7 Steps to Avoid Kubernetes Ransomware Disasters

How you can attain resilient application deployments on Kubernetes

Table of Contents

The Rise of Kubernetes Ransomware Attacks 3

Steps to Prepare for Attacks 4

 1. Secure the Cloud Host OS Kernel 4

 2. Control Data Protection System Access Authentication 5

 3. Secure Access Identities with Immutable Storage 6

 4. Confidently Back Up Your Data 7

 5. Energize your Restorations 8

 6. Monitor Kubernetes Deployments and Proactively Detect Anomalies 9

 7. Make Proactive Kubernetes Improvements 10

Veeam Kasten *for Kubernetes* 11

About Veeam Software & Veeam Kasten 12

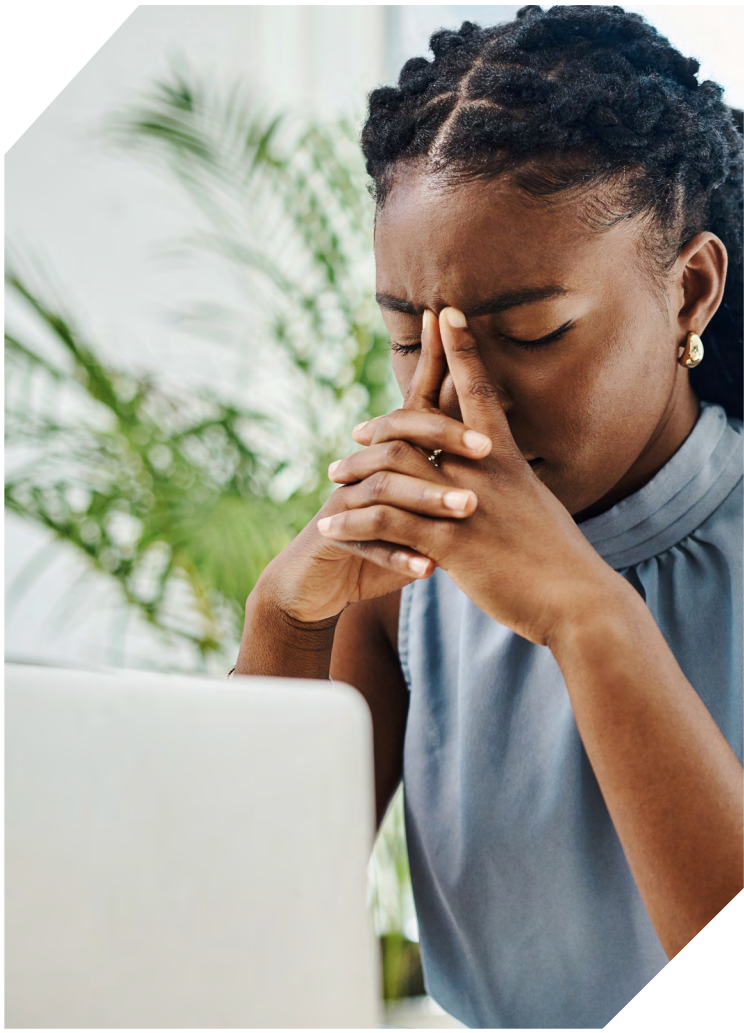
The Rise of Kubernetes Ransomware Attacks

Kubernetes has emerged as the dominant microservices container platform, originating from Google[1] and gaining support from various industry participants. Now in its tenth year of public adoption, Kubernetes still garners skepticism about its security, which has led organizations to question its readiness for widespread adoption. Intensifying these security concerns are ransomware status reports; for example, the Veeam Data Protection Trends Report 2024 confirms that an astounding 75% of companies suffered at least one ransomware attack in the preceding twelve months.

By responding to the current threat landscape, businesses can strengthen the security of their Kubernetes deployments. The following seven protective measures capture how we can fortify our Kubernetes resilience and security, increase uninterrupted operational periods, and safeguard our critical data. Our exploration begins with the fundamental step of securing the cloud host OS kernel, which forms the bedrock of every Kubernetes deployment. With the foundation secured and Veeam Kasten installed, you too will be ready to release the resiliency of Kubernetes. We are going to emphasize the significance that freedom of choice has in safeguarding your Kubernetes applications, and hopefully empower you to make secure choices that drive long-term success. Get ready to fortify your Kubernetes platform and safeguard your critical assets against ransomware threats with these 7 steps!

75%

of companies suffered at least one ransomware attack in the preceding twelve months



Steps to Prepare for Attacks

1. Secure the Cloud Host OS Kernel

A persistent security concern with Kubernetes is that it relies on the underlying host OS kernel. This concerns all of us, since if there is a vulnerability or compromise in the kernel, it can potentially impact all containers that run on that node. This contrasts with virtual machines (VMs), which have independent operating systems built into their architecture, so security issues or compromises in one VM will not directly affect adjacent VMs. The driving force for choosing Kubernetes over VM platforms remains: Kubernetes is an agile development and production platform with maximum cloud foundation flexibility.

Implementing the following measures is a vital step to protecting yourself against ransomware attacks in a Kubernetes environment:

- Regularly patch and update the host OS kernel: Keep your host OS kernel up to date with the latest security patches and updates to mitigate known vulnerabilities and reduce the risk of exploitation.
- Harden host operating systems and nodes: Use hardened host OS images and adhere to best practices for securing your OS and Kubernetes nodes. This includes disabling unnecessary services, removing unused packages, and consistently applying security patches.

When we regularly patch and update the host OS kernel, we also mitigate known vulnerabilities and reduce the risk of exploitation. Hardening the host OS and nodes, including using hardened host OS images like those from Iron Bank and following best practices for securing operating systems can create a more secure environment.

However, if your Kubernetes platform is deployed in a hybrid environment , it is important that the application platform owner ensures their cloud providers maintain same vigilance with the latest security patches to your underlying cloud infrastructure.

- Choose a secure cloud provider: Use cloud providers that prioritize security and provide features that enhance the security of your underlying infrastructure. Look for regular patching and update schedules, as well as current compliance certifications.
- Optionally, choose a managed service provider (MSP): MSPs deliver many services on top of cloud services, including storage, security and other optional managed services.

Addressing the reliance on the host OS kernel is of utmost importance to ensure confidence in the overall security and integrity of your Kubernetes environments. By prioritizing this security concern, organizations, regardless of type or scale, can effectively minimize the risks associated with host cloud vulnerabilities that spill into Kubernetes deployments. This proactive approach ensures that known vulnerabilities do not become an overwhelming concern, thus establishing a robust foundation for the security and integrity of containerized application platforms.

2. Control Data Protection System Access Authentication

Veeam Kasten prioritizes comprehensive and granular protection by offering a variety of secure user access methods for user dashboards and APIs. These methods, including basic and token-based authentication and options for both direct and API access can provide more confidence in our deployments. For example, with Veeam Kasten, users can get a token from an OpenID Connect (OIDC) provider for authentication. Veeam Kasten also supports a refresh token workflow (such as the ones used in SSO) to ensure that once authenticated, user sessions can remain active even after access tokens expire. This implementation eliminates the need for frequent re-authentication, which leads to a smoother user experience.

Security doesn't stop there! To further enhance data security within the storage infrastructure, Veeam Kasten partners incorporate multi-factor authentication (MFA), which adds an extra layer of protection. With your deployment in Azure AKS, you can deploy MFA. This robust authentication mechanism requires users to provide multiple forms of authentication before being granted access to sensitive information or being allowed to make changes. By enforcing MFA, the barrier is raised for unauthorized access attempts, thus making it more challenging for attackers to breach your system. You can start to breathe easier at this point, but you're not done yet.

With authentication established, additional security measures through mechanisms like role-based access control (RBAC) are important and can streamline your security workflow. RBAC ensures that system access is exclusively granted to authorized users based on their assigned roles and privileges. By implementing RBAC, you can ensure security with an out-of-the-box toolset via the principle of least-privilege access. This empowers organizations to assign specific roles and permissions to users and enables fine-grained control over access rights. Collectively, these features offer a comprehensive range of user security protections, effectively reducing the attack surface and mitigating the risk of ransomware attacks.

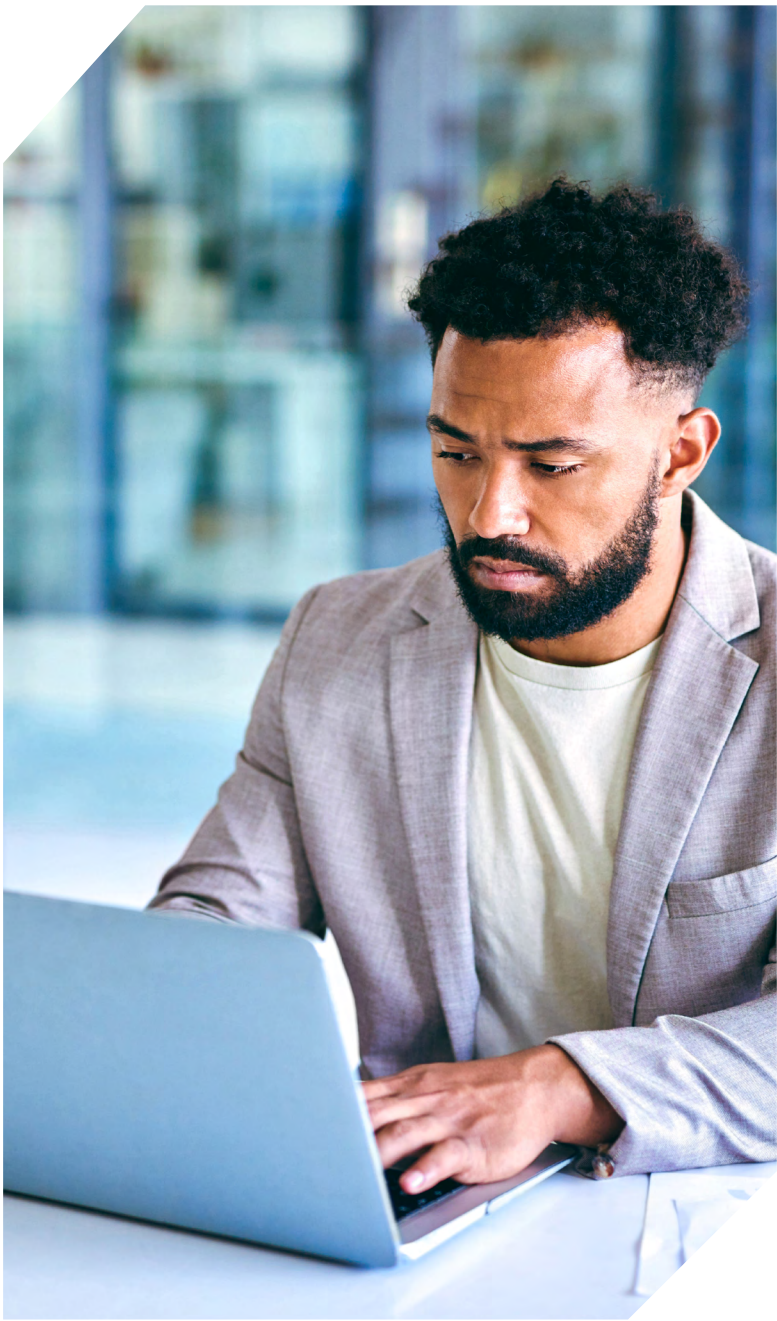
Serving US Federal Clients

Veeam Kasten can be deployed as part of a US DOD Federal supplier solution because it meets the statutory requirements set forth by the US Department of Defense. Those requirements include enterprise-grade data immutability, a validated software supply chain SBOM, delivery from Iron Bank hosted on Platform One, and compliance with FIPS 140-3 secure information protocols. Following the steps outlined in this paper, in addition to meeting the federal statutory obligations listed here, Veeam Kasten is the solution of choice for many of our customers interested in maintaining the highest security levels. Whether or not you are a FedGov supplier, this can apply to you too.

3. Secure Access Identities with Immutable Storage

Ransomware attacks pose a significant threat to organizations, with identity databases often being targeted to covertly infiltrate production networks . In fact, according to the most recent CyberArk findings, "Threat Landscape Report 2024", 94% of security professionals reported at least one identity-related breach in the past year. To safeguard critical systems and protect revenue-generating activities, prioritizing access security is crucial. Immutable storage thus emerges as an effective solution, preventing unauthorized modification to secure user access credentials and maintaining a secure state for user access lists and configuration details. By leveraging immutable storage for identity databases, organizations can ensure the integrity of their access controls, effectively countering the risks associated with ransomware attacks.

By adopting these measures, organizations can fortify their defenses against ransomware attacks. Immutable storage can also safeguard critical data and access controls. Through proactive implementation of these security measures, organizations enhance their resilience against the evolving threat of ransomware and safeguard their critical systems and business operations.



94%

of security professionals reported at least one identity-related breach in the past year

4. Confidently Back Up Your Data

An effective backup plan not only safeguards critical data but serves as a crucial defense against ransomware attacks. By conducting regular backups and taking periodic snapshots, you can capture the state of your systems and applications, making it possible to restore them to a trusted state in the event of a ransomware incident. Additionally, Veeam recommends following the 3-2-1-1-0 Golden Backup Rule for all important backups. The 3-2-1 Rule includes maintaining three (3) copies of your backup data, using two (2) different types of media storage, and storing at least one (1) copy offsite. The last -1-0 part of the 3-2-1-1-0 Golden rule steps it up a notch with the last part including storing at least one (1) copy offline and being sure to have verified backups with (0) errors. The last step requires backup recovery verification which can be established as part of the backup process where recoverability has been established through testing. This makes sense for super-critical data.

Utilizing snapshots for serialization is particularly valuable when dealing with ransomware attacks. These snapshots allow you to track and restore changes made to data over time, which enables users to pinpoint when changes are made and roll back to a clean version. By prioritizing the streamlining of backup processes with advanced solutions like Veeam Kasten, we can significantly enhance our ability to protect critical data from ransomware threats. Regularly testing and fine-tuning disaster recovery (DR) processes further reinforces defense against ransomware and ensures that quick recovery and restoration minimizes the impact of an attack.

By adopting these practices and leveraging reliable backup solutions, you not only fortify our cybersecurity plan and protect against data loss, but also bolster your resilience against the growing threat of ransomware. With an effective backup plan in place, we maintain business continuity, can restore operations swiftly, and mitigate the financial and operational risks associated with ransomware attacks.

5. Energize your Restorations

For those of us concerned with protecting service level agreement (SLA) objectives, it is essential that you have confidence in the rapid restoration of operations in the event of disruption. This requires proper restoration methods, tools, and techniques to preserve your recovery time objectives (RTOs) and recovery point objectives (RPOs).

With Veeam Kasten, data backup and recovery processes can be streamlined, which enables faster and more efficient recoveries. Regular running of DR scenarios, along with fine-tuning based on the results, ensures that your recovery strategies align with your intended goals. Leverage the multi-app restore features of Veeam Kasten for seamless restoration of namespaces and data, use proper sequential order and parallel restoration where possible, including data-only restores, and ensures a swift return to operation. This feature is a game-changer, eliminating the need for sequential application restoration and significantly reducing production restore times.

With Veeam Kasten, restoration processes can be automated, thus enabling faster and more efficient recoveries. In a recent report by the Evaluator Group, "Enterprise-Grade Cloud Native Data Protection at Scale: Kasten vs Open-Source Alternatives", Veeam Kasten was demonstrated to restore 6X faster than the alternative. Regular testing of DR processes, along with necessary fine-tuning based on the result, will not only be faster with Veeam Kasten, but will ensure that recovery strategies demonstrably align with your intended RTO and RPO goals. By incorporating these measures, organizations like yours can confidently meet SLA objectives and minimize the impact of cyber intrusions, ultimately ensuring the continued smooth operation of your systems and services.

Optimizing Disaster Recovery

Efficient and Rapid Recovery

Streamlined Disaster Recovery

Proven Performance

6. Monitor Kubernetes Deployments and Proactively Detect Anomalies

Protection against ransomware attacks necessitates comprehensive and proactive attention, including robust monitoring and data analysis capabilities. We understand this need and therefore offer a powerful integrated solution that includes monitoring tools like Prometheus and a GUI enhancement with Grafana. These tools enable operators to effectively observe key performance and operating metrics that provide insights into the health and security your Kubernetes environment. With Grafana's intuitive dashboard, operators can also visualize and analyze data in a way that is easy to understand and take timely action.

To further enhance data analysis, Veeam collaborates with technology partners to ensure that customers have access to the best tools for ransomware protection. This includes integration with security information and event management (SIEM) solutions. By integrating Veeam Kasten with SIEM solutions, organizations can gain real-time insights into their Kubernetes deployments, allowing for prompt detection of any suspicious activities or indicators of compromise. These integrations also facilitate the offloading of application snapshots for detailed analysis while aiding in the planning of effective response scenarios in the event of a security incident.

By emphasizing collaboration, like with Veeam's SIEM partners, and incorporating real-time monitoring, Veeam strengthens your ability to defend against ransomware threats effectively. The integration of multiple SIEM providers allow customers the freedom to choose the SIEM integration that best suits their specific needs. This enables proactive identification of potential security breaches and immediate action to be taken to mitigate the impact of ransomware attacks. By leveraging the enhanced monitoring capabilities of Veeam Kasten, organizations can strengthen their security posture and ensure the resilience and integrity of critical applications and data within Kubernetes deployments.

7. Make Proactive Kubernetes Improvements

In the event of a ransomware attack, it can be critical to rapidly re-launch production systems on alternative (but safe) cloud environments. This ability is also useful to continuously make changes to the profile of production environments to achieve optimal performance and cost-efficiency. Seamless application mobilization across platforms is a powerful tool for navigating various cloud-hosted platforms that are designed for vendor lock-in while maintaining resilience against intrusions. With Veeam Kasten's application mobility and data protection tools , organizations can unlock unprecedented levels of performance, profitability, and user satisfaction.

The key to achieving optimal performance and cost-efficiency lies in the ability of organizations to make strategic adjustments to their test and production environments . However, navigating the diverse landscape of cloud-hosted platforms, which often aim to lock organizations into a specific vendor, presents challenges to maintaining resilience against intrusion. This is where seamless Kubernetes application and data mobility across platforms becomes an invaluable tool. It empowers organizations to move their applications effortlessly across different cloud-hosted platforms, thus breaking free from vendor lock-in and releasing new levels of flexibility and control. By harnessing this capability, organizations can optimize their performance and costs while fortifying their defense against cyberattacks. This ensures that organizations are not only adaptable and resilient, but able to make informed choices that drive success in today's dynamic IT landscape as well.

Veeam Kasten *for Kubernetes*

By following the seven essential steps outlined in this white paper, all of us can enhance the security and resilience of our Kubernetes environments. From securing the host OS kernel and controlling data protection system access authentication, to leveraging immutable storage and confidently backing up data, energizing restorations, proactively detecting anomalies, and making proactive Kubernetes improvements, Veeam Kasten is a tool that provides the necessary features to mitigate the risk of ransomware attacks.

A core value proposition of Veeam Kasten is its emphasis on security and resilience by offering secure access methods, MFA, RBAC, and integration with SIEM solutions for proactive anomaly detection anomalies. The ability to restore operations swiftly through efficient backup and recovery processes with seamless restoration features, ensures minimal disruption to business operations and helps users meet RTOs, RPOs, and SLAs with customers.

Veeam Kasten is part of a solution that enables organizations to optimize workload placement and effortlessly migrate applications across Kubernetes clusters or cloud providers, thus overcoming the challenges of vendor lock-in and gaining flexibility and control. By implementing Veeam Kasten as part of a Kubernetes security strategy, organizations can protect their critical data, ensure business continuity, and safeguard against the devastating effects of ransomware attacks. With its robust security features and comprehensive protection capabilities, Veeam Kasten empowers modern computing organizations to navigate the evolving threat landscape and achieve long-term success while reaping the rewards of Kubernetes deployments.

Be Prepared, Stay Informed

Your journey towards Kubernetes cyber resilience doesn't end here — it is just getting started. Expand your understanding, refine your strategies, and stay ahead of the curve. Let us help you transform challenges into opportunities by checking out our expanded collection of resources:

- 5 Kubernetes Backup Best Practices
- Kubernetes Backup for Dummies
- Ransomware Trends Report, 2024

References

1. The History of Kubernetes & the Community Behind it, Brendan Burns, kubernetes.io

Try Veeam Kasten Free

About Veeam Kasten & Veeam Software

About Veeam Kasten

As Kubernetes adoption accelerates in the cloud-native era, organizations need to address the critical requirement for protecting their Kubernetes applications. To keep businesses running, robust protection and recovery of your entire application along with data services must be addressed to overcome misconfiguration, outage, and security threats that compromise availability.

Trusted by the world's largest organizations, Veeam Kasten delivers secure, Kubernetes-native data protection and application mobility at scale and across a wide range of distributions and platforms. Proven to recover entire applications quickly and reliably and coupled with its core tenet simplicity, Kasten gives operations and application teams the confidence to withstand the unexpected. Learn more at: #1 Kubernetes Data Protection & Mobility.

About Veeam Software

Veeam®, the #1 global market leader in data resilience, believes every business should be able to bounce forward after a disruption with the confidence and control of all their data whenever and wherever they need it. Veeam calls this radical resilience, and we're obsessed with creating innovative ways to help our customers achieve it. Veeam solutions are purpose-built for powering data resilience by providing data backup, data recovery, data freedom, data security, and data intelligence. With Veeam, IT and security leaders rest easy knowing that their apps and data are protected and always available across their cloud, virtual, physical, SaaS, and Kubernetes environments. Headquartered in Seattle with offices in more than 30 countries, Veeam protects over 550,000 customers worldwide, including 74% of the Global 2000, that trust Veeam to keep their businesses running. Radical resilience starts with Veeam. Learn more at www.veeam.com or follow Veeam on LinkedIn @veeam-software and X @veeam.