PACKETVIPER®

USE CASE

Vendor Risk Management (VRM)

On Network, Real-Time Vendor Risk Management

The Challenge: Maintaining Continuous Digital Trust on Your Network

Vendor ecosystems are evolving at a dynamic rate. Each supplier granted network access is, in effect, a trusted partner; one that your business will rely on to strengthen your cyber defense posture. Ensuring ongoing digital trust requires "outside-in" ratings data as well as an understanding of behavior at the perimeter and behind the firewall.

Point-In-Time Assessments and Vendor Risk Scoring Mechanisms are Not Enough

The value of point-in-time data diminishes quickly and negates your ability to act in the most responsive manner. Vendor Risk Scoring mechanisms are necessary but sometimes insufficient. These scores only estimate the relative and comparative external security posture of your vendor, not how your vendors are continuously interacting with, and behaving on, your network.

PacketViper Supports Regulatory and Compliance Mandates

Many government and industry regulations like FFIEC, HIPAA, PCI DSS, SOX, COBIT5, and GDPR stipulate that risk management policies extend to third-party vendors, contractors and consultants. PacketViper supports those compliance mandates along with security controls frameworks including: SANS CIS CSC, NIST 800-53, NIST 800-171 and ISO 270002:2013. The control support covers: network analysis, network defense, and logging.

Deception Enforced VRM Policies and Adaptive Responses

PacketViper uses lightweight deception and patented features to continuously analyze vendor traffic as it interacts with your network in real time. This includes behavior at the edge and behavior behind the firewall.

Internal and external vendor specific traffic activity occurring outside of normal, pre-approved operating ranges hit decoys and 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.

Getting Started Is Easy

Set up PacketViper in either passive monitoring or active mode. Depending on the severity of the violation and the priority, more assertive responses can be taken.

Feature	Monitor Mode	Active Mode
Continuous policy enforcement	×	×
Open a ticket	×	×
Alert the team	×	×
Alert the vendor	×	×
Log the event	×	×
Initiate vendor review	×	×
Slow down the connection		×
Block the connection		×

How deception based VRM works

IDENTIFY Vendor Relationships
Define expected or contractual network operating ranges

PROTECT Valuable Data
Continuously monitor network connection attempts

DETECT Vendor Rules
Automatically follow inspection process

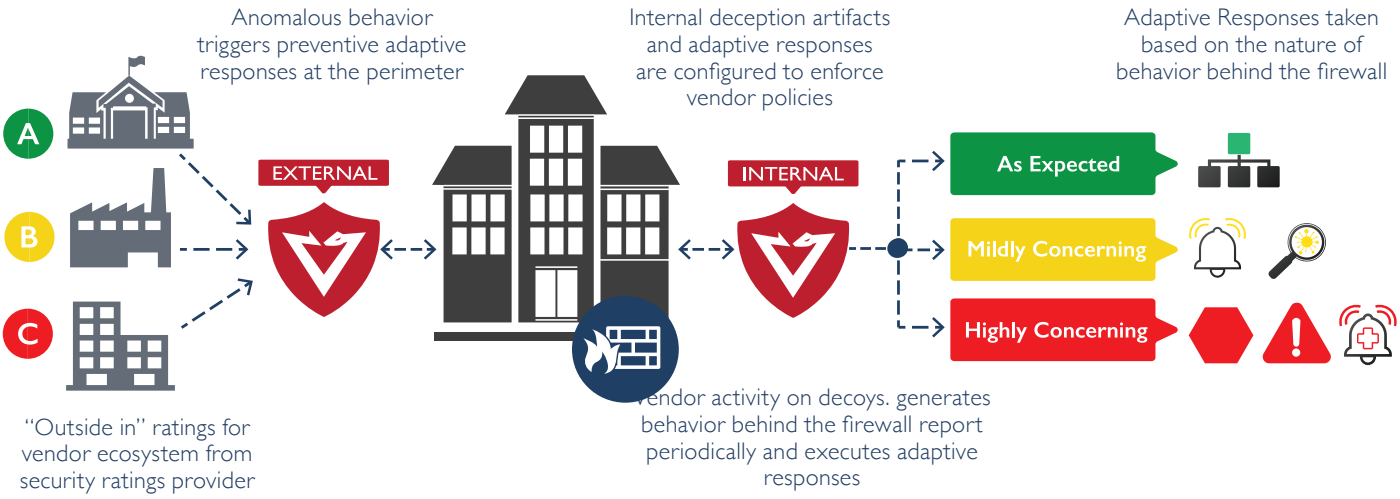
RECOVER or **RESPOND**
Automated actions based on vendor criticality and violation

According to a recent Ponemon Institute Third-Party Data Risk Study of 1,000 CISO's: **59%** of companies experienced a third-party data breach in 2018, yet only **16%** say they effectively mitigate third-party risks.

--2018 Annual Study, Data Risk in the Third-Party Ecosystem

PacketViper VRM Use Case

PacketViper establishes digital trustworthiness with comprehensive vendor monitoring and adaptive response management. Ongoing digital trust requires: favorable "Outside-in" ratings data, good behavior behind the firewall, and good behavior at the perimeter.



About PacketViper

PacketViper is a lightweight, active cybersecurity deception solution using agentless internal and external deception artifacts to prevent, detect and respond to threats automatically without complex orchestrations. Internal deception detects and responds to threats moving laterally within the network with virtually no false positives. External deception creates the appearance of a moving target, making the network harder to size up and keeping up to 70% of unwanted and uninvited threats off the network. PacketViper produces machine readable threat intelligence that is automatically applied and supports real-time policy enforcement.

Contact Us Today

Call: 855-758-4737
Email: info@packetviper.com