

























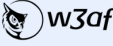






Name		Type	Description	Use cases and observations
<b>Amazon Firecracker</b> * <a href="https://firecracker-microvm.github.io">https://firecracker-microvm.github.io</a> * <a href="https://github.com/firecracker-microvm/firecracker">https://github.com/firecracker-microvm/firecracker</a>		Sandboxing, Isolation	Firecracker is an open source virtualization technology that is purpose-built for creating and managing secure, multi-tenant container and function-based services that provide serverless operational models. Firecracker runs workloads in lightweight virtual machines, called microVMs, which combine the security and isolation properties provided by hardware virtualization technology with the speed and flexibility of containers.	*
<b>Anchore Engine</b> * <a href="https://anchore.com/opensource">https://anchore.com/opensource</a>		SAST	A tool for deep image inspection and vulnerability scanning. It allows developers to perform detailed analysis on container images, generating a software bill of materials. Through seamless integration with CI/CD systems, Anchore Engine can prevent publication of images containing known vulnerabilities.	* It requires access to CVE DB when running for 1st time, after completed, CVE information is persisted into its PostgreSQL DB. * The Enterprise version has additional features such as RBAC for its API and Admin Web UI.
<b>Aporeto Tirreme</b> * <a href="https://github.com/aporeto-inc/tirreme-lib">https://github.com/aporeto-inc/tirreme-lib</a> * <a href="https://www.aporeto.com/opensource">https://www.aporeto.com/opensource</a>		Zero Trust Network	An open-source library curated by Aporeto to provide cryptographic isolation for cloud-native applications. Tirreme-lib is a Zero-Trust networking library that makes it possible to setup security policies and segment applications by enforcing end-to-end authentication and authorization without the need for complex control planes or IP/port-centric ACLs and east-west firewalls. Tirreme-lib supports both containers and Linux processes as well user-based activation, and it allows security policy enforcement between any of these entities.	* Uses the Zero-Trust Network approach to provide cryptographic isolation. * On November 2019 was acquired by Palo Alto Networks.
<b>AppArmor</b> * <a href="https://gitlab.com/apparmor/apparmor/-/wikis">https://gitlab.com/apparmor/apparmor/-/wikis</a> * <a href="https://kubernetes.io/docs/tutorials/clusters/apparmor/">https://kubernetes.io/docs/tutorials/clusters/apparmor/</a> * <a href="https://docs.docker.com/engine/security/apparmor">https://docs.docker.com/engine/security/apparmor</a>		Linux Runtime Protection	AppArmor is an effective and easy-to-use Linux application security system. AppArmor proactively protects the operating system and applications from external or internal threats, even zero-day attacks, by enforcing good behavior and preventing even unknown application flaws from being exploited. AppArmor security policies completely define what system resources individual applications can access, and with what privileges.	* Since AppArmor is a Linux kernel security module, it allows the sys admin to restrict programs' capabilities with per-program profiles. Profiles can allow capabilities like network access, raw socket access, and the RWX permissions on matching paths. * Used with SELinux and Seccomp on Kubernetes to implement Security at Pod level ( <a href="https://kubernetes.io/docs/tasks/configure-pod-container-security-context/">https://kubernetes.io/docs/tasks/configure-pod-container-security-context/</a> ).
<b>AquaSec Kube-Bench</b> * <a href="https://github.com/aquasecurity/kube-bench">https://github.com/aquasecurity/kube-bench</a>		Security Audit	Checks whether Kubernetes is deployed according to security best practices as defined in the CIS Kubernetes Benchmark. Note that it is impossible to inspect the master nodes of managed clusters, e.g. GKE, EKS and AKS. It supports the tests for Kubernetes as defined in the CIS Benchmarks 1.3.0 to 1.5.0 respectively.	* CIS Benchmark
<b>AquaSec Kuber-Hunter</b> * <a href="https://github.com/aquasecurity/kube-hunter">https://github.com/aquasecurity/kube-hunter</a> * <a href="https://aquasecurity.github.io/kube-hunter">https://aquasecurity.github.io/kube-hunter</a>		DAST	It hunts for security weaknesses in Kubernetes clusters. The tool was developed to increase awareness and visibility for security issues in Kubernetes environments. Active hunting mode will exploit vulnerabilities it finds, in order to explore for further vulnerabilities. Normal hunting will never change state of the cluster, while Active hunting can potentially do state-changing operations on the cluster, which could be harmful.	*
<b>AquaSec Trivy</b> * <a href="https://github.com/aquasecurity/trivy">https://github.com/aquasecurity/trivy</a>		SAST	Trivy is a simple and comprehensive vulnerability scanner for containers, suitable for Continuous Integration (CI). Trivy detects vulnerabilities of OS packages (Alpine, RHEL, CentOS, etc.) and application dependencies (Bundler, Composer, npm, yarn etc.). Trivy is easy to use. Just install the binary and you're ready to scan. All you need to do for scanning is to specify an image name of the container.	* It is suitable for CI while others don't such as: Anchore Engine, Clair, etc. <a href="https://github.com/aquasecurity/trivy#comparison-with-other-scanners">https://github.com/aquasecurity/trivy#comparison-with-other-scanners</a>
<b>Arachni</b> * <a href="https://www.arachni-scanner.com">https://www.arachni-scanner.com</a>		DAST	Arachni is a feature-full, modular, high-performance Ruby framework aimed towards helping penetration testers and administrators evaluate the security of modern web applications. The open-source security testing tool is capable of uncovering a number of vulnerabilities, including: Invalidated redirect, Local and remote file inclusion, SQL injection, XSS injection, etc.	*
<b>Caddy Server</b> * <a href="https://caddyserver.com">https://caddyserver.com</a> * <a href="https://github.com/caddyserver/caddy">https://github.com/caddyserver/caddy</a>		LB, Proxy, Ingress, Gateway	Caddy simplifies your infrastructure. It takes care of TLS certificate renewals, OCSP stapling, static file serving, reverse proxying, Kubernetes ingress, and more. Caddy runs great in containers because it has no dependencies—not even libc. Run Caddy practically anywhere.	
<b>Capsule8 Sensor</b> * <a href="https://github.com/capsule8/capsule8">https://github.com/capsule8/capsule8</a>		HIDS, RASP	The Capsule8 Sensor, which is based on KProbes, performs advanced behavioral monitoring (in real-time) for cloud-native, containers, and traditional Linux-based servers. It is intended to be run on a Linux host persistently and ideally before the host begins running application workloads. It is designed to support API clients subscribing and unsubscribing from telemetry dynamically to implement various security incident detection strategies.	* It is a sensor and requires be integrated with existing tool (log aggregation, ingestion, persistency, alerting, correlation, etc.) to work as Host Intrusion Detection System (HIDS)
<b>Cilium</b> * <a href="https://cilium.io">https://cilium.io</a> * <a href="https://github.com/cilium/cilium">https://github.com/cilium/cilium</a> * <a href="https://cilium.readthedocs.io/en/stable">https://cilium.readthedocs.io/en/stable</a>		Network Security	Cilium is an API-aware Networking and Security tool that uses eBPF and XDP. It secures transparently the network connectivity between application services deployed using Linux container management platforms like Docker and Kubernetes. Cilium works at Layer 3/4 to provide traditional networking and security services as well as Layer 7 to protect and secure use of modern application protocols such as HTTP, gRPC and Kafka.	* Implements Kubernetes SDN/CNI.
<b>Clair</b> * <a href="https://github.com/quay/clair">https://github.com/quay/clair</a> * <a href="https://github.com/arminc/clair-scanner">https://github.com/arminc/clair-scanner</a> * <a href="https://github.com/arminc/clair-local-scan">https://github.com/arminc/clair-local-scan</a>		SAST	Clair is an open source project for the static analysis of vulnerabilities in application containers (currently including AppC and Docker). Vulnerability data is continuously imported from a known set of sources (e.g. CVE) and correlated with the indexed contents of container images in order to produce lists of vulnerabilities that threaten a container.	* It is frequently used with Clair-Local-Scan ( <a href="https://github.com/arminc/clair-local-scan">https://github.com/arminc/clair-local-scan</a> ) and Clair-Scanner ( <a href="https://github.com/arminc/clair-scanner">https://github.com/arminc/clair-scanner</a> ) to perform scanning during CI/CD on premise (local).
<b>Cloudflare CFSSL</b> * <a href="https://cfssl.org">https://cfssl.org</a> * <a href="https://github.com/cloudflare/cfssl">https://github.com/cloudflare/cfssl</a>		PKI	CFSSL is CloudFlare's PKI/TLS swiss army knife. It is both a command line tool and an HTTP API server for signing, verifying, and bundling TLS certificates.	*
<b>Dagda</b> * <a href="https://github.com/eliasgranderubio/dagda">https://github.com/eliasgranderubio/dagda</a>		SAST	Dagda is a tool to perform static analysis of known vulnerabilities, trojans, viruses, malware & other malicious threats in docker images/containers and to monitor the docker daemon and running docker containers for detecting anomalous activities. In order to fulfill its mission, first the known vulnerabilities as CVEs, BIDs (Bugtraq IDs), RHBAs and RHBAs, and the known exploits from Offensive Security database are imported into a MongoDB to facilitate the search of these vulnerabilities and exploits when your analysis are in progress.	*
<b>Datawire Ambassador (Community Edition)</b> * <a href="https://www.getambassador.io">https://www.getambassador.io</a> * <a href="https://github.com/datawire/ambassador">https://github.com/datawire/ambassador</a>		LB, Proxy, Ingress, Gateway	Ambassador is an open source Kubernetes-native API Gateway built on Envoy, designed for microservices. Ambassador essentially serves as an Envoy ingress controller.	
<b>Docker Bench</b> * <a href="https://github.com/docker/docker-bench-security">https://github.com/docker/docker-bench-security</a>		Security Audit	The Docker Bench for Security is a script that checks for dozens of common best-practices around deploying Docker containers in production. The tests are all automated, and are inspired by the CIS Docker Benchmark v1.2.0.	* CIS Benchmark
<b>Dockle</b> * <a href="https://github.com/goodwithtech/dockle">https://github.com/goodwithtech/dockle</a>		SAST	Dockle is a container image Linter for security, detect container's vulnerabilities, helps build best-practice Dockerfile, supports CIS Benchmarks and DevSecOps practices (suitable for CI such as Travis CI, CircleCI, Jenkins, etc.).	* CIS Benchmark
<b>Envoy Proxy</b> * <a href="https://www.envoyproxy.io">https://www.envoyproxy.io</a> * <a href="https://github.com/envoyproxy/envoy">https://github.com/envoyproxy/envoy</a>		LB, Proxy, Ingress, Gateway	Envoy is a high performance C++ distributed L7 proxy designed for single services and applications, as well as a communication bus and "universal data plane" designed for large microservice "service mesh" architectures. Built on the learnings of solutions such as NGINX, HAPROXY, hardware and cloud LB, Envoy runs alongside every application and abstracts the network by providing common features, even Security, in a platform-agnostic manner.	* Envoy is hosted by the Cloud Native Computing Foundation (CNCF). * It is 'de-facto' small footprint edge and service proxy and embedded in opensource and commercial products, even in Cloud Providers such as AWS, Google and Azure. * Envoy Proxy in 2019: Security, Caching, Wasm, HTTP/3, and more ( <a href="https://blog.getambassador.io/envoy-proxy-in-2019-security-caching-wasm-http-3-and-more-e5ba82da0197">https://blog.getambassador.io/envoy-proxy-in-2019-security-caching-wasm-http-3-and-more-e5ba82da0197</a> )
<b>Ghostunnel Proxy</b> * <a href="https://github.com/square/ghostunnel">https://github.com/square/ghostunnel</a>		Proxy	Ghostunnel is a simple TLS proxy with mutual authentication support for securing non-TLS backend applications.	*
<b>Gloo Open Source</b> * <a href="https://gloo.solo.io">https://gloo.solo.io</a> * <a href="https://github.com/solo-io/gloo">https://github.com/solo-io/gloo</a>		LB, Proxy, Ingress, Gateway	Gloo is a cloud-native API Gateway and Ingress Controller built on Envoy Proxy to connect, secure and control traffic across all your application services. Modernize to microservices architecture and scale your edge operations with a lightweight, yet powerful control plane for distributed environments.	* The WAF features are WIP.
<b>Google gVisor</b> * <a href="https://github.com/google/gvisor">https://github.com/google/gvisor</a> * <a href="https://gvisor.dev/docs">https://gvisor.dev/docs</a>		Sandboxing, Isolation	gVisor is a user-space kernel, written in Go, that implements a substantial portion of the Linux system surface. It includes an Open Container Initiative (OCI) runtime called runsc that provides an isolation boundary between the application and the host kernel. The runsc runtime integrates with Docker and Kubernetes, making it simple to run sandboxed containers.	*
<b>Grabber</b> * <a href="http://rگاucher.info/beta/grabber">http://rگاucher.info/beta/grabber</a>		DAST	Grabber is a web application scanner. Basically it detects some kind of vulnerabilities in your website. Grabber is simple, not fast but portable and really adaptable. This software is designed to scan small websites such as personals, forums etc. absolutely not big application: it would take too long time and flood your network.	*
<b>Grafeas</b> * <a href="https://grafeas.io">https://grafeas.io</a> * <a href="https://github.com/grafeas/grafeas">https://github.com/grafeas/grafeas</a>		Software Supply Chain	Grafeas is an open-source artifact metadata API that provides a uniform way to audit and govern your software supply chain. It defines an API spec for managing metadata about software resources (container images, VMs, JAR, and scripts). You can use Grafeas to define and aggregate information about your project's components.	* Grafeas and Kritis integration: <a href="https://www.infoq.com/presentations/supply-grafeas-kritis">https://www.infoq.com/presentations/supply-grafeas-kritis</a>
<b>Hashicorp Consul Connect</b> * <a href="https://www.consul.io/docs/connect/index.html">https://www.consul.io/docs/connect/index.html</a> * <a href="https://www.consul.io/docs/connect/security.html">https://www.consul.io/docs/connect/security.html</a>		LB, Proxy, Ingress, Gateway	Consul Connect provides service-to-service connection authorization and encryption using mutual Transport Layer Security (TLS). Applications can use sidecar proxies in a service mesh configuration to establish TLS connections for inbound and outbound connections without being aware of Connect at all. Applications may also natively integrate with Connect for optimal performance and security. Connect can help you secure your services and provide data about service-to-service communications.	
<b>Hashicorp Vault Open Source</b> * <a href="https://github.com/hashicorp/vault">https://github.com/hashicorp/vault</a> * <a href="https://www.hashicorp.com/products/vault/pricing">https://www.hashicorp.com/products/vault/pricing</a>		PKI, Secrets Management	Vault is a tool for securely accessing secrets. A secret is anything that you want to tightly control access to, such as API keys, passwords, certificates, and more. Vault provides a unified interface to any secret, while providing tight access control and recording a detailed audit log.	* The Enterprise version includes HSM, MFA, Disaster Recovery, FIPS 140, etc.
<b>Heptio Ironclad</b> * <a href="https://github.com/heptiolabs/ironclad">https://github.com/heptiolabs/ironclad</a>		WAF	This is a reference configuration for running a web application firewall (WAF) on Kubernetes. It is a container build of ModSecurity+Ngix running the ModSecurity Core Rule Set along with a Go helper. The Ironclad container runs as a sidecar for your application. It proxies inbound requests to your application over localhost within the confines of a single Kubernetes Pod.	* "Take this with a grain of salt because this project is not actively maintained. I think the sidecar approach has benefits, especially if you have a lot of application-specific rules/exceptions that you want to version alongside each application." * <a href="https://www.youtube.com/watch?v=xVEWYgFc4eg">https://www.youtube.com/watch?v=xVEWYgFc4eg</a>

<b>In-toto</b> <a href="https://in-toto.io">* https://in-toto.io</a> <a href="https://github.com/in-toto/in-toto">* https://github.com/in-toto/in-toto</a>		Software Supply Chain	A framework to secure the integrity of software supply chains. in-toto is designed to ensure the integrity of a software product from initiation to end-user installation. It does so by making it transparent to the user what steps were performed, by whom and in what order. As a result, with some guidance from the group creating the software, in-toto allows the user to verify if a step in the supply chain was intended to be performed, and if the step was performed by the right actor.	*
<b>Istio</b> <a href="https://istio.io">* https://istio.io</a> <a href="https://github.com/istio/istio">* https://github.com/istio/istio</a>		LB, Proxy, Ingress, Gateway	Istio lets you connect, secure, control, and observe services. Istio makes it easy to create a network of deployed services with load balancing, service-to-service authentication, monitoring, and more, with few or no code changes in service code. You add Istio support to services by deploying a special sidecar proxy throughout your environment that intercepts all network communication between microservices, then configure and manage Istio using its control plane functionality.	* Istio uses Envoy Proxy in different way to implement Sidecar, API Gateway and Ingress Controller, which are the way to deliver security controls over the data plane. * Istio includes a CA and SPIFFE specs to implement Identity-based Security ( <a href="https://istio.io/docs/concepts/security">https://istio.io/docs/concepts/security</a> ).
<b>Kritis</b> <a href="https://github.com/grafeas/kritis">* https://github.com/grafeas/kritis</a>		Software Supply Chain	Kritis is an open-source solution for securing your software supply chain for Kubernetes applications. Kritis enforces deploy-time security policies using the Google Cloud Container Analysis API, and in a subsequent release, Grafeas.	* Grafeas and Kritis integration: <a href="https://www.infoq.com/presentations/supply-grafeas-kritis">https://www.infoq.com/presentations/supply-grafeas-kritis</a> * In Kubernetes, Kritis works as an Admission Controller.
<b>KubeSec.io</b> <a href="https://kubesecc.io">* https://kubesecc.io</a> <a href="https://github.com/controlplaneio/kubesecc">* https://github.com/controlplaneio/kubesecc</a>		Risk Analysis	Security risk analysis for Kubernetes resources.	*
<b>Linkerd</b> <a href="https://github.com/linkerd/linkerd2">* https://github.com/linkerd/linkerd2</a>		LB, Proxy, Ingress, Gateway	Linkerd is a service mesh, designed to give platform-wide observability, reliability, and security without requiring configuration or code changes.	* Linkerd is a Cloud Native Computing Foundation (CNCF) project.
<b>ModSecurity</b> <a href="https://modsecurity.org">* https://modsecurity.org</a> <a href="https://kubernetes.github.io/ingress-nginx/user-guide/third-party-addons/modsecurity">* https://kubernetes.github.io/ingress-nginx/user-guide/third-party-addons/modsecurity</a>		WAF	ModSecurity is an open source, cross platform web application firewall (WAF) engine for Apache, IIS and Nginx that is developed by Trustwave's Spiderlabs. It has a robust event-based programming language which provides protection from a range of attacks against web applications and allows for HTTP traffic monitoring, logging and real-time analysis.	* For Kubernetes, it should be integrated to NGINX Ingress Controller.
<b>Moloch</b> <a href="https://molo.ch">* https://molo.ch</a> <a href="https://github.com/aol/moloch">* https://github.com/aol/moloch</a>		NIDS	Moloch augments your current security infrastructure to store and index network traffic in standard PCAP format, providing fast, indexed access. An intuitive and simple web interface is provided for PCAP browsing, searching, and exporting. Moloch exposes APIs which allow for PCAP data and JSON formatted session data to be downloaded and consumed directly.	*
<b>NAXSI</b> <a href="https://github.com/nbs-system/naxsi">* https://github.com/nbs-system/naxsi</a>		WAF	It is an open-source, high performance, low rules maintenance WAF for NGINX. NAXSI means Nginx Anti XSS & SQL Injection. Technically, it is a third party nginx module, available as a package for many UNIX-like platforms. This module, by default, reads a small subset of simple (and readable) rules containing 99% of known patterns involved in website vulnerabilities.	* It should be adapted to work in Kubernetes.
<b>NeuVector Kubernetes CIS Benchmark</b> <a href="https://github.com/neuvector/kubernetes-cis-benchmark">* https://github.com/neuvector/kubernetes-cis-benchmark</a>		Security Audit	A set of scripts inspired by CIS Kubernetes Benchmark that checks best-practices of Kubernetes installations	* CIS Benchmark
<b>NGINX Ingress Controller</b> <a href="https://kubernetes.github.io/ingress-nginx">* https://kubernetes.github.io/ingress-nginx</a> <a href="https://github.com/kubernetes/ingress-nginx">* https://github.com/kubernetes/ingress-nginx</a>		LB, Proxy, Ingress, Gateway	Ingress Controller for Kubernetes based on NGINX.	
<b>Notary</b> <a href="https://github.com/theupdateframework/notary">* https://github.com/theupdateframework/notary</a>		Software Supply Chain	Notary is a project that allows anyone to have trust over arbitrary collections of data. Publishers can digitally sign collections and consumers can verify integrity and origin of content. This ability is built on a straightforward key management and signing interface to create signed collections and configure trusted publishers. With Notary anyone can provide trust over arbitrary collections of data. Using The Update Framework (TUF) as the underlying security framework, Notary takes care of the operations necessary to create, manage, and distribute the metadata necessary to ensure the integrity and freshness of your content.	* The Notary project has officially been accepted in to the Cloud Native Computing Foundation (CNCF). * It can be integrated into K8s through Admission Controller specific implementation like IBM Portieris ( <a href="https://github.com/IBM/portieris">https://github.com/IBM/portieris</a> ). * Single Source of Truth for 'Software Supply Chain'
<b>Open Policy Agent (OPA)</b> <a href="https://www.openpolicyagent.org">* https://www.openpolicyagent.org</a>		Security Policy	OPA is an open source, general-purpose policy engine that unifies policy enforcement across the stack. OPA provides a high-level declarative language that let's you specify policy as code and simple APIs to offload policy decision-making from your software. You can use OPA to enforce policies in microservices, Kubernetes, CI/CD pipelines, API gateways, and more.	* Falco and OPA are usually used together. * OPA is hosted by the Cloud Native Computing Foundation (CNCF).
<b>OpenSCAP</b> <a href="https://www.open-scap.org">* https://www.open-scap.org</a>		DAST	With oscap you can check security configuration settings of a system, and examine the system for signs of a compromise by using rules based on standards and specifications. The oscap uses SCAP which is a line of specifications maintained by the NIST which was created to provide a standardized approach for maintaining system security. The oscap mainly processes the XCCDF which is a standard way of expressing a checklist content and defines security checklists. It also combines with other specifications such as CPE, CCE and OVAL to create a SCAP-expressed checklist that can be processed by SCAP-validated products.	* The SCAP Workbench is a graphical utility that offers an easy way to perform common oscap tasks.
<b>OSSEC HIDS</b> <a href="https://www.ossec.net">* https://www.ossec.net</a> <a href="https://www.ossec.net/docs">* https://www.ossec.net/docs</a> <a href="https://github.com/ossec">* https://github.com/ossec</a>		HIDS	OSSEC is an Open Source Host-based Intrusion Detection System. It performs log analysis, integrity checking, Windows registry monitoring, rootkit detection, real-time alerting and active response. It runs on most operating systems, including Linux, OpenBSD, FreeBSD, Mac OS X, Solaris and Windows.	* If you want to explore the strategies to use OSSEC on Public Cloud Infrastructures, I recommend reading this: <a href="https://atomicorp.com/ossec-con2019">https://atomicorp.com/ossec-con2019</a>
<b>OWASP Zed Attack Proxy (ZAP)</b> <a href="https://www.zaproxy.org">* https://www.zaproxy.org</a> <a href="https://github.com/zaproxy/zaproxy">* https://github.com/zaproxy/zaproxy</a>		DAST	Zed Attack Proxy (ZAP) is a free, open-source penetration testing tool being maintained under the umbrella of the Open Web Application Security Project (OWASP). ZAP is designed specifically for testing web applications and is both flexible and extensible. At its core, ZAP is what is known as a "man-in-the-middle proxy." It can be used as a stand-alone application, and as a daemon process.	* Webapp Security Proxy
<b>OwlH Net</b> <a href="https://www.owlh.net">* https://www.owlh.net</a> <a href="https://github.com/OwlH-net">* https://github.com/OwlH-net</a> <a href="http://documentation.owlh.net">* http://documentation.owlh.net</a>		NIDS	OwlH was born to help security engineers to manage, analyze and respond to network threats and anomalies using Open Source Network IDS Suricata and Zeek, offering: Centralized Rule management and Network IDS nodes Configuration Management, Software TAP to capture cloud and distributed traffic in cloud and hybrid dispersed environments, Traffic Forensics with Moloch, Centralized Visualization and Compliance Mapping.	*
<b>Project Calico</b> <a href="https://www.projectcalico.org">* https://www.projectcalico.org</a>		Network Security	Calico is an open source networking and network security solution for containers, virtual machines, and native host-based workloads. Calico supports a broad range of platforms including Kubernetes, OpenShift, Docker EE, OpenStack, and bare metal services.	* SDN
<b>Rancher Load Balancer Controller</b> <a href="https://github.com/rancher/lb-controller">* https://github.com/rancher/lb-controller</a>		LB, Proxy, Ingress, Gateway	L7 Load Balancer service managing load balancer provider configured via load balancer controller. Pluggable model allows different controller and provider implementation. v0.1.0 has support for Kubernetes ingress as a controller, and Rancher Load Balancer as a provider. Rancher provider is a default one, although you can develop and deploy your own implementation (nginx, traffic, etc).	*
<b>Seccomp</b> <a href="https://www.kernel.org/doc/Documentation/prctl/seccomp_filter.txt">* https://www.kernel.org/doc/Documentation/prctl/seccomp_filter.txt</a> <a href="https://kubernetes.io/docs/concepts/policy/pod-security-policy">* https://kubernetes.io/docs/concepts/policy/pod-security-policy</a>		Linux Runtime Protection	Seccomp filtering provides a means for a process to specify a filter for incoming system calls. The filter is expressed as a Berkeley Packet Filter (BPF) program, as with socket filters, except that the data operated on is related to the system call being made: system call number and the system call arguments. This allows for expressive filtering of system calls using a filter program language with a long history of being exposed to userland and a straightforward data set.	* Used frequently with AppArmor and SELinux on Kubernetes to implement Security at Pod level ( <a href="https://kubernetes.io/docs/tasks/configure-pod-container/security-context">https://kubernetes.io/docs/tasks/configure-pod-container/security-context</a> ). * With Seccomp you can selectively choose which syscalls are forbidden/allowed to each container.
<b>SELinux</b> <a href="https://selinuxproject.org">* https://selinuxproject.org</a> <a href="https://github.com/SELinuxProject">* https://github.com/SELinuxProject</a> <a href="https://kubernetes.io/docs/concepts/policy/pod-security-policy">* https://kubernetes.io/docs/concepts/policy/pod-security-policy</a>		Linux Runtime Protection	SELinux is a security enhancement to Linux which allows users and administrators more control over access control. SELinux adds finer granularity to access controls. Instead of only being able to specify who can read, write or execute a file, for example, SELinux lets you specify who can unlink, append only, move a file and so on. SELinux allows you to specify access to many resources other than files as well, such as network resources and interprocess communication (IPC).	* Used frequently with AppArmor and Seccomp on Kubernetes to implement Security at Pod level ( <a href="https://kubernetes.io/docs/tasks/configure-pod-container/security-context">https://kubernetes.io/docs/tasks/configure-pod-container/security-context</a> ).
<b>Snort IDS</b> <a href="https://www.snort.org">* https://www.snort.org</a>		IDS	Snort's open source network-based intrusion detection/prevention system (IDS/IPS) has the ability to perform real-time traffic analysis and packet logging on Internet Protocol (IP) networks. Snort performs protocol analysis, content searching and matching. The program can also be used to detect probes or attacks, including, but not limited to, operating system fingerprinting attempts, semantic URL attacks, buffer overflows, server message block probes, and stealth port scans. Snort can work as sniffer, packet logger, and NIDS.	*
<b>SonarQube Community Edition</b> <a href="https://www.sonarqube.org">* https://www.sonarqube.org</a>		SAST	In addition to exposing vulnerabilities, it is used to measure the source code quality of a web application. Despite being written in Java, SonarQube is able to carry out analysis of over 20 programming languages. Furthermore, it gets easily integrated with continuous integration tools to the likes of Jenkins.	*
<b>SPIFFE</b> <a href="https://spiffe.io">* https://spiffe.io</a>		Zero Trust Network	SPIFFE, the Secure Production Identity Framework For Everyone, provides a secure identity, in the form of a specially crafted X.509 certificate, to every workload in a modern production environment. SPIFFE removes the need for application-level authentication and complex network-level ACL configuration.	* It is used by The SPIRE Project, Istio Citadel, Envoy Proxy, Pinterest, Kong Kuma, Hashicorp Consul, The Ghostunnel proxy, etc.
<b>SPIRE</b> <a href="https://spiffe.io/spire/">* https://spiffe.io/spire/</a> <a href="https://scytale.io/opensource-spiffe">* https://scytale.io/opensource-spiffe</a>		Zero Trust Network	SPIRE is a production-ready implementation of the SPIFFE ( <a href="https://spiffe.io">https://spiffe.io</a> ) APIs that performs node and workload attestation in order to securely issue SVIDs to workloads, and verify the SVIDs of other workloads, based on a predefined set of conditions.	*
<b>Suricata-IDS</b> <a href="https://suricata-ids.org">* https://suricata-ids.org</a>		NIDS	It is a free and open source, mature, fast and robust network threat detection engine. The Suricata engine is capable of real time intrusion detection (IDS), inline intrusion prevention (IPS), network security monitoring (NSM) and offline pcap processing. Suricata inspects the network traffic using a powerful and extensive rules and signature language, and has powerful Lua scripting support for detection of complex threats.	*
<b>Sysdig &amp; Sysdig Inspect</b> <a href="https://github.com/draios/sysdig">* https://github.com/draios/sysdig</a> <a href="https://github.com/draios/sysdig-inspect">* https://github.com/draios/sysdig-inspect</a>		HIDS, RASP	Sysdig is a full-system exploration, troubleshooting and debugging tool for Linux systems. It records all system calls made by any process, allowing SysAdmins to debug the operating system or any processes running on it. - Cysdig is a simple, intuitive, and fully customizable curses UI for Sysdig. - Sysdig Inspect is a powerful web interface for container troubleshooting and security investigation.	* Sysdig instruments your physical and virtual machines at the OS level by installing into the Linux kernel and capturing system calls and other OS events. Sysdig also makes it possible to create trace files for system activity, similarly to what you can do for networks with tools like tcpdump and Wireshark. This way, problems can be analyzed (Forensics) at a later time, without losing important information.

<b>Sysdig Falco</b> <a href="https://falco.org">* https://falco.org</a> <a href="https://github.com/falcosecurity/falco">* https://github.com/falcosecurity/falco</a>		HIDS, RASP	Falco is a behavioral activity monitor designed to detect anomalous activity in your applications. Falco audits a system at the most fundamental level, the kernel. Falco then enriches this data with other input streams such as container runtime metrics, and Kubernetes metrics. Falco lets you continuously monitor and detect container, application, host, and network activity -all in one place- from one source of data, with one set of rules.	* Falco is the first runtime security project to join CNCF Incubating stage. * Falco provides runtime security with an implementation of the Extended Berkeley Packet Filter (eBPF), which allows the tool to capture system calls at the level of the Linux kernel, without impacting performance.
<b>Traefik</b> <a href="https://containo.us/traefik">* https://containo.us/traefik</a> <a href="https://github.com/containous/traefik">* https://github.com/containous/traefik</a>		LB, Proxy, Ingress, Gateway	Traefik (pronounced traffic) is a modern HTTP reverse proxy and load balancer that makes deploying microservices easy. Traefik integrates with your existing infrastructure components (Docker, Swarm mode, Kubernetes, Marathon, Consul, Etc, Rancher, Amazon ECS, ...) and configures itself automatically and dynamically. Pointing Traefik at your orchestrator should be the only configuration step you need.	
<b>w3af</b> <a href="http://w3af.org">* http://w3af.org</a> <a href="https://github.com/andresriancho/w3af">* https://github.com/andresriancho/w3af</a>		DAST	w3af is an open source web application security scanner which helps developers and penetration testers identify and exploit vulnerabilities in their web applications. The scanner is able to identify 200+ vulnerabilities, including Cross-Site Scripting, SQL injection and OS commanding.	*
<b>Wapiti</b> <a href="https://wapiti.sourceforge.io">* https://wapiti.sourceforge.io</a> <a href="https://sourceforge.net/p/wapiti/git/ci/master/tree">* https://sourceforge.net/p/wapiti/git/ci/master/tree</a>		DAST	Wapiti allows you to audit the security of your websites or web applications. It performs "black-box" scans (it does not study the source code) of the web application by crawling the webpages of the deployed webapp, looking for scripts and forms where it can inject data. Once it gets the list of URLs, forms and their inputs, Wapiti acts like a fuzzer, injecting payloads to see if a script is vulnerable.	*
<b>Wazuh HIDS</b> <a href="https://wazuh.com">* https://wazuh.com</a> <a href="https://github.com/wazuh/wazuh-kubernetes">* https://github.com/wazuh/wazuh-kubernetes</a> <a href="https://github.com/wazuh/wazuh-docker">* https://github.com/wazuh/wazuh-docker</a>		HIDS	Wazuh provides a security solution capable of monitoring your infrastructure, detecting threats, intrusion attempts, system anomalies, poorly configured applications and unauthorized user actions. It also provides a framework for incident response and regulatory compliance.	* It is a fork of OSSEC. * It can be integrated with Splunk, ELK, EFK and provides an RESTful API. * Although It is intended to be used on premise for old-school infrastructure, It has been adapted to work in Container-based and Public Cloud.
<b>Weave Net</b> <a href="https://www.weave.works/oss/net">* https://www.weave.works/oss/net</a> <a href="https://github.com/weaveworks/weave">* https://github.com/weaveworks/weave</a>		Network Security	Weave Net creates a virtual network that connects Docker containers across multiple hosts and enables their automatic discovery. With Weave Net, portable microservices-based applications consisting of multiple containers can run anywhere: on one host, multiple hosts or even across cloud providers and data centers.	* SDN
<b>Zeek (formerly Bro IDS)</b> <a href="https://www.zeek.org">* https://www.zeek.org</a> <a href="https://www.bro.org">* https://www.bro.org</a>		NIDS	Zeek is an open-source network security platform (formerly named Bro) that illuminates your network's activity in detail, with the stability and flexibility for production deployment at scale.	*

[ Security along Container-based SDLC - OSS Tools List | <http://holisticsecurity.io/2020/02/10/security-along-the-container-based-sdlc> | Updated by 2020/02/10 ]