RGS
Rancher Government Solutions

Solution Brief

Zero Trust Container Protection

NeuVector provides real-time, automatic container security to stop attacks dead in their tracks.

NeuVector is an automated inline preemptive defense platform for Kubernetes designed to apply zero trust policy enforcement between container pairs in live traffic without the use of latent runtime scanning or image comparisons.

NeuVector

NeuVector defeats our nation's adversaries by defending US Government Kubernetes container traffic inline and in real-time using a patented application and packet aware container defense solution.

NeuVector provides proactive zero trust security that stops attack attempts dead at the application layer, between container pairs, before they can move, acquire, or damage your containers. Unlike runtime and scanning solutions that provide reactive security, NeuVector goes to work *before a breach alert* shows up in your kernel or call table. It *proactively shuts down malicious code execution* before it has a chance to impact the victim, target container, or application.

NeuVector's patented Container Deep Packet Inspection (DPI) is what sets it apart. Using this capability, NeuVector automatically learns your container service behaviors upon installation, establishes your zero trust protective policies, and applies policy to preemptively terminate attack attempts.

NeuVector's Container DPI goes even further to protect your containers and clusters by providing real-time automatic contextual packet analysis of each connection request to identify and terminate zero day, malware, and packet-embedded attacks, invisible to other container security products. By providing full visibility into live packet flows and applications traversing your Kubernetes east-west and north-south traffic planes and holding the preemptive defensible position to block attacks, NeuVector assures you always have real-time visibility and control of your defensive security posture.

Investing in NeuVector means you lessen your reliance on signature and CVE chasing and reduce your scan and patch burden. With NeuVector you eliminate Layer-3 guesswork like port labels, IP tables, extended Berkley Packet Filter (eBPF) assumptions, and Kubernetes feed estimates, becoming application and packet aware.

NeuVector provides high performance, low latency protection you can count on for tactical, deterministic, or mission-critical deployments. Because NeuVector is a Kubernetes-native container itself, it deploys in less than 5 minutes with a HELM chart or less than 15 minutes with a simple YAML file modification.

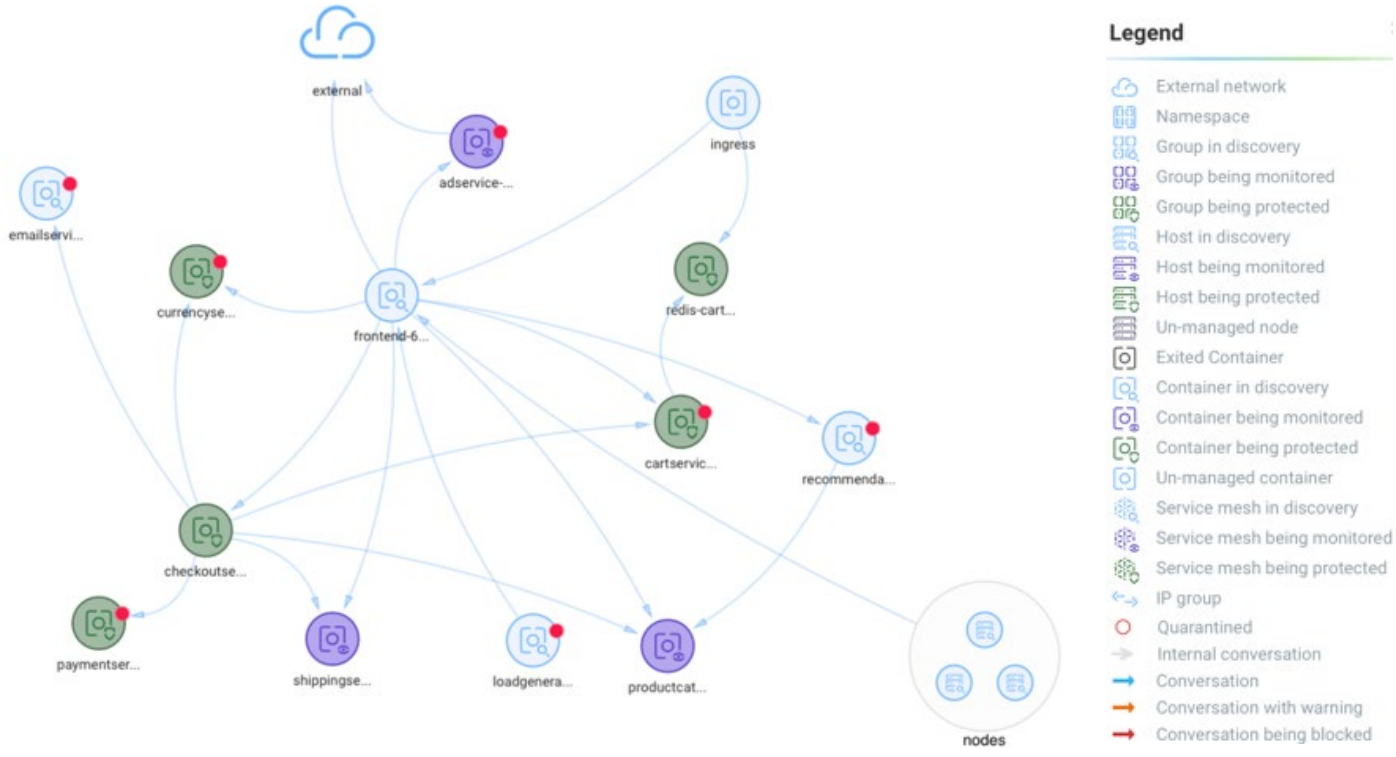
NeuVector is an air gap security solution, which is never dependent on any external cloud, internet, remote, or SaaS resource. NeuVector is 100% self-contained and is always under your control.

NeuVector Solution Highlights

- Pushbutton Security as Code allows you to protect any application or new cluster in seconds with a key stroke. Simply select the service protections you need and generate a complete security manifest in seconds. The NeuVector platform will generate a custom zero trust policy set in the form of a deployable security YAML file you can replicate to protect a new application, to stand up a new production cluster, or deploy protection anywhere, including on aircraft or in terrestrial, spatial, or shipboard applications. Because NeuVector Security as Code is transportable, you can create agency-wide policy and assure consistent core enforcement across architectures.

- Powerful admission control as well as multi-cluster and tenant security federation, make securing multiple cluster deployments easy. Role Based Access Controls (RBAC) and federated multi-cluster security policy assure boundaries, tenants, commands, and ops are kept appropriately segmented and compartmentalized.

- NeuVector gives you live traffic visibility and operational protection (previously not possible) and includes all the built-in supply chain security tools you need to assure full lifecycle container protection.



NeuVector. Container Protection that Runtime Solutions Cannot Match.

Protection Capabilities Overview

Below are a few of NeuVector's core capabilities. Have a requirement you don't see below? Let's connect.

- Deep Packet Inspection of live container traffic detects and blocks multi-vector container attacks automatically.
- Comprehensive and fully automatic zero trust multi-vector rule creation within seconds of installation with no manual policy configuration.
- Container application defense stands between attacker and target containers to preemptively terminate malicious attacks protecting one container from another.
- Gated application segmentation and threat protection stands at Layer-7 terminating any traffic connection requests not specifically allowed by your zero trust policy set.
- Automatic next generation protocol detection validates permitted connections and assures packet content is free of embedded, injected, tunneling, and other sophisticated attacks.
- Pushbutton Security as Code generates a replicable defensive security manifest in seconds. Instantly generate a deployable zero-trust security policy set for any application or new cluster with a click.
- Patented transparent Layer-7 protection for encrypted service mesh traffic and the mesh control plane assures mesh content and infrastructure is defended.
- Protocol Decoders automatically identify and protect over 35 cloud native application protocols.
- DPI automatically detects and terminates DDoS, DNS, SQL Injection, SlowLoris, DNS, and ICMP tunneling, and other packet level attacks invisible to Layer-3 scanning platforms.
- Once deployed, NeuVector automatically terminates forbidden and malicious behaviors assuring unmanned tactical deployment protection and operational continuity.
- Patented Container Data Loss Prevention (DLP) protects PII, sensitive, or cross domain data in a container native Kubernetes construct assuring data is not exposed, moved, or co-pollinated where not allowed.
- Automated packet capture assures you have exacting forensic recourse on any security event. Webhook controls will automate event and PCAP forwarding to your SEIM or forensics team.
- Customizable whitelist / blacklist rules based on namespace, label, IP address, DNS name, etc.
- Three operation modes--discover, monitor, and protect--ensure your entire build, ship, and run SDLC is protected.
- Process control permissions allow only pre-authorized execution, automatically blocking suspicious and unauthorized process behaviors, port scanning, and reverse shell execution.
- Detects and blocks root privilege escalation and breakout attempts.
- Automatically blocks malicious CVE, malware, and zero-day attacks, whether asset is patched or not with NeuVector attack countermeasures.
- Container Drift is simply not allowed.

Vulnerability & Compliance Management

- Full lifecycle supply chain protection.
- Accurate layered image scanning with built in vulnerability and compliance explorers make workflow management, remediation, and reporting easy.
- Registry scans for Amazon ECR, Azure Container Registry, Docker, Gitlab, Google Container Registry, IBM Cloud Container Registry, JFrog Artifactory, OpenShift Registry, Red Hat Public Registry, Sonatype Nexus and more.
- Compliance templates for PCI, GDPR, HIPAA, NIST, and others with custom compliance creation to apply DISA STIG or other frameworks as needed. Automatically assess exposure and provide gap remediation report.
- Admission control rules block vulnerable images and apply pod security rules to assure production is always protected.
- Initiate automatic or manual packet capture and download PCAP files.
- Parallel scanner pods for massive scanning scalability.
- Scanner Autoscaling.
- Automatic container forensic container quarantine isolates cluster from dangers without destroying the container forensic research data.
- Includes Kubernetes, GKE, and OpenShift CIS security benchmark analysis.
- Plug-ins for Jenkins, CircleCI, Bamboo, Azure Dev Ops and others,

Host & Platform Security

- Automatic host and orchestration platform vulnerability and compliance runtime scanning including scans for Kubernetes, OpenShift, and Docker CIS benchmarks.
- Single and multi-cluster security management console for host process blocking, federated policy management, and risk monitoring.
- Centralized CVE vulnerability scanning allows for federation of scanning function in multi-cluster deployments. Federate scan results across multiple clusters with exacting RBAC control.
- Supported platforms: all major linux distributions running Docker engine CE or EE, including RHEL, Ubuntu, Debian, CentOS, CoreOS, and SUSE.
- Integrated with orchestration and management platforms: Kubernetes, Red Hat OpenShift (certified container and operator), Rancher (catalog listed), AWS ECS/EKS, Mesos etc., Google GCP/GKE, Azure/AKS, IBM Cloud, OKE, PKS, Diamanti, VMWare Tanzu, and PKS.
- Deployed 100% airgap under the complete control of the managing agency.
- LDAP/Active Directory, OIDC and SAML support for role/group mapping and single sign-on (SSO), automated OpenShift RBACs, and custom roles support.
- Automation through ConfigMaps, CRDs, REST API and CLI for cloud-native 'Security as Code' deployments.
- Run-times supported: docker, containerd, and CRI-O.

About Rancher Government Solutions

Rancher Government Solutions (RGS) is specifically designed to address the unique security and operational needs of the U.S. Government and military as it relates to application modernization, containers, and Kubernetes.

Rancher is a complete open source software stack for teams adopting containers. It addresses the operational and security challenges of managing multiple Kubernetes clusters at scale, while providing DevOps teams with integrated tools for running containerized workloads.

RGS supports all Rancher products with US based American citizens who are currently supporting programs across the Department of Defense, Intelligence Community, and civilian agencies.

To learn more contact us at info@ranchergovernment.com or 844-RGS-7779.