RANCHER®
BY SUSE

SUSE NeuVector

Protection Without Compromise - From Dev to Production

THE 2 MAJOR COMPONENTS OF NeuVector

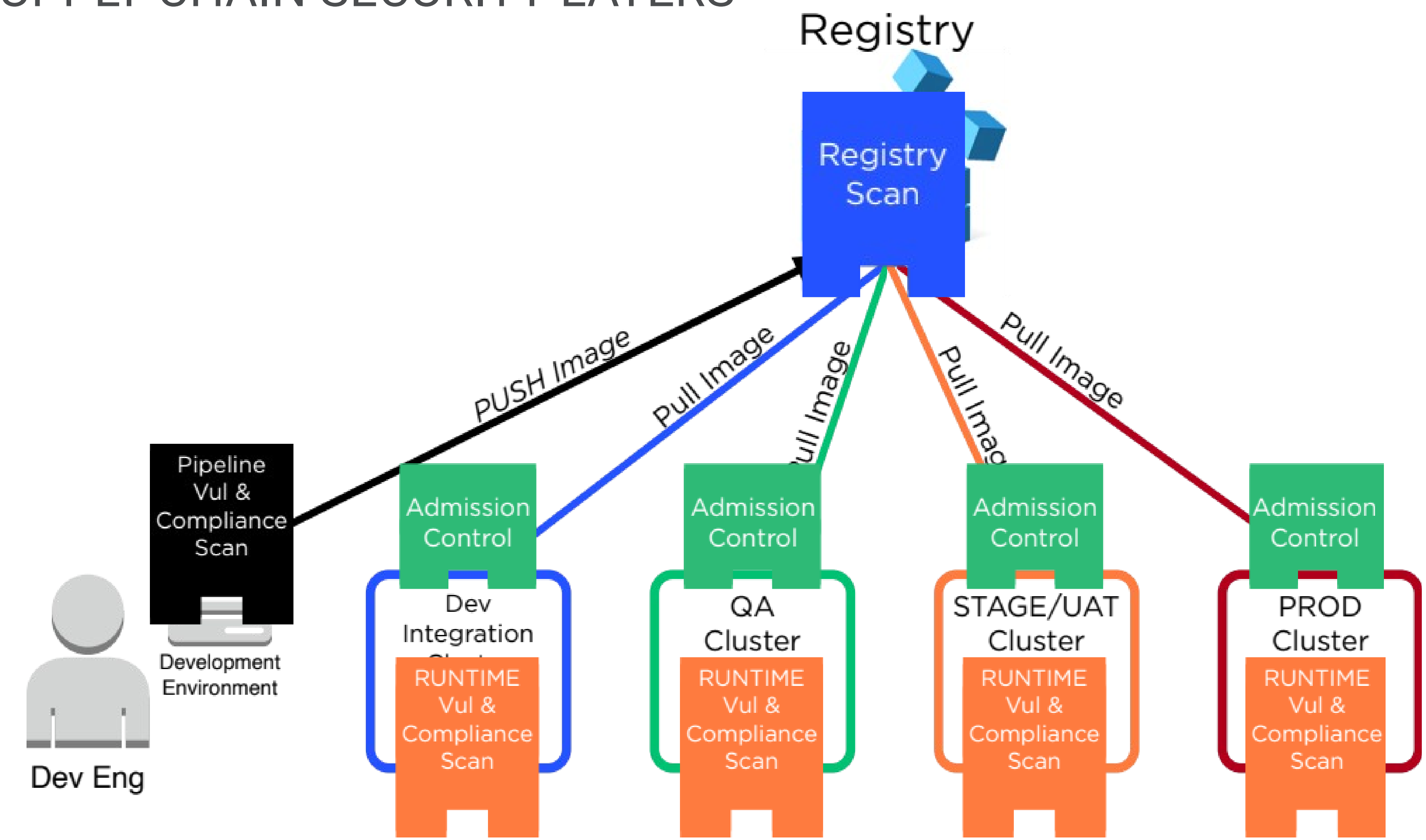
Supply Chain Scanning

Vulnerabilities / Compliance

Runtime Security

Network / Processes / File Protection

4 SUPPLY CHAIN SECURITY LAYERS



CVE DATABASE SOURCES

Source	URL
nvd and Mitre	*https://nvd.nist.gov/feeds/*
SUSE SLE/SLES	*https://ftp.suse.com/pub/projects/security/oval/*
Rancher OS	*https://rancher.com/docs/os/v1.x/en/about/security/*
Alpine	*https://github.com/alpinelinux/alpine-secdb*
Ubuntu	*https://launchpad.net/ubuntu-cve-tracker*
Debian	*https://security-tracker.debian.org/tracker/data/json*
RedHat	*https://www.redhat.com/security/data/oval/*
Amazon	*https://alas.aws.amazon.com/*
Busybox	*https://www.cvedetails.com/vulnerability-list/*
NGINX	*http://nginx.org/en/security_advisories.html*
NodeJS	*https://www.npmjs.com/advisories/*
Ruby	*https://github.com/rubysec/ruby-advisory-db*
OpenSSL	*https://www.openssl.org/news/vulnerabilities.html*
Apache	*https://www.cvedetails.com/vendor/45/Apache.html*
Java	*https://openjdk.java.net/groups/vulnerability/advisories/*
Python	*https://github.com/pyupio/safety-db*
Microsoft Mariner	*https://github.com/microsoft/CBL-MarinerVulnerabilityData*

NeuVector CVE Database is Updated via 17 Security Sources Nightly

THE 2 MAJOR COMPONENTS OF

NeuVector

Supply Chain Scanning

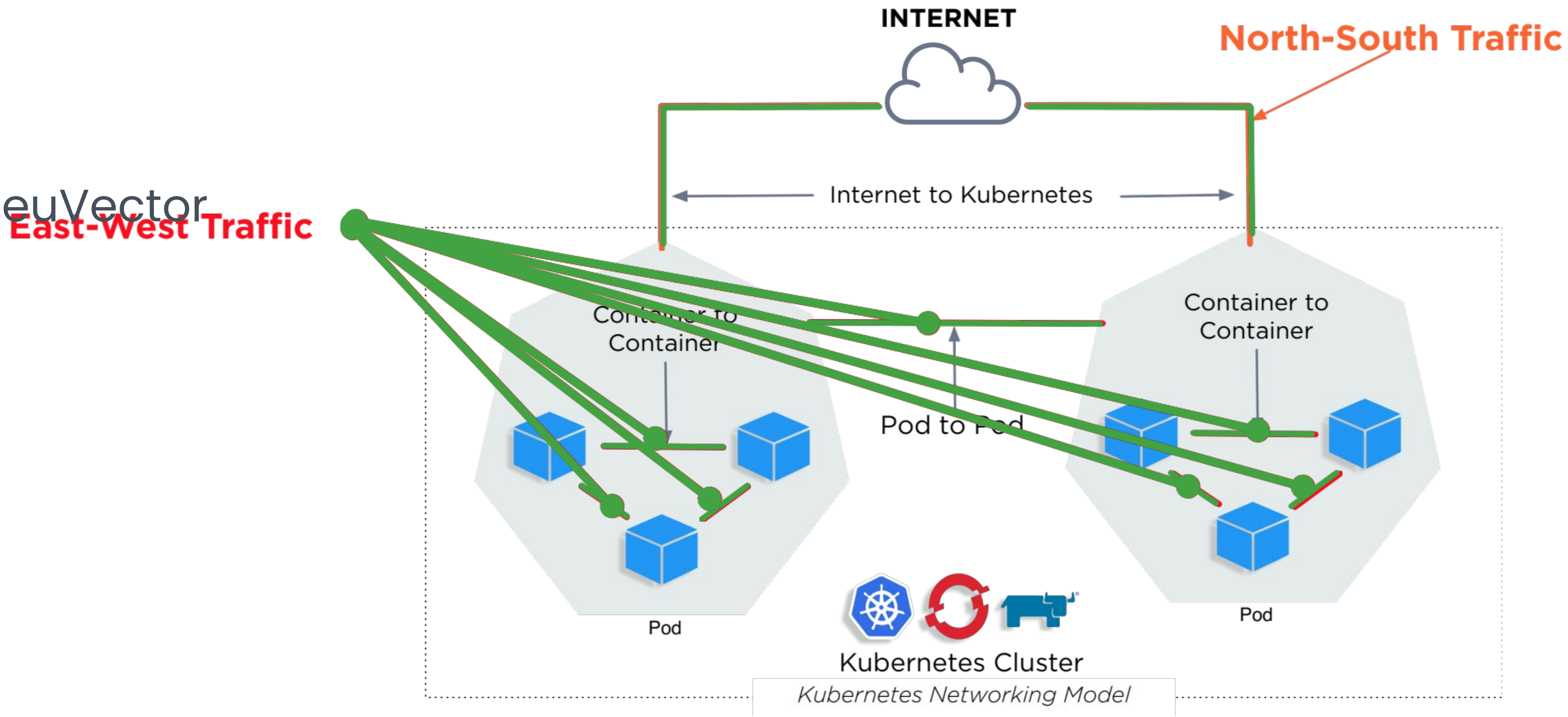
Vulnerabilities / Compliance

Runtime Security

Network / Processes / File Protection

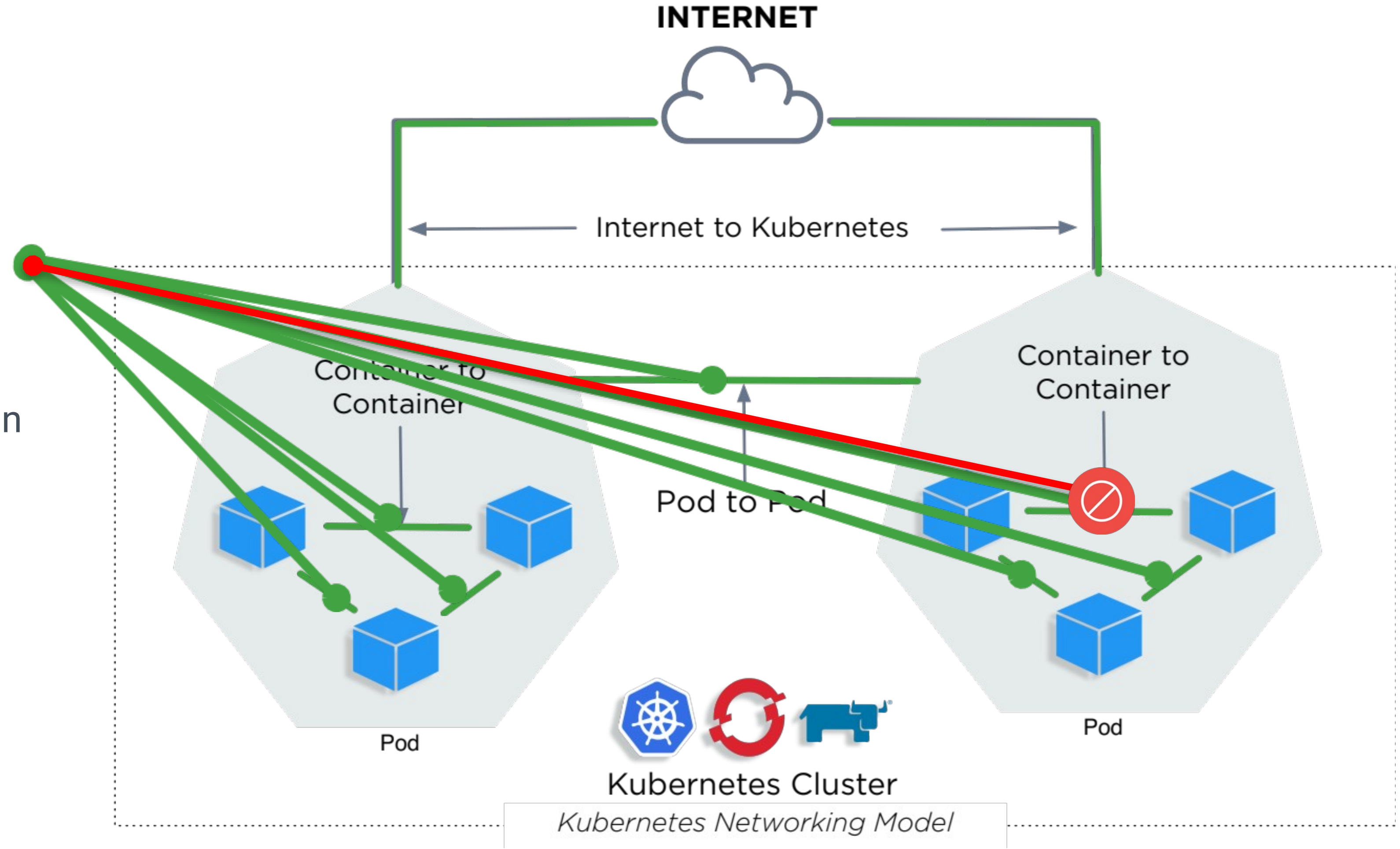
RUNTIME BEHAVIORAL INSPECTION

SUSE NeuVector



RUNTIME BEHAVIORAL INSPECTION

SUSE NeuVector



K8's Deep Packet Inspection
(PATENTED)

- Layer 3/4 Port
- Layer 7 Protocol

+

- Processes

APPLICATION PROTOCOLS RECOGNIZED

- HTTP/HTTPS
- SSL
- SSH
- DNS
- DNCP
- NTP
- TFTP
- ECHO
- RTSP
- SIP
- ICMP
- gRPC
- MySQL
- Redis
- Zookeeper
- Cassandra
- MongoDB
- PostgresSQL
- Kafka
- Couchbase
- ActiveMQ
- ElasticSearch
- MemCache
- Oracle
- RabbitMQ
- Radius
- VoltDB
- Consul
- Syslog
- Etcd
- Spark
- Apache
- Nginx
- Jetty
- NodeJS

35 Layer-7 Application Protocols as 5.0.0 – May 2022

THREATS AUTOMATICALLY DETECTED

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

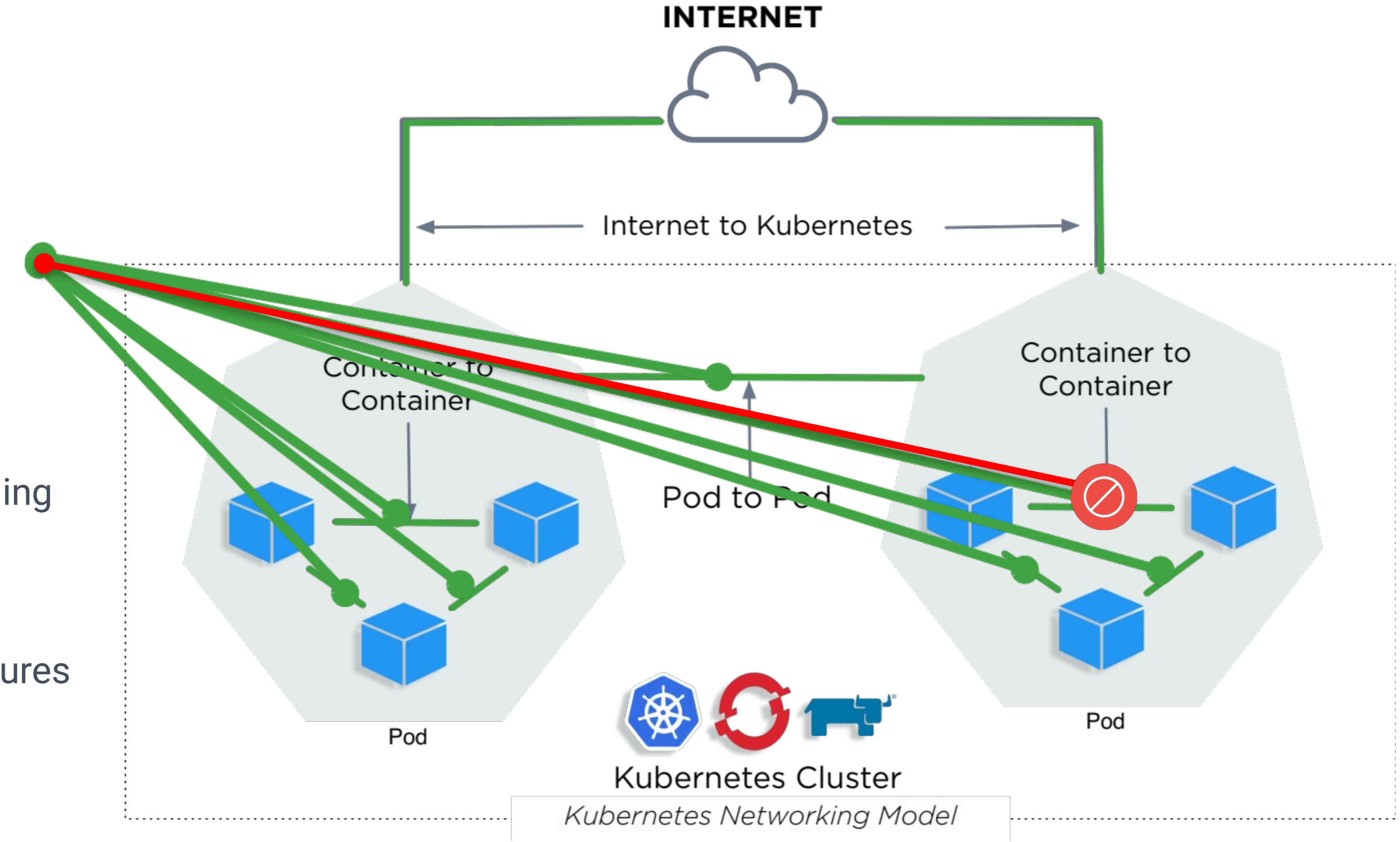
23 Network-based Attacks as of 5.0.0 – May 2022

RUNTIME BEHAVIORAL INSPECTION

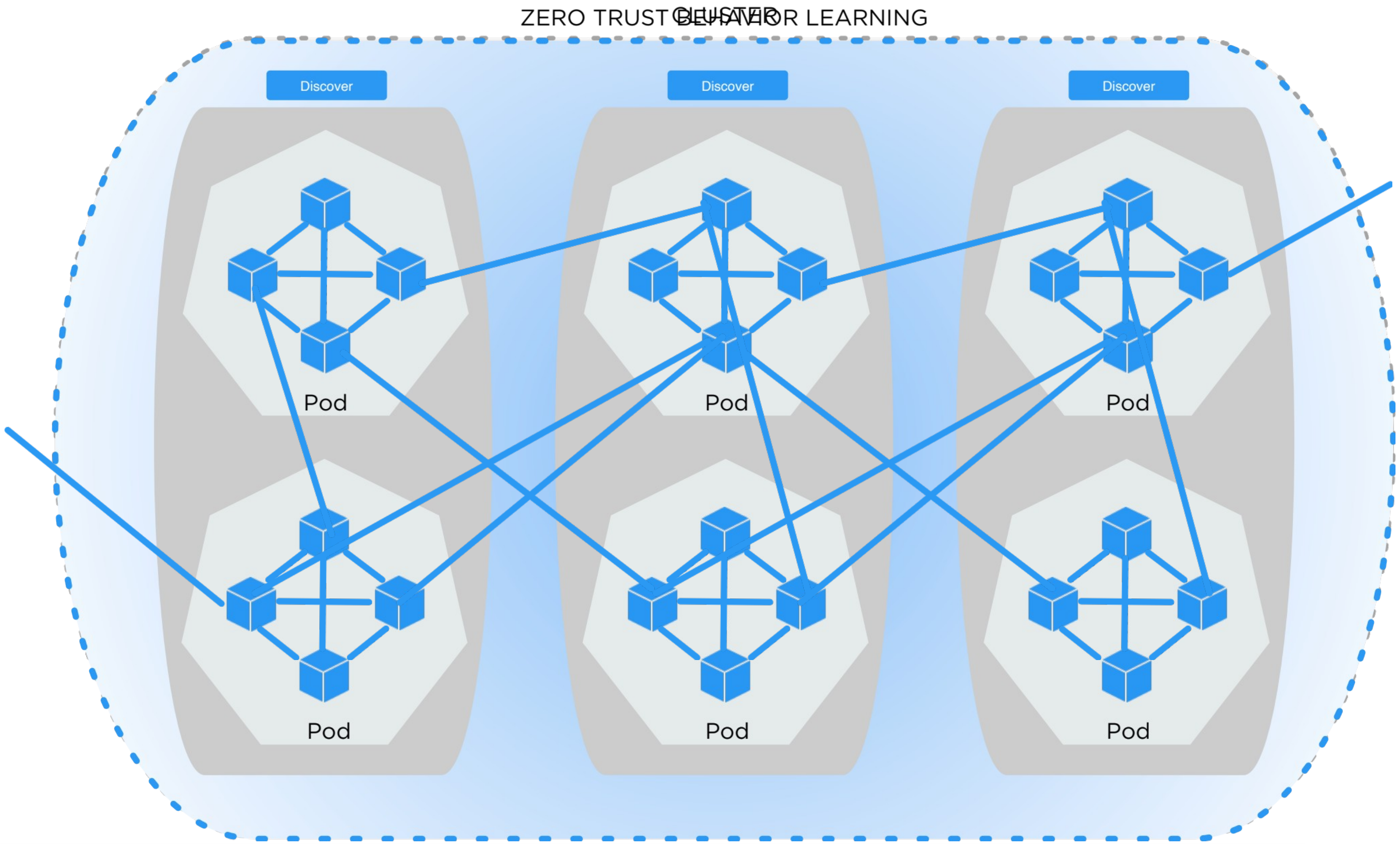
SUSE NeuVector

DPI enables

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



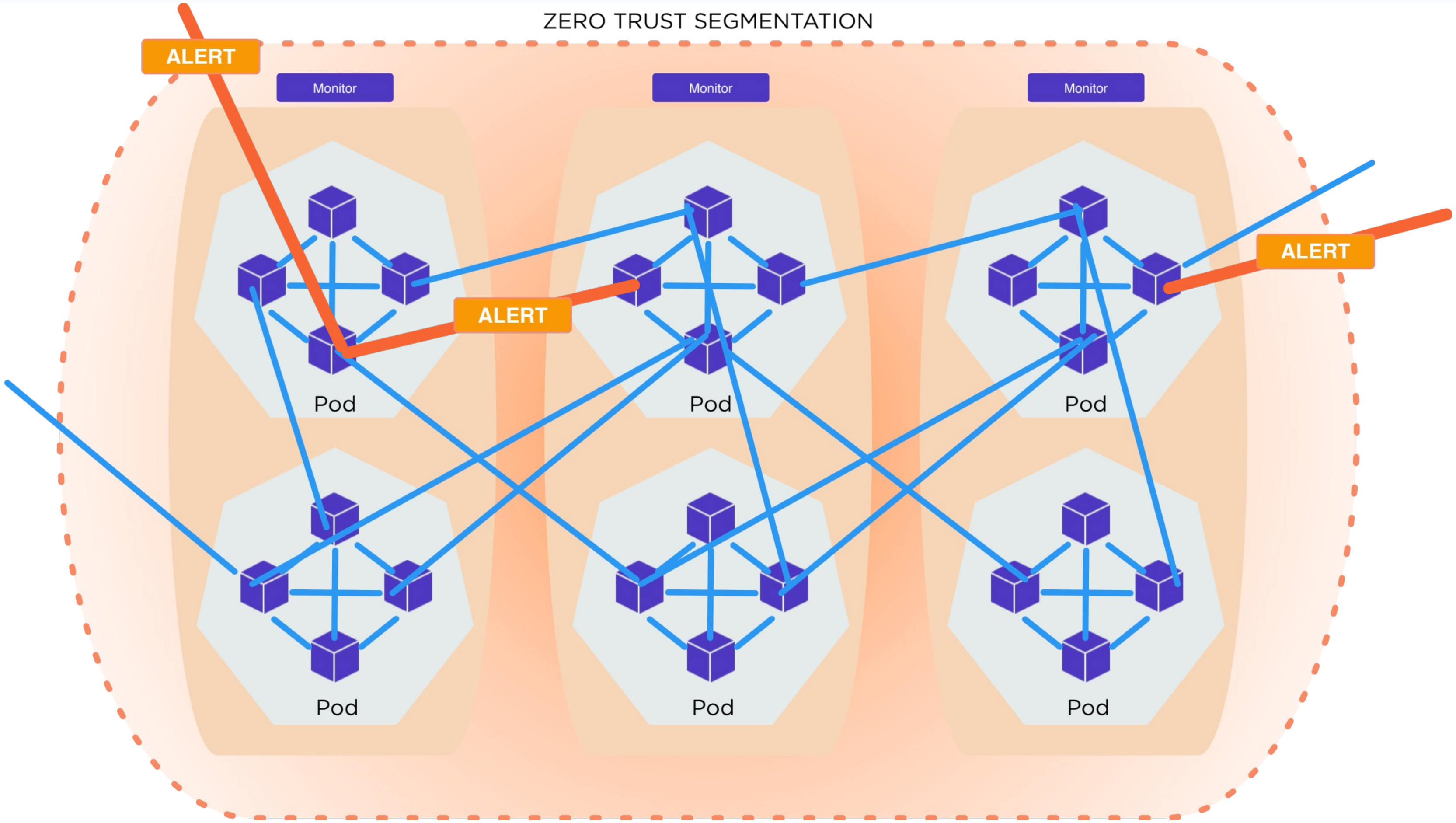
AUTOMATED *BEHAVIORAL-BASED* ZERO-TRUST



Discover

Identifies application behavior (Learning Mode)

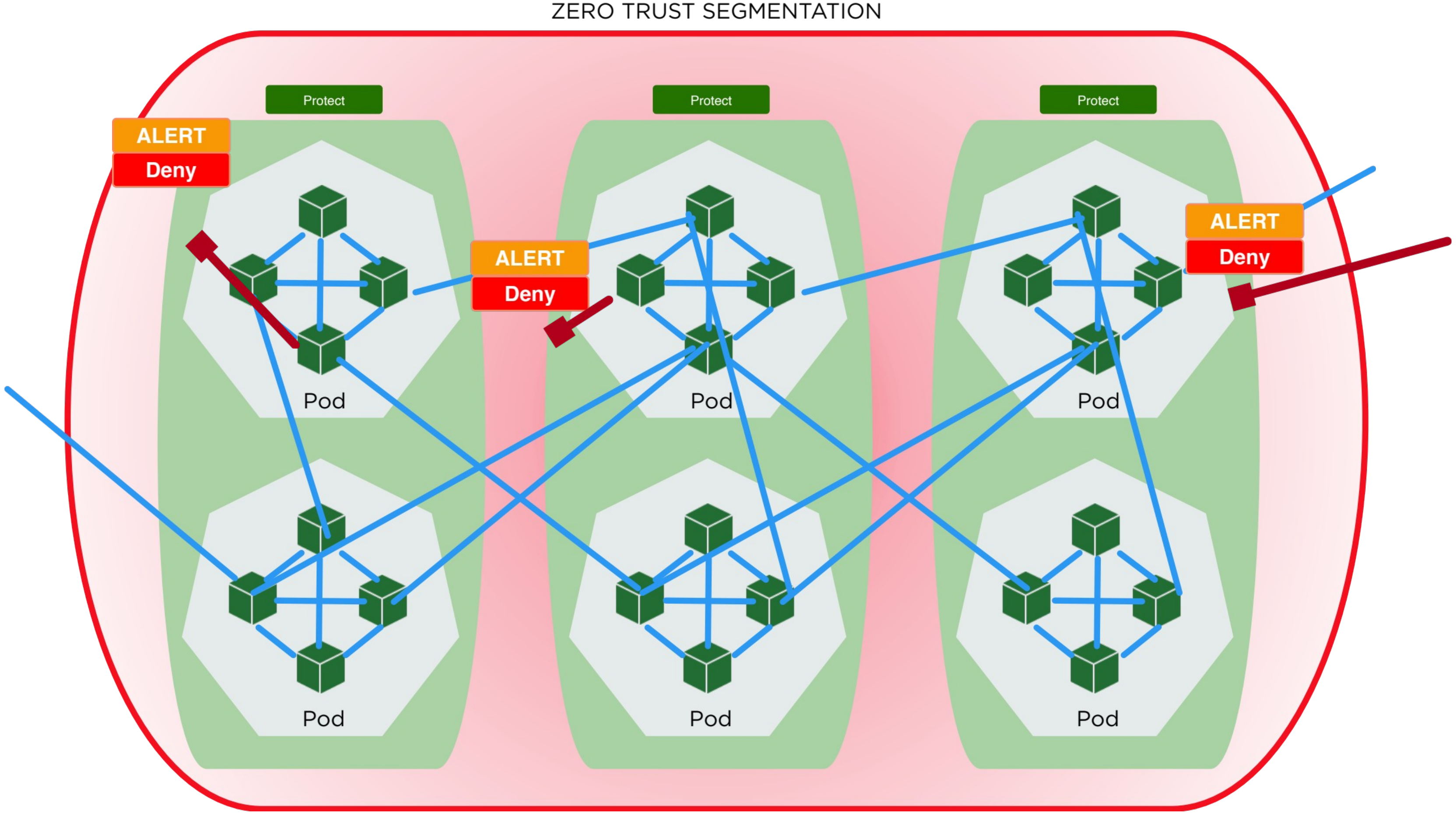
AUTOMATED *BEHAVIORAL-BASED* ZERO-TRUST



Discover Identifies application behavior (Learning Mode)

Monitor Alerts to any anomalous application behavior

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

Onboarding Experience

Installation typically takes:

- < 20 minutes via kubectl in Kubernetes
- < 5 minutes via helm chart

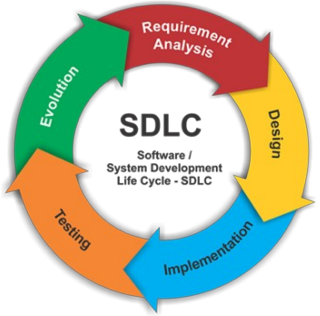
Configuration is less than 5 minutes.

POC engagements are supported by engineers!

- Installation
- Test Plans
- Operational Overview
  - CI/CD automation support
  - Overview / Training

DEVOPS PIPELINE TO PRODUCTION SECURITY

Full SDLC Vulnerability Management



Compliance / DLP

CIS Center for Internet Security®

GDPR

PCI Security Standards Council®

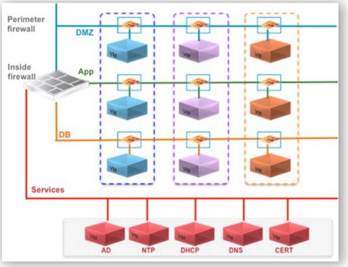
HIPAA

NIST

NeuVector

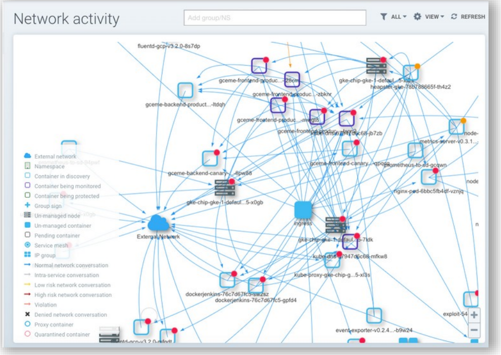
Full Lifecycle
Container
Security Platform

Layer 7 Application Micro-Segmentation



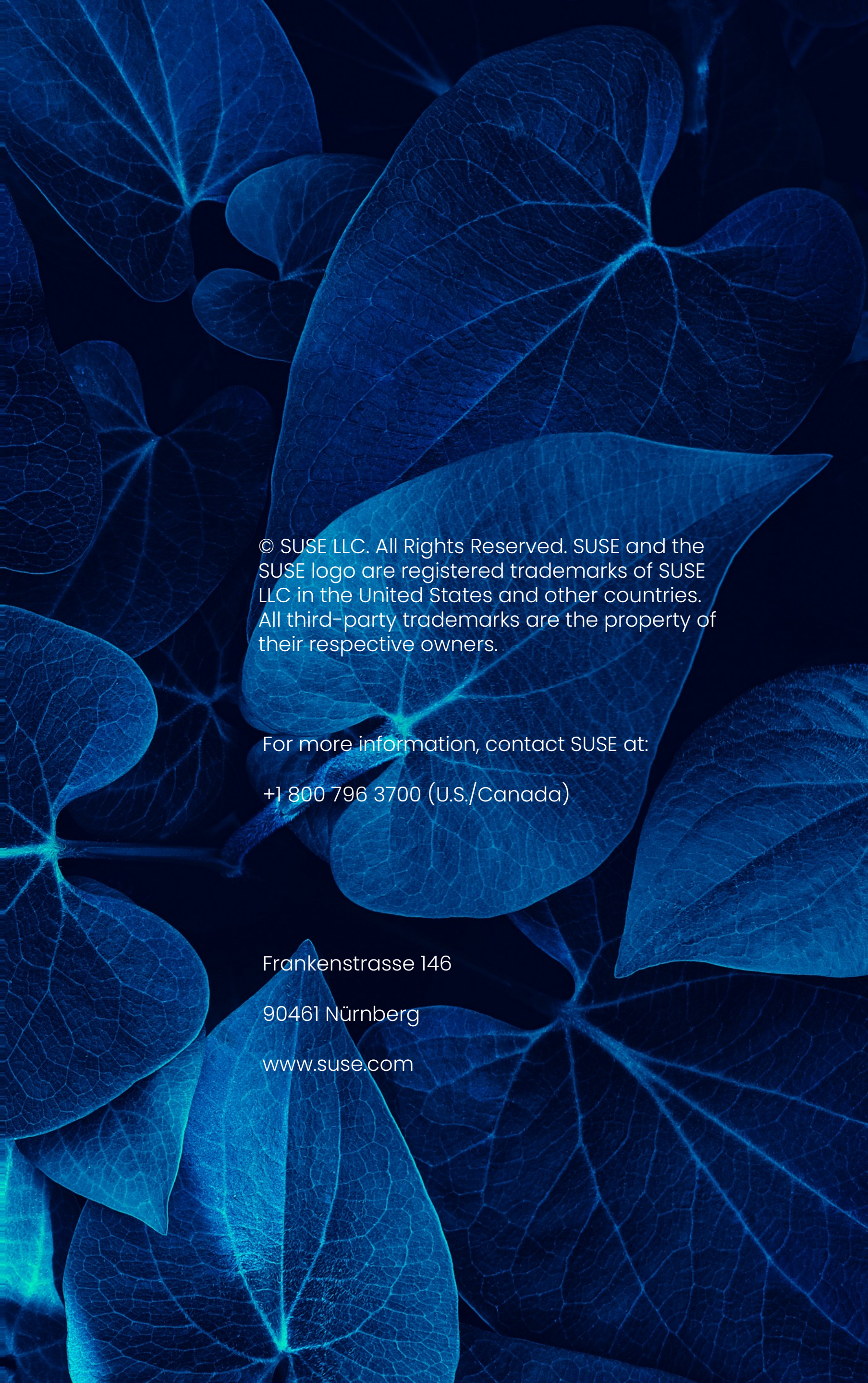
Zero-Day Attack Prevention

Policy Automation & Behavior Baselining


Network activity
Add group/NS
ALL
VIEW
REFRESH
External network
Namespace
Container in discovery
Container being monitored
Container being protected
Group sign
Un-managed node
Un-managed container
Pending container
Service mesh
IP group
Normal network conversation
Intra-service conversation
Low risk network conversation
High risk network conversation
Violation
Denied network conversation
Proxy container
Quarantined container
fluentd-gcp-v3.2.0-8s7dp
gceme-frontend-produc...-28cm
gke-chip-gke-1-defaul...5-xl3s
heapster-gke-78b788665f-th4z2
gceme-frontend-produc...-zbknr
gceme-backend-product...-ltdqh
gceme-frontend-produc...-mwgt8
kube-dns-6794fd6c68-jb7zb
metrics-server-v0.3.1...
gceme-frontend-canary...-qpqcg
prometheus-to-sd-gcqwn
gceme-backend-canary-...-6pw88
nginx-pod-6bbc5fb4df-vznjq
gke-chip-gke-1-defaul...5-x0gb
ingress
External Network
gke-chip-gke-1-defaul...5-7ldk
kube-dns-6794fd6c68-mfkw8
kube-proxy-gke-chip-g...5-xl3s
dockerjenkins-76c7d67fc5-sw2sz
dockerjenkins-76c7d67fc5-gpfd4
exploit-54
event-exporter-v0.2.4...-b9w24

RANCHER BY SUSE

Thank you



For more information, contact SUSE at:

+1 800 796 3700 (U.S./Canada)

Frankenstrasse 146

90461 Nürnberg

www.suse.com