JULY 2023

SUSE

NeuVector

BY SUSE

Holger Moenius
Solution Specialist - NeuVector
holger.moenius@SUSE.com

Protection Without Compromise

— *From Dev to Production*

THE CHALLENGE

Container environments are rapidly becoming more prevalent

Traditional Security tools don't work in these environments

Kubernetes abstracts the complexity of container networking for the trade-off of network visibility

Supply Chain Security

Full image life-cycle security from dev to prod

Zero Trust Runtime

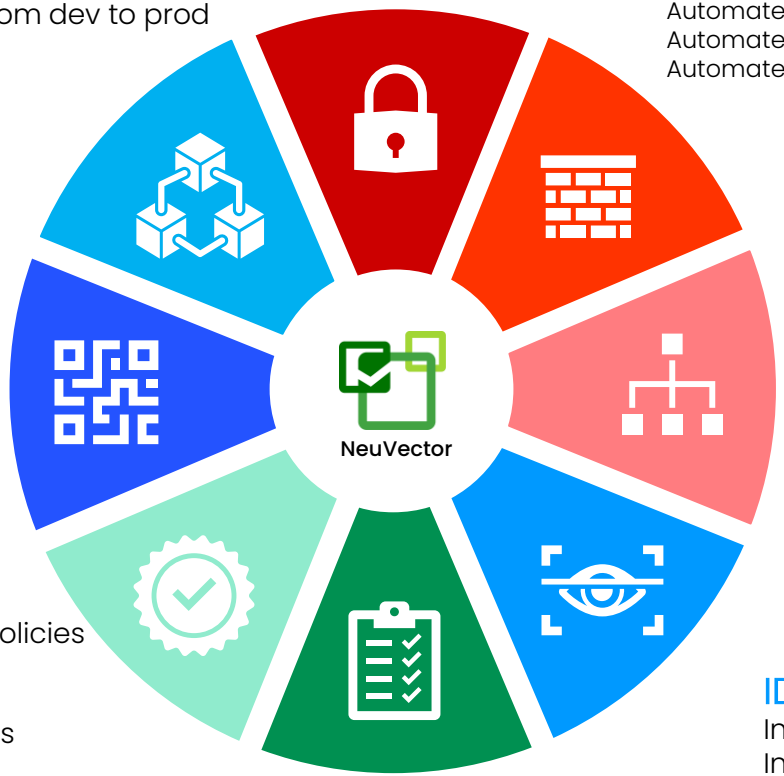
Automated Discovery
Automated Layer 7 Network Policies
Automated Container Process Policies
Automated Policy export Security-as-Code

Vulnerability Scanning

Pipeline
Platform
Registry
Host Nodes

Layer 7 Network

Patented Deep Packet Inspection
Layer 7 Protocol Validation
Detection of 23 network attacks
Threat-triggered Packet Capture



Compliance Scanning

CIS Benchmarks
NIST GDPR
PCI HIPAA

Workload Security

Multi-cluster policy management
No SaaS / No Agents / Air-Gap
Image Drift Prevention
Network / Process Segmentation

Admission Control

CVE aware Pod Security Policies
Registry Control
Complex Rules
Alert Only / Enforce modes

IDP/IPA

Intrusion Detection
Intrusion Prevention
Privilege Escalation
Container Escape

DEFENSE IN DEPTH – NEUVECTOR SECURITY LAYERS

Supply Chain Layers

- Vulnerability Scanning
- CIS Benchmark Scanning
- Admission Control
- Image Signature Verification

Runtime Layers

- Zero-Trust Segmentation
- Network Threat Detection
- Vulnerability / CIS Scanning
- Data Leak Prevention (DLP)
- Ingress WAF Sensors

NeuVector BY SUSE

THE 2 MAJOR COMPONENTS OF

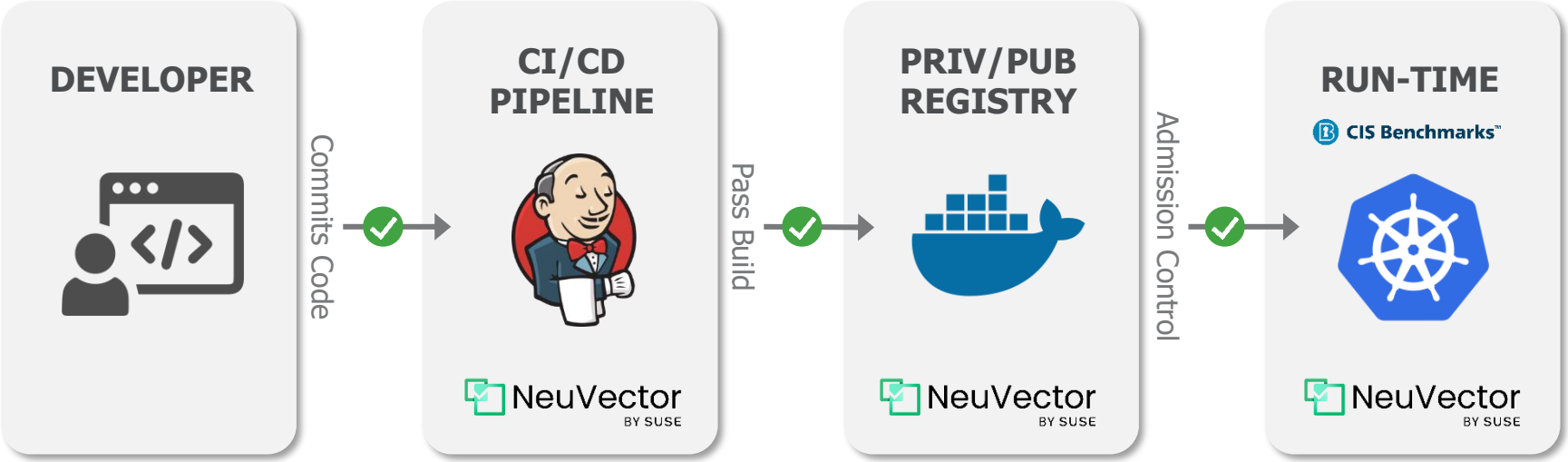
Supply Chain Scanning

Vulnerabilities / Compliance

Runtime Security

Network / Processes / File Protection

VULNERABILITY & COMPLIANCE MANAGEMENT



NEUVECTOR CVE SOURCES

CVE Database Sources	
CVE NVD and Mitre	
OS based	**Application based**
Alpine	.NET
Amazon	apache
Debian	busybox
Microsoft mariner	golang
Oracle OS	Java maven
Rancher OS	Kubernetes
Red Hat/CentOS	nginx
SUSE Linux	npm
Ubuntu	openssl
	python
	ruby

NeuVector CVE Database is Updated via 22 Vendor Sources every 24 hours as of 5.2.0 July 2023

NeuVector BY SUSE

NeuVector
BY SUSE

ADMISSION CONTROL POLICIES

- No coding or yaml – *Point & Click*
- **Alert Only** *and* **Blocking** modes
- Multiple criteria per policy
- Allow & Deny policies
- Any level of granularity (pod, namespace, cluster)
- Export rules via YAML to other clusters
- Auto-federate rules to other clusters
- CI/CD pipeline pre-deployment check

New in 5.2.0

Monitor/Protect mode now configurable per rule

31 Pre-Built NeuVector Admission Control Policies	
Custom Criteria	Labels
Allow Privilege Escalation	Modules
Count of high severity CVE	Mount Volumes
Count of high severity CVE with fix	Namespace
Count of medium severity CVE	PSP Best Practice
CVE Names	Resource Limit Configuration (RLC)
CVE Score	Run as privileged
Environment variables with secrets	Run as root
Environment variables	Service Account Bound High Risk Role
Image ID	Share host's IPC namespaces
Image compliance violations	Share host's PID namespaces
Image without OS information	Share host's Network
Image Registry	User
Image Scanned	User Groups
	Violates PSA policy
New in 5.2.0 >> Image Signed	Image Sigstore Verifiers

UNDERSTANDING THE PERSPECTIVES

THE 2 MAJOR COMPONENTS OF

Supply Chain Scanning

Vulnerabilities / Compliance

Runtime Security

Network / Processes / File Protection

SIGNATURE MATCHING VS ZERO TRUST

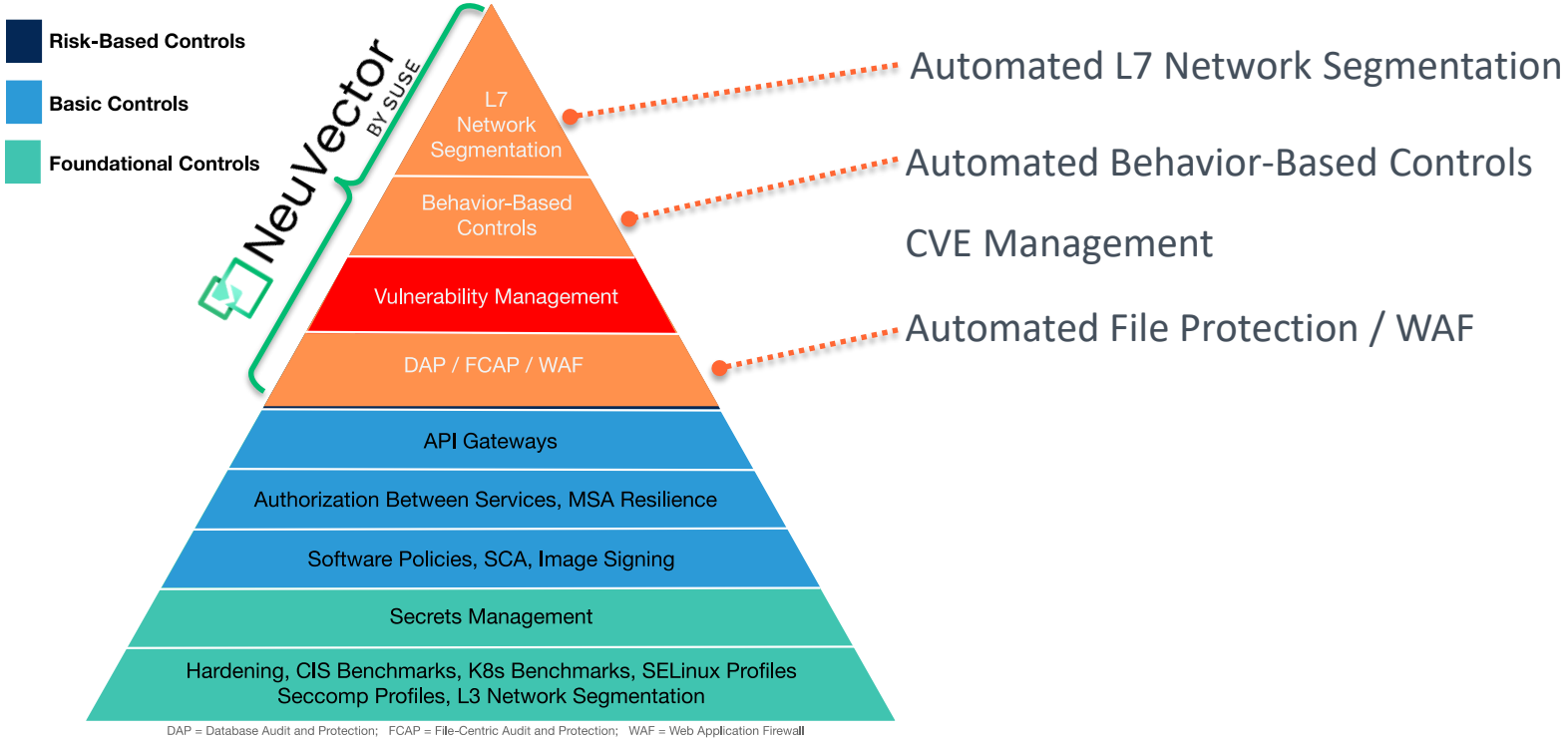
Signature Matching Controls

- CVEs
- DLP
- Network Attacks
- OWASP Top 10
- Admission Control

Zero-Trust Controls

- Automated Learning
- Network
- Process
- File Access
- Security as Code

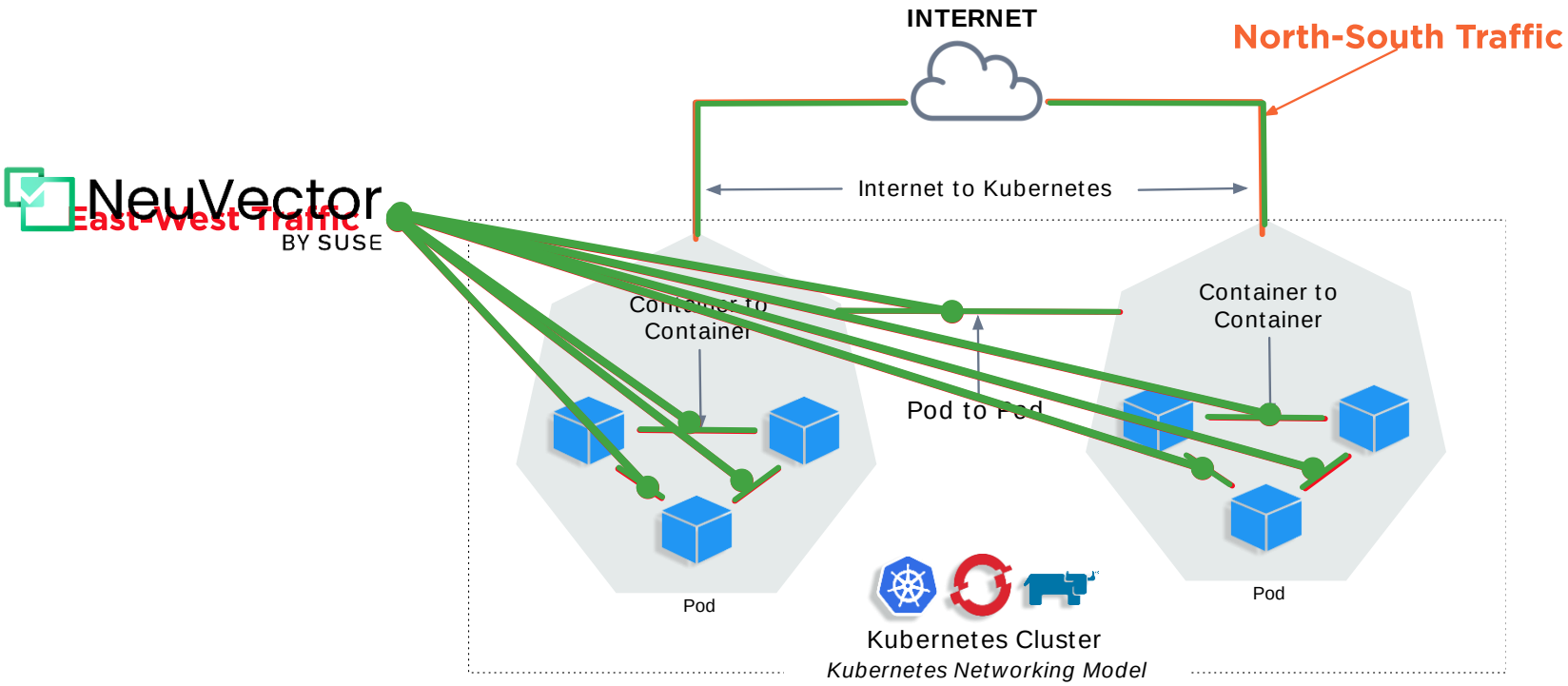
GARTNER'S CONTAINER SECURITY CONTROL HIERARCHY



DAP = Database Audit and Protection; FCAP = File-Centric Audit and Protection; WAF = Web Application Firewall

Source: Gartner Technical Report 718483 April 2020 - *Containers: 11 Threats and How to Control Them* PAGE 9

RUNTIME NETWORK & PROCESS DETECTION



RUNTIME NETWORK & PROCESS DETECTION

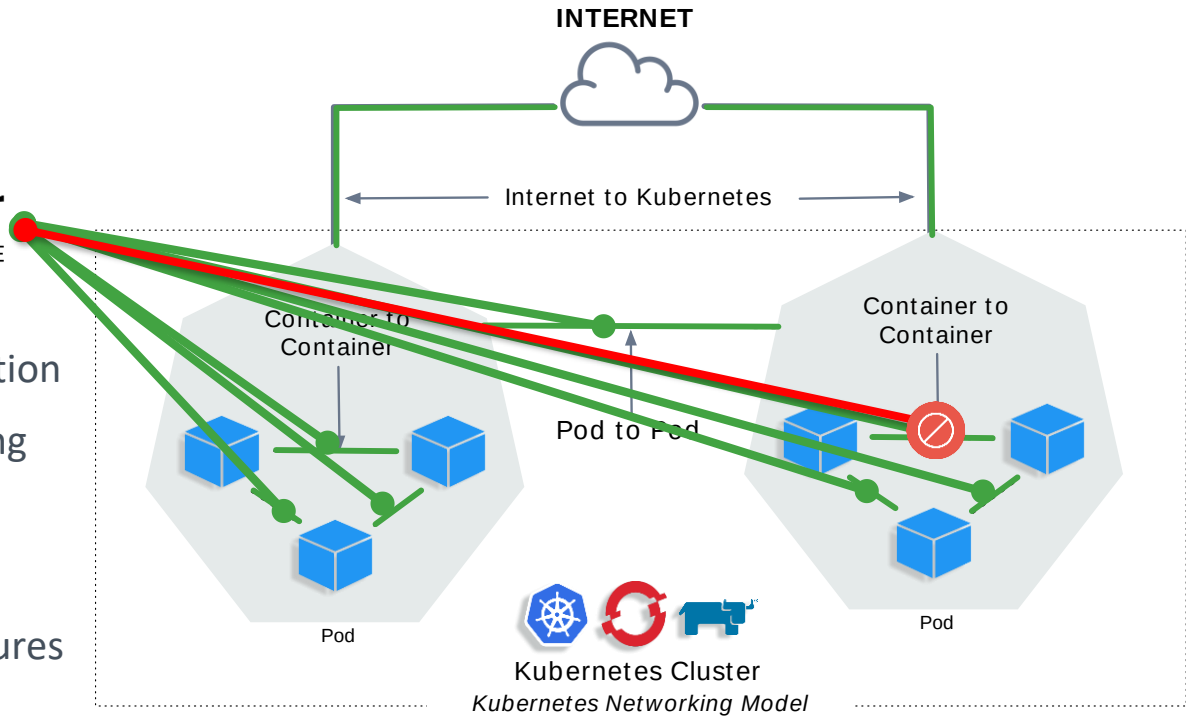
NeuVector
BY SUSE

DPI enables

- Automated Behavioral Learning
- Auto-Gen Security Policy
- Security as Code
- Zero-Day Countermeasures
- Unpatched CVE Countermeasures
- Packet Capture
- Data Loss Prevention
- WAF

K8's Deep Packet Inspection
(PATENTED)

- Layer 3/4 Port
- Layer 7 Protocol
- Processes



NeuVector
BY SUSE

APPLICATION (LAYER 7) PROTOCOLS VALIDATED

HTTP/HTTPS
SSL
SSH
DNS
DNCP
NTP
TFTP
ECHO
RTSP
SIP
MSSQL
gRPC

MySQL
Redis
Zookeeper
Cassandra
MongoDB
PostgresSQL
Kafka
Couchbase
ActiveMQ
ElasticSearch
Oracle

RabbitMQ
Radius
VoltDB
Consul
Syslog
Etcd
Spark
Apache
Nginx
Jetty
NodeJS

35 Layer-7 Application Protocols as of 5.2 – July 2023

NeuVector BY SUSE

NETWORK ATTACKS AUTOMATICALLY DETECTED & BLOCKED

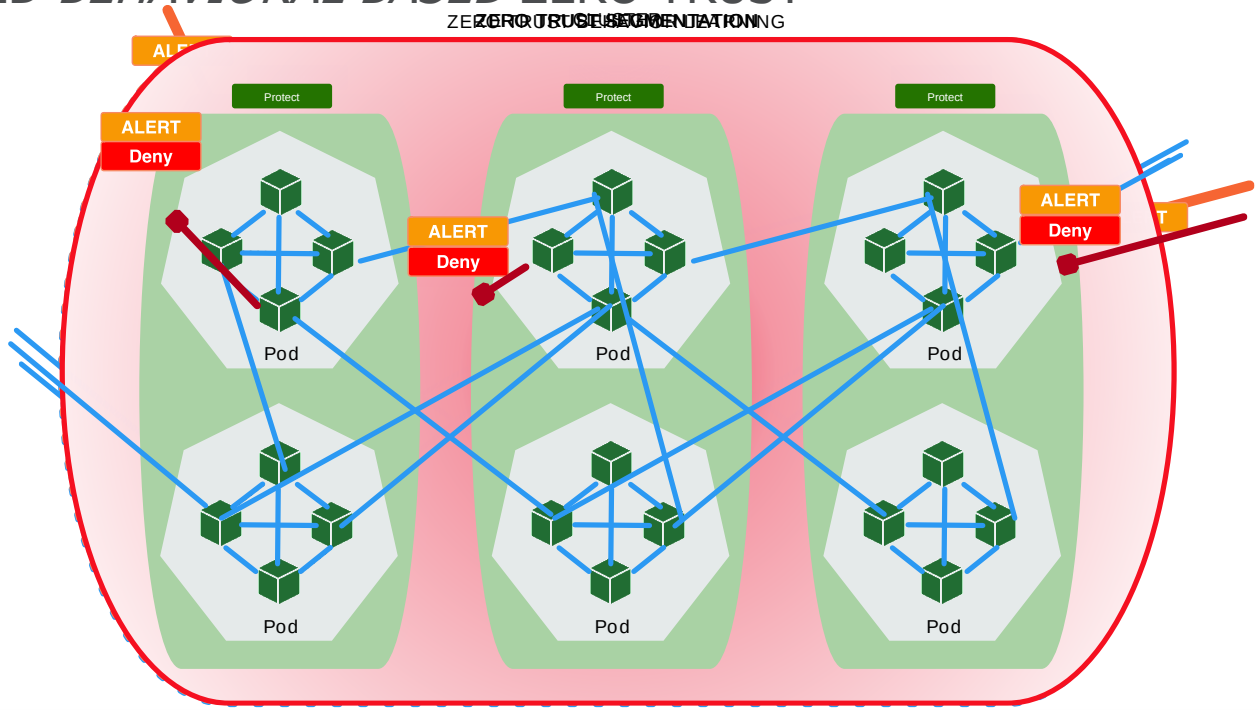
ATTACK DETECTION TRIGGERS AUTOMATIC PACKET CAPTURE

Apache Struts RCE	DNS Null Type	K8's Man-in-the-middle
Cipher Overflow	DNS Tunneling	PING Death
HTTP Negative Content	DNS Zone Transfer	SQL Injection
MySQL Access Deny	HTTP Slowloris DDoS	SSL Heartbleed
Detect SSH 1, 2, or 3	HTTP Smuggling	SYN flood
Detect SSL TLS v1.0	ICMP Flood	TCP small window
DNS Buffer Overflow	ICMP Tunneling	TCP split handshake
DNS Flood DDoS	IP Teardrop	TCP Small MSS

24 Network-based Attacks as of 5.1.1 – March 2023

NeuVector BY SUSE

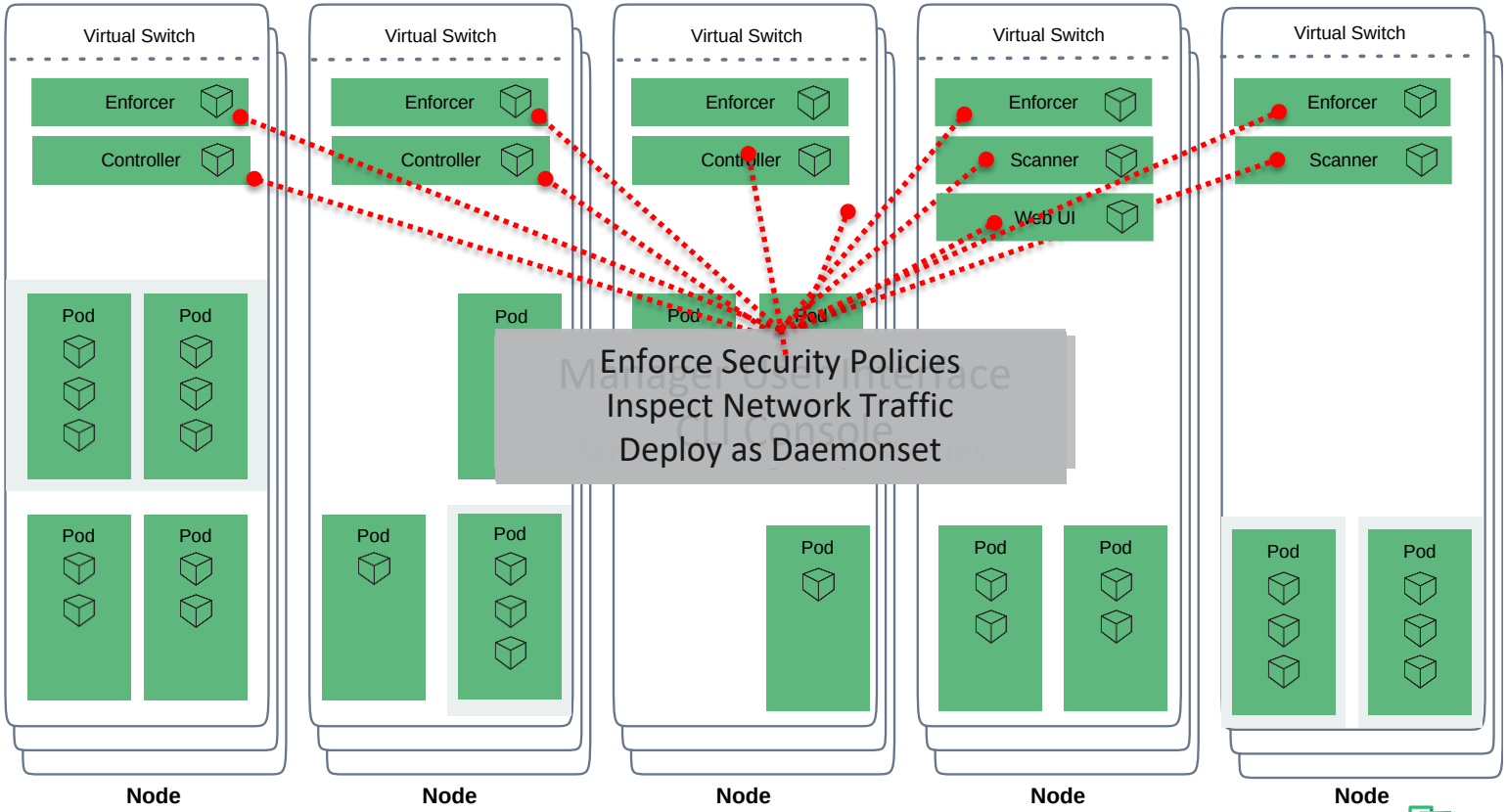
AUTOMATED *BEHAVIORAL-BASED* ZERO-TRUST



Discover	Identifies application behavior (Learning Mode)
Monitor	Alerts to any anomalous application behavior
Protect	Denies on any anomalous application behavior

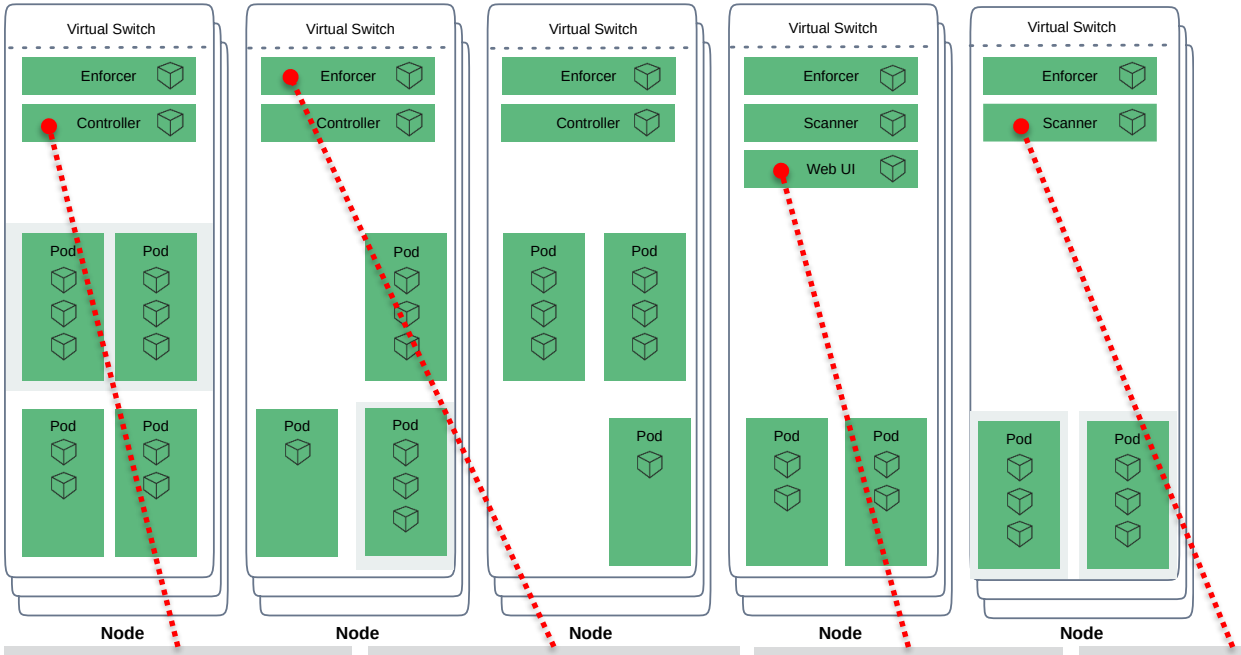
NeuVector BY SUSE

NEUVECTOR ARCHITECTURE / DEPLOYMENT



NeuVector BY SUSE

NEUVECTOR ARCHITECTURE / DEPLOYMENT



NeuVector is deployed as containers

NeuVector does not use:
Agents
Side-car Proxies
Code Injection
IP Table Manipulation
Port Labels

NeuVector can use eBPF Probes for process identification if available
(not required)

eBPF is not adequate for Layer 7 Identification, Validation or Blocking

(if it was, we'd be using it.)

Controllers
Manages Policies
Complete REST API
3 Instances for HA

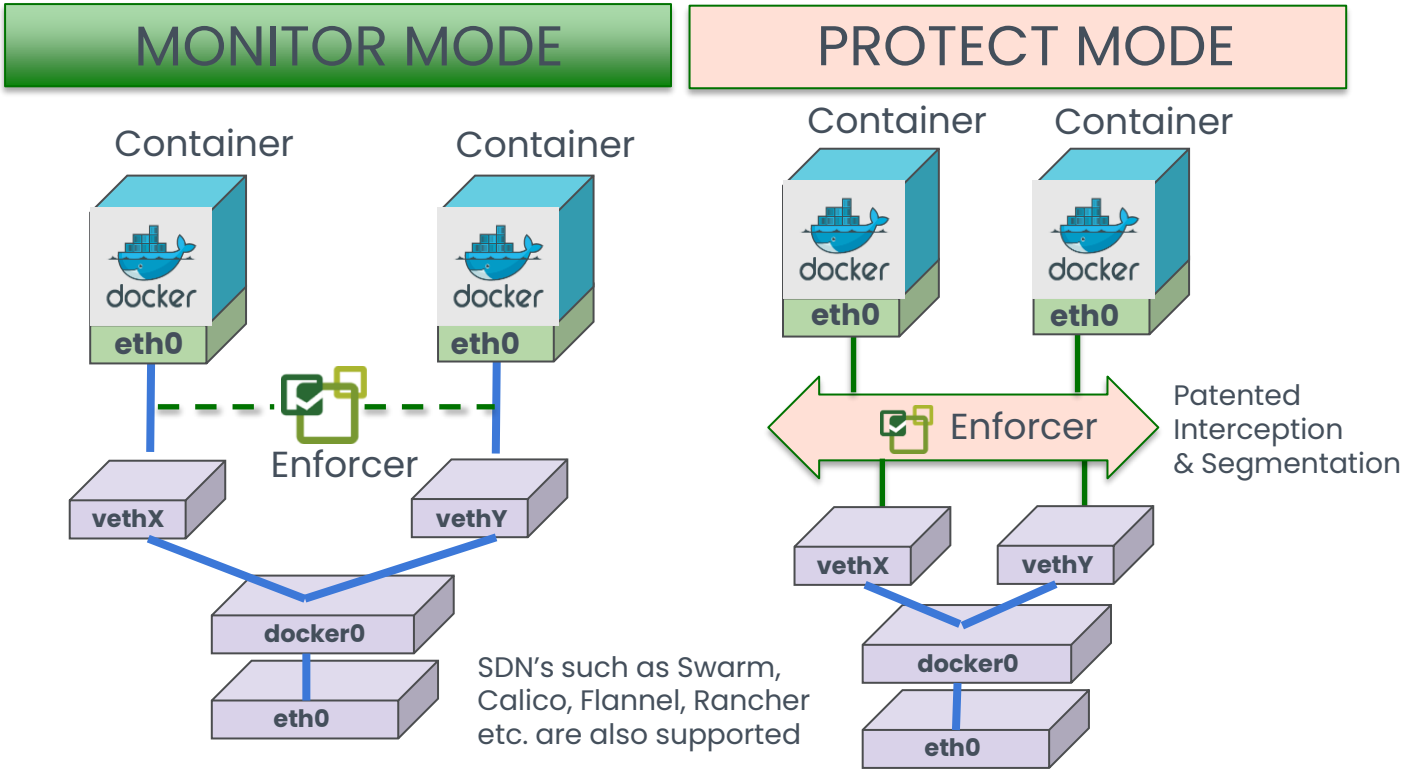
Enforcers
Enforce Security Policies
Inspect Network Traffic
Deploy as Daemonset
1 Per Worker Node

WebUI
CLI Console

Scanners
FAST
Parallel scanning
Scales for large repositories

NeuVector BY SUSE

NEUVECTOR ENFORCER NETWORK INSPECTION



NeuVector BY SUSE

NEUVECTOR: COMMUNITY VS. PRIME

	Community	Prime
Pipeline, Registry, Run-Time Vulnerability Scanning with updated CVE database	◉	◉
Compliance checks and Reports	◉	◉
Zero-trust run-time security controls	◉	◉
SLA backed Product Support services, RCA, troubleshooting		◉
Vulnerability (CVE) investigation, triage assistance		◉
Best practices, hardening assistance (e.g. segmentation, network and process profiling, admission controls)		◉
Run-time threat rules configuration, optimization. Access to assets and services (e.g. performance tuning, CVE lookups)		◉
Built-in, supported native integration with Rancher Manager and Rancher Distributions (e.g. UI Extension)		◉

Q&A

NeuVector
BY SUSE

Holger Moenius
Sr Solution Sales
holger.moenius@SUSE.com

SUSE