NeuVector
Full Lifecycle Container Security

Container Security Platform Specifications

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 enforced by DNS name or IP
- Packet capture: automated and manual pcap files
- 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: Discover, 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, and more

Run-Time Container
Incident Detection & Prevention

- Container process baseline, monitor, blocking including unauthorized, port scanning, reverse shells
- Root privilege escalation and breakout detection
- Container file system monitor, block, 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 & threats per-connection, quarantine
- Initiate packet capture and download PCAP files

Vulnerability Management,
Compliance & Auditing

- Full life-cycle vulnerability (CVE) & compliance scanning – during build, registry scans, and run-time. Plug-ins for Jenkins, CircleCI, Bamboo… plus REST API
- Language scans include java, ruby, python, nodejs
- Registry scans for Docker, AWS ECR, Azure ACR, GCR, jFrog, RedHat/OpenShift, Gitlab, Nexus, IBM & more
- Kubernetes, GKE, OpenShift CIS security benchmarks
- Secrets auditing and scanning for 20+ secret types
- Admission control rules block vulnerable images
- Compliance templates for PCI, GDPR, HIPAA, NIST etc.

NeuVector
Full Lifecycle Container Security

Container Security Platform Specifications

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, with host process blocking
- Kubernetes, OpenShift, Docker CIS benchmark tests

Cloud-Native Automation and Integration

- 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, PKS
- Compatible with network plug-ins and overlays including Calico, Flannel, Weave, OpenShift etc.
  SYSLOG / SIEM support-advanced correlation/alerting
- Customizable webhook notifications
- LDAP/Active Directory, OIDC and SAML support for role/group mapping and single sign-on (SSO), automated OpenShift RBACs, custom roles support
- Automation through ConfigMaps, CRDs, REST API and CLI for cloud-native 'Policy as Code' deployments
- 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

- Exploit risk scoring dashboard with application protocol analysis and usage – downloadable PDF & CSV reports including PCI, HIPAA, NIST, GDPR
- Single and multi-cluster management console for federated policy management and risk monitoring
- Inspect container labels, port and volume mappings, processes, service and namespaces
- Monitor container resource consumption including CPU, memory, process history and network packets

Performance, High Availability & Security

- Lightweight 'Enforcer' container on each host supports multiple Gb/s network filtering throughput
- Parallel scanner pods for massive scanning scalability
- Customer proven and tested to 1000 node clusters
- CPU and memory can be allocated to NeuVector containers for guaranteed and scalable performance
- Multiple 'Controller' containers for high availability
- NeuVector containers are hardened, monitored, and certified by Docker and Red Hat OpenShift
- Recommended Controller and Enforcer memory: 1GB

NeuVector
Full Lifecycle Container Security

www.neuvector.com