NeuVector

KUBERNETES PROTECTION IN PRODUCTION

NEUVECTOR CONTAINER SECURITY PLATFORM

About NeuVector

NeuVector, the leader in Container Network Security, delivers highly integrated, automated security for Kubernetes and OpenShift, and is the only next generation container firewall with packet-level interrogation and enforcement.

NeuVector delivers east-west container traffic visibility, container protection, and host security in a complete end-to-end container security platform. NeuVector customers include global leaders in financial services, healthcare and publishing.

Founded by industry veterans from Fortinet, VMware, and Trend Micro, NeuVector has developed patent-pending behavioral learning for container security.

kubernetes

redhat CERTIFIED TECHNOLOGY

docker CERTIFIED Container

aws partner network

RANCHER

MESOS

Contact Us

info@neuvector.com
2880 Zanker Road, Suite 109
San Jose, CA 95134

Containers Bring New Security Demands, and Threats

Your enterprise is quickly moving toward a container-based application deployment strategy, across multi-cloud and on-prem platforms. These Kubernetes, Docker and OpenShift environments operate at a highly automated scale with hundreds, and even thousands, of containers continuously interacting. The combination of east-west container traffic explosion, low network visibility and legacy security tools leave security teams blind, powerless and at-risk. Your challenge is to deploy this container strategy with confidence. NeuVector, the leader in container network security, delivers the first and only Kubernetes container security platform with east-west traffic visibility, container protection, and host security in a highly integrated, automated security solution.

The NeuVector Solution

NeuVector delivers a complete end-to-end container security solution featuring unique network packet visibility and protection, a container process & file system monitor, and vulnerability management. NeuVector automatically scales, requires zero-configuration with no error-prone manual policy updates, even as the number or types of containers expand or contract to meet service demands. NeuVector instantly detects and prevents container attacks and violations, suspicious processes, and application vulnerabilities during the entire CI/CD pipeline from build to ship to run-time.

The solution is a container itself and is simple to deploy on greenfield or brownfield environments. No agents, no coding, and no embedding required!

Try NeuVector Today

Register for the download or request a demo at https://neuvector.com

Arvato Infoscore Moves to Microservices Securely with NeuVector

Company

Arvato Infoscore Gmbh, a global financial services subsidiary of Bertelsmann, helps ecommerce companies detect and prevent consumer fraud.

PROJECT SUMMARY

Migrate to a secure microservices architecture to deploy and iterate rapidly using a CI/CD pipeline.

ENVIRONMENT

Must deliver services with high availability and parallelization, with secure connections to legacy and external services.

- Nodejs on Ubuntu
- Docker
- Rancher
- ELK Stack - Elasticsearch, Logstash, and Kibana
- Graphana
- NeuVector Container Security

The Container Project

A year ago, Arvato embarked on an ambitious plan to migrate to a microservices based architecture with Docker containers as a key enabler. This would enable Arvato to be more effective in processing consumer and device data from customers to detect fraud. But strict data protection laws in Germany means this has to be done securely. In addition, TÜV compliance regulations require logical separation of applications.

Arvato has successfully deployed the first phase of the migration to production, but not without a few challenges. The project required development of a new big data app as well as migration of an existing application. There were initial difficulties debugging connections between services. Several technologies and platforms were tested before deployment to production.

Getting run-time visibility and security was a final hurdle.

The NeuVector Solution

NeuVector was selected to "inject intelligence" into the run-time environment for visibility and security.

- ✓ **Apply security best practices to containers and microservices**
- ✓ **Get network visibility to debug and protect containers**
- ✓ **Enables TÜV compliance through segmentation & scanning**

"NeuVector provides the network inspection, visualization, and security needed for dynamic container environments. The solution integrates easily into our automated workflow and the built-in intelligence lets us scale quickly. It even helped us debug network connections from mis-configured application updates."

- Tobias Gurtzick, Security Architect

NeuVector provided image vulnerability scanning, network observation, and detection of traffic flows. This was critical for validating all internal and external connections. In the production environment, NeuVector provides automated application segmentation, high availability, and rolling updates, which will enable Arvato to continue to expand securely.