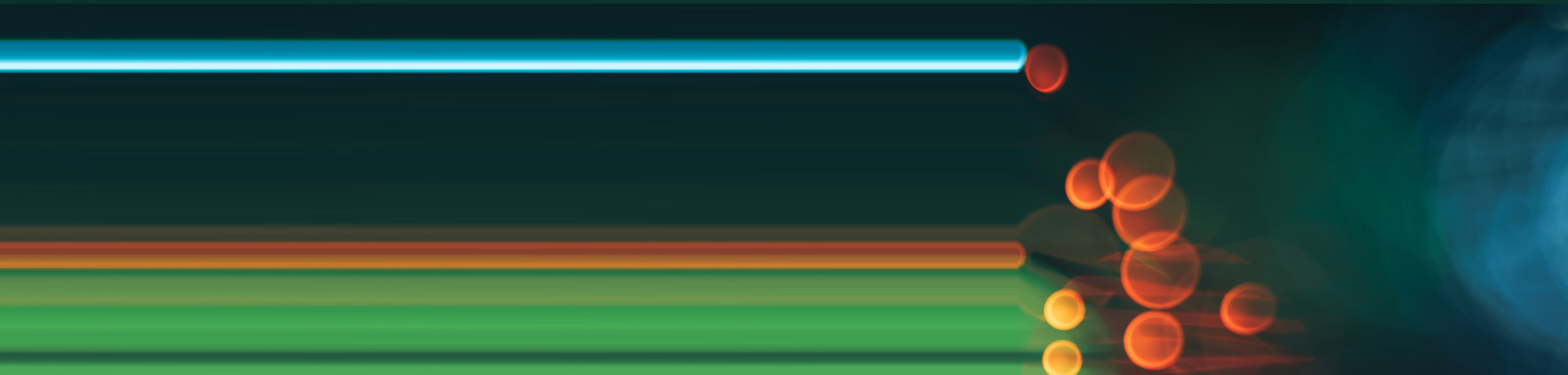
SUSE

Protect against unknown security vulnerabilities

Bastian Hofmann
Field Engineer



kubernetes

The Kubernetes Cluster

KUBERNETES / SECURITY / CONTRIBUTED

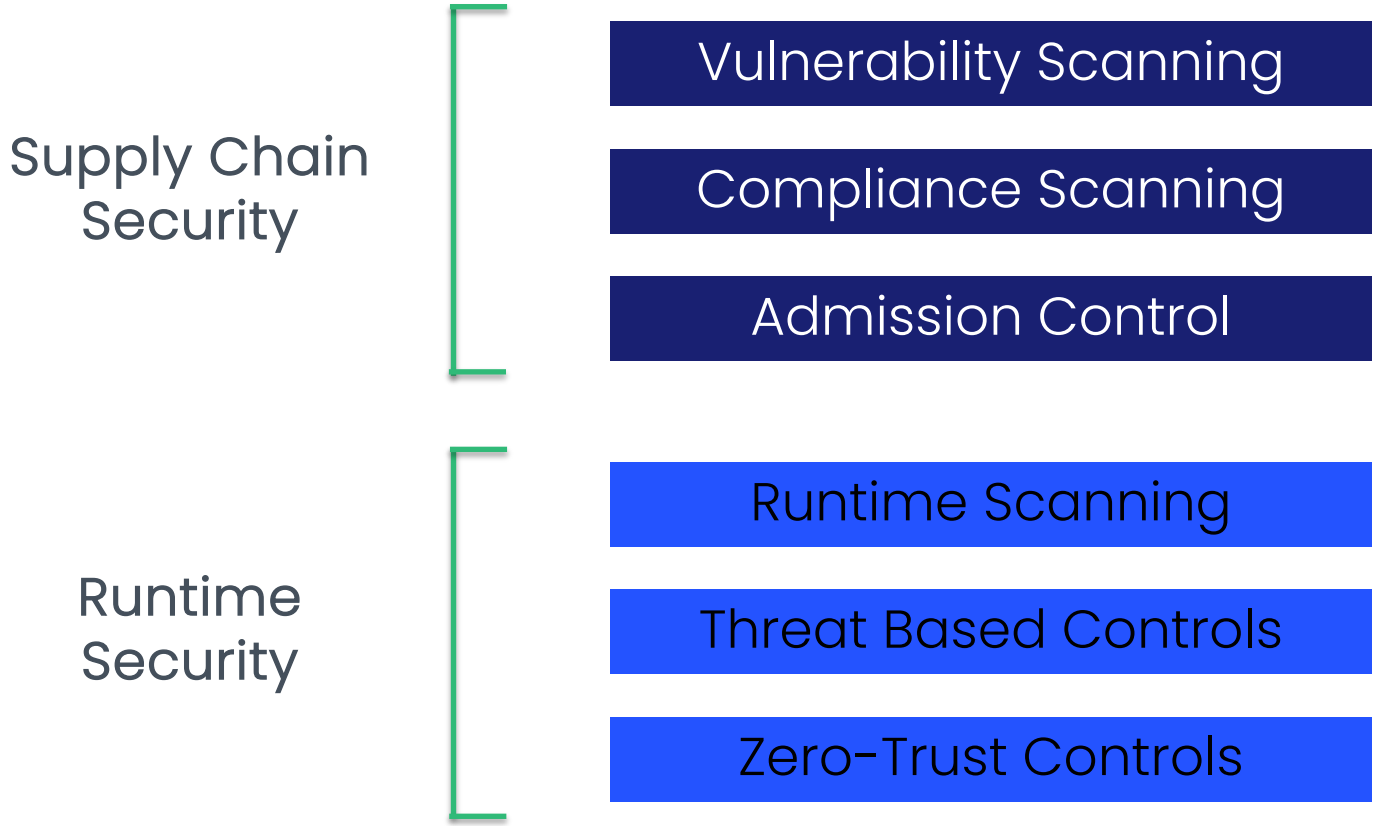
Kubernetes Is a High-Value Cyberwar Target

9 Mar 2022 10:00am, by Michael Clark

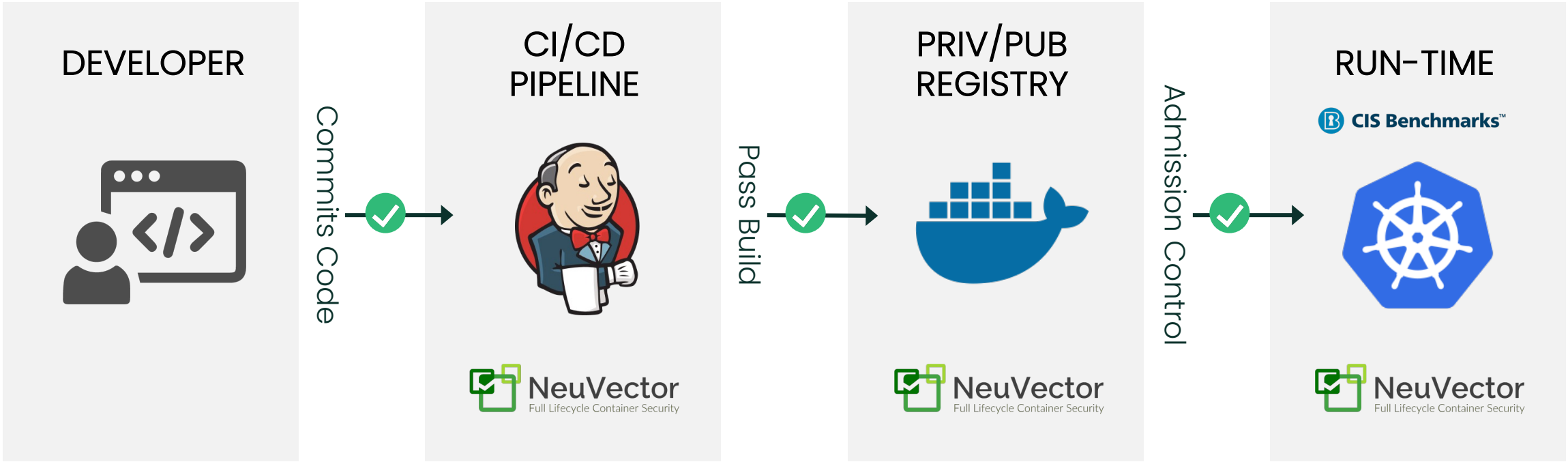
https://thenewstack.io/kubernetes-is-a-high-value-cyberwar-target/

Your applications

Layered Security: Defense In Depth



Vulnerability & compliance management



NeuVector is Unique

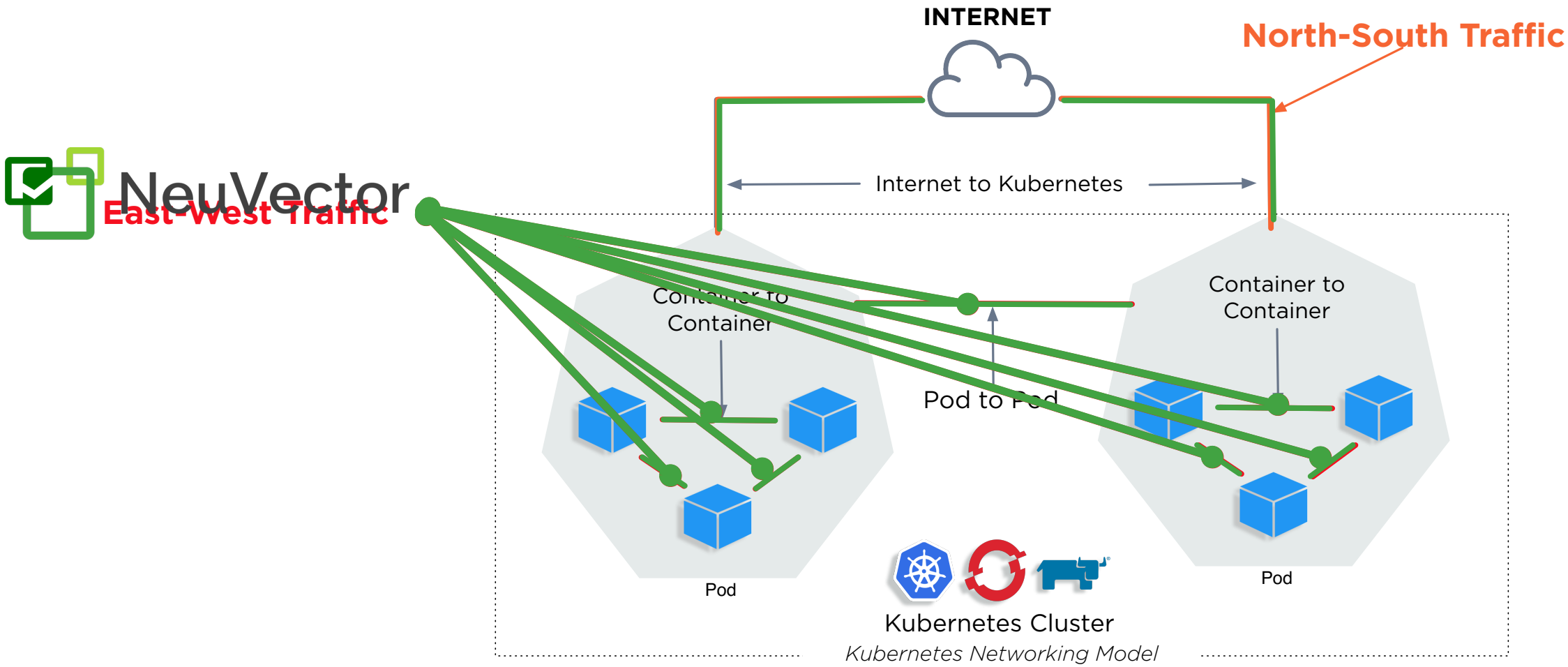
- Fast & Accurate
- Scalable to 100s of 1,000s of images
- Support for Air-Gapped Environments
- Easy to deploy – Kubernetes native

Run Time Security: Defense in Depth

Threat Based Controls
CVEs
WAF & DLP
Network Attacks
OWASP Top 10
Admission Control

Zero-Trust Controls
Automated Learning
Network
Process
File Access
Security as code

Runtime Behavioral Inspection

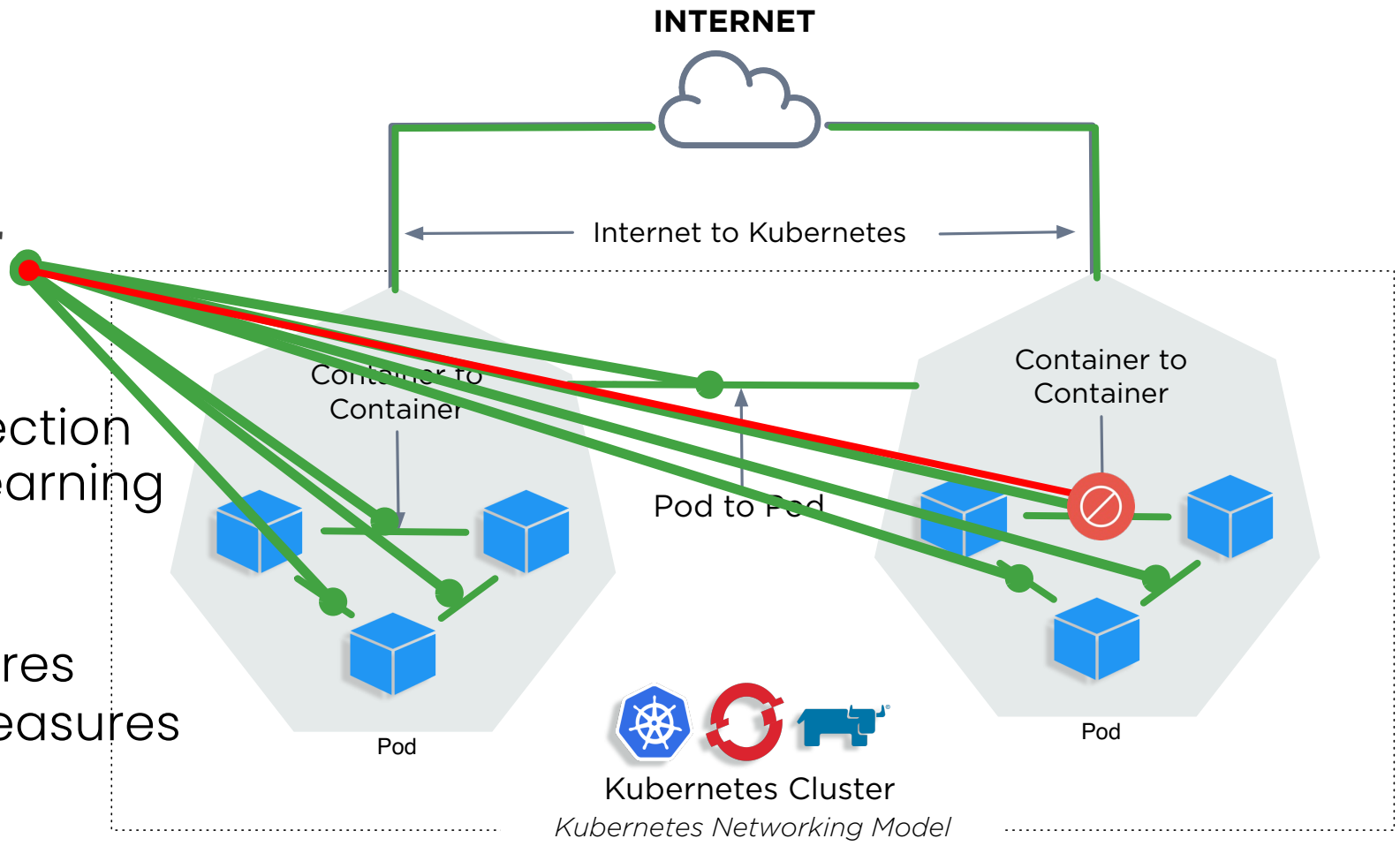


Runtime Behavioral Inspection

NeuVector

DPI enables
K8's Deep Packet Inspection (PATENTED)

- Automated Behavioral Learning
- Auto-Gen Security Policy
  - Layer 3/4 Port
  - Layer 7 Protocol + Processes
- Security as Code
- Zero-Day Countermeasures
- Unknown CVE Countermeasures
- Packet Capture
- Web Application Firewall
- Data Loss Prevention



Application Protocols Recognized

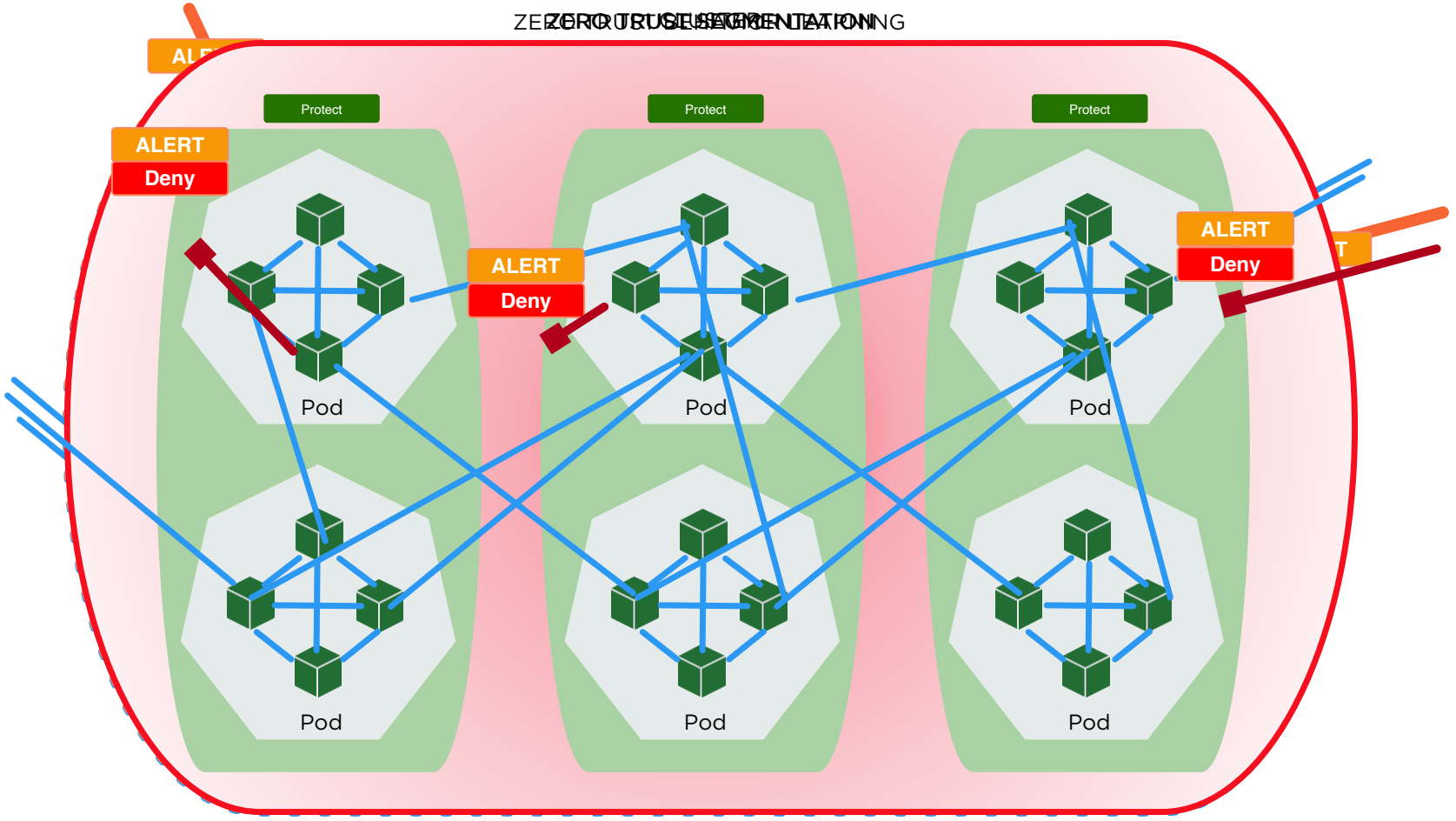
HTTP/HTTPS
SSL
SSH
DNS
DNCP
NTP
TFTP
ECHO
RTSP
SIP
ICMP
gRCP
MySQL
Redis
Zookeeper
Cassandra
MongoDB
PostgresSQL
Kafka
Couchbase
ActiveMQ
ElasticSearch
MemCache
Oracle
RabbitMQ
Radius
VoltDB
Consul
Syslog
Etcd
Spark
Apache
Nginx
Jetty
NodeJS

35 Layer-7 Application Protocols as of February 2022

Threats Automatically detected

SYN Flood	ICMP Flood	IP Teardrop
TCP Split Handshake	Ping Death	DNS Flood DDoS
Detect SSH 1, 2, or 3	Detect SSL TLS v1.0	SSL Heartbleed
HTTP Neg Content	HTTP Smuggling	MySQL Access Deny
TCP small window	DNS Buffer Overflow	DNS Null Type
DNS Zone Transfer	ICMP Tunneling	DNS Tunneling
SQL Injection	Apache Struts RCE	K8's MitM CVE-2020-8554
TCP Small MSS	Cipher Overflow	

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 is Unique

- Automate Security Policies
- Network Visibility in Production
- Zero Trust Protections - network, process and file access
- WAF & DLP
- Compliance scans (PCI, GDPR, NIST, ...)

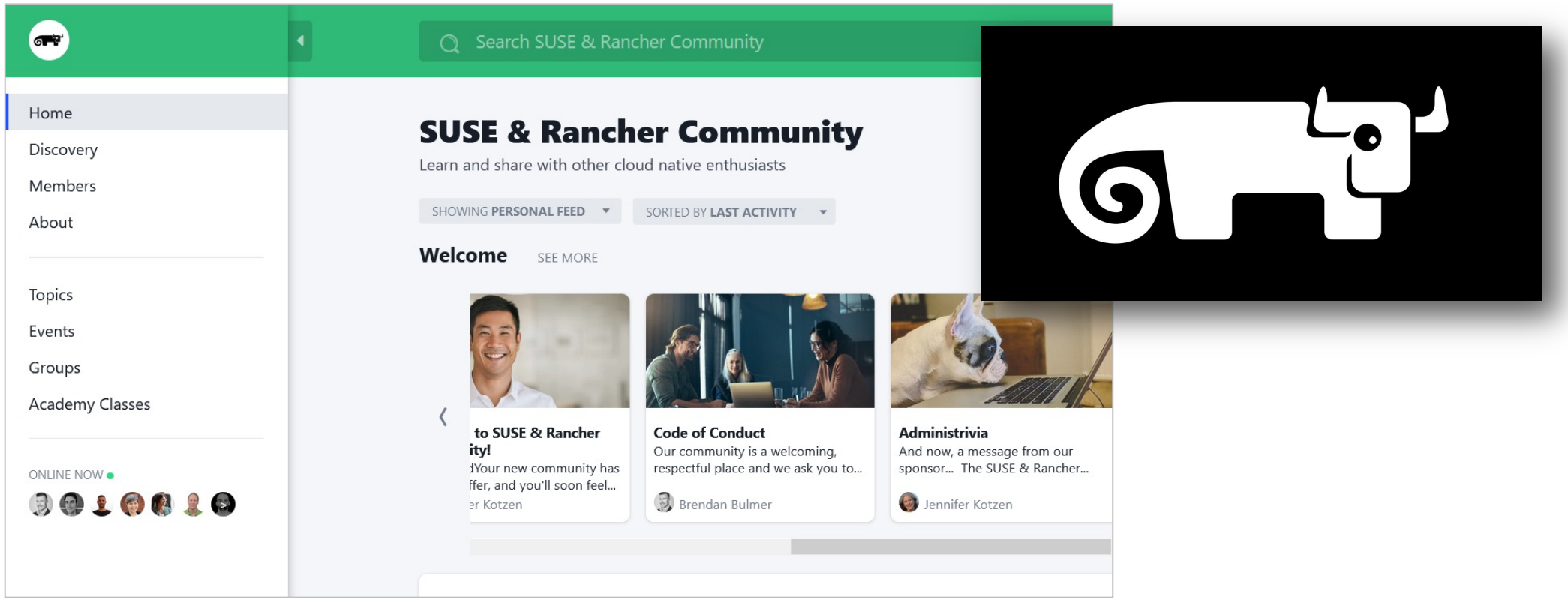
Demo

Resources

- https://neuvector.com/
- https://open-docs.neuvector.com/
- https://rancher.com
- https://suse.com

Join the SUSE & Rancher Community

https://community.suse.com



SUSE

Thank you

For more information, contact SUSE at:

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

Maxfeldstrasse 5

90409 Nuremberg

www.suse.com