NeuVector

Container Security Platform
Datasheet

Complete Run-Time Protection Without Compromise

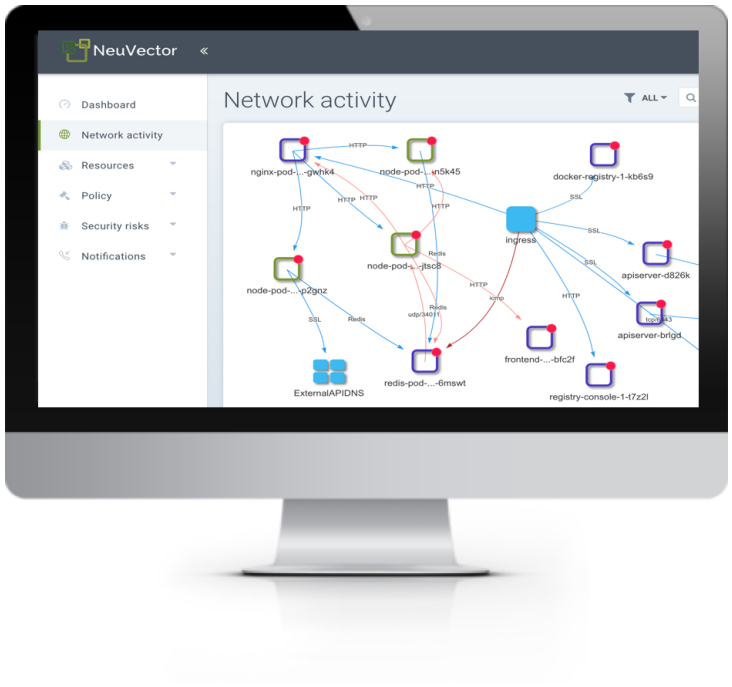
NeuVector, the leader in container network security, delivers highly integrated, automated run-time container security which includes the only next generation container firewall.

NeuVector Benefits

- ✓ Detect and prevent attacks and suspicious behavior at multiple points in a 'kill chain.'
- ✓ Support compliance & auditing requirements for container projects with CI/CD integration
- ✓ Visualize and capture network sessions to ease application debugging and investigations

Container Security Protections

- ❖ **Layer 7 Container Firewall w/ DLP**
  - **Detect Violations & Threats**
- ❖ **Host & Container Incident Detection**
  - **Monitor for Suspicious Processes and File System Changes**
- ❖ **Compliance & Auditing**
  - **Scan for Vulnerabilities & Test Security Settings from Build to Run**



Use Cases

- ✓ Secure East-West traffic for microservices migration projects
- ✓ Protect against insider attacks which bypass network L3/L4 protections
- ✓ Protect sensitive data, PII, credit cards etc. with the only container DLP engine
- ✓ Monitor and protect any internet facing container applications
- ✓ Provide continuous container security from Build to Ship to Run

NeuVector Integrates Into Your Ecosystem and is Docker & Red Hat Certified

docker CERTIFIED Container · kubernetes · redhat CERTIFIED TECHNOLOGY · aws · Microsoft Azure · RANCHER

Contact NeuVector: info@neuvector.com https://neuvector.com

Network Security – Container Firewall

- Layer 7 – application layer – network inspection
- Deep Packet Inspection (DPI) with Container DLP
- Application segmentation and threat protection even with encrypted service meshes e.g. Istio, Linkerd2
- Detect threats: DDoS, DNS, SQL Injection, SlowLoris…
- Tunneling detection – ICMP, DNS
- Ingress and egress rules enforce by DNS name or IP
- Packet capture: automated and manual
- Automated behavioral learning based whitelist rules
- Real-time visualization of containers, connections, violations, threats with network details
- Customizable whitelist / blacklist rules based on namespace, label, IP address, DNS name etc.
- DLP: credit card, PII, accounts, other regex matching
- 3 – modes: Discovery, Monitor, Protect for services, running in tap/mirror or inline (blocking) mode
- Application & protocol detection: HTTP/S, SSL, SSH, DNS, DNCP, NTP, TFTP, ECHO, RTSP, SIP, ICMP, MySQL, Oracle SQL, MS SQL, Redis, Zookeeper, Cassandra, MongoDB, PostgresSQL, Kafka, Couchbase, ActiveMQ, ElasticSearch, RabbitMQ, Radius, VoltDB, Consul, Syslog, Etcd, Spark, Apache, Nginx, Jetty, NodeJS, gRPC, ...

Container Incident Detection and Prevention

- Container process / syscall baseline & monitoring
- Suspicious process & anomaly detection & blocking: Netstat/port scanning, reverse shell
- Root privilege escalation and breakout detection
- Container file system monitoring and auto-rescan

Alerting, Logging & Response

- Automated incident response rules - customizable
- Alerts and logging by source, destination, container, other incident data and sent via SYSLOG or webhooks
- Block violations and threats per-connection
- Quarantine suspicious containers
- Initiate packet capture and download PCAP files

Compliance & Auditing

- Full life-cycle vulnerability (CVE) scanning – during build (Jenkins plug-In), registry scans, and run-time
- Languages including java, ruby, python, nodejs
- Registry support for Docker, Amazon ECR, Microsoft ACR, GCR, jFrog, RedHat/OpenShift, Nexus and others
- Kubernetes & Docker CIS security benchmark tests
- Admission control prevents vulnerable images
- Enables Compliance for PCI, TUEV, GDPR…

Host & Platform Security

- Vulnerability scanning – live during run-time, for hosts and orchestration platforms such as Kubernetes
- Suspicious process, file system activity & privilege escalation detection
- Docker Bench and Kubernetes CIS benchmark host security tests

Integration and Compatibility

- Integrated with orchestration and management platforms: Kubernetes, Docker EE (certified container), Red Hat OpenShift (certified container), Rancher (catalog listed), AWS ECS/EKS, Mesos etc., Google GCP/GKE, Azure, IBM Cloud
- Compatible with network plug-ins and overlays including Calico, Flannel, Weave, OpenShift (ovs, multi-tenant), Docker Swarm etc.
- SYSLOG / SIEM support-advanced correlation/alerting
- Webhook notifications for integrations with notification servers and Slack
- LDAP and SAML support for role/group mapping and single sign-on (SSO), automated OpenShift RBAC and Kubernetes integration
- Automation through REST API and CLI
- Run-times supported: docker, containerd, CRI-O
- Supported platforms: all major linux distributions running Docker engine CE or EE, including RHEL, Ubuntu, Debian, CentOS, CoreOS, SuSE

Resource Monitoring, Visualization & Reporting

- Monitor nodes, containers, Controllers and Enforcers
- Single and multi-cluster management console for policy management and security incident monitoring
- Comprehensive security event and risk reporting
- Inspect container labels, port and volume mappings, processes, service and namespaces
- Monitor container resource consumption including CPU, memory, and network packets

Performance, High Availability, & Security

- Lightweight, distributed network and container inspection supporting multiple Gb/s throughput
- CPU and memory can be allocated to NeuVector containers for guaranteed and scalable performance
- Controllers deployed in high availability cluster with automated synchronization and failover
- NeuVector containers are hardened, monitored, and certified by Docker and Red Hat OpenShift
- Recommended Enforcer memory: 1GB, 500 MB min.