What You're Getting Wrong About Kubernetes Security

Containers are transforming how organizations deploy and use applications. But securing your organization's containerized deployments means looking beyond assumptions and asking the hard questions about Kubernetes security.

Assumption 1:

My Kubernetes platform offers adequate container workload protection.

The Truth:

While Kubernetes has a few security features, it is NOT a security platform developed with the mission of protecting against exploits and zero-day attacks.

Assumption 2:

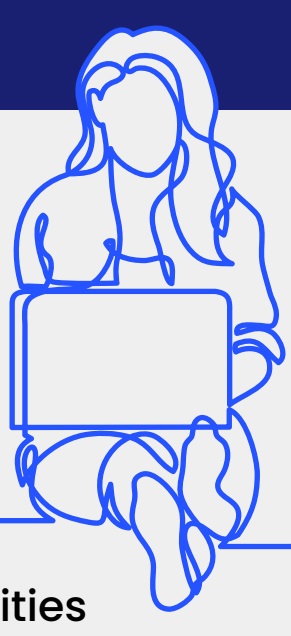
Combining traditional security tools like firewalls and IDS/IPS with Kubernetes built-in network security will adequately protect against network attacks on containers.

The Truth:

Traditional security tools, as well as built-in Kubernetes network policy, are blind to network based attacks and don't provide state-of-the-art network protections to containers such as application (Layer 7) segmentation, DLP, container WAF, packet capture and Zero Trust based network protections.

Assumption 3:

Scanning images, containers, pods, and production nodes for vulnerabilities is enough.



The Truth:

Scanning for common vulnerabilities and exposures is like looking in the rearview mirror—it doesn't protect you against zero-day attacks, insider attacks, embedded malware and backdoors and other attacks against production workloads.

Assumption 4:

My cloud provider and network policies create secure container environments.

The Truth:

Public cloud providers make it clear that you are responsible for a significant portion of securing your applications, network and infrastructure from attack.

Hard Questions:

Am I really doing enough to secure my container environment?

Do I have the network visibility and protection needed to keep ahead of the ever growing attack surface of container environments?

The Hard Truth:

If you're not applying Zero Trust principles and securing your container environment from pipeline to production, you're not doing enough.

	Other Container Security Solutions	SUSE NeuVector
Vulnerability Scanning	✓	✓
Automated Security Policies (Security as Code for DevOps and DevSecOps)	✗	✓
Deep Packet Inspection (DPI) (for all network traffic within a cluster)	✗	✓
Data Loss Prevention (DLP) and Web Application Firewall (WAF)	✗	✓
Layer 7 Firewall Protection	✗	✓
Allow-listing and Deny-listing for Zero Trust Security	✗	✓
Cross-platform Fully Undetectable (FUD) Malware Protection	?	✓

About SUSE NeuVector

NeuVector is the industry's first full lifecycle container security and compliance solution that's production-ready and used globally by leading enterprises. Our Zero Trust, cloud native approach to security simplifies and automates security for Kubernetes-native applications from pipeline to production, allowing your organization to move quickly and take a proactive approach in your container security strategies.

We're 100% open source, community-driven and enterprise-ready.

Secure your containers anywhere with SUSE NeuVector.

Learn more by visiting

https://www.suse.com/solutions/security/

SUSE