Data Sheet

SUSE Neuvector Unified Kubernetes Security and Compliance Platform

SUSE Neuvector at a Glance

SUSE Neuvector is a unified security and compliance platform that simplifies and automates security, while providing defense-in-depth for Kubernetes-native applications from pipeline to production.

SUSE

Advantages

- Behavior-Based Zero Trust Container Segmentation
- Automated Security Policy Creation & Enforcement
- Layer 7 Complete Container Network Visibility
- Comprehensive Compliance Assessment and Reporting
- Threat Mitigation and Zero Day Prevention

> At Reputation.com, we understand the power of a company's reputation. Operating a safe and secure IT infrastructure is paramount to our own reputation. SUSE Neuvector with its focus on uncompromised runtime security, and container network security at the Layer 7 level, provides us with the visibility to secure container traffic, combined with automation, enforcement and mitigation capabilities."
>
> Senior Director of IT and InfoSec
> Reputation.com

Full Lifecycle Container Security

Cloud computing and the shift to container infrastructures accelerate business, yet introduce new security concerns. Kubernetes, the de facto standard for container orchestration, adds a layer of complexity to security with limited enterprise expertise to address it. Organizations face new risks in this distributed computing environment and cannot rely on traditional security measures to protect their networks or applications.

SUSE Neuvector empowers global organizations to comprehensively secure their Kubernetes-native applications without compromising business velocity. The SUSE Neuvector unified security and compliance platform simplifies and automates security, while providing zero trust security for Kubernetes-native applications from pipeline to production. SUSE Neuvector delivers unmatched network visibility and protection, streamlined automation, and compliance enforcement for security, DevOps, and infrastructure teams.

The Solution of Choice for Securing Modern Container Infrastructures

Zero Trust Container Security

- Control access across any container deployment with Layer 7 Network and Process security policies automatically created from application behavior
- Export and apply security policies across clusters (Security as Code) to replicate your zero trust segmentation
- Identify any and all anomalous network traffic or container processes with the option to Monitor (alert-only) or Protect (alert and block)

Simplified Compliance

- Assess and report on all major standards including PCI. NIST, GDPR. and HIPAA
- Implement patented container Data Loss Prevention (DLP) to comply with SOC2 requirements for container segmentation, data privacy, and more

Continuous Network Protection

- Obtain Layer 7 network visibility within and between Kubernetes pods using network traffic as the source of truth
- Identify and validate application protocols to prevent tunneling and zero-day attacks
- Detect network threats with patented deep packet inspection
- Automatically block both known and unknown threats

DevOps Friendly Automation

- Shift left automated behavior learning and automated policy creation for fine-grained security with no increase in development toil
- Automate pipeline scanning, runtime scanning and runtime security to secure applications from pipeline to production

SUSE Neuvector Technical Overview

The SUSE Neuvector container security and compliance platform is the security standard for modern container infrastructures. No other solution has the depth and breadth of coverage to deliver observability, security and automation across all major cloud platforms and orchestrators. Our patented technology includes deep packet inspection and behavioral learning to identify appropriate container behaviors and allow only approved whitelisted network connections, processes, and file access within the container environment.

DevOps teams gain vulnerability and compliance management capabilities that include automated CI/CD scanning and role-based admission controls. SUSE Neuvector provides complete attack detection and prevention at run-time, actively protecting application environments in production. SUSE Neuvector deploys as a container, making it highly scalable.