

SUSE | Best Practices for Zero Trust Container Security on AWS

Please stand by. The webinar will begin shortly.

SUSE | Best Practices for Zero Trust Container Security on AWS

Webinar

Your Presenters



**Dominik
Wombacher**

Sr Partner Solutions Architect
Amazon Web Services
domwom@amazon.de



**Jain
Joseph**

Presales Consultant
SUSE
Jain.Joseph@suse.com

Agenda

1. NeuVector by SUSE
2. Amazon EKS – Shared responsibility model
3. NeuVector by SUSE on Amazon EKS demo
4. Further Information & Call to Action

NeuVector and AWS

Complementary security
products for a cloud native
world.



The Challenges?

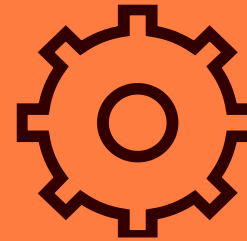
Containers increasing popularity makes them more attractive for attackers



Traditional Security tools don't work well in these environments



Containers automation requires security to be automated too.



Kubernetes dynamic nature poses new challenges for network security



NeuVector Layered Security



**Supply Chain
Security**

Vulnerability Scanning

Compliance Scanning

Admission Control

**Runtime
Security**

Runtime Scanning

Threat Based Controls

Zero-Trust Controls

Why NeuVector by SUSE on Amazon EKS

- SUSE strategic relationship with AWS – creating more value for customers; co-innovation, improved delivery and operational experiences
- Whole lifecycle container security & governance in the customer segment of the AWS shared responsibility model (more on this to follow)
- Fast time to launch
- Commercial agility & utilisation of cloud budget (PAYG /Private Offer)
- Procurement on marketplace of SUSE container services retires 50% against AWS Enterprise Discount Program (EDP)

Accelerate, secure & optimise your AWS EKS adoption with NeuVector by SUSE

Amazon Elastic Kubernetes Service (EKS)

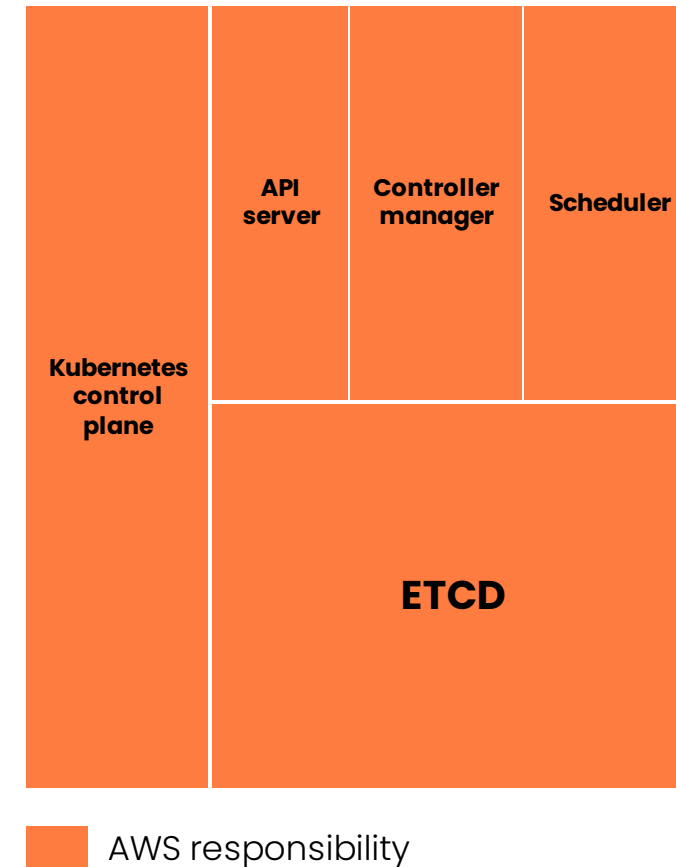
Security & Best Practices

Dominik Wombacher
Senior Partner Solutions Architect
domwom@amazon.de

Amazon EKS

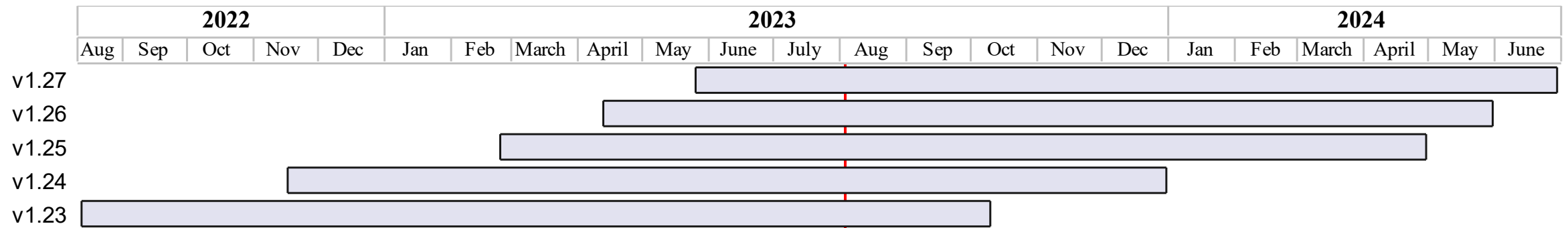
Overview

- **Managed** Kubernetes **Service**
- Tightly **integrated** with **AWS services**
- Built with the **Community**
- **Conformant** and **Compatible**



Amazon EKS

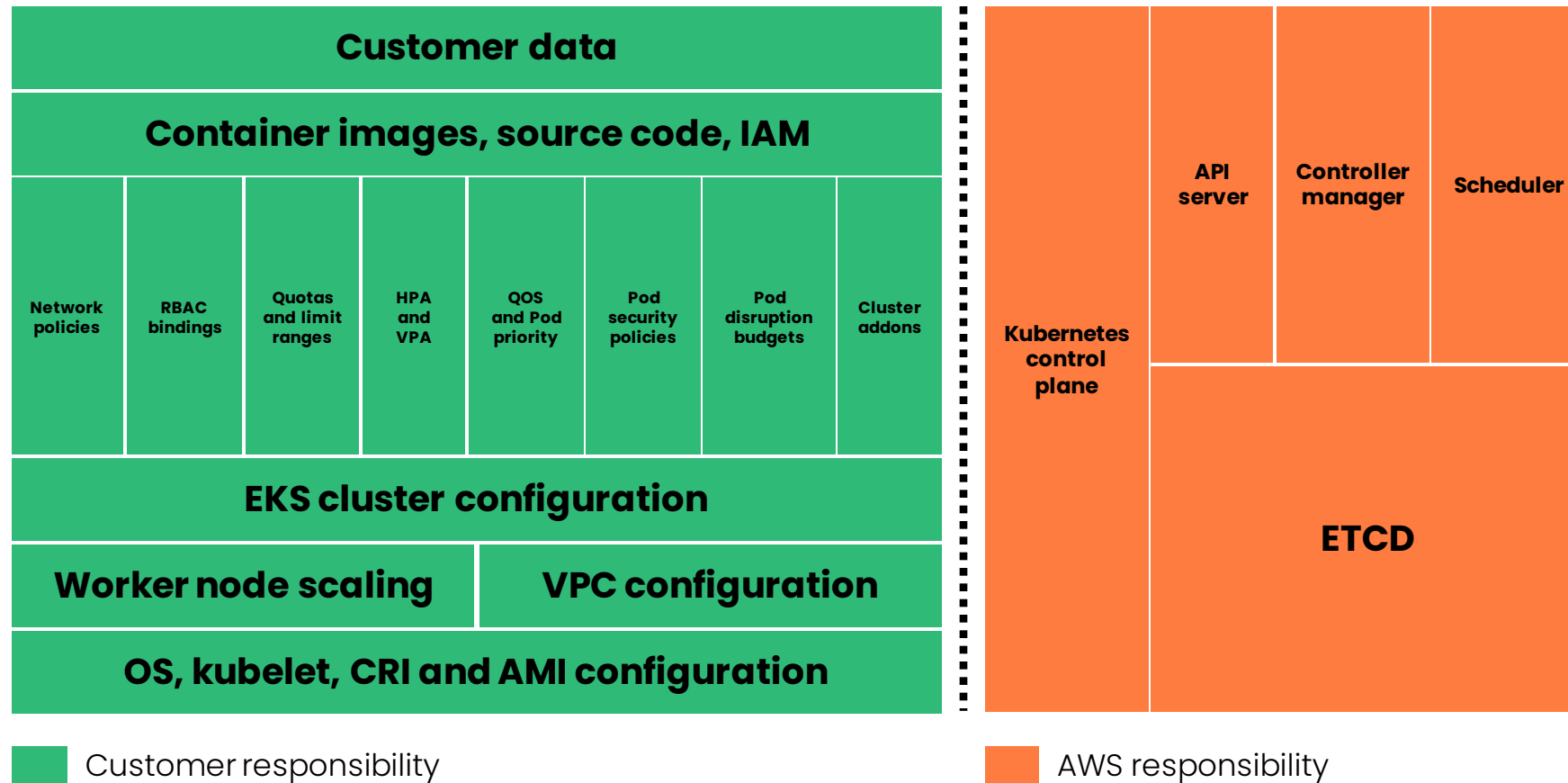
Kubernetes releases & lifecycle



End of support dates for v1.24 – v1.27 are approximate and are updated with an exact date when it's known.

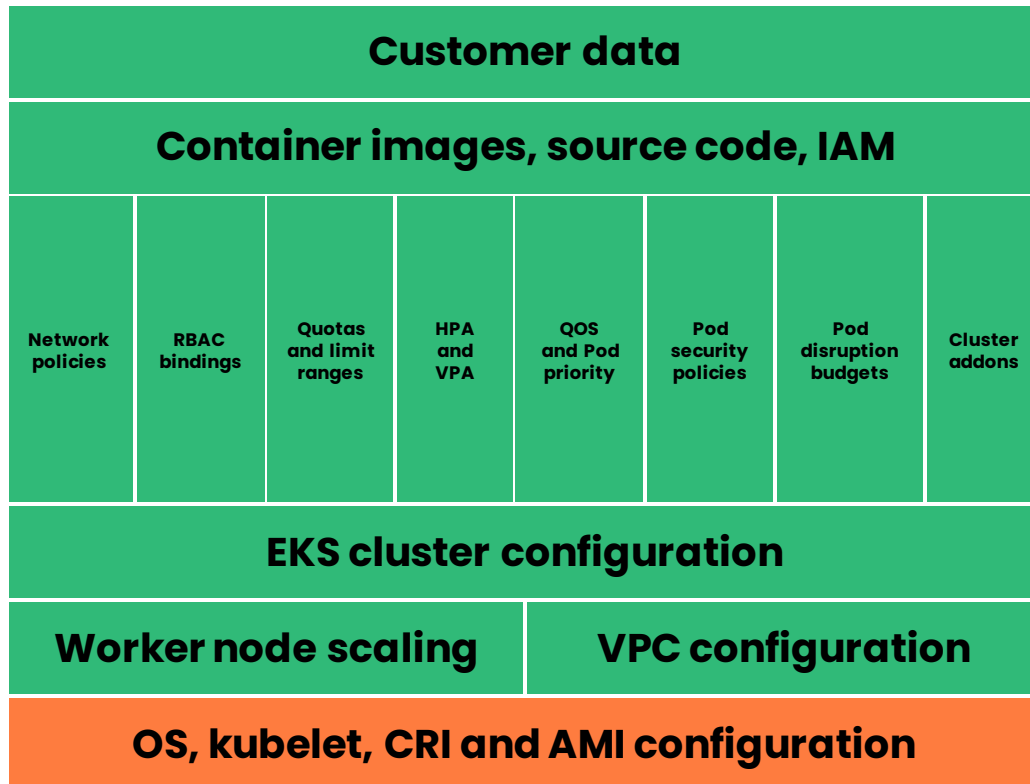
Amazon EKS

Shared responsibility model



Amazon EKS

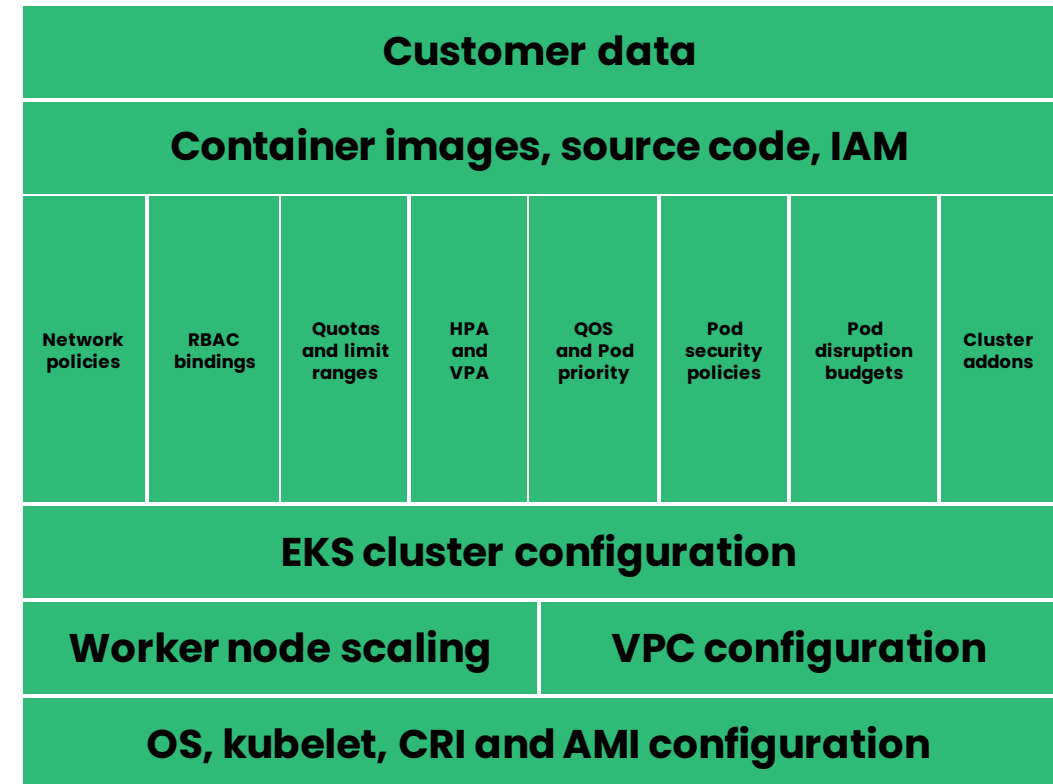
Managed Node Groups



 Customer responsibility

 AWS responsibility

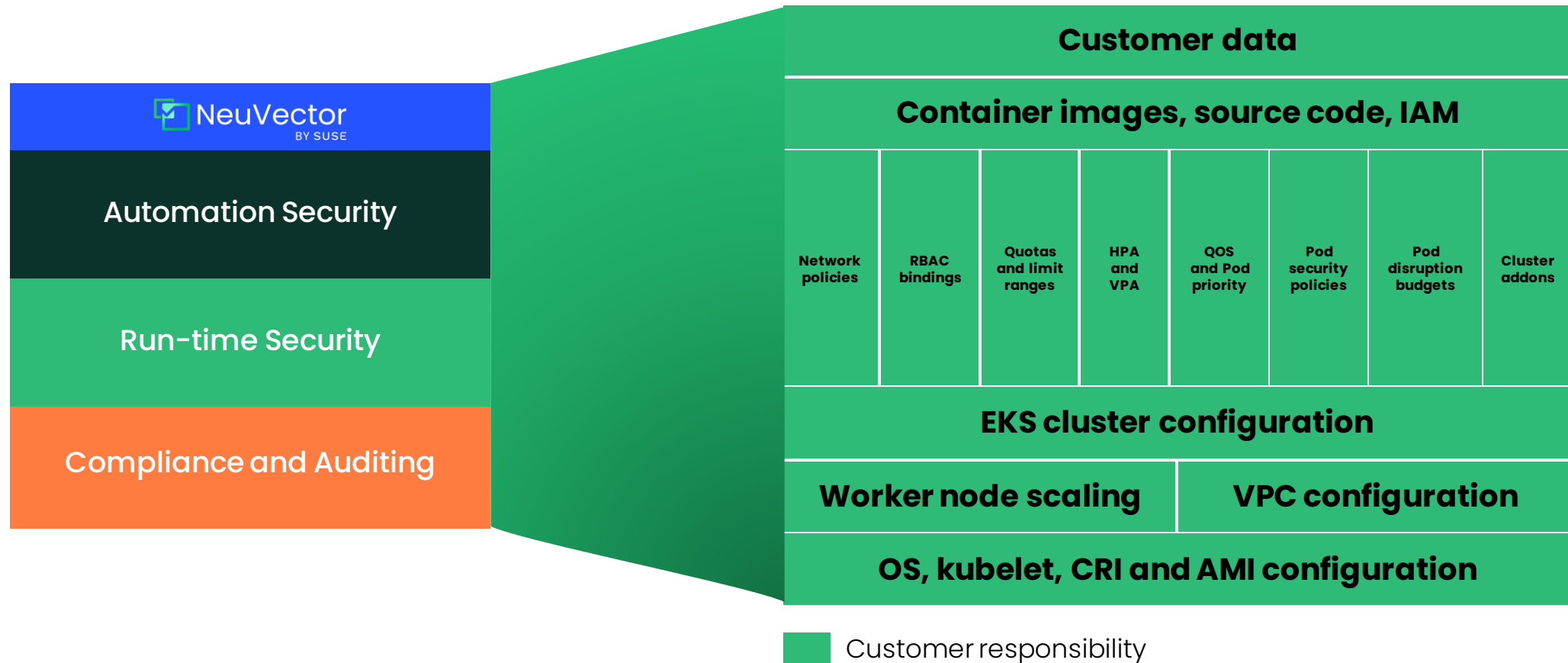
Self Managed Workers



 Customer responsibility

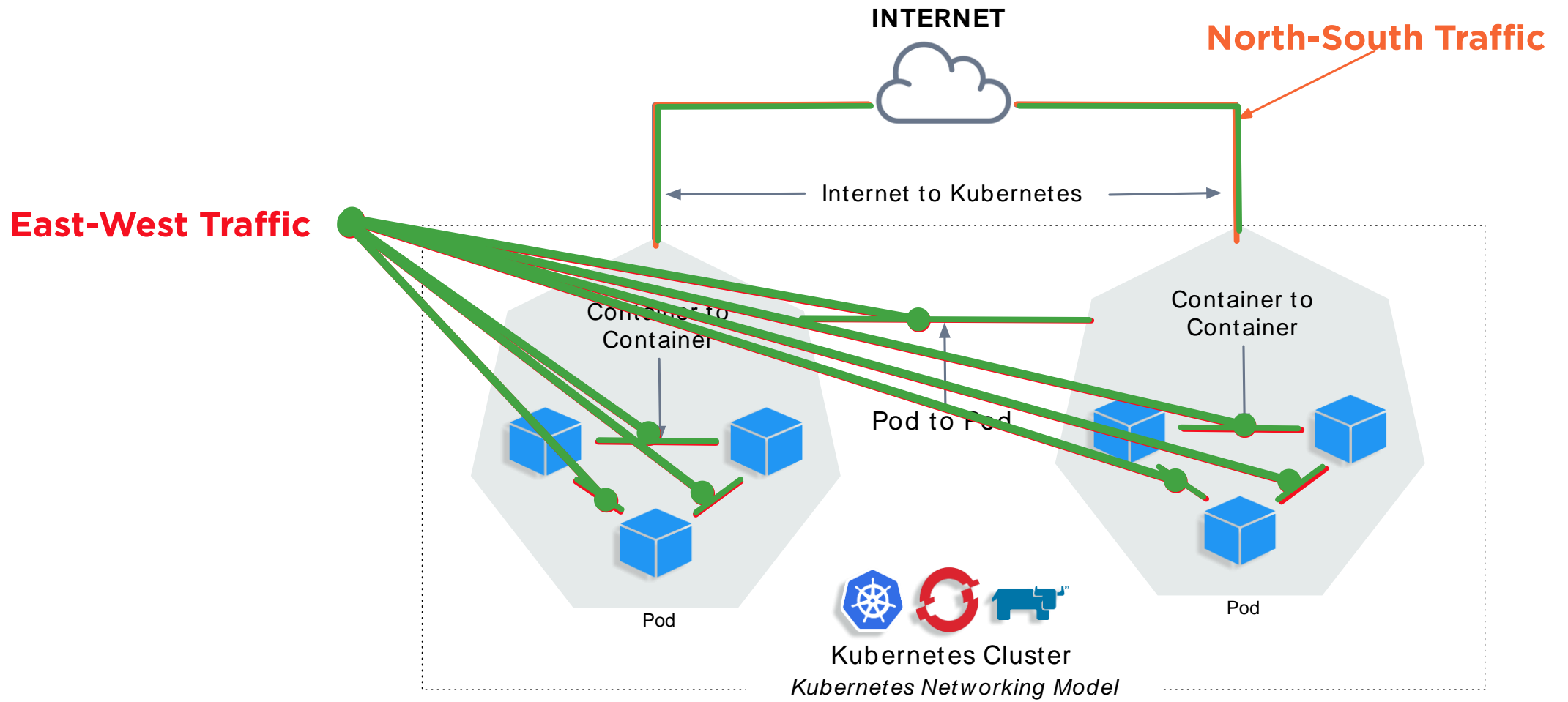
NeuVector by SUSE on Amazon EKS

Complementing the shared responsibility model



NeuVector on EKS demo

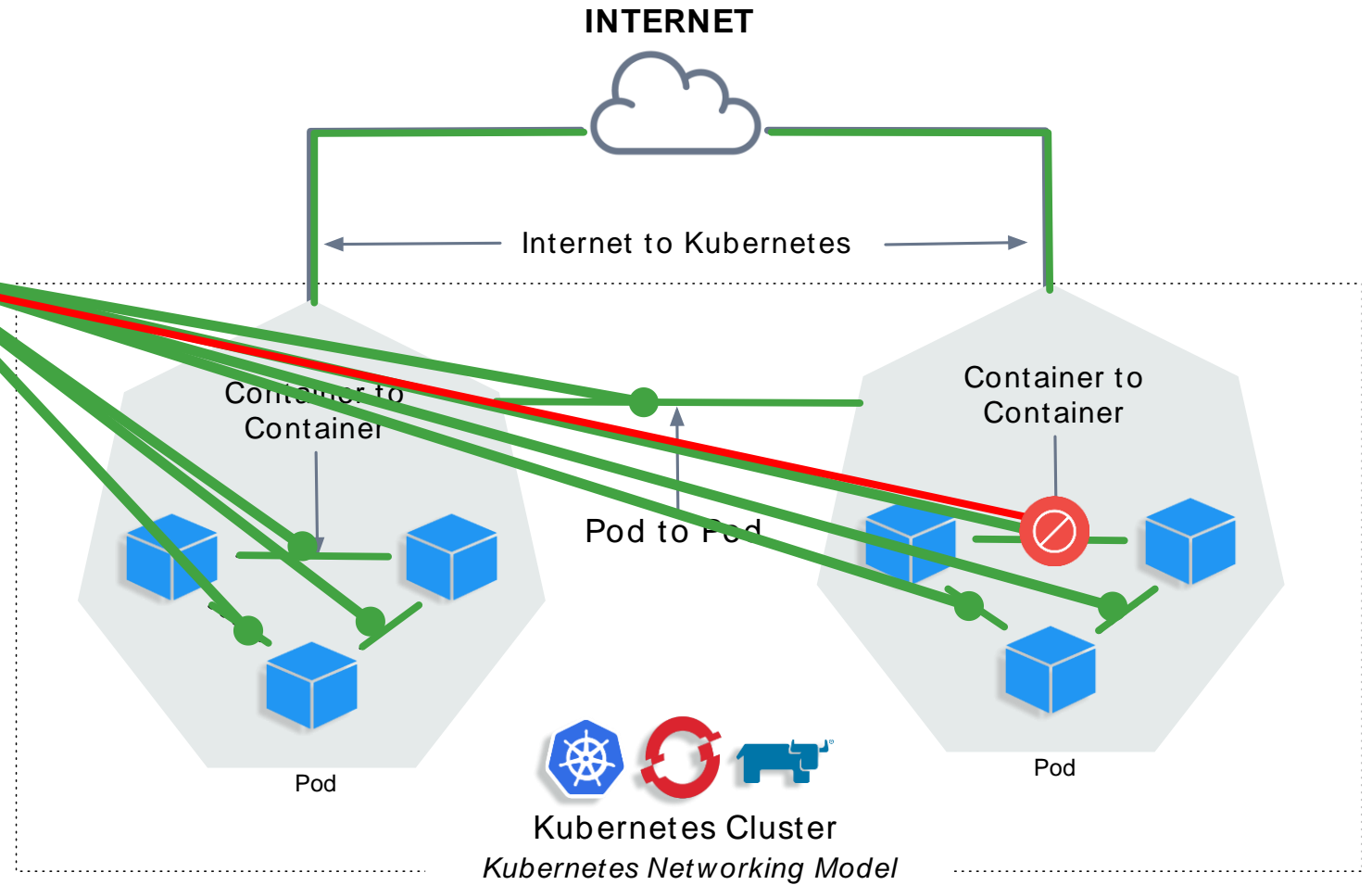
Jain Joseph
Presales Consultant
Jain.Joseph@suse.com



NeuVector BY SUSE

K8's Deep Packet Inspection (PATENTED)

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

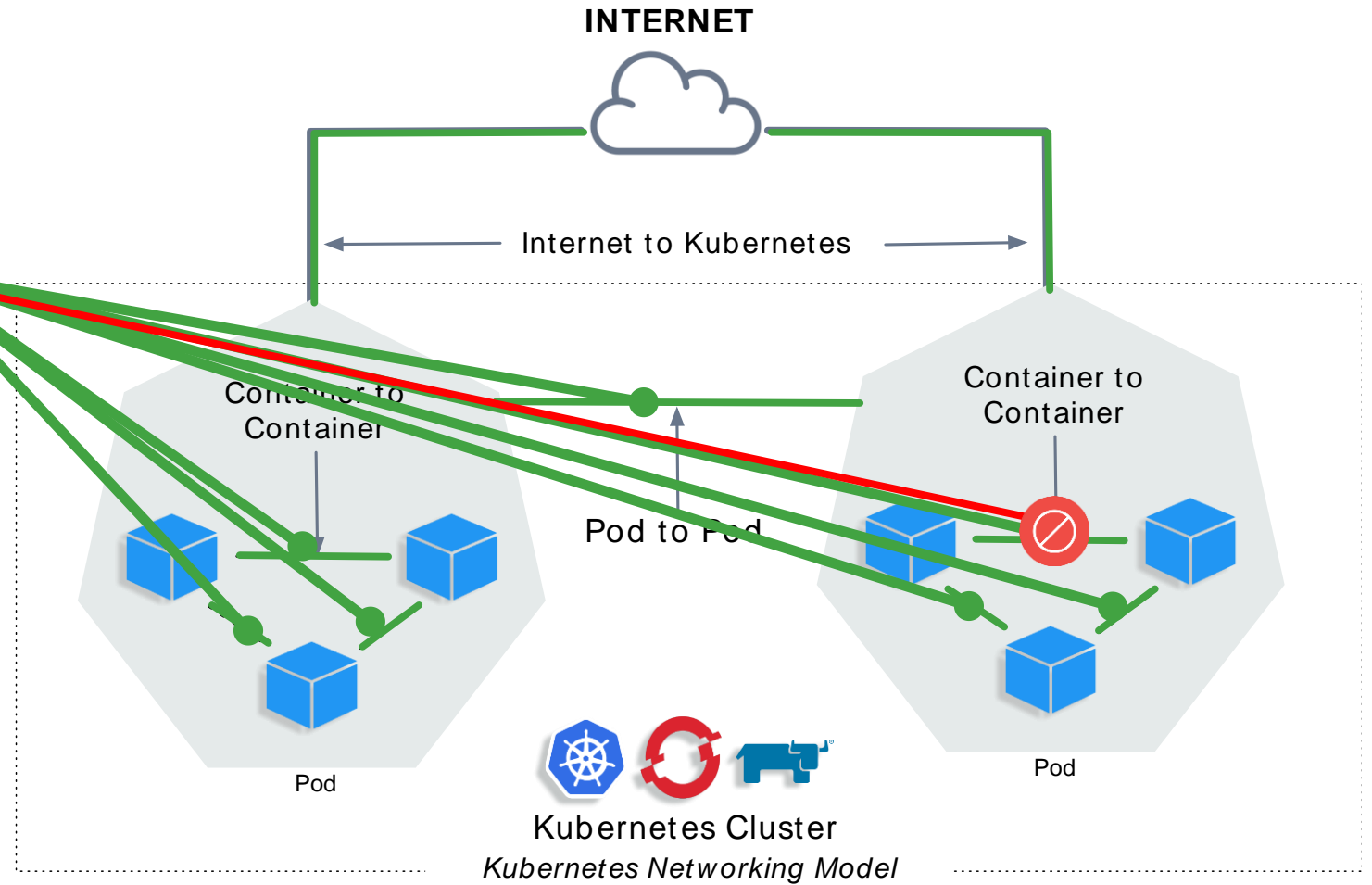


NeuVector

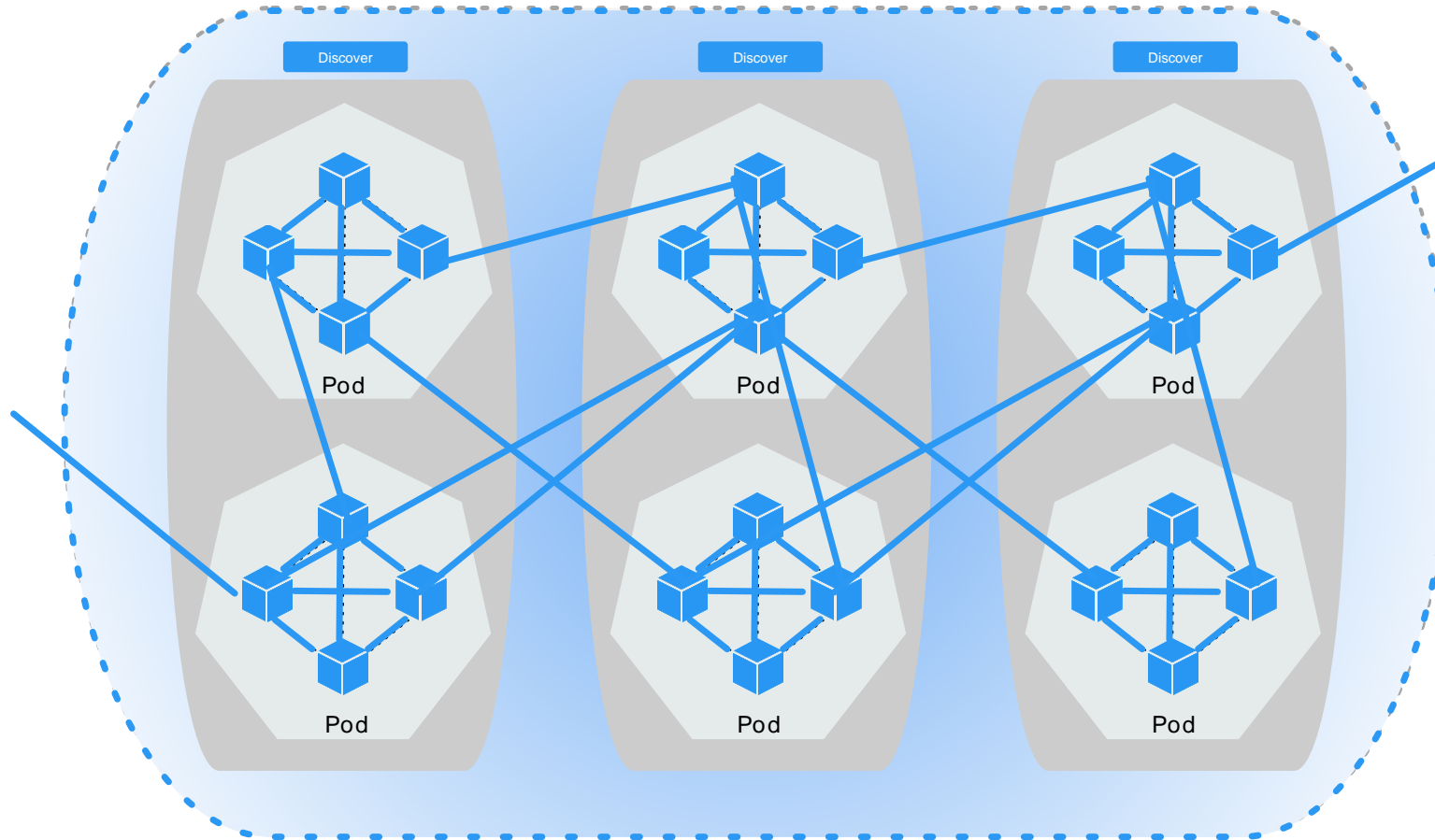
BY SUSE

DPI enables

- Automated Behavioral Learning
- Visibility You Didn't Have Before
- Auto-Gen Security Policy
- Security as Code
- Zero-Day Countermeasures
- Unknown CVE Countermeasures
- Packet Capture
- Data Loss Prevention



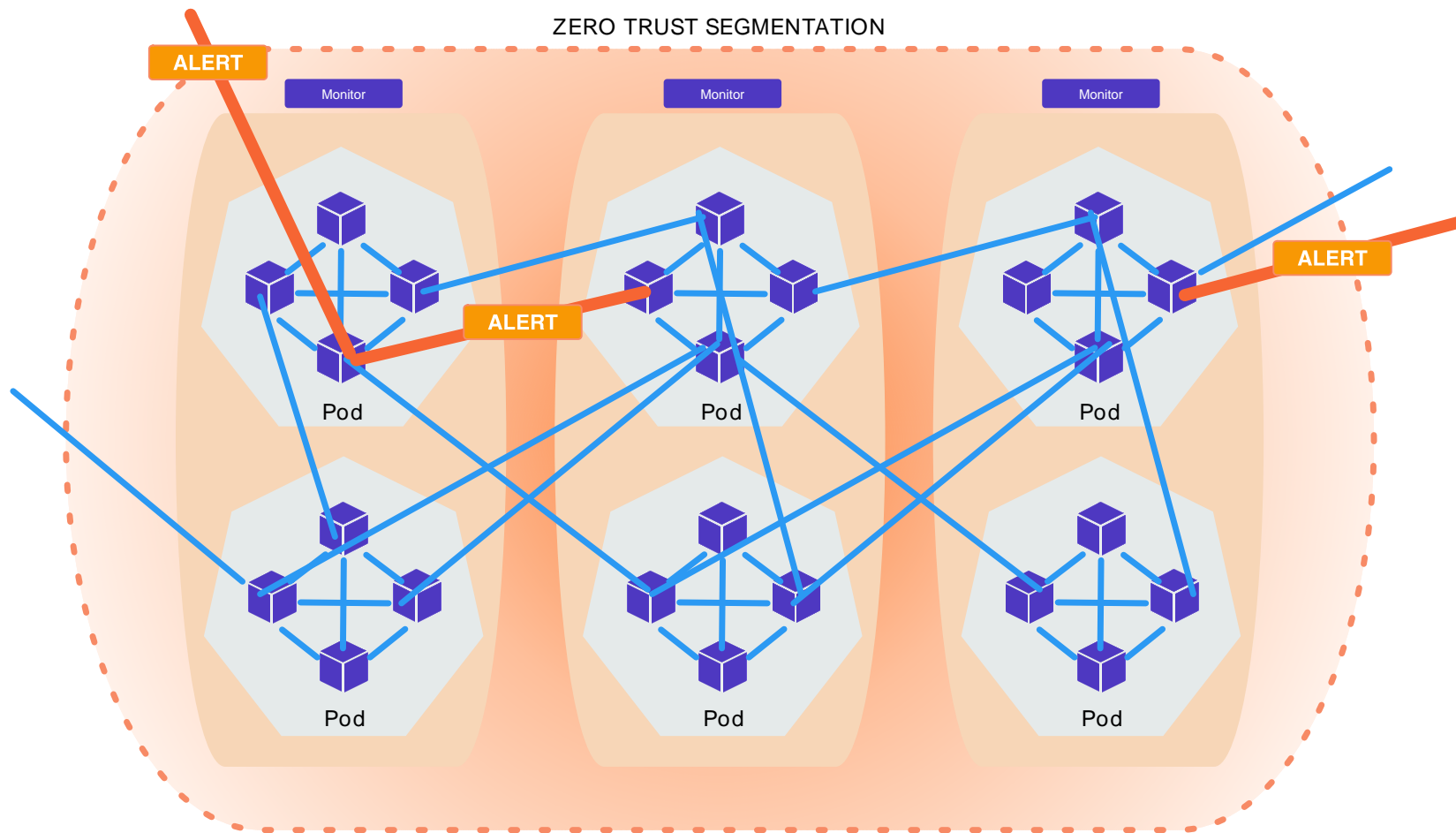
ZERO TRUST CLUSTER



Discover

Identifies application behavior (Learning Mode)





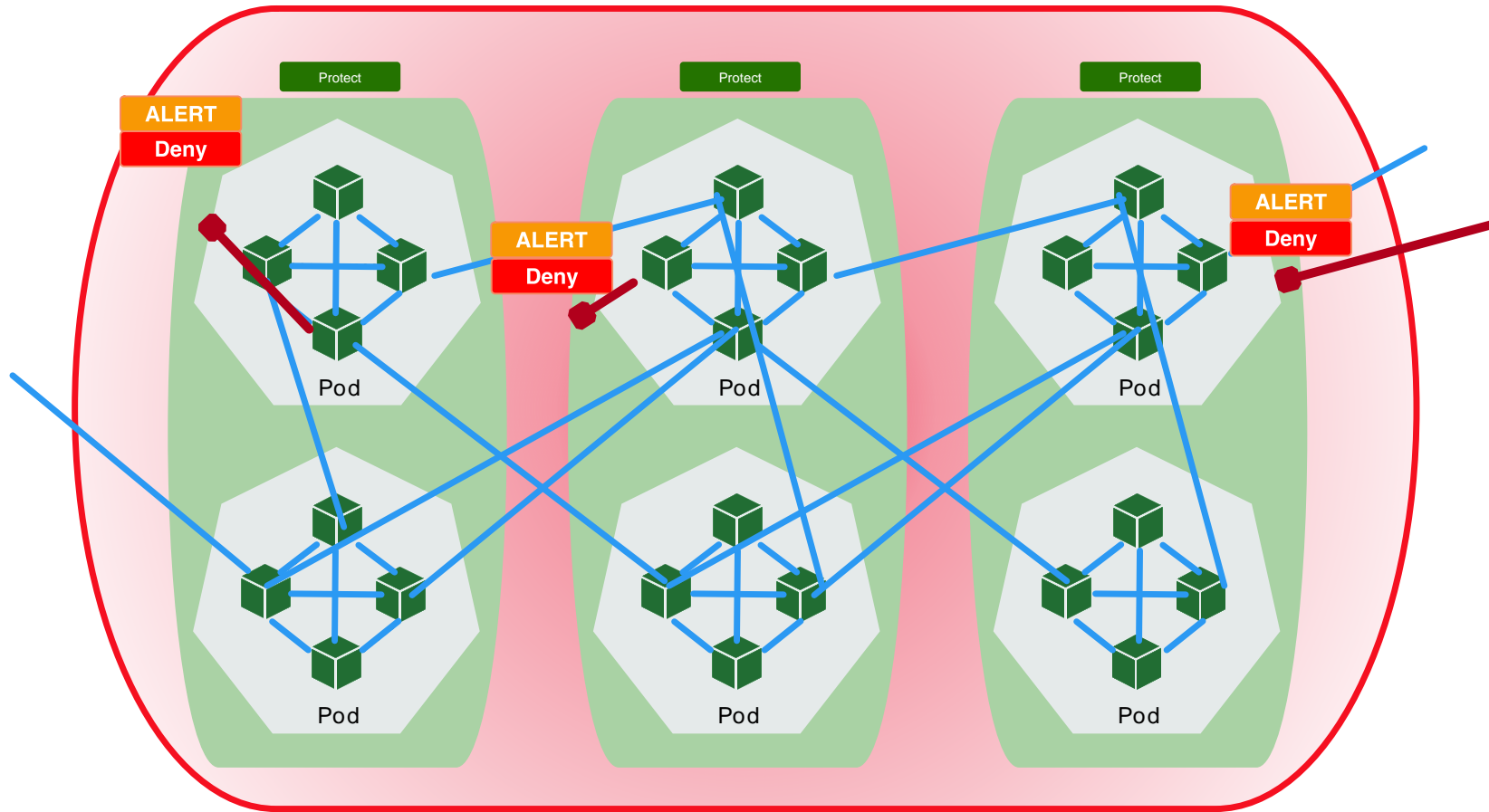
 Discover

Identifies application behavior (Learning Mode)

 Monitor

Alerts to any anomalous application behavior

ZERO TRUST SEGMENTATION



 Discover

Identifies application behavior (Learning Mode)

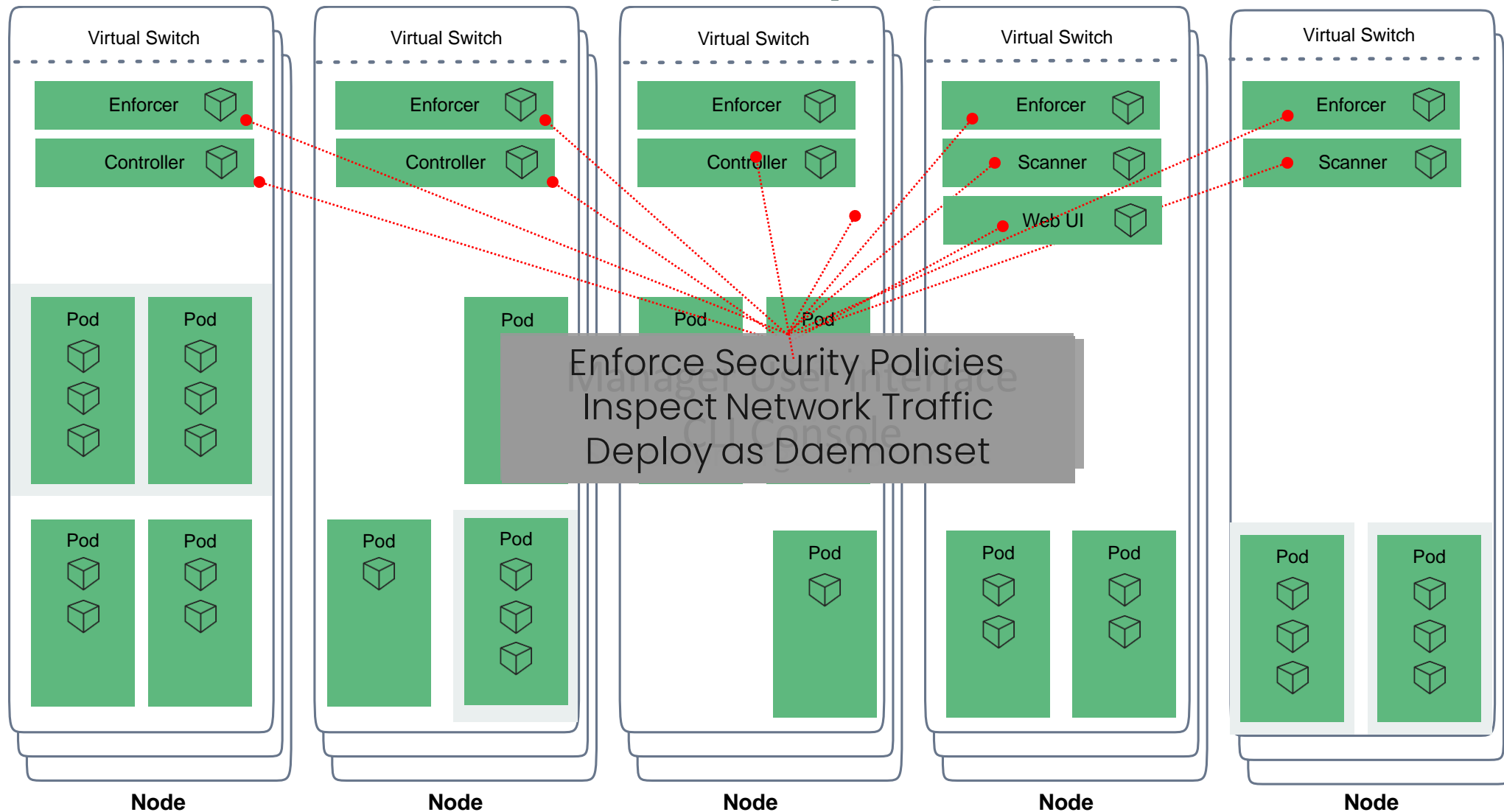
 Monitor

Alerts to any anomalous application behavior

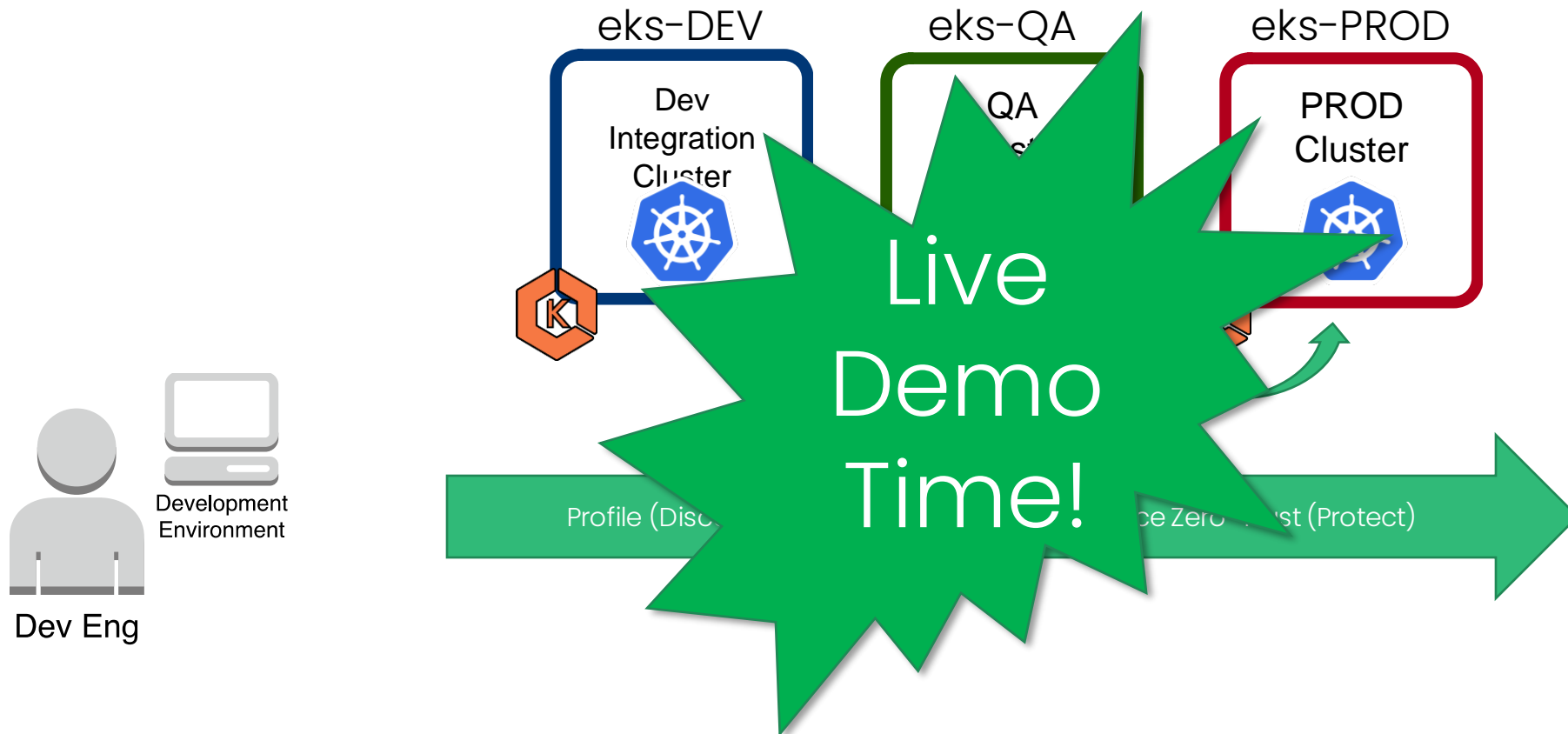
 Protect

Denies on any anomalous application behavior

NeuVector architecture / deployment

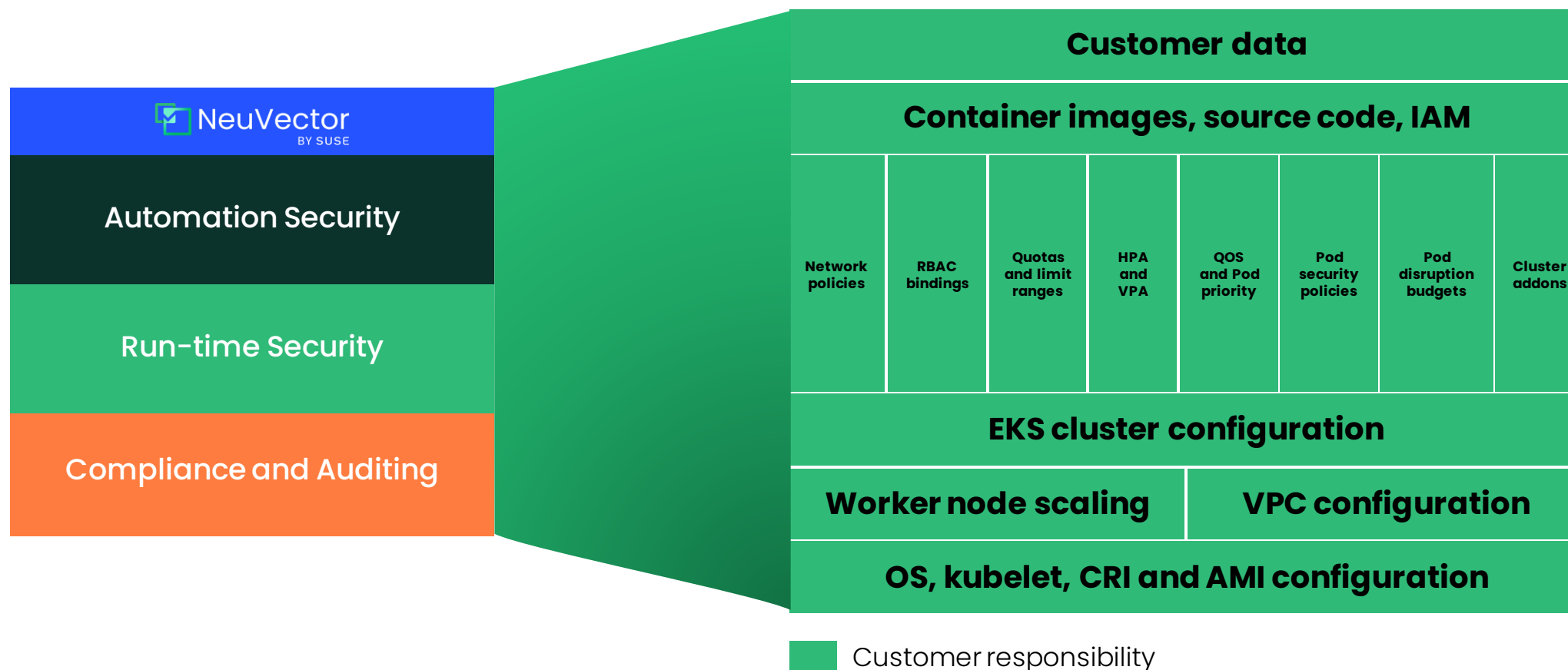


Securing your environment from development to production



NeuVector by SUSE on Amazon EKS

Complementing the shared responsibility model



Further information

- [Blog: Introducing NeuVector with Enterprise Support on the AWS marketplace](#)
- [The Ultimate Guide to Kubernetes Security on AWS white paper](#)
- [Blog: Protect Kubernetes Containers on AWS](#)
- [Rodeos: Explore the SUSE Events page using tags to find Rodeos for NeuVector and Rancher](#)



Call to Action

Accelerate, secure & optimise your AWS EKS adoption with NeuVector by SUSE



Link to AWS listing
for EU & UK

NeuVector Prime (EU and UK only)
By: SUSE
Latest Version: NeuVector Prime 5.2.0-s1
NeuVector Prime is the only 100% open source, Zero Trust container security platform. (This listing is for EU and UK based AWS accounts) Continuously scan throughout the container
Linux/Unix

Pricing Information
Use this tool to estimate the software and infrastructure costs based on your configuration choices. Your usage and costs might be different from this estimate. They will be reflected on your monthly AWS billing reports.

Estimating your costs
Choose your region and fulfillment option to see the pricing details. Then, modify the estimated price by choosing different instance types.

Fulfillment Option
NeuVector Prime via Helm

Software Pricing Details
NeuVector Prime (EU and UK only)

The table shows current software pricing. Additional taxes or fees may apply. Use of Local Zones or WaveLength infrastructure deployment may alter your final pricing.

Unit type	Cost/unit
5 to 15 nodes per month per node	\$112.00
16 to 50 nodes per month per node	\$105.00
51 to 100 nodes per month per node	\$98.00
101 to 250 nodes per month per node	\$91.00
251 to 1000 nodes per month per node	\$84.00
> 1000 nodes per month per node	\$78.00

Infrastructure price
Amazon EC2 and Amazon EKS are required. For detailed infrastructure costs, please refer to Amazon EC2 or Amazon EKS pricing.

Additional Resources
[NeuVector on AWS FAQ](#)
[Project Documentation](#)
[SUSE Support Center \(SSC\)](#)

Helm chart
Helm charts are Kubernetes YAML manifests combined into a single package that can be installed on Kubernetes clusters. The containerized application is deployed on a cluster by running a single helm install command to install the seller-provided Helm chart.

Product Overview
NeuVector Prime is a 100% open source Kubernetes container security platform built for enterprise-grade environments. Supported by a strong community of users, NeuVector provides full lifecycle container security from build, pipeline, registry to production. NeuVector enables you to run Kubernetes SECURELY everywhere - from cloud to on-prem or at the edge. In addition to end-to-end vulnerability and compliance scanning, NeuVector provides unique runtime protection which combines a layer7 container firewall with workload process/file protections. The network protection of NeuVector uses deep packet inspection (DPI) to monitor and block network threats, segmentation violations, and unauthorized ingress or egress connections. This technology enables data leak protection (DLP) rules, web application firewall (WAF) rules, API security validation, and is compatible with service meshes such as Istio and AWS App Mesh. NeuVector is a cloud-native solution which deploys easily on EKS to protect workloads and hosts from vulnerability exploits and zero-day attacks. The deployment is a set of containers (manager, controller, enforcer, scanner) which can be managed through the console or rest API. This deployment configures a AWS load balancer service to expose the manager console. For more information on NeuVector see the project documentation at <https://open-docs.neuvector.com/>.

Usage Information
Fulfillment Options
NeuVector Prime via Helm
Helm chart
Supported services: [Learn more](#)
Amazon EKS
[View usage instructions](#)

End-user license agreement
By subscribing to this product you agree to terms and conditions outlined in the product [End User License Agreement \(EULA\)](#)

Interested in running a Proof of Concept with NeuVector by SUSE on AWS?

PoC/accelerator funding available by request (subject to use case/availability) – Contact aws@suse.com



Thank you

<https://www.suse.com>

© SUSE LLC. All Rights Reserved. SUSE and the SUSE logo are registered trademarks of SUSE LLC in the United States and other countries. All third-party trademarks are the property of their respective owners.

For more information, contact SUSE at:

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

Frankenstrasse 146

90461 Nürnberg

www.suse.com