White Paper

NeuVector Container Security

Unparalleled Zero Trust Protection

Preemptive Container and Application Armor for your Kubernetes Clusters

NeuVector
Full Lifecycle Container Security

RGS
Rancher Government Solutions

What is Container Protection?

Container protection is the ability to stop an attack before it can cause damage to its intended target—no matter what the attack vector. Comprehensive container protection is critical to deploying a technology stack that aligns with the Office of Management and Budget's (OMB) strategy to move the US Government toward a "zero trust" approach to cybersecurity. The OMB's strategy is a critical part of President Biden's Executive Order on Improving the Nation's Cybersecurity. There are many container security solutions available on the market but there is only one designed to preemptively protect containers. That solution is NeuVector from Rancher Government Solutions (RGS).

When it comes to zero trust, NeuVector is unambiguous and unapologetic. With NeuVector's zero trust product suite, you can now stop attacks that other container security products can't even detect. Our solution blocks attacks before they succeed without taking down pods or destroying container applications. With NeuVector you are kept secure and protected without losing the agility that is the hallmark of open source technologies.

What is Zero Trust?

Zero trust security should not only detect and alert security teams to anomalies, but also preemptively block malicious code execution and anomalous behaviors in real-time, stopping the attack dead in its tracks before it is able to penetrate your software stack. There are dozens of marketing efforts by software vendors that discuss container security and zero trust, but few (if any) of them protect container traffic from attack by applying in-line, real-time enforcement.

NeuVector zero trust protection aligns with OMB's vision. Our packet level protection mechanisms block attacks before they reach or damage their intended targets, including containers and applications. The following NeuVector zero trust capabilities are critical when evaluating the best zero trust solution for your organization:

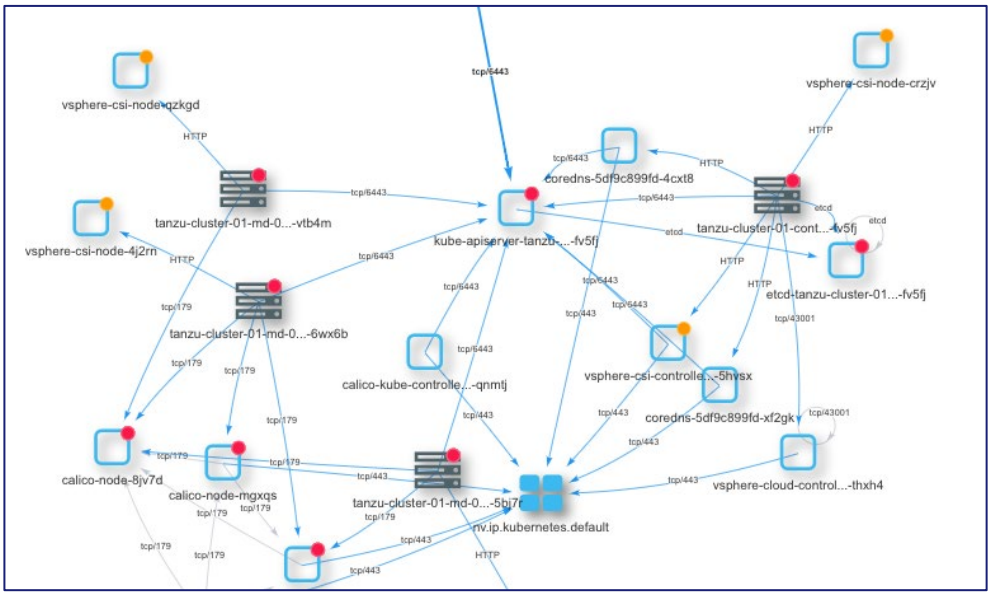
- Attack blocking must be preemptive—before an attack can execute or reach its intended target.
- Enforcement must exist between container pairs to protect one container from another.

- Policy must have multi-vector visibility and control points.
- Protection must be packet and application content aware to make accurate decisions.
- Solution must have the ability to block attacks on vulnerabilities — whether a vulnerability is patched or not.
- Enforcement must have the ability to stop both known and unknown attacks.
- Solution must have complete control of the attack kill chain—the mechanisms attackers use to execute attacks.
- Enforcement should not permit container drift.
- Blocking must be gated—stopped dead at that protection demarcation point.
- Policy creation must be automatic and based upon your specific live data and application payload.
- Solution must have visibility and control of packet flow content.
- Enforcement blocks any anomalous behavior that does not meet multi-vector zero trust policy permissions.
- Solution must be transparent to automatically prohibit what is not allowed but keep you agile.

The NeuVector Protection Platform

A Zero Trust Container Defense System Specifically Designed for Kubernetes

NeuVector secures containerized networks the very same way wired networks are secured within the Federal Government and DoD, with in-line, application, packet aware controls and gated hard-stop blocking. No boundary, traffic plane, or enclave goes unprotected with NeuVector.



NeuVector detects and blocks attacks in real-time and provides container and application protection not possible with the best scanners and other shift-left container security technologies.

NeuVector sits in-line, seeing and controlling container packet flows, and is “application aware”, controlling over 35 cloud native application protocols. Patented Container Deep Packet Inspection (DPI) powers our visibility and protection controls.

The platform is simple to deploy, simple to manage, and makes meeting both the OMB directive and attaining container network Authorization to Operate (ATO) easier.

There is no tedious policy configuration with NeuVector, it automatically learns which traffic flows are normal using visibility into your service behaviors at the packet level. You can easily establish and lock down your zero trust perimeter just moments after platform installation. Real-time packet, application, process, and file system behaviors automatically define your zero trust policy.

Container DPI gives you the behavioral detail and accuracy necessary to stop malicious action or anomalous behaviors without errors or false positives. NeuVector stands as the enforcement gateway between each container pair applying your agency’s zero trust policy.

At NeuVector, zero trust is more than a marketing buzzword. We created and patented container DPI to provide the visibility and control needed for fast and accurate packet and application-level protection. Without packet content and application visibility and control, you’ll never have zero trust. For zero trust protection you must know and control which data is traversing your traffic planes at all times.

NeuVector is a proven technology to those who look to move container security strategy from post-event, reactive detection, and patch technologies to the much stronger protection found with a preventative, proactive approach. NeuVector is ideal for those in IT security or DevSecOps looking for more than what “runtime” solutions can offer.

The platform is simple to deploy, simple to manage, and makes meeting both the OMB directive and attaining container network Authorization to Operate (ATO) easier.

Wait, Why Isn't My Good Old Runtime Security Enough?

The short answer is Runtime cannot block between container pairs unless the control point (the blocking enforcement function) is deployed there. Runtime lacks the traffic position and contextual understanding of what is running at the application and packet levels to deliver container protection or zero trust with the needed accuracy. In other words, runtime security lacks the packet and application content information needed to provide protection.

Remember zero trust is not arbitrary: it's exacting. It should not be based upon image or runtime scans and should know in detail what is traversing your traffic planes in real-time. Zero trust protection should be able to block any connection attempt that does not adhere to your zero trust policy.

If the connection request does not have explicit permission, it should be forbidden, hard-stop blocked, and prevented from crossing that demarcation point. Runtime is a valid security layer, one of many, but does not provide zero trust security in and of itself.

Any container security solution predicated on runtime scanning, image analysis, kernel feeds, or the ability to identify and remediate vulnerabilities will fall short of the preemptive protection and "zero trust promise" outlined in the OMB memo.

What's Next?

Agencies are now placing more emphasis on getting in front of our attackers. Recognizing that vulnerability chasing and the detect and patch process is a losing long-term strategy if the goal is preemptive protection as outlined in the Zero Trust OMB Memo. Increasingly agencies are working to deploy preventative security technologies where a defense system automatically blocks attacks that don't meet zero trust policy before they can cause operational harm. As a country, we can protect our national security if we stay one step ahead of our enemies.

Staying ahead means evaluating the security measures you currently have in place and identifying the gaps where you are not able to stop nefarious actors before they breach your systems and network.

How Do I Evaluate My Current Security Measures?

When evaluating container protection paths to zero trust the first question you should ask your IT teams is: Can we block an attack attempt between container pairs, stopping an attempted attack before it breaches the target container or the system kernel?

We recommend you ask your internal team these additional questions to help further validate what a move to zero trust might look like and the reasons you should move to it now:

- Is your current container security strategy predicated on scanning for attacks and vulnerabilities in your clusters where the perimeter has already breached?
- With your current security schema, are you waiting for an attack to appear in your infrastructure to take defensive action?
- Can your existing container security stop an attack against an unpatched asset?
- With your existing approach, are you able to block embedded malware execution, packet level, application-layer, and insider attacks?
- Can you protect against a zero day attack (something never-seen-before by very definition)?
- Would a better strategy be to stop all attack execution attempts no matter what entry vector and no matter which kill chain elements are used, known or unknown?

Fast & Easy Zero Trust Protection Deployment with NeuVector

Scanning, detection, patch, and remediation processes are well known best practices for any DevOps pipeline, test, quality assurance, or staging environment. You should have them in place and be using them regularly. They need to run continuously for DevOps / DevSecOps continuity. They help achieve some level of container security but are insufficient when it comes to stopping our nation state adversaries from successfully attacking our containerized assets. They are not in-line with the very traffic they are supposed to protect.

NeuVector provides the added layer of security that proactively protects your containerized assets before they are breached and complements the reactive scanning methods you likely already have in place. NeuVector deploys in minutes with no sidecars, no code injection, no agents, no Extended Berkeley Packet Filter (eBPF) map estimates, and layer 3 assumptions.

In addition, NeuVector comes with the following features to provide you the most robust zero trust environment available today:

- All the traditional application security preparation tools you might need so that you can continue to strengthen the integrity of your pipeline builds as they progress to production.

- Powerful admission control that acts as the automatic gatekeeper, standing guard between your DevOps and production deployment environments, assuring nothing makes it into production that doesn't meet your security standards.
- NeuVector is orchestrator agnostic, which means that no matter which container solutions you use—Rancher, Red Hat Open Shift, Tanzu, straight Kubernetes—we protect them all.
- NeuVector integrates with your chosen Continuous Integration (CI) tools and will protect services running in any cloud or hybrid mix of service provider networks.
- NeuVector comes with federated multi-cluster security management so you can push layer-7 zero trust controls across multiple clusters while allowing for seamless cluster management autonomy at the enclave level.
- NeuVector is designed to run 100% on premise in air-gap deployments if needed.

Ready to Learn More?

The NeuVector team at Rancher Government Solutions welcomes the opportunity to demonstrate the difference between traditional container security and what NeuVector container protection brings to bear to protect our national assets with uncompromising zero trust.

Click the link below to connect with one of our container security specialists to learn more about your path to zero trust.

Schedule my zero trust security briefing!

About Rancher Government Solutions

Rancher Government Solutions (RGS) is specifically designed to address the unique security and operational needs of the US 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 NeuVector and all Rancher products with US-based American citizens with the highest security clearances who are currently supporting programs across the Department of Defense, Intelligence Community, and civilian agencies.

NeuVector — an RGS security solution — is the leader in full lifecycle container security, delivering uncompromising end-to-end security for modern container infrastructures. NeuVector offers a cloud-native Kubernetes security platform with comprehensive vulnerability management, automated CI/CD pipeline security, and complete run-time security, including the industry's only container firewall to block zero days and other threats. With NeuVector, DevOps, DevSecOps, and enterprise security teams have the tools and protection they need to automatically secure the entire container pipeline — from build to ship to run.

RGS is committed to helping the US Government run Kubernetes securely everywhere. To learn more about Rancher Government Solutions, please contact us at:

Info@rancherfederal.com
844-RGS-7779
ranchergovernment.com

1900 Reston Metro Plaza
Suite 600
Reston, VA 20190

Disclaimer:

The author and Rancher Government Solutions assume no responsibility or liability for any errors or omissions, or for the results obtained from the use of this information. All information in this article is provided "as is." Rancher Government Solutions is available to help with any implementation roadblocks.