Kubernetes security: Best practices for enterprise deployment

Thomas, Brian E . CIO ; Framingham (Jul 29, 2019).

ProQuest document link

ABSTRACT (ENGLISH)

[...]these types of deployments are just as susceptible to exploits and attacks from attackers and insiders as the traditional environments. [...]it is more important to ensure your large-scale Kubernetes environment has the right deployment architecture and that you use security best practices for all these deployments. Critical items to look at when considering cluster security are: * Exploitation in the attack surface due to the various vulnerabilities in each container, especially when using container orchestrations means like Docker and Kubernetes. * Increased east-west traffic that needs to be monitored, especially across host and cloud environments. * The security team's ability to ensure that security automation is keeping up with an ever-changing container environment. * Visibility into the deployment process and the Kubernetes pods themselves, including how they are cross-communicating. * Means for malicious behavior detection in the east-west communication between containers, including detecting exploits within a single pod or container. * The use of best access security practices, review/planning and documentation of the Kubernetes clusters in order to better understand internal threats. [...]your Kubernetes environment needs to properly deploy segmentation for network connections and certain containers.

FULL TEXT

Several years later and containers are still the hype for application deployment and migration. CIO Online contributor Paul Rubens broke it down into digestible chunks –explaining benefits, gotchas, container management systems, security and much more. So now that we have figured out more reliable and efficient ways to deploy and scale software across platforms, it has also provided ways for nefarious actors to exploit these containers.

In the last couple of years, while there have been some great improvements around security with containers and their orchestration systems such as Kubernetes, there have been several major vulnerabilities and exploits discovered.

It's impressive that container implementation and management tools like Kubernetes allow businesses to automate just about every aspect of application deployment, delivering amazing business benefits. On the flip side, as teams have become more interested in deploying Kubernetes, so have attackers become more interested in compromising Kubernetes clusters.

[Learn how free tools can support your cybersecurity efforts. | Sign up for CIO newsletters.]

One thing that is widely agreed upon by the security pros –as Kubernetes adoption and deployment grows, so will the security risks. There have been multiple recent events in the cloud and mobile dev spaces where these environments were compromised by attackers. This included everything from disruption, crypto mining, ransomware, and data stealing.

Of course, these types of deployments are just as susceptible to exploits and attacks from attackers and insiders as the traditional environments. Thus, it is more important to ensure your large-scale Kubernetes environment has the right deployment architecture and that you use security best practices for all these deployments.

As Kubernetes is more widely adopted, it becomes a prime target for threat actors. "The rapid rise in adoption of Kubernetes is likely to uncover gaps that previously went unnoticed on the one hand, and on the other hand gain more attention from bad actors due to a higher profile," says Amir Jerbi, CTO at Aqua Security.

There have been critical and notable vulnerabilities discovered since 2015 that have made Security and DevOps think twice about their planning and deployment architecture. Some of the more serious flaws allow full administrator access on any node running in a Kubernetes cluster, which would allow hackers to inject malicious code, bring down the entire cluster environment or steal sensitive data.

Cluster security

When it comes to cluster security, there are several things to consider. The dynamic make-up of containers creates security challenges in the Kubernetes environments. Critical items to look at when considering cluster security are:

* Exploitation in the attack surface due to the various vulnerabilities in each container, especially when using container orchestrations means like Docker and Kubernetes.

* Increased east-west traffic that needs to be monitored, especially across host and cloud environments.

* The security team's ability to ensure that security automation is keeping up with an ever-changing container environment.

* Visibility into the deployment process and the Kubernetes pods themselves, including how they are cross-communicating.

* Means for malicious behavior detection in the east-west communication between containers, including detecting exploits within a single pod or container.

* The use of best access security practices, review/planning and documentation of the Kubernetes clusters in order to better understand internal threats.

It's also very important that the security process is streamlined so it doesn't slow or hinder the App/Dev teams. One thing to consider for containerized deployments across the enterprise and beyond is the need to ensure that the security process for approvals time is reduced. Additionally, your security alert process must be simplified and be able to easily identify the most important attacks. Lastly, your Kubernetes environment needs to properly deploy segmentation for network connections and certain containers.

Enterprise Kubernetes security risks

As mentioned, the rise in the popularity of these tools is accompanied by an increased risk of exploitation by attackers. Risk tolerance for some vulnerabilities varies according to size, level of complexity and environment. However, key security risks to be aware of include the following:

* Attacks in Kubernetes environments can be instigated by an outsider or an insider –knowingly or not (commonly by phishing attacks).

* Containers may be compromised when an app vulnerability or misconfiguration is overlooked, thereby allowing a threat actor to get in and start looking to further access and larger disruption.

* Pod connections that are unauthorized, again due to compromised containers, try to access other pods on other or the same hosts. The type of network monitoring and filtering needs to be Layer 7 in order to detect and thwart attacks on trusted IP addresses.

* Data theft, also known as "exfiltration", in your environment. There are many ways this type of attack is deployed and hidden via network tunneling to hide the exfiltration.

* Exploiting the Kubernetes infrastructure itself, such as the Kubelets and API server.

* Orchestration tool compromise allows attackers to disrupt applications and get access to other resources needed to run the environment.

Best practices for Kubernetes security

There is an age-old saying that you should do something right or don't do it at all. Sometimes it may not be so obvious, but it is especially important when it comes to better overall security you need to deploy Kubernetes with the right concepts and architecture to start.

Kubernetes capabilities and deployments have become more popular due to the increased capabilities of this orchestration tool –from a simple pod architecture for a small deployment or larger scale Kubernetes integration across platforms. Of course, so has the complexity of these deployments and the security risks surrounding them. Here are some important tips on best Kubernetes deployment practices:

* Least privilege must be enforced. Using this type of model to prevent widespread access enables better containment of an attack if it happens. It's best to use the built-in pod security policy to determine and restrict the pod's ability.

* Strong authentication best practices should always be deployed, and authentication is a must for all Kubernetes modules.

* Cluster segmentation configurations and deployments run in a similar vein to the previously least privilege. It's best to contain an attack or breach to a subset of your cluster. Using virtual clusters that are detached from each other in the same infrastructure environment is best practice.

* Utilizing a firewall that is native to the container helps block activity across the network when using segmentation.

* Environment monitoring for incidents that may occur despite your implementation of best security practices. There are specific third-party security tools that prevent the spread of attacks and identify policy violations in your environment.

* Define the roles between operational, development and security teams. Duty segregation is a best practice and should be documented with clear roles and responsibilities.

Items to consider

Whatever size your project and environment are, whether it be a single internal pod for a particular platform migration or a large cloud deployment with many clusters, it's important that your DevOps and security teams work collaboratively in the planning process. This includes identifying the proper roles and responsibilities and having regular communications between all teams. Simply put, a well-laid plan, with all the stakeholders involved upfront, is the first step in building a more secure container environment.

DETAILS

Subject:	Visibility; Internet crime; Containers; Segmentation; Security; Security management; Exploitation; Communication; Best practice; Automation; Planning
Business indexing term:	Subject: Best practice Automation
Publication title:	CIO; Framingham
Publication year:	2019
Publication date:	Jul 29, 2019
Publisher:	Foundry
Place of publication:	Framingham
Country of publication:	United States, Framingham
Publication subject:	Business And Economics--Computer Applications
ISSN:	08949301
Source type:	Trade Journal

Language of publication:	English
Document type:	News
ProQuest document ID:	2266190441
Document URL:	https://www.proquest.com/trade-journals/kubernetes-security-best-practices-enterprise/docview/2266190441/se-2?accountid=17215
Copyright:	Copyright CXO Media, Inc. Jul 29, 2019
Last updated:	2022-10-24
Database:	ProQuest Central

LINKS

Available at KU Leuven?