PACKETVIPER®

Use Case

Deception-Based Vendor Risk Management (VRM)

Real-Time, Connected Vendor Policy Enforcement

The challenge: Maintaining continuous digital trust on your network

Vendor ecosystems are evolving at a dynamic rate. Each supplier granted network access is a partner that you are relying on to contribute to your ongoing cyber defense posture. Ensuring the ongoing digital trust of your connected vendor ecosystem requires “outside-in” ratings data as well as an understanding of real-time, connected vendor behavior behind the firewall and at your network boundaries.

Point-in-time assessments and vendor risk scoring are necessary but insufficient. The value of point-in-time data diminishes quickly and negates your ability to act in the most timely and responsive manner. These scores only estimate the relative and comparative external security posture of your vendor. They are blind to how your vendors are continuously interacting with, and behaving on, your network.

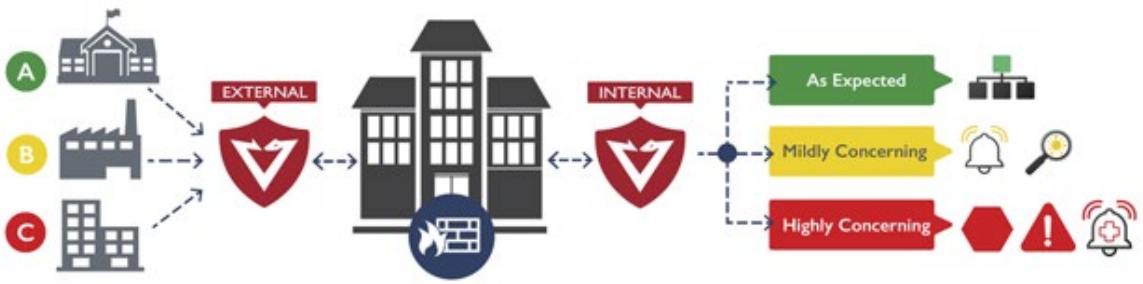
Introducing VRM with Deception360

Ongoing digital trust requires not only favorable “Outside-in” ratings data, but also good behavior behind the firewall and at your network boundaries. Deception360 offers a deception-based way to establish digital trustworthiness with comprehensive, real-time connected vendor monitoring and wire-speed, and available adaptive response management.

Deception360 uses lightweight deception and patented features to continuously analyze vendor traffic as it interacts with your network in real-time. Again, this includes behavior at the edge, as well as behind the firewall. Internal and external vendor-specific traffic activity occurring outside of normal, pre-approved operating ranges will hit decoys and then can be easily identified and acted upon. If your business enlists a new vendor, access to common services via ports 80 and/or 443 can be granted based upon network ranges and specific IP addresses. Unique rules can be assigned to each vendor based on perceived vendor risk.

How it works

Set up vendor monitoring with Deception360 in either passive monitoring, or active mode. Depending on the severity of the anomalous connected vendor behavior, various responses can be taken. The solution can easily evolve from mirror mode to in-line security. When inline, customers can act on threats directly from the solution, up to and including blocking. When inline, the solution also harvests and applies new machine-readable threat intelligence (MRTI) at wire-speed.



Get regular reports at the vendor-specific level indicating where policy violations have occurred. Wire-speed, continuous analysis of vendor traffic and connection attempts support security controls such as *NIST 800-53 SR-3 Supply chain controls and processes.*

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.