the **GORILLA GUIDE®** to...

Ransomware in Kubernetes

Foundation Edition

DAN SULLIVAN

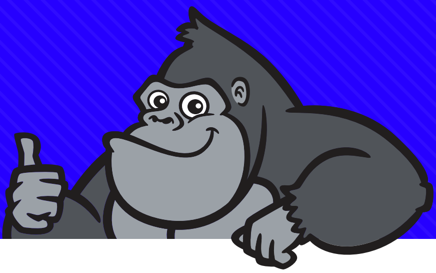
INSIDE THE GUIDE:

- Common Attack Vectors and the Impact of Ransomware on Kubernetes
- Best Practices: Patch Management, Network Segmentation, and Backups
- Leveraging Kasten K10 to Recover from Ransomware Attacks

KASTEN by Veeam

POWERED BY ActualTech MEDIA

the GORILLA GUIDE® to...



Ransomware in Kubernetes

By Dan Sullivan

POWERED BY ActualTech MEDIA

Full 7th Floor
130 West 42nd Street
New York, NY 10036

www.actualtechmedia.com

PUBLISHER'S ACKNOWLEDGEMENTS

DIRECTOR OF CONTENT DELIVERY

Wendy Hernandez

CREATIVE DIRECTOR

Olivia Thomson

SENIOR DIRECTOR OF CONTENT

Katie Mohr

WITH SPECIAL CONTRIBUTIONS FROM KASTEN BY VEEAM®

Mike Carcerano
PRINCIPAL PRODUCT MANAGER

Thomas Keenan
SR. PRODUCT MARKETING MANAGER

Tom Leyden
VP OF MARKETING

ABOUT THE AUTHOR

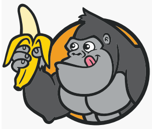
Dan Sullivan is an architect specializing in cloud architecture, data engineering, and analytics. He has designed and implemented solutions for a wide range of industries and is the author of multiple books and online courses.

ENTERING THE JUNGLE

CALLOUTS USED IN THIS BOOK

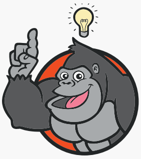
SCHOOL HOUSE

In this callout, you'll gain insight into topics that may be outside the main subject but are still important.



FOOD FOR THOUGHT

This is a special place where you can learn a bit more about ancillary topics presented in the book.



BRIGHT IDEA

When we have a great thought, we express them through a series of grunts in the Bright Idea section.

DEEP DIVE

Takes you into the deep, dark depths of a particular topic.

EXECUTIVE CORNER

Discusses items of strategic interest to business leaders.

DEFINITION

Defines a word, phrase, or concept.

GPS

We'll help you navigate your knowledge to the right place.

KNOWLEDGE CHECK

Tests your knowledge of what you've read.

WATCH OUT!

Make sure you read this so you don't make a critical error!

PAY ATTENTION

We want to make sure you see this!

TIP

A helpful piece of advice based on what you've read.

Introduction

Cyberattacks are so pervasive now that enterprises should assume they will become a victim of one at some point. That is not fear mongering; it's simply a reflection of the environment enterprises operate in. Of the organizations surveyed for the Veeam 2023 Data Protection Trends Report, 85% said they experienced a cyberattack in the prior 12 months. These attacks are not limited to legacy systems, either. Increasingly, Kubernetes is a target for malware attacks, including ransomware attacks.

Fortunately, tools and practices are available that can significantly reduce the adverse impact of ransomware attacks. In this guide, we review the threat of ransomware in Kubernetes, common attack vectors used to deploy malware and the impact of ransomware on Kubernetes clusters. Next, we present several best practices for preventing ransomware attacks, as well as recovering from ransomware attacks, when they occur. This guide also provides advice on how to implement a robust backup strategy, which is essential for protecting your organization from ransomware attacks.

Ransomware in Kubernetes

Ransomware is malicious software that encrypts data on compromised systems, making the data inaccessible and unusable until victims pay a ransom to attackers. According to Veeam's 2023 Ransomware Trends Report, although 80% of victims paid ransom, as many as 25% of those who did were not able to recover their data. Only 16% were able to recover data without paying a ransom, and they did so by using immutable backups, separate accounts for backups, or both.

Many ransomware attacks target Windows servers, but the idea that ransomware is only a problem for Windows platforms is a mistake. Red Hat's State of Kubernetes Security Report 2023 reports that 40% of respondents are most concerned about ransomware attacks, and 53% of them had experienced ransomware attacks in the prior 12 months.

In addition to misconfigurations, attackers can exploit secret leakage, overly permissive access controls, and vulnerabilities in the application stack.

Kubernetes is a widely used platform for container orchestration, and its popularity makes it a logical target for cybercriminals. However, for attackers to successfully compromise a Kubernetes cluster, they first need to find a vulnerability to exploit. Doing so may be easier than we would like to believe—CSO cites a study of Kubernetes clusters belonging to over 350 organizations where two common misconfigurations were identified: anonymous users granted privileges and misconfiguration of the kubectl proxy with flags that expose the Kubernetes cluster to the Internet.

In addition to misconfigurations, attackers can exploit secret leakage, overly permissive access controls, and vulnerabilities in the application stack.

The combination of up to 80% of victims paying ransoms, the increasing adoption of Kubernetes by enterprises, and the difficulty of keeping Kubernetes clusters secure has created a compelling opportunity for cybercriminals to expand the threat of ransomware attacks to Kubernetes platforms.

Understanding Ransomware in Kubernetes

Managing the risk of ransomware attacks in Kubernetes requires understanding both common attack vectors and the impact of ransomware attacks on Kubernetes clusters.

COMMON ATTACK VECTORS

The four most common attack vectors are supply chain attacks, vulnerability exploitation, misconfigurations, and credential theft.

Supply Chain Attacks

Supply chain attacks target software providers to gain access to systems belonging to the customers of those providers. Supply chain attacks often begin as advanced persistent threats against vendors. SolarWinds, for example, experienced a supply chain attack in 2020 when attackers were able to deliver malware across SolarWinds Orion network management system, which was used by over 30,000 organizations. The SolarWinds incident demonstrates how effective supply chain attacks can be for delivering malicious payloads to a large number of targets.

> **Regardless of how attackers exploit a cluster—whether by using supply chain attacks, vulnerabilities, misconfigurations, credential theft, or some combination—the impact of ransomware on Kubernetes clusters is substantial.**

Vulnerability Exploitation

In addition to compromising a software product used by a target organization, attackers can also exploit both known and zero-day vulnerabilities in the Kubernetes platform or application stack.

Like any other complex software, Kubernetes harbors vulnerabilities. For example, a known vulnerability discovered in 2019 allowed attackers with access to system logs to access bearer tokens captured during high verbosity logging. Due to a more recently discovered vulnerability, users could gain access to secure endpoints in the control plane if untrusted users were allowed to modify Node objects. As both examples demonstrate, a vulnerability by itself may not be exploitable unless some specific condition, such as a misconfiguration, is also in place.

Be sure to check out the official CVE feed for Kubernetes.

Misconfigurations

Misconfigurations are especially problematic because they can occur in a variety of ways. For example, creating a cluster with default configurations may be the fastest way to stand up a cluster, but the default configuration may not meet the security requirements of your use case.

Kubernetes configurations may change frequently. In some cases, a simple change, like modifying the number of CPUs available for a pod, is not likely to introduce vulnerabilities. However, changes to network configurations or role-based access controls should be carefully reviewed before they are deployed. Using Continuous Integration/Continuous Deployment (CI/CD) pipelines and policies that require a review of configuration changes is a good practice for reducing the risk of misconfigurations.

Still, there may be times when Kubernetes administrators must make on-the-fly changes to a resource configuration. For example, if a critical service is down and changes need to be made to a deployment, an administrator may need to change a configuration in the cluster manually. While resolving an issue with a critical service is the top concern in such situations, we should be careful to review any emergency changes and implement them using standard procedures as soon as possible—for example, updating the version-controlled copy of the configuration file.

Credential Theft

Weak and shared credentials are another attack vector that can be used to compromise a Kubernetes cluster. Well-established best practices for reducing the risk of credential theft include storing usernames, passwords, and keys in password managers. Care should also be taken with kube-config files that contain keys allowing for administrative access to Kubernetes clusters.

> **As with any complicated system, competing interests must be balanced with business objectives.**

Secrets vaults should be used to store credentials and other secrets needed by service accounts. Developers sometimes define environment variables when creating containers to store usernames and passwords needed by services. While this may seem like a reasonable approach when the container is sufficiently isolated and only accessible by trusted components, security depends on other controls being in place. A misconfigured firewall rule that allows unwanted traffic could suddenly allow an attacker to reach a container and access environment variables. Logging services that include environment variables in log messages are another way for secrets kept in environment variables to leak outside of the container.

IMPACT OF RANSOMWARE IN KUBERNETES CLUSTERS

Regardless of how attackers exploit a cluster—whether by using supply chain attacks, vulnerabilities, misconfigurations, credential theft, or some combination—the impact of ransomware on Kubernetes clusters is substantial. Surveying the damage of ransomware on an organization leads to at least three significant types of impacts, including encrypted data held hostage, downtime and business disruption, and reputational damage.

Encrypted Data Held Hostage

The most obvious impact of a successful ransomware attack is that data is encrypted and effectively inaccessible. Strong encryption is practically impossible to crack without a decryption key. This is an advantage when an organization wants to protect the confidentiality of messages and data, but can be used against the organization in the case of ransomware.

An alternative to decrypting data is recovering from a copy of the data. Backups are the obvious candidate for this and are commonly employed. A potential problem with recovering from backups is that they, too, can be encrypted. Imagine an attacker has gained access to the cloud account you use for your Kubernetes clusters. If backups are stored in object storage under the same account, then they can also be encrypted by the attacker.

Downtime and Business Disruption

If data and applications are encrypted, the applications will not function, which can severely hamper business services. If a ransomware attack is limited to back-office services, it may take longer for the full impact to be noticed outside the organization; however, as most enterprises have engaged in digital transformation to improve customer-facing applications and services, the impact to customers and business partners will be immediate.

Reputational Damage

Another impact that follows from business disruption is reputational damage. Word spreads quickly about companies that become victims of cybercrime. In 2013, the retailer Target suffered a data breach in which attackers stole information on more than 40 million payment cards. In the next quarter, Target's earnings were down 43%.

Even when disruptions are less obvious, regulation and reporting requirements may require companies to disclose substantial breaches such as ransomware attacks.

Unfortunately, the reputational damage that results from a ransomware attack can take longer to undo than the time it takes to restore your data.

Best Practices for Ransomware Prevention and Response

Best practices for avoiding a successful ransomware attack combine preventive measures with recovery mechanisms. The prevention measures are designed to reduce the chances of an attacker exploiting a vulnerability to deploy malware into your Kubernetes environment. Assuming preventive measures are enough for addressing the risks from ransomware is wishful thinking—recovery procedures must be put in place, as well.

REGULAR SOFTWARE UPDATES AND PATCH MANAGEMENT

Keeping software up to date is an effective way to reduce exposure to known vulnerabilities. The software industry and security professionals have created widely used databases for tracking known vulnerabilities, such as Mitre's CVE and the National Vulnerability Database from the U.S. National Institute of Standards and

Technology (NIST). When a vulnerability is discovered, information about the vulnerability, the level of risk associated with it and mitigation steps are widely shared through these databases.

Software developers routinely release new features, bug fixes, and patches to correct vulnerabilities. Automation tools can be used in deployment pipelines to scan images for known vulnerabilities before deploying them to a cluster.

As with any complicated system, competing interests must be balanced with business objectives. For example, a known vulnerability may require an upgrade that also breaks a production service. It's important to weigh the impact of modifying the production service to work with the upgrade versus eliminating the vulnerability. Ideally, following established practices for prioritizing patches and updates can help determine how to balance the risk of a vulnerability with the cost of applying patches.

NETWORK SEGMENTATION AND ISOLATION

Isolating resources in Kubernetes is an effective way to limit the scope of damage when a system is compromised. By default, Kubernetes networks allow workloads to communicate with each other. This is probably more permissive than needed for most Kubernetes clusters running production workloads.

In a microservices architecture, services tend to communicate with a relatively small set of other services. For example, a user interface service may collect data from users and send it to a database proxy, which verifies the sender and applies application firewall rules—checks for SQL injection and the like—before sending the data on to the database service. This kind of constrained communication pattern is common, so there's often no need for services to communicate with all the other services.

In Kubernetes, you can implement network segmentation at multiple levels, including pods, namespaces, and labels (see **FIGURE 1**). By segmenting network traffic to allow communication only between services that must send data to each other, you can limit the scope of damage in the event a service in a cluster is compromised. Network policies in Kubernetes can be used to limit pod communications to only specific assets, as well. Additional services, such as service meshes like Istio, offer other ways to segment traffic. Container Network Interface (CNI) plugins, such as Project Calico, can provide additional network segmentation and security features.

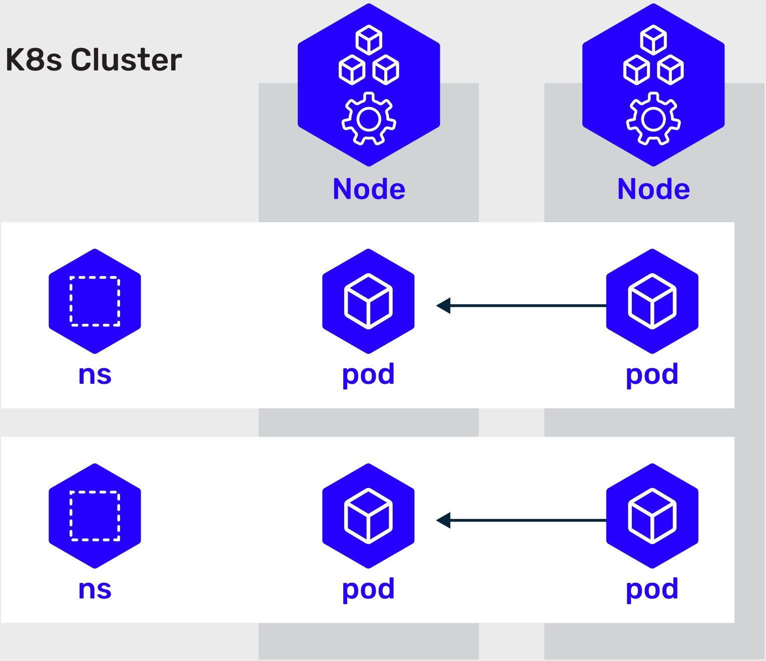
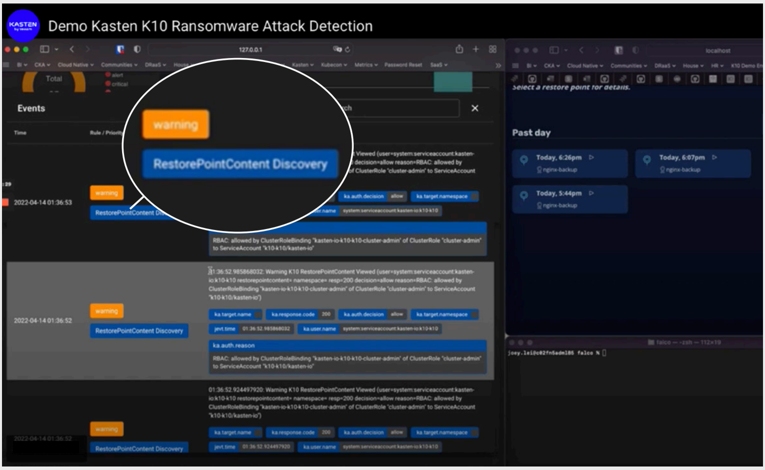


FIGURE 1: Kubernetes can segment networking at multiple levels. In this diagram, network communications are restricted to within namespaces

MONITORING AND ANOMALY DETECTION

Observability tools for monitoring, collecting, and analyzing metrics and logs can help to detect suspicious and unwanted behavior in a Kubernetes cluster. Unusual traffic patterns on assets, such as network traffic between pods that don't normally communicate, can be a sign of malicious activity (see **FIGURE 2**).

For example, an attacker may be able to use Secure Shell to access a container that has a database command-line utility that was unintentionally included in the container image. From there, the attacker can use the command-line utility to probe databases on another pod. Repeated patterns of activity, such as entering at one point and probing multiple other endpoints in the system, may also indicate an attempted attack.



Select a restore point for details.

```
2022-04-14 01:36:53  warning  RestorePointContent Discovery
... Viewed (user=system:serviceaccount:kasten-
... decision=allow reason=RBAC: allowed by
... of ClusterRole "cluster-admin" to ServiceAccount
ka.auth.decision allow   ka.target.namespace
ka.user.name system:serviceaccount:kasten-io:k10-k10
RBAC: allowed by ClusterRoleBinding "kasten-io-k10-k10-cluster-admin" of ClusterRole "cluster-admin"
to ServiceAccount "k10-k10/kasten-io"

2022-04-14 01:36:52  warning  RestorePointContent Discovery
01:36:52.985868032: Warning K10 RestorePointContent Viewed (user=system:serviceaccount:kasten-
io:k10-k10 restorepointcontent= namespace= resp=200 decision=allow reason=RBAC: allowed by
ClusterRoleBinding "kasten-io-k10-k10-cluster-admin" of ClusterRole "cluster-admin" to ServiceAccount
"k10-k10/kasten-io")
ka.target.name   ka.response.code 200   ka.auth.decision allow   ka.target.namespace
jevt.time 01:36:52.985868032   ka.user.name system:serviceaccount:kasten-io:k10-k10
ka.auth.reason
RBAC: allowed by ClusterRoleBinding "kasten-io-k10-k10-cluster-admin" of ClusterRole "cluster-admin"
to ServiceAccount "k10-k10/kasten-io"

2022-04-14 01:36:52  warning  RestorePointContent Discovery
01:36:52.924497920: Warning K10 RestorePointContent Viewed (user=system:serviceaccount:kasten-
io:k10-k10 restorepointcontent= namespace= resp=200 decision=allow reason=RBAC: allowed by
ClusterRoleBinding "kasten-io-k10-k10-cluster-admin" of ClusterRole "cluster-admin" to ServiceAccount
"k10-k10/kasten-io")
ka.target.name   ka.response.code 200   ka.auth.decision allow   ka.target.namespace
jevt.time 01:36:52.924497920   ka.user.name system:serviceaccount:kasten-io:k10-k10
```

```
joey.lei@c02fn5adml85 falco % 
```

FIGURE 2: Observability tools and alerts help to detect suspicious activity within a cluster

Monitoring changes in roles and permissions granted to users and service accounts is a best practice, as is following the Principle of Least Privilege and granting only the minimal set of permissions needed by users or service accounts to perform the functions for which they are responsible.

☑ **Assess any anomalous network traffic** or unusual access control configurations as possible malicious activity.

INCIDENT RESPONSE PLAN AND TRAINING

Preventive measures and monitoring help to limit the amount of damage done to a system, but should not be the sole means of protection. Incident response planning and training is another Kubernetes security best practice. This involves deciding when to declare that an incident needs a specialized response, identifying whom to communicate with about the incident and whom to enlist in the response effort, and what actions to take to mitigate the impact of a malicious act.

> **Isolating resources in Kubernetes is an effective way to limit the scope of damage when a system is compromised.**

Following these best practices requires implementing the right tools, and some of the most important tools for managing ransomware risk are data management tools, such as Kasten K10 by Veeam.

Securing Kubernetes with Kasten K10

Kasten K10 is a cloud native data management platform designed for protecting Kubernetes applications and their data. It is also the first cloud native backup and recovery ransomware protection solution. Developed for DevOps teams, Kasten K10 enables engineers to implement backup, disaster recovery, and application mobility operations with ease.

Kasten K10 discovers applications and related artifacts in a Kubernetes environment and implements policies to manage data according to your specific requirements. It also works across storage platforms and clusters while providing observability into the state of your data management operations.

> **Following these best practices requires implementing the right tools, and some of the most important tools for managing ransomware risk are data management tools, such as Kasten K10 by Veeam.**

Kasten K10 is designed for cloud native architectures that build applications using microservices. These microservices are distinct components of an application and protecting an application requires us to protect each component and orchestrate protection across components. Kasten K10 is designed to support common deployment patterns in Kubernetes. It is also customizable to support more complex backup and restore operations.

There are three parts to protecting Kubernetes from a ransomware attack: providing early threat detection, having encrypted and immutable backups, and enabling accelerated recovery. Early threat detection requires raising an early flag on potential malicious activity or imminent attacks. Next, it is important to always have a safe and consistent copy of your application and data. Finally, you need to quickly and securely restore to avoid business downtime. Kasten K10 is a key component in implementing this strategy effectively.

Reduce the Risks

Ransomware is a threat to Kubernetes users. The complexity of deploying, configuring, and managing Kubernetes clusters can lead to vulnerabilities that ransomware attackers can exploit. In addition to configuration vulnerabilities, there are potential risks from supply chain attacks and software vulnerabilities.

One way to reduce the risk of an attack is to understand how Kubernetes works. KubeCampus.io by Kasten is a free resource for learning all aspects of Kubernetes, including security, networking, application management and troubleshooting.

> **Developed for DevOps teams, Kasten K10 enables engineers to implement backup, disaster recovery, and application mobility operations with ease.**

As you build your knowledge of Kubernetes security and data management, the benefits of Kasten K10 will become more apparent. Ransomware defense demands a proactive approach, and Kasten provides both immutable backups and automatic, policy-driven creation of those backups.

In addition, we can incorporate other tools to prevent misconfiguration of policies, such as Kyverno. By employing Kubernetes native policy management tools, developers are able to deploy resources and applications while mitigating the risk of introducing a misconfigured policy. Kasten K10 also integrates with Amazon GuardDuty and Red Hat Advanced Cluster Security for early threat detection by monitoring and correlating of events across the application platform.

Although it’s not always possible to predict or prevent ransomware attacks, implementing a comprehensive set of defensive controls will help to block them. Creating an incident response plan and automated backups will help you to recover in the event of a worst-case ransomware scenario.

ABOUT KASTEN BY VEEAM®

Kasten by Veeam® is the leader in Kubernetes backup. Kasten K10 is a Cloud Native data management platform for Day 2 operations. It provides enterprise DevOps teams with backup/restore, disaster recovery and application mobility for Kubernetes applications. Kasten K10 features operational simplicity and integrates with relational and NoSQL databases, all major Kubernetes distributions, and runs in any cloud to maximize freedom of choice. Our customers are confident that their Kubernetes applications and data are protected and always available with the most easy-to-use, reliable, and powerful Cloud Native data management platform in the industry. For more information, visit www.kasten.io or follow @kastenhq on Twitter.

ABOUT ACTUALTECH MEDIA

ActualTech Media, a Future company, is a B2B tech marketing company that connects enterprise IT vendors with IT buyers through innovative lead generation programs and compelling custom content services.

ActualTech Media's team speaks to the enterprise IT audience because we've been the enterprise IT audience.

Our leadership team is stacked with former CIOs, IT managers, architects, subject matter experts and marketing professionals that help our clients spend less time explaining what their technology does and more time creating strategies that drive results.

If you're an IT marketer and you'd like your own custom Gorilla Guide® title for your company, please visit actualtechmedia.com.