PACKETVIPER®

USE CASE

Vendor Risk Management (VRM)

On Network, Real-Time VRM

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.

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 also 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.

Continuous Monitoring with Automated Actions Against Anomalies

Once configured, PacketViper uses lightweight deception and patented features to continuously analyze vendor traffic as it interacts with your network in real time.

Recon scans and IP traffic activity occurring outside of normal, pre-approved operating ranges hit decoys and can be easily identified, acted upon and reported. 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 it works

Deception Based Vendor Risk Management Process

IDENTIFY Vendor Relationships

Define expected or contractual network operating ranges.

Real-time reporting on any attempt to reach a non-sanctioned, network component via a connection request, scan or flood.*

PROTECT Valuable Data

Continuously monitor network connection attempts.

Spreading deception decoys and sensor throughout the network provides a practical and cost-effective means to continuously diagnose and monitor the company interaction with third-party networks.

DETECT Vendor Rules

Automatically follow inspection process.

Validate business, country, port/protocol, threat intelligence, time/rate, and any custom rules.

RECOVER or RESPOND

Automated actions based on vendor criticality and violation.

Connection attempt conforms to vendor rules, traffic follows normal operations.

Connection attempt does NOT conform, set options to respond and secure perimeter.

- Slow down connection**
- Block connection**
- Alert security team
- Log the event for compliance reporting
- Alert the vendor
- Initiate vendor review

*FTP and SFTP protocols not monitored.

**Requires PacketViper to be in Active Mode

30 DAY RISK-FREE TRIAL

RISK FREE
Satisfaction Guaranteed

Try all the PacketViper features for thirty days risk free.

Get full functionality and see the difference deception can make for your organizaiton.

See for yourself.

About PacketViper

PacketViper is cybersecurity deception technology featuring a lightweight deception that produces heavyweight, practical results including dynamic network defense, relief of security related operational costs and burdens, and 3rd party risk monitoring with real-time policy enforcement.

Contact Us Today

Call: 855-758-4737

Email: info@packetviper.com