



# NeuVector by SUSE

February 2024

Gabriel Stein  
Partner Solutions Architect



# Why NeuVector?

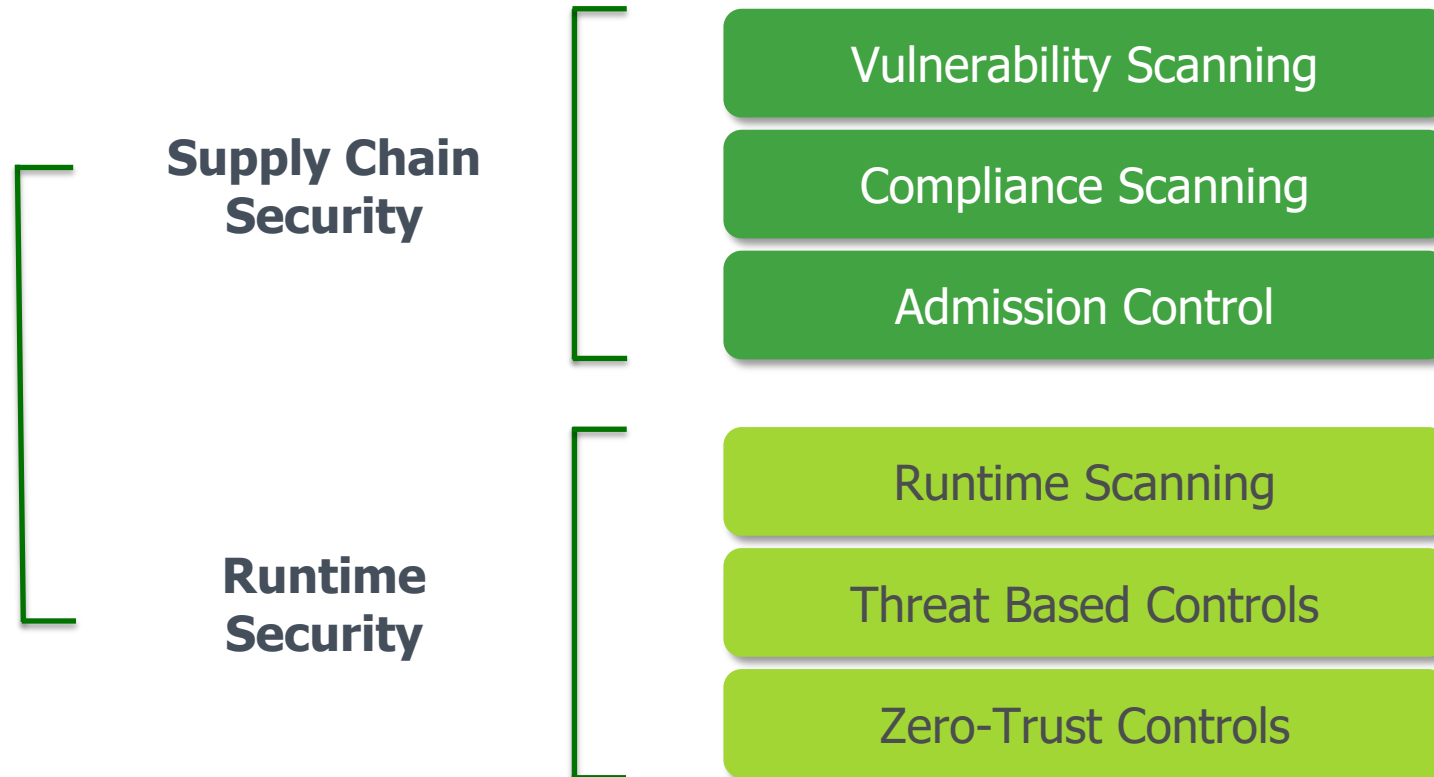
Full Lifecycle Container  
Security



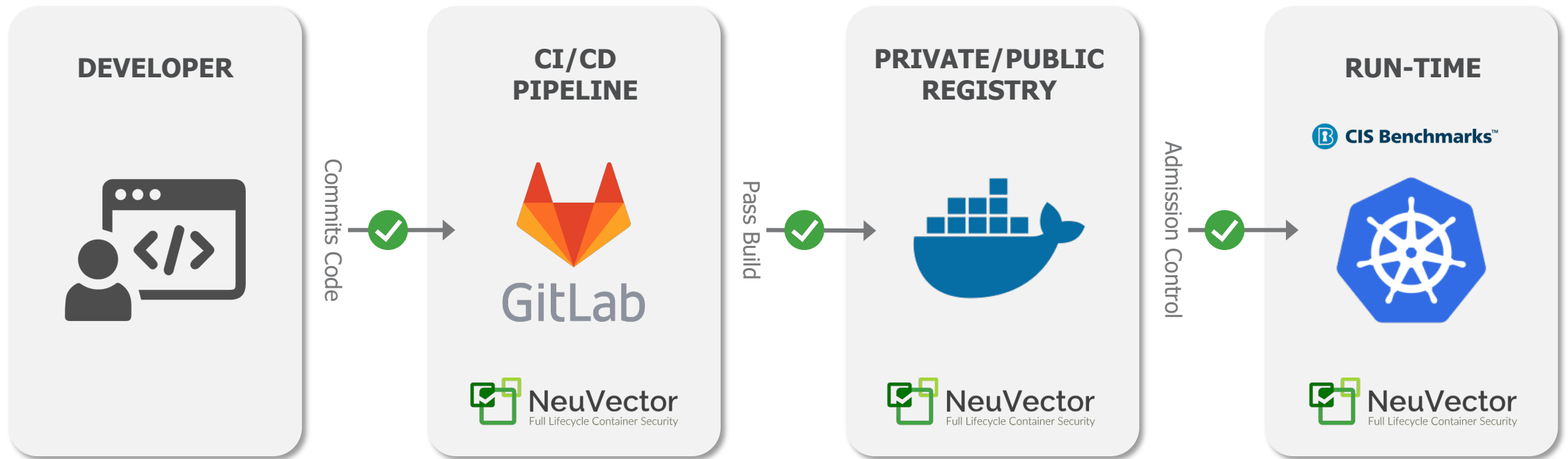
Copyright © SUSE 2021



# NeuVector Layered Security



# Scanning & Compliance Management



# Runtime Security: Defense in Depth

## Threat Based Controls

CVEs

DLP

Application & Network Attacks

OWASP Top 10

Admission Control

## Zero-Trust Controls

Automated Learning

Network

Process

File Access

Application



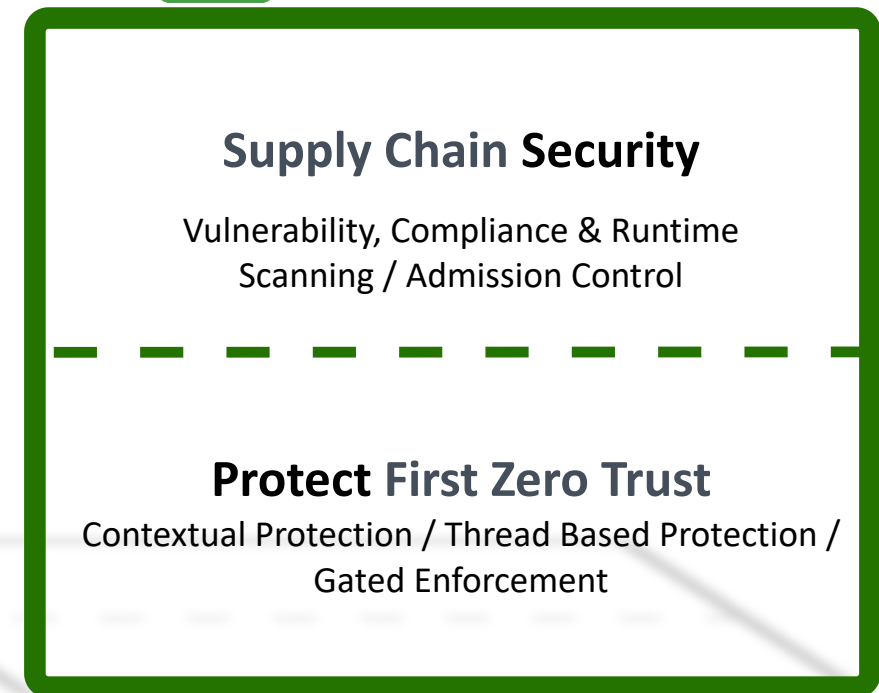
# NeuVector Security

## Supply Chain Security

- No known vulnerabilities, check against 17 vulnerability databases.
- Compliance with PCI, GDPR, HIPAA, NIST.
- Control which containers get admitted into your cluster.

## Protect First Zero-Trust

- Tailor made protection for your application based on its behavior, avoid false positives.
- Network packet level attack prevention, layer 3 and layer 7, understand, detect and protect.
- Attacks don't cross the demarcation point, blocked before reaching your applications.



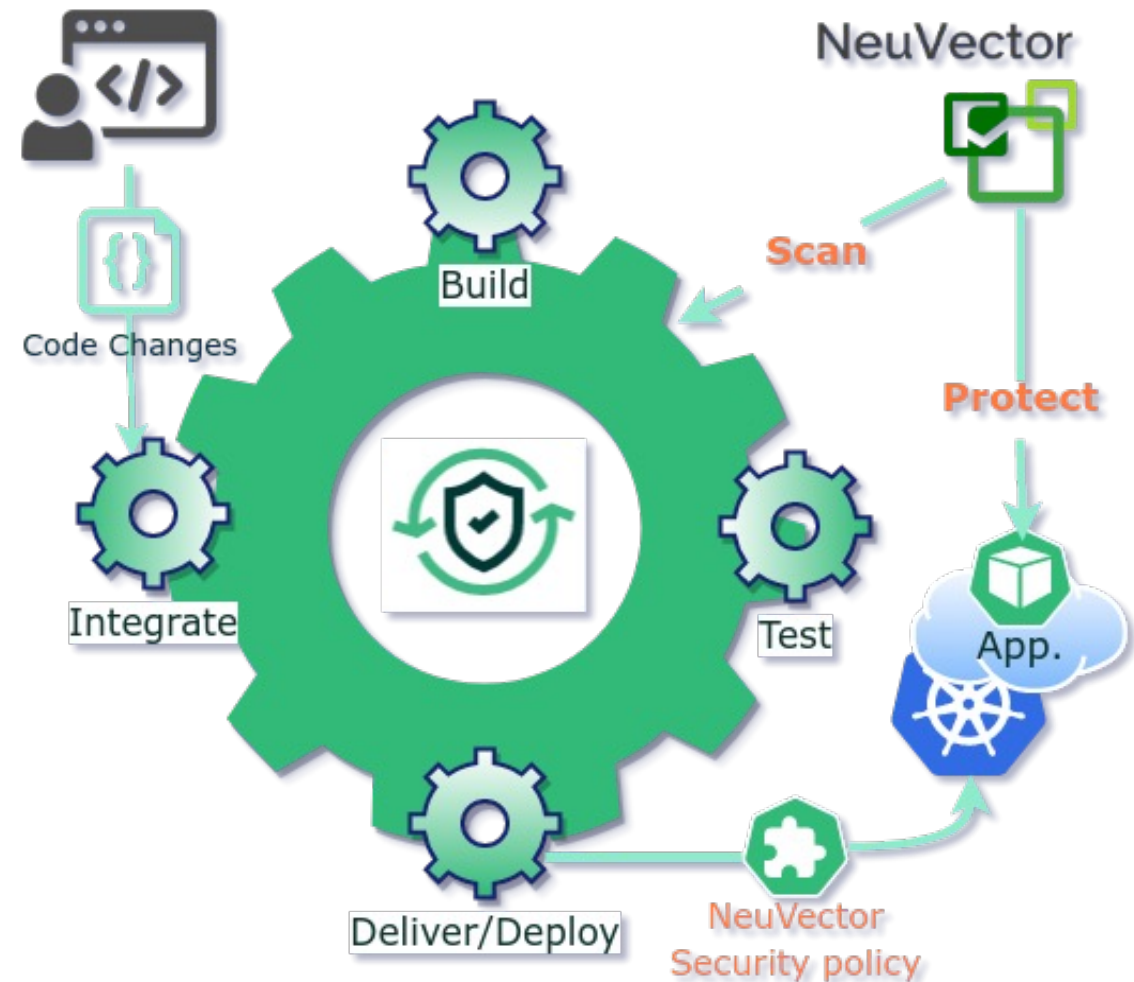
# Fits your CI/CD pipelines

NeuVector is made to be automated

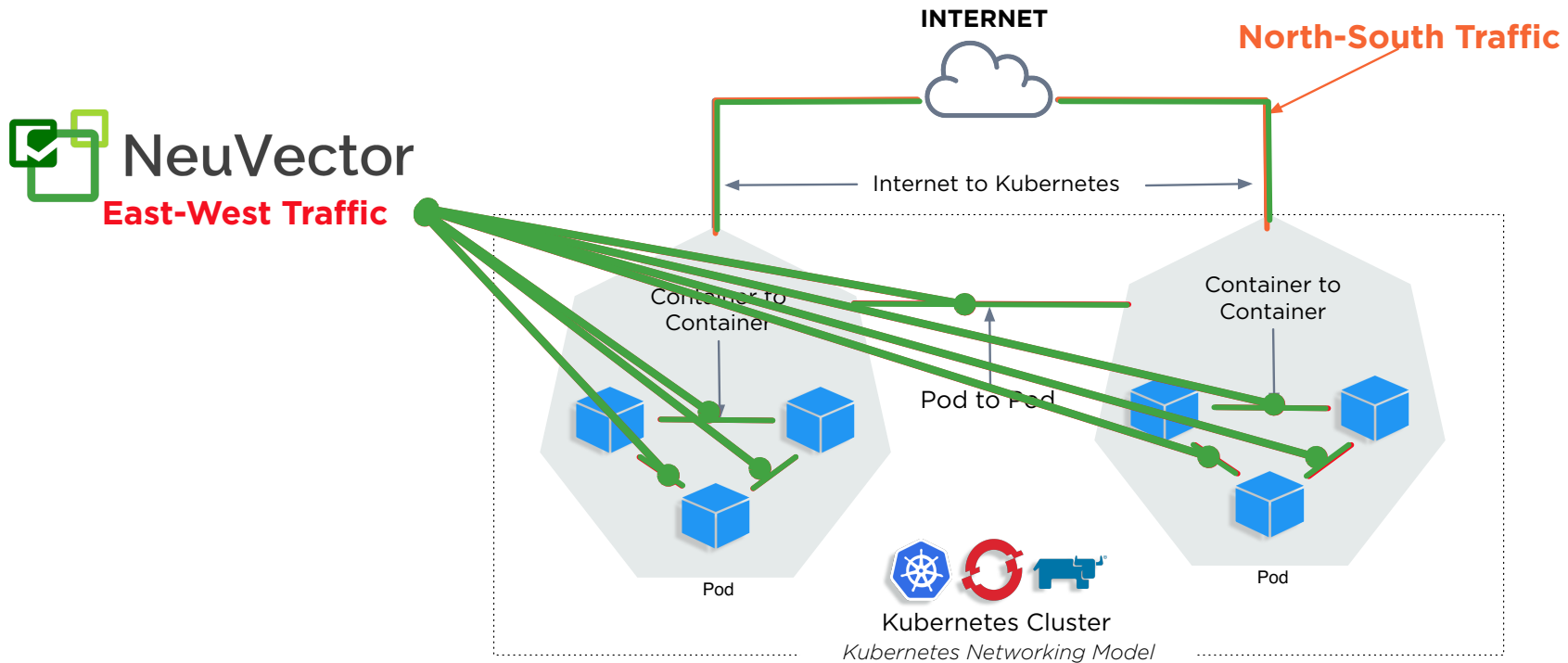
NeuVector is Kubernetes native so no need to do workarounds

You can apply your Zero-Trust security policies from the very moment your application starts running in your Kubernetes cluster.

Not just protecting your application can be automated also scanning your infrastructure as another step in your pipeline to make sure your application is running on top of a secure environment and supply chain.

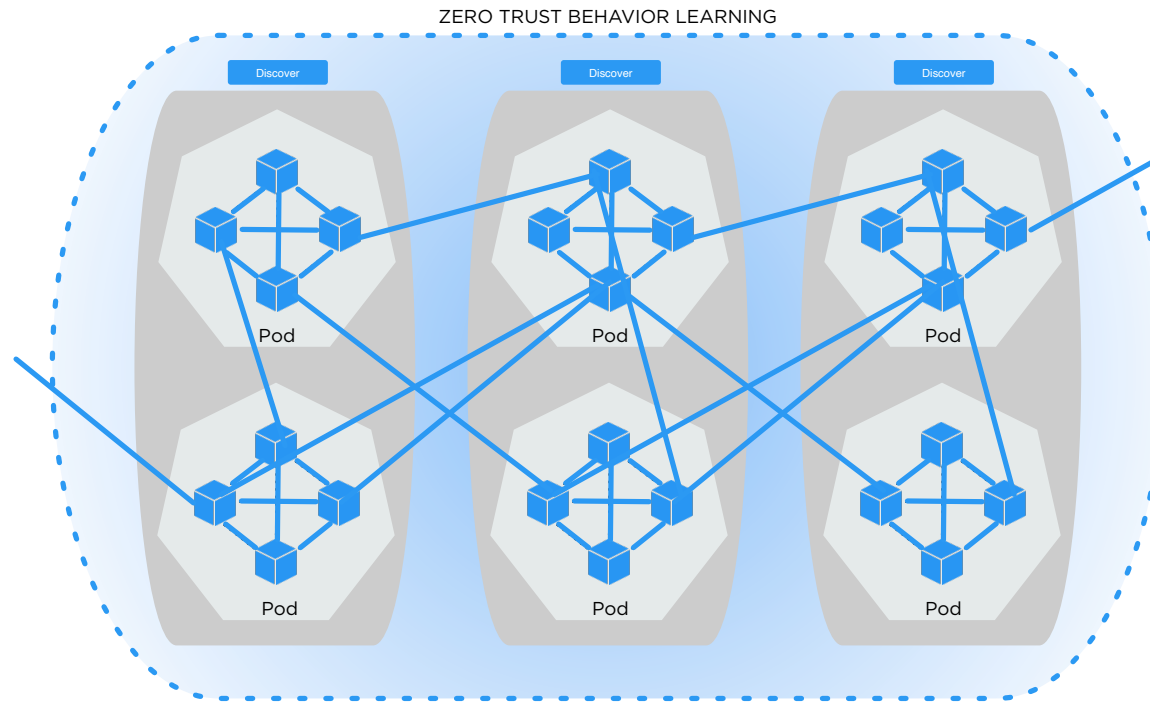





# Runtime Behavioral Inspection



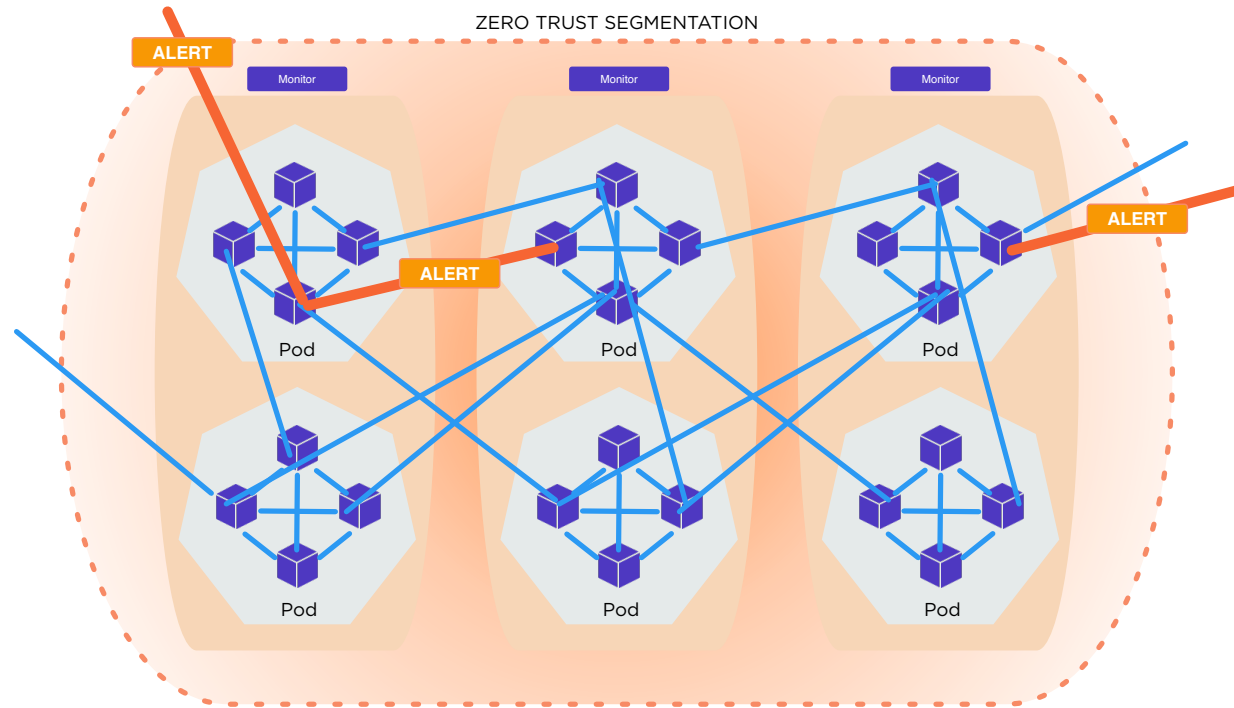





# Automated Behavioral-Based Zero-Trust



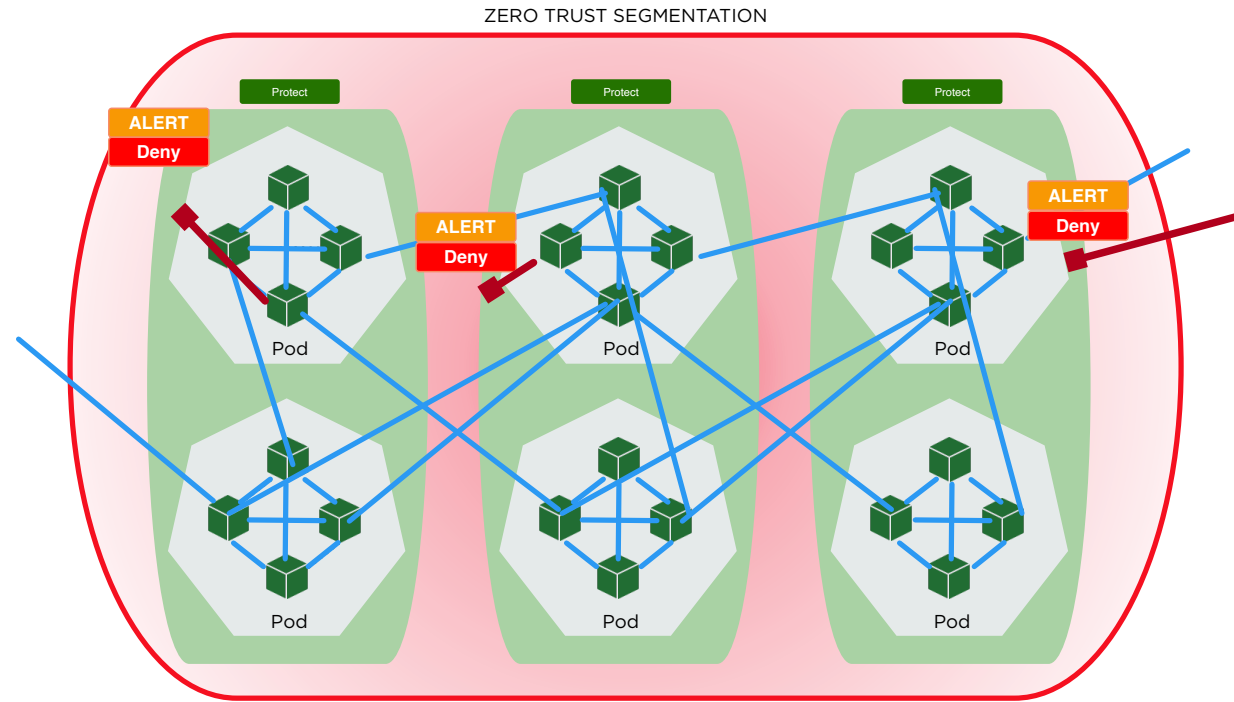
- 
-  Discover **Identifies** application behavior (Learning Mode)
  -  Monitor **Alerts** to any anomalous application behavior
  -  Protect **Denies** on any anomalous application behavior




# 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

# 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



Thank you

For more information, contact SUSE at:

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

Maxfeldstrasse 5

90409 Nuremberg

[www.suse.com](http://www.suse.com)