

Trend Vision One[™] - Container Security

Simplify container security with advanced image scanning, policy-based admission control, and runtime protection, detection, and response

Modern application development strategies are becoming more prevalent among companies looking to increase the speed that new capabilities and features are delivered, driving additional customer value. However, with the endless benefits of cloud-native application development come with a major risk: lack of security and fragmented tooling. Today's organizations are challenged to meet the objectives of both security teams and application teams, as they operate with different resources and priorities. On top of that, microservice-based architectures are changing how organizations transition to cloud, container, and serverless platforms, requiring an integrated platform approach to cloud security.

With the technology's many benefits, containers have become mainstream. According to the Cloud Native Computing Foundation (CNCF), <u>88% of organizations are using containers today</u>, and the majority are running them in production. Container environments have also become quite diverse, with many organizations running containers on-premises and in the cloud, and Kubernetes has emerged as the de facto aid to assist with orchestration and streamline operations.

Security teams are facing new challenges

With production workloads shifting to cloud-native platforms and DevOps teams adopting security best practices across their build pipelines and runtime deployments, security solutions need to be designed to succeed across hybrid- and multi-cloud environments (physical, virtual, cloud, containers, and serverless). With security teams absorbing more cloud security responsibilities, you need trusted security controls in place from build-time to runtime. This promotes tool consolidation and collaboration of security and compliance requirements without interfering in continuous integration/continuous delivery (CI/CD) development cycles.

Introducing Trend Vision One[™] - Container Security

Delivering container image security, container admission control policy, and container runtime protection, detection, and response. Container Security enables earlier and faster detection of malware, vulnerabilities, and compliance violations. Your security operations and application teams are able to address and remediate issues before they can be exploited in production, decreasing cost and complexity.

Define policies once and manage container risk

Select and define policies so that only the most secure Kubernetes container are deployed with container admission control. Integrating directly with Kubernetes, Container Security can define the policy that either allows or blocks the image from running. This is based on preferences you've defined once, including whether it is a privileged container or whether it has been scanned for malware and vulnerabilities. This gives your security team control over the containers that are allowed to run in their environment.

Runtime protection gives your security team an additional layer of defense. This provides you with alerts and indicators of attacks (IoA) across running containerized applications with insights aligned to the MITRE ATT&CK framework. Get visibility of risks in running containers, discover attempts to run disallowed commands or illegally access files, and detect and respond to suspicious activity with extended detection and response (XDR) capabilities.

End-to-end container protection

Container Security helps DevOps teams deploy security with immediate and continuous protection, from the build pipeline to runtime. With support for leading container platforms including Amazon EKS, Amazon ECS, AWS Fargate, Azure AKE, and Google GKE, Container Security can be seamlessly integrated across your existing Cl/CD toolchains and container environments. Implementing effective security earlier in the software build-pipeline helps to achieve consistent results faster in the development cycle and reduces manual security steps and application downtime. In addition, runtime protection, detection, and response shields running containers from evolving threats and allows for the investigation of activities across layers. Simplify resource management with a clear and organized overview of your Kubernetes clusters' inventory.



Admission control policy



Container runtime protection

2	Trend Vision C	ne™∣conta	ainer Protection			٥	A 0	8
হ	O Important: The "	Preview" period	of this pre-release feature ends on 2023-09-28 00:0	0:00 at which point this becomes a paid feature. View details				
ø	Policies Rulesets	Winerabilities	s Events Artifact Scanner					
3	Filter by: Policy 🗸	Q. Enter poli	icy rame Apply				Last 30 days 👒	a
\times			Kubernetes Runtime 🔿 ECS Runtime					
[9]]	Action Time		Policy		Cluster .	Rule		
F	0 64 2023-0	9-2102:29				New executable created (spen+create)		
-	· Log 2023-0	99-21 02:29				New executable created (chmod)		
<u>e=</u>						New executable created (chmod)		
®	0 161 2023-0	99-21 02:29				New executable created (spen+create)		
.2.	C LOg 2023-0	09-21 02:29				New executable created (chmod)		
8	· · · · · 2023-0	29-20 11:03				(11811)Escape attempt detected in privileged container		
\$	O Leg 2023-0	09-2011:00				(T1810)Leunch Privileged Container		
	O Log 2023-0	09-20 11:00				(T1010)Launch Privlieged Container		
0	· Log 2023-0	29-2011:00				New executable created (open+create)		
	· 161 2023-0	29-201100				New executable created (chmod)		
	0 [64] 2023-0	99-2011:00				New executable created (chmod)		
-	C LOI 2023-0	09-2010-59				(T1554)Create Hidden Files or Directories		
\propto	C Leg 2023-0	29-2010-58	Starbase_backand		starbaset	(T1543)Launch Package Management Process in Container		
103	C [Terriner] 2023-0	09-20 10-58	Starbase_backend		starbase1	(T1496)Detect crypto miners using the Stratum protocol		
÷	O [L0] 2023-0	99-2010.57	Starbase_backend			New esecutable created (chmod)		
	Thi	ne: 2023-09-3	20 10:58	Container Name:	ny-shel			
	Acti	kon: () [Terni		Container ID:	fecb053b207a645bd00cc3a4ed4e3c2ee2f6b89e0f36ee6e6880cc50bb0509cee			
	Rule Nat	me: (T1496)De	etect crypto miners using the Stratum protocol	Image Name:	docker.iq/librarglubuntu			
	Clust	ter: starbase1		Image Tag:	latest			
	Pal	ity: Starbase	backend particula	Insage Digest: Event Number	sha295.aabed3295a3.64bcede1dc895a24476c4d7e003aa899283c275daadbdce3c1054 7772108			
	Device/Network Addre	155		Event Category:	process			
		ID: 72cb45cb	-46c6-4st3-s01b-s38f7M2ee62	Process ID:	20442			
	Pod Nar	ne: my-shell			curl -X POST -F usernamentvend stratum-top://tratum.fakepool/rend.trend:3333			
	Pod Lab	els: narcmy-sh	wi .	Executable:	cul			
	натозра	ion: desuit		Process Arguments: Process Name	 A POST - P Userhamelinend telecimi-scp.//eneumclakepooleenstrenst.co.s.s 			
				Parent Process:				
				Parent Process Name:	bash			
				Hee NUTROET:				
-								
12								
>>								

Container vulnerability view

Network Network Network Network Network Network Network Network Network Network Network Network Network Network Network Network Network Network Network Network Network Network Network Network Network Network Network Network Network Network Network Network Network Network Network	Note: N	_												
		Trend Vision	Trend Vision One ^{Tw} Consister Insteadure											
Notable	Note: <th>0 Important: The</th> <th colspan="10">Important: The "Invited" sense of the pre-release feature ends on 2022-02-28 03000.00 at which point this become a paid feature, Vew details</th>	0 Important: The	Important: The "Invited" sense of the pre-release feature ends on 2022-02-28 03000.00 at which point this become a paid feature, Vew details											
<form> Note: Note</form>			Puldes Nakars Nakardillika Evens ArtiketSerrer											
		Filter Dy: None	Filter Day Marco V Scientify Marco V 0											
image image option image option image option image option	IntIntIntIntIntIntIntIntCC 2000 COCC 20	Rubernetes LCS												
one of seven to the seven t	non-second non-second<		Severity	+ Image	Cluster		Package Name	Package Version	Fix Available					
<table-container>NoteN</table-container>	of off off off off off off off off off	CVE-2018-25009	Critical	/ vulnerables/web-dvwa			lovetpi		• 0.5.2-1+deb0u1					
<table-container> Origination • Or</table-container>	<table-container> Order order</table-container>	CVE-2017-0923	Critical	/ vulnerables/web-dvwa	starbase1		Ibapache2-mod-php7.0	7.0.30-0+deb9u1	N/K					
0 for 0 0 for 0 0 mandem (mathem (m	Of Dig NGOf Other Marked	CVE-2019-11039	Critical	i vuherables/web-dvwa				7.0.30-0+deb9u1	• 70.33- 0+det905					
<table-container> Origination • Or</table-container>	<table-container>On SeriesOne of the seriesAnd the</table-container>		Critical	/ vulnerables/web-dvwa			php7.0-gd	7.0.30-0+deb9u1						
6 for 3 min9 for 3 m	n f and marked mark	CVE-2018-18314	Critical	i vuherables/web-dvwa			peri-base	5.24.1-3+deb9u4	\$.24.1- 3+deb9u5					
Off 50%off magnetingoff magneti	On 2013In OrdValue (Markel Am)Value (Markel Am)	CVE-2019-18218	Critical	i vuherables/web-dvwa			php7.0-common	7.0.30-0+deb8u1	70.33- 0+deb9u/11					
Original SectorOriginal Sect	On the field of the second	CVE-2019-10082	Critical	 vulnerables/web-driva 			apache2-data	2.4.25-3+665945	2.4.25- 3+deb0x8					
60.59 9.000 waxaayoo daya 1001 9.000 10.300<	Of Dig Reg 0 Or Di	CVE-2018-18312	Critical	 vulnerables/web-dvwa 			Ibperi5.24	5.24.1-3+deb9u4	5241- 3+deb8u5					
GADE STRAIN 0.00000000000000000000000000000000000	Child State Notice Notice Notice Notice Notice Child State State State State State State Child State State State State State State <t< td=""><td>CVE-2010-25013</td><td>Oritical</td><td>/ vulnerables/web-dvwa</td><td></td><td></td><td>lbwebpű</td><td></td><td> 0.5.2-1+deb9u1 </td></t<>	CVE-2010-25013	Oritical	/ vulnerables/web-dvwa			lbwebpű		 0.5.2-1+deb9u1 					
Point	Open Series Note of the Series of the Seri	CVE-2019-11036	Critical	i vulnerables/web-dvwa			php7.0-mysql	7.0.30-0+deb9k/1	70.33- 0+deb8u5					
Second	Are are brack to brack to achieve that is a brack to br	CVE-2018-18312	Critical	/ vulnerables/web-dvwa				5.24.1-3+deb9u4	5.24.1- 3+det04.0					
이대 이	Off.2003/Decomposition Parkage Writism 82-3 Tandam	Description: A faw was found in I Vulnerability Info	llowebp in versions before 1.0.1. An out-of-bounds read	was found in function WebPMuxCreateInternal. Th	e Nghest threat from this vulnerability is to data confident	iality and to the service availabilit								
source number number<	investige 6 chical					Package Version	0.5.2-1							
Registrice Registrit Registrit Registrit	Ansage Manage					Fix Available	 0.5.2-1+deb9u1 							
Integrational Control	Name Name <th< td=""><td></td><td colspan="2">iamo ibwetpi</td><td></td><td></td><td></td><td></td><td></td></th<>		iamo ibwetpi											
Image Benefity Benefity <t< td=""><td>Imp of one Andersee Andersee Andersee Andersee A</td><td>Image Informatio</td><td colspan="11">Image Information:</td></t<>	Imp of one Andersee Andersee Andersee Andersee A	Image Informatio	Image Information:											
Name None Optimization And additional distribution distrease distrease distribution distrease distribution distribution	https:// doe/d page and an 2019 of addation of addatio addatio addation of addation of addatio addation of addation o		828 docker.lo/vulnerables/web-dvwel/shu256.dae203fe11646a86937e104db0027ader295H26da68a92b40e3b1811337daa7				vulnerables/web-dvwa							
Synt what was the activity set was activi	Open Australization Australizatio Australization Australization Australization Austral		docker.io											
Detection Control Names to the Names of Names	Detection Numerical National Statement Stateme	Ogen wulde de CONTRECENTES DE												
Cather Round Name Round Name Name Name Name Name Name Name Name	Container Nacera Symp Namespan Part Stretering Ann Ann Pal Adval 12754-25 1073	Detection Inform	ation:											
dem dem Pol defail 2024-631122	ene den Pol deux IES-68/8122							Namespace						
					Pod			default	2023-09-26 11:23					

Proven Leadership

- A Leader in the Forrester New <u>Wave™</u>: Extended Detection and Response, Q4 2021
- Ranked #1 for Cloud Workload Security Market Share for the 6th consecutive year (2023)
- <u>MITRE Engenuity ATT&CK (2023)</u> #1 in the protection category, with 100% detection of all critical attack steps.

Key Advantages

Address security issues before they can be exploited in production

Container Security provides image scanning to detect threats present in directly installed apps and apps that were installed via a package manager. Fix issues fast with actionable insights, enabling developers to remediate issues before deployment via their existing tools and workflows.

Ensure ongoing container security

Policy-based deployment control, through a native integration, ensures the Kubernetes deployments you run in your production environment are safe.

Container Security enables you to create policies that allow or block deployments based on a set rules that include pod and container security properties and the results of container image and registry scans. When an image is ready to be deployed with Kubernetes, the admission control webhook is triggered, which checks whether the image is safe to deploy and either allows or blocks it from running.

Protection with full visibility, detection, and response

Once deployed, protect containers with runtime protection for additional assurance. Discover and block suspicious activity, get visibility of vulnerable running containers and container drift, and detect, track, and investigate crosslayer threats or activities with XDR.

Learn more about host-based security. Visit the <u>Trend Vision One™ - Workload</u> <u>Security</u> webpage



Container Security capabilities

1. Continuous and automated container image scanning

What we look for:

Container Security generates and scans a software bill of materials based on the container image. This allows you to ensure issues are fixed early and filter out false positives by correlating patch layers with packages that are vulnerable in the same image. Container Security will scan images for:

- Malware detection
- Vulnerability assessment
- Policy compliance

Scan images in your CI/CD build pipeline, ensuring your images are secured from the first build and remain protected from future unknown threats.

2. Container admissions control policy

Using native Kubernetes integration, Container Security can define policies that ensure that only compliant containers run in production environments. Container Security admission control policies allow you to:

- Build policies based on container image scanning and detection
- Only allow images that meet specific application or organization security policies to run in Kubernetes
- Define advanced policies-such as disallowing images set as privileged containers-or allow exceptions based on names or tags

3. Container runtime protection

Runtime protection ensures containers running in your environment continue to be protected even after they've been deployed, giving you:

- Kubernetes cluster inventory
- Visibility of vulnerable running containers
- Protection from attempts to run disallowed commands, illegally access files, container drift, and other suspicious activity
- Context to detect, track, and investigate cross-layer threats or activities with XDR

System requirements:

- Kubernetes 1.14.0 or greater on a Kubernetes Certified platform (or equivalent).
- Helm 3.0.1 or greater

For more information visit trendmicro.com/container_security

Deployment and Integration

Container Security provides a valuable step in your CI/CD pipeline.

To perform policy-based deployment control, create a Kubernetes cluster (or open your existing Kubernetes cluster) and install the policy-based deployment controller. Next, create a policy that Container Security will enforce for the cluster. Finally, test the policy.

Visit the Trend Vision One - Container

<u>Security Documentation</u> page for more information on how to get started, use cases, and more.

For more information, please visit trendmicro.com

©2023 by Trend Micro Incorporated. All rights reserved. Trend Micro, the Trend Micro t-ball logo and Trend Vision One are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice. [DS05_Vision_One_Container_Datasheet_231011US]

For details about what personal information we collect and why, please see our Privacy Notice on our website at: trendmicro.com/privacy