Securing Kubernetes Applications

CYBERARK®

Security Governance and Compliance for Cloud-Native Applications

SOLUTION BRIEF

Simplify security compliance, protect machine identities and manage secrets effectively while securing Kubernetes workloads with scalable, resilient governance for cloud-native environments.

APPLICATION SECURITY FOR KUBERNETES ENVIRONMENTS

Organizations running applications on Kubernetes need comprehensive security solutions combining automated certificate lifecycle management, validated workload identity and dynamic secrets management to ensure compliance, resilience and robust governance across multi-cluster Kubernetes environments.

- Automated certificate lifecycle management (CLM)
- Machine identity security
- Secrets management
- Multi-cluster governance
- Policy-driven identity issuance
- Integration with developer workflows

Challenge

Securing Applications in Multi-Cluster Kubernetes Environments

Ensuring the highest levels of security for applications running across different Kubernetes environments involves several challenges for security teams. It is difficult to maintain compliant certificate lifecycle operations and governance across multi-cluster environments because Kubernetes deployments often rely on untrusted, self-signed private certificate authorities (CAs). This introduces vulnerabilities and risks of certificate-related outages.

Secrets management also poses a significant challenge, as secrets are often over-provisioned, stored insecurely, or mismanaged. These practices increase the likelihood of breaches and unauthorized access, exacerbated by the lack of centralized visibility into certificates and workload identities.

Balancing the Drive for Faster Automation and Security Compliance

Another critical challenge is balancing automation with security oversight to meet developer needs without compromising compliance. Modern Kubernetes setups often involve distributed development teams deploying a diverse set of workloads, including virtual machines, custom apps and hosted services across multiple clouds. This fragmentation makes it difficult to implement unified security policies. Runtime security incidents, leaked long-lived credentials, and non-compliance will open the door to cyberattacks. Tackling this threat requires solutions that integrate seamlessly with developer workflows while enabling robust governance. Effective solutions must address these gaps with automated certificate management, validated workload identities and policy-driven secrets management to ensure resilience and scalability in cloud-native applications.

Modern machine identity security and secrets governance in Kubernetes help enforce security policies, enhance compliance, prevent outages and safeguard security from misuse.

KEY SECURITY OUTCOMES

CyberArk's solution for secure cloud-native applications provides higher levels of platform efficiency and resilience while enabling enterprise-wide trust and governance.

- Remove all certificate-related outages.
- Ensure verified access using workload identity.
- Use trusted PKI for all workload authentication.
- Deploy developer automation with built-in security.
- Implement policy-managed secrets to remove unauthorized access.
- Improve security audits and incident remediation.
- Build robust workload identity security.
- Enforce PKI policy with security oversight.

CyberArk's cloud-native solution for secure applications is purpose-built to integrate seamlessly with the cloud native ecosystem's most critical open-source projects, enabling organizations to achieve greater automation and security without requiring developer teams to alter their existing workflows.

Solution

Automated Security Governance for Kubernetes Environments

To ensure robust security across Kubernetes environments, a solution must automate machine identity management and implement the latest technologies for workload identity security and secrets management. CyberArk's solution for machine identity security leverages established cloud-native open-source tooling such as cert-manager. This helps ensure the solution addresses critical security challenges like non-compliant developer activity such as using untrusted or unmanaged certificate authorities, which can lead to attacks or result in outages. It automates certificate lifecycle management, enforces security policies and prevents risks from expired certificates, ensuring trusted workload authentication. With dynamic secrets management and enhanced visibility across clusters, the solution removes operational inefficiencies and shadow IT, delivering comprehensive security governance and ensuring compliance.

Manage Policies Centrally and Deploy Locally

Security teams can ensure compliance and tackle threat management by using CyberArk's solutions to secure their Kubernetes applications with trusted public key infrastructure (PKI) and policy-controlled identity issuance for secure workload communication and eliminating non-compliant practices such as storing machine identity credentials in insecure or unmanaged storage locations. Policies can be created and managed centrally by security teams and deployed locally and easily by platform teams using highly automated workflows, which allow developers to focus on applications while ensuring compliance. By integrating security into development processes, the solution promotes a DevSecOps culture, reducing the complexity of managing machine identities and secrets. Using a scalable and resilient solution for platform teams and offering comprehensive security oversight across multi-cluster Kubernetes environments, CyberArk can help ensure the highest workload security standards resulting in operational efficiency and strong security governance.

To learn more contact CyberArk.