# : radware

# Securing Cloud-Native Kubernetes Applications

WEB APPLICATION FIREWALL TECHNICAL WHITE PAPER

SHARE THIS WHITE PAPER



# TABLE OF CONTENTS

>	Overview	3
>	Containers, Microservices and Service Meshes	3
>	Kubernetes Orchestration	3
	Container	4
	Cluster	4
	Node (Minion)	4
	Pod	4
	Service	4
>	Cloud-Native Application Security Challenges	5
	The Good Old OWASP Top 10 for Web Applications	5
	The API Role in Modern Applications	5
	The New OWASP Top 10 for APIs	5
>	DevSecOps Requirements	5
>	Radware's Kubernetes Web Application Firewall (WAF)	6
>	The Architecture — Designed for Kubernetes	6
	Data Plane Policy Enforcer	6
	Controller	7
	Management Portal	7
	Management APIs	8
>	Security — Robust Application and Data Protection	9
	Active Protection and Report-Only Mode	9
	Access Control	9
	Expressions	9
	Signatures	9
	JSON and XML Parsing	9
	Data Leakage Protection	9
	Source Blocking	9

# 

Application security has historically taken a back seat to application delivery. Traditional IT security teams view themselves as gatekeepers; they must do their jobs correctly or their organizations face increased risk. They incorporate high security standards into every operation, but achieving these standards takes time, testing and iterations. Development teams fret because this slows application development and often does not ensure comprehensive protection.

When businesses look to optimize and accelerate application development life cycles and deliver their applications in public clouds (typically referred to as cloud-native applications), security becomes a greater challenge. Cloud-native apps usually run in new architectures that provide unprecedented efficiency, flexibility and cost-effectiveness. Development and operations (DevOps) groups emerged to take an active role in application delivery by selecting the tools and budget to set the development and deployment pace. Automation platforms, powerful orchestration frameworks, open-source toolsets and visibility solutions all play a major role in these environments.

Development, security and operations (DevSecOps) represent the security component of DevOps and seek to fit security due diligence into processes that drive speed, agility and continuous delivery. However, DevSecOps may find it challenging to deliver security to continuous delivery processes if they lack automation, orchestration tools and visibility and have inferior application protection.

# **⊖** Containers, Microservices and Service Meshes

Transitioning from a monolithic architecture to a microservice architecture allows applications to be deployed more frequently. Different microservices can be independently delivered in a more reliable manner. In parallel, container technology emerged, which is a perfect match to microservices. Each microservice is deployed across multiple containers to allow for quick rollout and scalability, improving quality and reducing time to market.

A service mesh is a layer that handles the interservice communication in a microservice architecture. Its purpose is to reduce the complexity associated with a microservice architecture by providing scalability through load balancing, telemetry, traffic routing, health checks, etc.

One of the challenges with the transition to a microservice architecture has to do with the scale of objects provisioned. In the monolithic era, few monolith web instances were load balanced. Today, there are thousands of containers which need to be automatically spawned.

# **OKUBERNETES Orchestration**

With the growth of the microservice architecture, a new space of containerized application orchestration frameworks has evolved, and Kubernetes is one of its largest components, given its adoption by most organizations.

Kubernetes is an open-source platform for managing containerized workloads and services and facilitates automating application deployment, scaling and management.

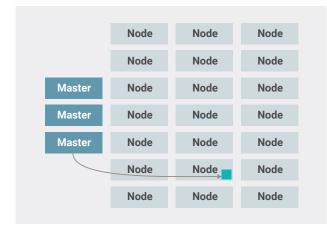
Kubernetes defines a set of objects and building blocks to orchestrate the containerized applications.

# Container

- Programs running on Kubernetes are packaged as containers
- Limit of one process per container

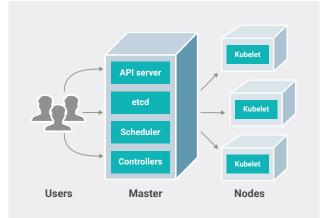
## Cluster

- One master machine and multiple worker machines (nodes)
- A master coordinator between all nodes



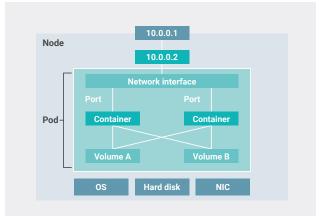
# Node (Minion)

- A worker machine (cloud workload, virtual machine or physical machine) that contains services to run a pod
- Has a host name
- Has an IP address



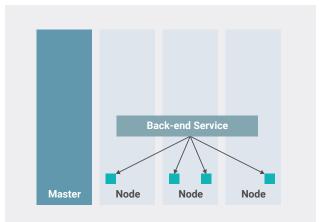
# Pod

- > An instance of the microservice
- > The smallest unit of a cluster
- Represents a running process on a cluster
- Runs on a single container or multiple containers
- Different containers of a single pod communicate with each other using "localhost"
- Has an IP address



# Service

Exposes an application running on a set of pods as a network service



# **Ocloud-Native Application Security Challenges**

With all the power that microservice architectures and service mesh infrastructures provide, they do not address application and data security challenges. In addition to the already known application security challenges, which are as relevant now as in the past, the distributed nature of microservice apps introduces latencies, topology changes and challenges with managing many microservices.

## The Good Old OWASP Top 10 for Web Applications

The Open Web Application Security Project (OWASP) provides security professionals with an overview of the most critical web application security risks. Injections, broken authentication, cross-site scripting (XSS) and sensitive data exposure are just a few examples of risks that are as relevant for cloud-native apps as they are for monolithic applications.

### The API Role in Modern Applications

Modern apps make intensive use of APIs across different use cases: internet of things (IoT) applications, machine-to-machine communication, event-driven web applications, automated actions in web frameworks, function-as-a-service (FaaS) apps, mobile apps, etc. All of these use cases refer to north-south communication, which is client-to-app traffic. Most of the APIs serving these use cases are REST APIs with JSON bodies (REST-JSON). A smaller portion of the APIs are simple object access protocol (SOAP) based with XML structured data formats.

As these APIs are running on top of the HTTP protocol, most of the web app security risks are as relevant for APIs as they are for web apps. Additionally, APIs introduce additional security challenges, mostly around authorization and access control, as the APIs may be served independently.

## The New OWASP Top 10 for APIs

With the growing adoption of APIs, the OWASP organization has produced the API Security Project under which it has published the OWASP API Security Top 10 Release Candidate. Examples of the API security risks referred to in the project include broken object level authorization, excessive data exposure, lack of resources and rate limiting, and injection, all of which may lead to data theft or service disruption.

# DevSecOps Requirements

By their nature, cloud-native apps are running in cloud environments, leveraging and consuming the different services which the public cloud vendors offer, such as workloads, storage, Kubernetes orchestration services, content delivery networks (CDNs), etc. These services provide simple delivery while using industry standard open-source projects or public cloud technology.

However, the quality of the security services offered by the public cloud vendors is inadequate for different reasons. The complexity of the security operation, the continuous research investment required and the constantly changing threat landscape are three of the primary reasons.

DevSecOps seek to address this gap in quality of security offering while looking for a security solution that will fit into their ecosystem. The solution must be behind the cloud vendor CDN service, be scalable, offer complete support for automation to integrate into the Kubernetes orchestration system, provide detailed security visibility and reporting, keep the footprint low, maintain low false-positive posture, and address the most critical security risks associated with APIs and mobile apps.

# Radware's Kubernetes Web Application Firewall (WAF)

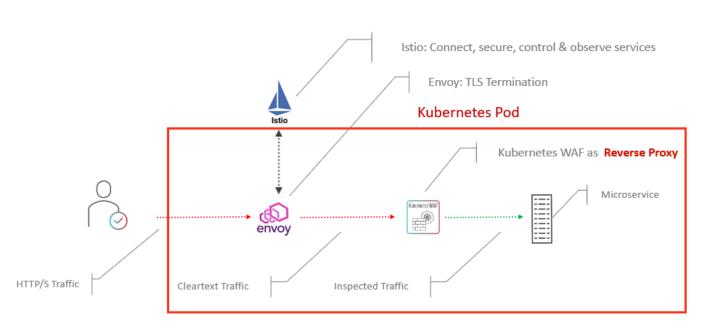
Radware's Kubernetes WAF is designed to fit into the Kubernetes orchestration system in a service mesh architecture to provide the best of both worlds: market-leading application security with advanced automation and the elasticity required by today's DevSecOps teams. It offers its own management portal, integrating common visibility and reporting platforms such as Elastic and Prometheus. The security offering includes web and API security for applications and microservices running in Kubernetes.

# The Architecture – Designed for Kubernetes

Radware's Kubernetes WAF consists of a distributed architecture with security sidecars deployed at the pod level in the data plan and a management back end running on the same Kubernetes cluster for the control plane. It is based on four primary components.

#### Data Plane Policy Enforcer

The Kubernetes WAF data plane policy enforcer runs as a security sidecar in the same pod as the microservice. It functions as a reverse proxy before the microservice and can work after either a sidecar proxy (e.g., Istio/Envoy) or any other ingress method outside of the pod (e.g., NGINX ingress controller). In both cases, SSL termination is accomplished before the enforcement, by either Istio or the Kubernetes cluster's ingress controller, to allow the enforcer to handle clear text traffic. In any case, all reverse proxies are supported. The solution enables single termination of TLS traffic only at the host level and thus eliminates the need to manage multiple certificates across different parties.

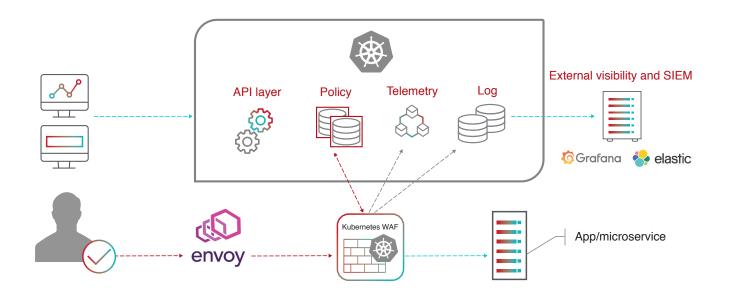


#### **Kubernetes Pod**

# Controller

The Kubernetes WAF centralized control plane back end is running in the same Kubernetes cluster as the application. It provides centralized administration, management, reporting and forensics, via either APIs or the management portal GUI. Kubernetes will provision the data plane enforcer to allow seamless scalability and elasticity. Since the policy is centrally stored and managed in the controller, any policy change that is applied manually by the administrator or automatically generated by the machine learning modules will be synchronized automatically across all data path policy enforcers. Telemetry information is collected from the policy enforcer and pushed to the controller for analytics and auto-policy processes.

Logs are sent from the enforcer to a centralized logging module in the controller to allow centralized forensics and analytics and allow forwarding of the logs to external visibility and security information and event management (SIEM) systems such as Elastic and Prometheus.



An essential part of the control plane is the auto-policy generation engine. Machine learning algorithms map the application resources, analyze potential threats and then apply and tune the security policy. This process runs automatically whenever a new microservice is introduced or a modification is being pushed.

### **Management Portal**

The Kubernetes WAF management portal provides a GUI to monitor and manage Kubernetes WAF security. It consists of:

- Dashboards which provide visualization of real-time telemetry and security events tailored for the DevOps and SecOps users.
- Forensics which provide detailed security event reports with drill-down analysis, analytics and exception handling. Each security event can be excluded from future inspection if deemed legitimate traffic. Additionally, full transaction logs are visible under the access logs.
- Security profiles which provide security configuration settings for the system. Users can define flexible classifiers based on client traffic attributes (HTTP header values), and the compatible policy will be applied.

	es WAF							Ļ (	💄 User Name
All and a second percent pe								Last 30	Im 🕘 🤅
Indexed versions       1,458       Paperde versions       1,458       Paperde versions	es Dashboard	WAF for Kubernetes D	ashboard						
Image: Control of the state of the stat		Security Events	View Details	Security Eve	nts	View Details	Security Even	ents	View Details
		Blocked Events	1.458	Reported Event		1.458	Legitimate Ever	nts	1 4 5 8
			1,430			1,430			1,430
		OWASP Top 10	Top Attack Category	0 C ×	Top Sources	0 [] ×	Geo Location		0 C ×
		A1 A1 A3	HTTP RFC violations	1504		184			
		140 143	Information Laukage	20.64		Rosk.			155
		A4	Automation	19.04		ROSK.		6197	
			Parn Traversal	mex	111.120.67.178	RODAK			-
Alternative descent for the set of the se			4	0.0.11					0.00.00
Id				O LIX	Traffic	TPS Mbp	0 [] X		
		Reported		1505				Akrts	
Accoss and provide a state of the st		Modified		8.04	300				
<complex-block>  Image: And and and a lot with the destination of the desti</complex-block>		7 5	B virtmax_255.480	18.66				7-	- 58
Security Events       Image: Market Type       Market Type       Market Type			virtmax_255-ABC	mer		June 16 Jul 16	Aug 16 Sep 16		
<ul> <li>Source</li> <li>Uit</li> <li>Tag</li> <li>Profile</li> <li>Source</li> <li>Source</li> <li>Tag</li> <li>Novi 1001, 2018 13:12:20</li> <li>Pattern Volat.</li> <li>Command Exec</li></ul>			/ OWASP 2017 Top 10	Mapping - <b>A1-Injectio</b>	n				
Bource       Util         Bource       Date         Date 1020M       23 de 1020M       2.01020M       2.01020M       2.01020M       11.01020M       12.01020M		Security Analytics		Mapping - <b>A1-Injectio</b>	n				30m 🕘 (
Image       20 m 100 M	hboard	Security Analytics OWASP 2017 Top 10 Mapping - All rejection > Attack Type		Mapping - <b>A1-Injectio</b>		VENTS 11.040-21			30m 🕘 (
Image: Notifie	hboard	Security Analytics OWASP 2017 Top 18 Mapping - Allipector 3		Mapping - A1-Injectio		49/175 1,2,482			30m 🕘 (
Security Events       Image: Control of the security and the secure the secure the security and the secure the security	shboard	Security Analytics OWERF201Top 16 Mageing - Atligation - 3 Attack Type Source URI		Mapping - A1-Injectio		KINS U MO 21			30m 🕘 (
Time And Date     Title     Thesit     Tag     Profile     URI     Transaction ID <ul> <li>Nov 1019, 2018 1512.20</li> <li>Pattern Voldt</li> <li>Command Exec</li></ul>	sehboard	Security Analytics		Mapping - A1-Injectio		49/175 14.862.972			30m 🕘 (
Time And Date     Title     Theat     Tag     Profile     URI     Transaction ID       Nov 1001, 2018 1512:2.0     Pattern Voldz.     Command Exec	hboard	Security Analytics	(Alt) unget/d X	50	TOTAL D	10.06220		Last	30m () (
Signature Engine Intercepted Additions Request, Which Includes ABlock, Loren Journ Dolor SB Amet, Connectation: Additioning Elit. Asenean Commodo Liguéa.         Exclude         > Nor 1011, 2018           Time         17 ad 2019 15.33.53         Policy Name         Age/Index         > Nor 1011, 2018           UIII         Crime Ew         Modole         Signature         > Nor 1011, 2018           Signature         79/0         Policy Vision         Glassifier         > Nor 1011, 2018           Tog         Age1         Classifier         Classifier         > Nor 1011, 2018           Profife         Obduel Wass Graphity Age1 Polity         Transaction ID         Artil S132 Bed-Math Antil 253B Bed-Math Antil An	ard	Security Analytics	(Alt) unget/d X	50	TOTAL D	10.06220	TI JA TOZO AM	20 12.0/1929.04	30m (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)
Time         17.04 2019 1530.53         Policy Name         Appl Paloy           URI         x0md Exe         Module         Signature         > Nor 1019, 2018           Signature         7982         Policy Hash         69885/4907704588885(217413737648657)         > Nor 1019, 2018           Tog         App1         Classifier         Classifier         Classifier         > Nor 1019, 2018           YEF Header         Module         Signature Appl Phote         Transaction ID         Antel Städeb-4464.421 712810294817         > Nor 1019, 2018           XFF Header         XForwarded For         Mothod         GET         > Nor 1019, 2018           Source Host Mare         Mash Stade Forwarded For         Action Renote Address         > Nor 1019, 2018           Source Host Mare         By Parlam         Action Renote Address         > Nor 1019, 2018           Totle         Parlam         Action Renote Address         > Nor 1019, 2018		Security Analytics	Alt angerid x	25 29 AP 1022 M	TOTAL (* 	18.00 E	на взет на г	20 12.0/1929.04	30m (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)
UR1     //md/Ee     Module     Signature       Signature     700     Policy Yash     40845742077325746427441373746427441       Tag     April     Classifier     026887420772683257481737546427441       Tag     April     Classifier     026887420772683257481737546427441       Profide     Dedukt/wasa Sumpic-Appit Profite     Transaction 10     A1132348644464.447.1728832594817       XFF Header     Xmarsuber Appit Profite     Action     6CUMITY-JARCE       Source Horit Name     Namingh-Appit Deploymente Y44M1855047403     Action     SCUMITY-JARCE       Event Berl     op Jaman     Action     SCUMITY-JARCE     Sci Nor 10h.2018       Title     Namin Valution Detected     Toment Lisencofned     Sci Nor 10h.2018	ard	Security Analytics	e Threat	23 July 1023 AM	2.04 1929 MI URI	200 E.M. 1920AM	ны 1030 ми пала 1030 ми	12 Juli 1000 MM	30m (1) ( × (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)
Signature         7992         Policy Hash         64885/4491785pd4ebb8tec31491378pdeeb7ed           Tag         App1         Classifier         Classifier         Classifier         App1	pard	Security Analytics	AtD rangestal X	29 An 1020 AM Tag Profile 2 app1 default/was1	TOTAL E 2.44 1020 AM 5.34 102 URI to sample-app1 / cmd.exx	2.48 <sup>2</sup> 2.49 <sup>2</sup> 2.49 <sup>2</sup> 2.49 <sup>2</sup> 2.49 <sup>2</sup> 7.77 7.77 7.77 7.77 7.77 7.77 7.77 7.	11.34.1920 AM	201 12.0/1022/M	30m (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)
Tag         App1         Classifier         Classifier         Classifier           Profile         Default/Wass Sample App1 Profile         Table 2013 2486 4467-172810370:0117         > Nov 1001, 2018           XFF Header         XForwardod-For         Mathod         6ET         > Nov 1001, 2018           Source Host Name         Wass Sample App1 Profile         Action         SECURITY_FAGE         > Nov 1001, 2018           Event Ref.         By Patern         Actor Remote Adversure         Actor Remote Adversure         > Nov 1001, 2018           Table         Patern Volution Detected         Toren Name         Command Saectrion         > Nov 1001, 2018		Security Analytics	AltD sangerid ×	29 Am 1020 AM Tag Profile L. Lorent psame Dolor Sit Amet, Policy Name	URI 2.04 1929AM 8.04 192 E.Bample-app1 / cond ex Consectativer Adjacoing El Aq01Paley	2.48 <sup>2</sup> 2.49 <sup>2</sup> 2.49 <sup>2</sup> 2.49 <sup>2</sup> 2.49 <sup>2</sup> 7.77 7.77 7.77 7.77 7.77 7.77 7.77 7.	11.34.1920 AM	Социре 12.AI 16.25 АМ Э. Социре -12.56160.390 Ехсіцие Э. Э.	30m (1) x 10 10 10 10 10 10 10 10 10 10
XFF Header         XForwarded For         Method         GET           Source Hoat Name         was inpike Appl Deployment 746/INESE Windle         Action         BECURT_MAGE         > Nov1010, 2018           Event Net         by Patiann         Action Texter Advess         Action Texter Advess         > Nov1010, 2018           Table         Patienn Wasking Description         Action Texter Advess         > Nov1010, 2018         > Nov1010, 2018	board	Security Analytics	AltD sangerid ×	29 AM 1027 AM Tag Profile Tag Profile Loren Josen Dolor Sit Anet, Policy Hame Module	TOTAL ID 2.0.1922/M URI URI sample-app1 //md ex consectedre Adjacong El AgetPaday Sputus	ELAN ELANDEAL	11.34.1920 AM	I Colleges 12 Art 16 20 AM Colleges 12 Debb0 190 2 Colleges 12 Debb0 190 2 De	30m (1) ( × (1) 12 ∧1/1525 MC 12
Score Host Name         Waas Sample Age) Opeignment 74ddf16550 Vmdub         Action         SEQURITY_PAGE         > Nov 101h, 2018           Even Ref.         by Pattern         Actor Reende Address         Actor Reende Address         > Nov 101h, 2018           Title         Pattern Volation Detected         Threat Name         Command Security         > Nov 101h, 2018	pard	Security Analytics	e Threat a Reguest, Which Includes A Bloc 32	29 An 1020 AM Tag Profile app1 default/wass k. Loren Ipsam Dolor Sit Amet, Module Policy Name Module Classifier	URI 2.04 1929AM 8.04 192 URI 4.04 1929AM 8.04 192 URI 4.04 1920AM 8.04 192 Signatures Signatures Signatures Consectedure Adjacency El Signatures	20.42 20.43 20.44	11.34.1920 AM	I Colleges 12 Art 16 20 AM Colleges 12 Debb0 190 2 Colleges 12 Debb0 190 2 De	30m (1) ( × ) 12 J/1 120 J/4 12 J/4
Event Ref.         By Pettern         Actor Remode Adress         > Nov 1811, 2018           Tob         Pattern Wolation Detected         Threat Name         Command Execution         > Nov 1811, 2018	shboard	Security Analytics	e Threat a Reguest, Which Includes A Bloc 32	29 APT 1029 AM Tag Profile Loren Josen Dolor Sit Anet, Policy Heah Classifier Taneaction ID	URI 2.04/92/04/ 2.04/92/04/ 2.04/92/04/ URI 4.94/92/04/ URI 4.94/92/04/ Signature Sign	20.42 20.43 20.44	11.34.1920 AM	I Collape -1258b0390 Exclude > >	30m (1) ( x (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)
	shboard	Security Analytics	e Threat en Volat Command Exec s Request, Which Includes A Bloc s5	23 Art 1028 AM	TOTAL E TOTAL E 2.01923/04 5.0192 LURI LURI LURI LURI LURI LURI LURI LURI	20.42 20.43 20.44 E.A.1922.44 Trr s. a.97 t. Aenean Commodo Ligal ab886c374/1375faet6/ad	11.34.1920 AM	12.bit K20 AM	30m (1) ( x ) 10 Jul 100 MA 10 Ju
Attack Hame Code Rijection > Nov 16th, 2018	hboard	Security Analytics	e Threat en Volat Command Exec s Request, Which Includes A Bloc s5	29 An 1020 AM Tag Profile Sp An 1020 AM Tag Profile L Lorent psum Dolor Sit Amet, Module Policy Name Module Policy Name Classifier Transaction ID Matheod Action	TOTAL D TOTAL D TOT	20.42 20.43 20.44 E.A.1922.44 Trr s. a.97 t. Aenean Commodo Ligal ab886c374/1375faet6/ad	11.34.1920 AM	12.bit K20 AM	30m (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)
	pard	Security Analytics	Atti rangendi X      Atti	29 Art 1029 AM Tag Profile a app1 default/wass b. Lorem (psam) Dolor Sit Amet, Policy Heah Classifier Transaction ID Method Action Actor Remote Addr	TOTAL D TOTAL D TOT	20.42 20.43 20.44 E.A.1922.44 Trr s. a.97 t. Aenean Commodo Ligal ab886c374/1375faet6/ad	11.34.1920 AM	12.bit K20 AM	30m (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)

### Management APIs

Every configuration and operation on the Kubernetes WAF can be performed without the GUI via Kubernetes compatible APIs.

Security profiles are defined as Kubernetes custom resource definitions (CRDs), and they are managed in the same way as other Kubernetes resources. This approach allows for full management and configuration of security profiles via native Kubernetes APIs without using the management portal.

Telemetry and log collection are accomplished with Prometheus to allow external visibility with commonly integrated tools like Grafana, including traffic metrics, statistics, Kubernetes WAF resource usage and security event data.

Security logs can be pushed to an external Elastic platform for detailed visibility and reporting using Kibana dashboards.

# **⊖** SECURITY – ROBUST APPLICATION AND DATA PROTECTION

## Active Protection and Report-Only Mode

Radware's Kubernetes WAF provides protection modules originated from Radware's WAF, AppWall<sup>®</sup>, but tailored to deliver WAF protection to Kubernetes-aligned security solutions. Each module can be set to a report-only mode, which generates security logs for violations but will not block traffic or activate a protection mode.

### Access Control

The access control module allows the defining of web resources and APIs that should be accessible. Requests to nonlisted resources will be blocked or logged, depending on the policy settings. Policy settings can be defined at a full path level or file extension level or by a regular expression definition.

#### **Expressions**

The expressions security module is based on regular expression and logical rules for detection of known types of attacks, such as SQL and non-SQL injections.

#### Signatures

The signatures security module is based on a string match engine to detect attack patterns in HTTP requests. Signature rules detect known types of attacks such as XSS, predictable resource locations, directory traversal, etc.

### JSON and XML Parsing

Both JSON and XML bodies are parsed, JSON/XML validity checks are applied, and key values are extracted for further inspection by the other protection modules, such as signatures and expressions. This allows detection of common API attacks such as XML bombs, manipulation of APIs and detection of embedded attacks.

### **Data Leakage Protection**

The data leakage protection module identifies sensitive information in application responses, allowing the masking of sensitive data. Examples of sensitive data are credit card numbers, Social Security numbers, server error messages, etc.

## Source Blocking

This module provides per-source correlation of security violations for the blocking of persistent attack agents.

# **⊖** Conclusion

With its advanced automation, policy generation and robust security, Radware's Kubernetes WAF provides DevSecOps with the flexibility and automation needed to allow for the timely development and deployment of secure applications across hybrid computing environments.

### **About Radware**

Radware<sup>®</sup> (NASDAQ: RDWR) is a global leader of cybersecurity and application delivery solutions for physical, cloud and software-defined data centers. Its award-winning solutions portfolio secures the digital experience by providing infrastructure, application and corporate IT protection and availability services to enterprises globally. Radware's solutions empower more than 12,500 enterprise and carrier customers worldwide to adapt quickly to market challenges, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit www.radware.com.

Radware encourages you to join our community and follow us on: Radware Blog, LinkedIn, Facebook, Twitter, YouTube, Radware Connect app for iPhone<sup>®</sup> and our security center DDoSWarriors.com that provides a comprehensive analysis of DDoS attack tools, trends and threats.

© 2019 Radware Ltd. All rights reserved. The Radware products and solutions mentioned in this document are protected by trademarks, patents and pending patent applications of Radware in the U.S. and other countries. For more details, please see: https://www.radware.com/LegalNotice/. All other trademarks and names are property of their respective owners.