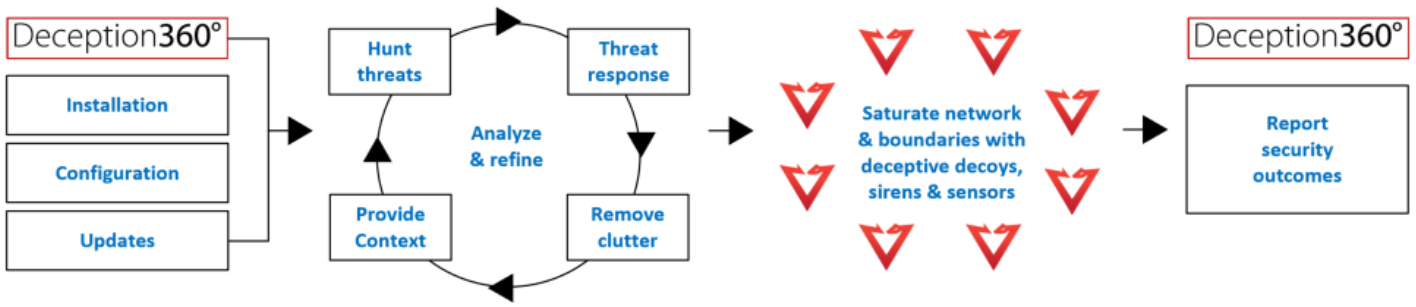
Building trust

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.

Deception360 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 kill chain provides a robust defense for your critical assets.

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.

A basic summary of the process that powers Deception360 is as follows:



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.

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.