Codesealer

KUBERNETES SECURITY PRACTICES WITH CODESEALER

Explore how Codesealer helps with Kubernetes security challenges and enhances cluster protection through dynamic traffic security, ingress hardening, and seamless integration, ensuring resilient and secure deployments.

BROUGHT TO YOU BY CODESEALER

www.codesealer.com

Content

Codesealer

Introduction

Kubernetes has become the cornerstone of modern containerized application deployments, providing scalability, flexibility, and automation. However, the growing adoption of Kubernetes has also exposed it to a variety of security risks, including misconfigurations, supply chain vulnerabilities, and evolving cyber threats. To mitigate these risks, robust security mechanisms must be embedded into the Kubernetes lifecycle.

Codesealer is a security solution designed to safeguard Kubernetes environments through dynamic traffic protection, enhanced ingress security, and simplified integration. This paper outlines the key security challenges in Kubernetes and demonstrates how Codesealer addresses these challenges effectively.

Challenges in Kubernetes Security

Kubernetes has transformed modern application deployment with its scalability and flexibility, but its widespread adoption has introduced significant security challenges. As clusters grow in complexity, they become increasingly vulnerable to a range of sophisticated threats and operational risks. A deep understanding of these challenges is essential to implementing effective security measures and maintaining the integrity of Kubernetes environments.

Key Challenges in Kubernetes Security:

- **Dynamic Threat Landscape**: Kubernetes clusters are often targeted by attacks such as unauthorized access, lateral movement, and malicious workloads.

- **Ingress Vulnerabilities**: Misconfigured ingress controllers can expose sensitive application endpoints to external threats.

- **Container Exploits**: Vulnerabilities in container images can lead to privilege escalation and data breaches.

- **Supply Chain Risks**: The reliance on third-party components increases the risk of malicious code infiltrating the cluster.

- **Complexity of Configurations**: Kubernetes' flexibility often leads to misconfigurations, making clusters susceptible to attacks.

Codesealer’s Approach to Kubernetes Security

Codesealer introduces a multi-layered security framework tailored for Kubernetes environments. Its architecture emphasizes simplicity, scalability, and comprehensive protection.

Traffic Protection

Codesealer secures ingress and egress traffic by intercepting requests at the ingress controller level. This ensures that malicious requests are blocked before reaching the application, reducing the risk of common web attacks such as SQL injection, cross-site scripting (XSS), and DDoS.

Dynamic Application Shielding

By dynamically monitoring and securing APIs and web applications, Codesealer provides real-time protection against exploitation. It incorporates features such as domain allowlisting and content validation to protect sensitive resources.

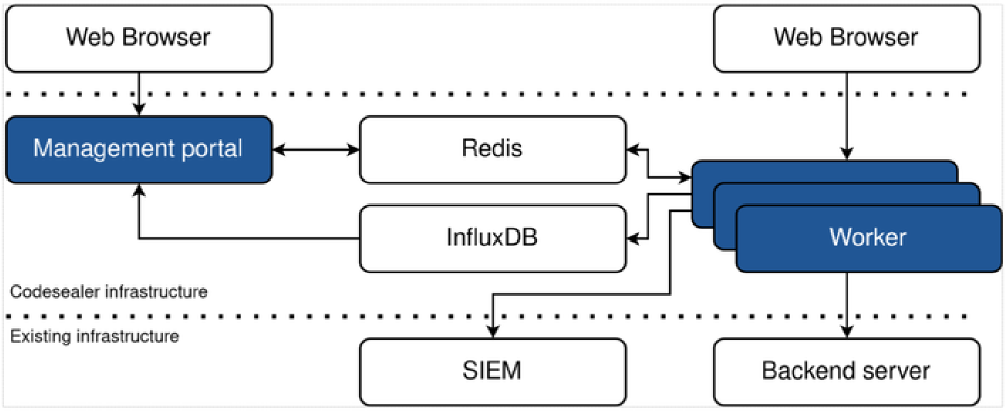
Web Application Firewall (WAF)

Codesealer integrates a robust WAF that enhances application layer security by inspecting traffic for malicious patterns. Advanced rules and analytics enable proactive blocking of attacks, reducing response times and minimizing impact.

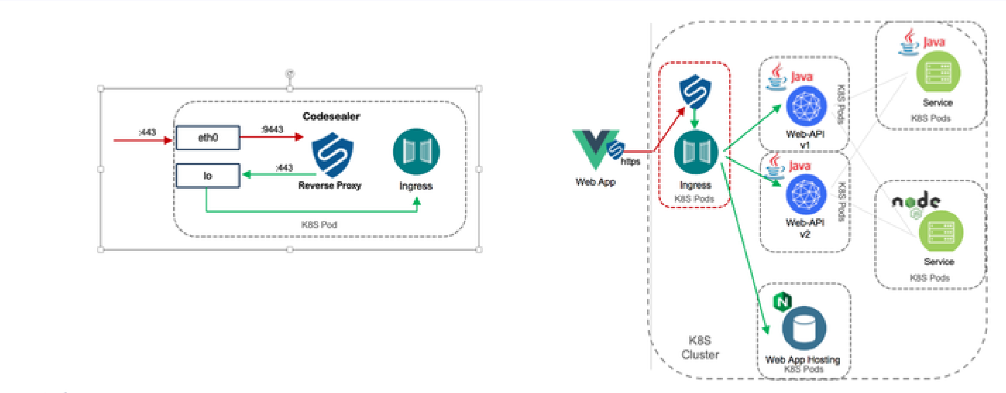
Operational Modes

Codesealer offers two flexible deployment modes, catering to different operational needs:

1. **Standalone Mode:**
   - Deployed as an independent proxy, Codesealer secures multiple applications across the cluster.
   - This mode is ideal for multi-application environments, enabling horizontal scalability without affecting application performance.



2. **Sidecar Mode:**
   - Integrated as a sidecar container within an existing ingress controller pod.
   - This mode secures ingress traffic without requiring changes to the application, offering a seamless security enhancement.



Kubernetes Integration

Codesealer is designed to seamlessly integrate into Kubernetes environments, enhancing security without disrupting existing workflows. By prioritizing flexibility and ease of use, it enables organizations to protect their applications across various setups, from development to production, while maintaining consistent performance and reliability.

Codesealer is compatible with a wide range of Kubernetes ingress controllers, including:

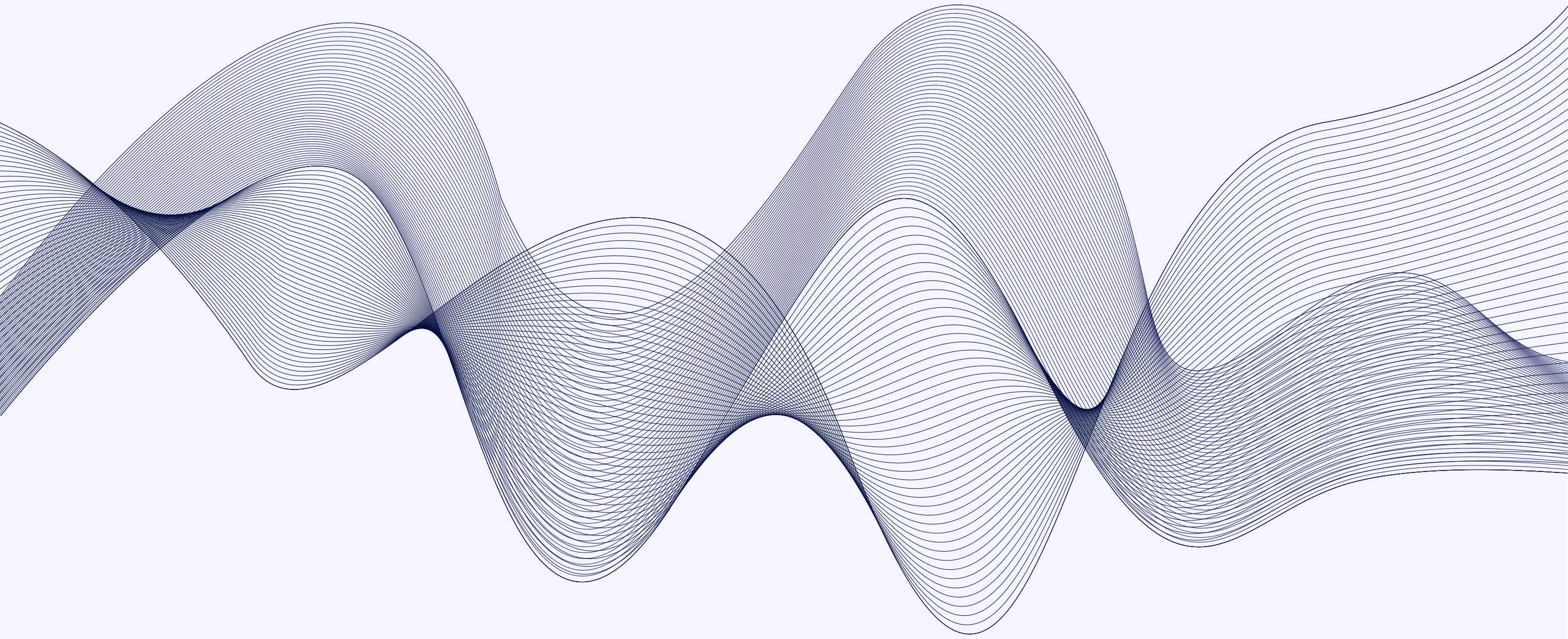
- NGINX Ingress Controller
- Istio Gateway
- Kubernetes Gateway
- Cloud provider-specific ingress solutions (AWS, Azure, GCP)

Additionally, it supports environments like Minikube and Kind, ensuring secure development and testing setups.

Ready to secure your Kubernetes deployments?

Reach out to our team today to learn more about Codesealer's protection features and discover how we can fortify your web applications against evolving cyber threats. It's extremely easy (and free) to run a test with us on any existing URL, ensuring that you can see the benefits without any time-consuming setup. Schedule a consultation or request a demo to witness the transformative impact of Codesealer firsthand.

info@codesealer.com
Codesealer A/S
Njalsgade 76, 3rd Floor
2300 Copenhagen S
CVR 39228920



Codesealer

www.codesealer.com