Automated Security and Compliance for Kubernetes

The exploding use of container orchestration calls for solutions to secure Kubernetes environments despite unique challenges. Ermetic protects K8s environments and enables compliance with accuracy and ease, freeing Dev/Ops to scale Kubernetes with confidence.

Why a Specialized Solution for K8s Security?

Kubernetes environments function as “a cloud within a cloud.” To achieve visibility and control in complex multi-cloud frameworks, solutions for securing Kubernetes clusters must be built for that purpose. Using K8s managed services? Your cloud provider secures only the infrastructure – you are responsible for securing your data that runs on it.

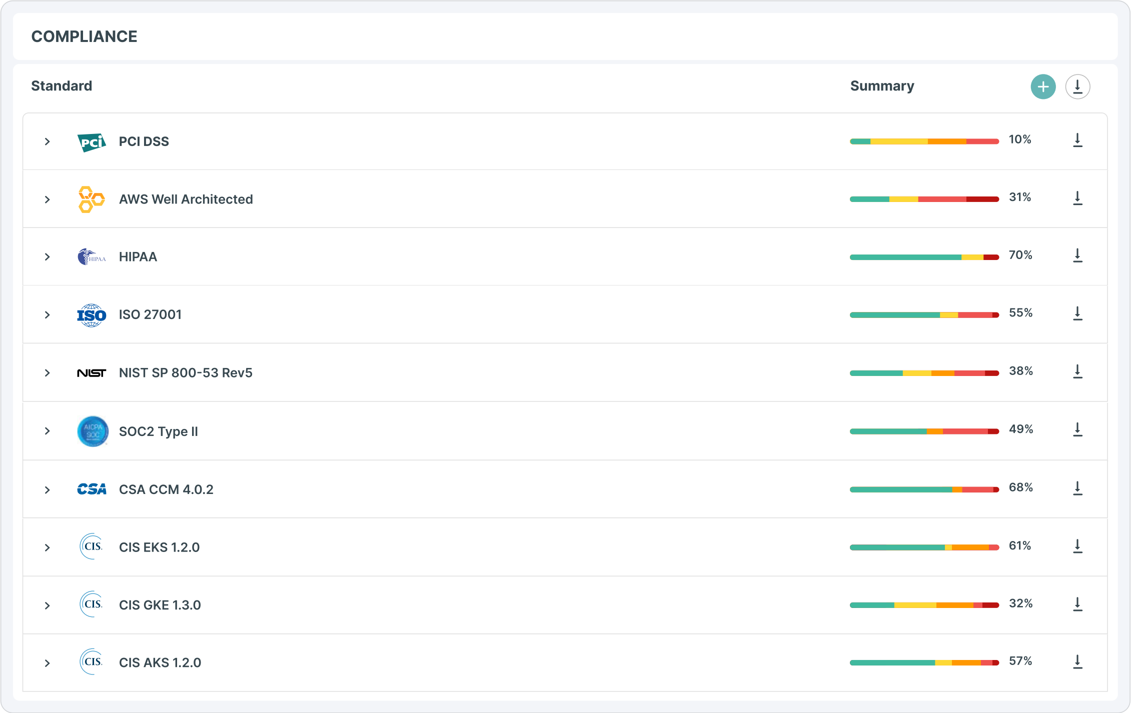
What Are the Challenges?

Kubernetes' powerful management of containerized workloads and services introduces complex security challenges especially in multicloud environments. These issues include a lack of visibility into settings, misuse of images, breakdowns in communication and runtime monitoring difficulties. Existing tools only provide simple analysis, leading to false positives that hamper developer productivity and miss detecting risks. They lack risk correlation that enables teams to address and mitigate what matters most.

Use Cases for Securing K8s using Ermetic

Using Ermetic gives you insight and control for diverse Kubernetes security use cases:

- Full, runtime visibility into Kubernetes resources across multicloud deployments
- Vulnerability management that scans container images in K8s clusters
- Detection of misconfigurations and malware
- Least privilege enforcement for user and service identities in Kubernetes RBAC
- Compliance mapping to K8s policies and audit reports
- Workload risk prioritization, proactive alerts and detailed remediation steps
- Threat detection and integration with SIEM and other tools for fast incident response



COMPLIANCE

Standard	Summary
PCI DSS	10%
AWS Well Architected	31%
HIPAA	70%
ISO 27001	55%
NIST SP 800-53 Rev5	38%
SOC2 Type II	49%
CSA CCM 4.0.2	68%
CIS EKS 1.2.0	61%
CIS GKE 1.3.0	32%
CIS AKS 1.2.0	57%

Ermetic monitors standards and best practice compliance including CIS Kubernetes for AWS, Azure and GCP

What Ermetic KSPM Can Do for You

Ermetic automates agentless scanning and secure management of Kubernetes clusters in AWS, Azure and Google Cloud. It provides single-pane visibility into resources beyond containers, including virtual machines, serverless functions and K8s clusters. It combines KSPM with CWP, CSPM, CIEM and IaC to see within Kubernetes components including network and internal RBAC. It detects, prioritizes and remediates container vulnerabilities and risks with pinpoint accuracy.

Ermetic KSPM capabilities include:

- **Complete inventory.** Get detailed, contextualized visibility into all Kubernetes resources including clusters, nodes, namespaces, deployments, servers and service accounts

- **Continuous posture assessment.** Easily detect misconfigurations in cloud and K8s resources

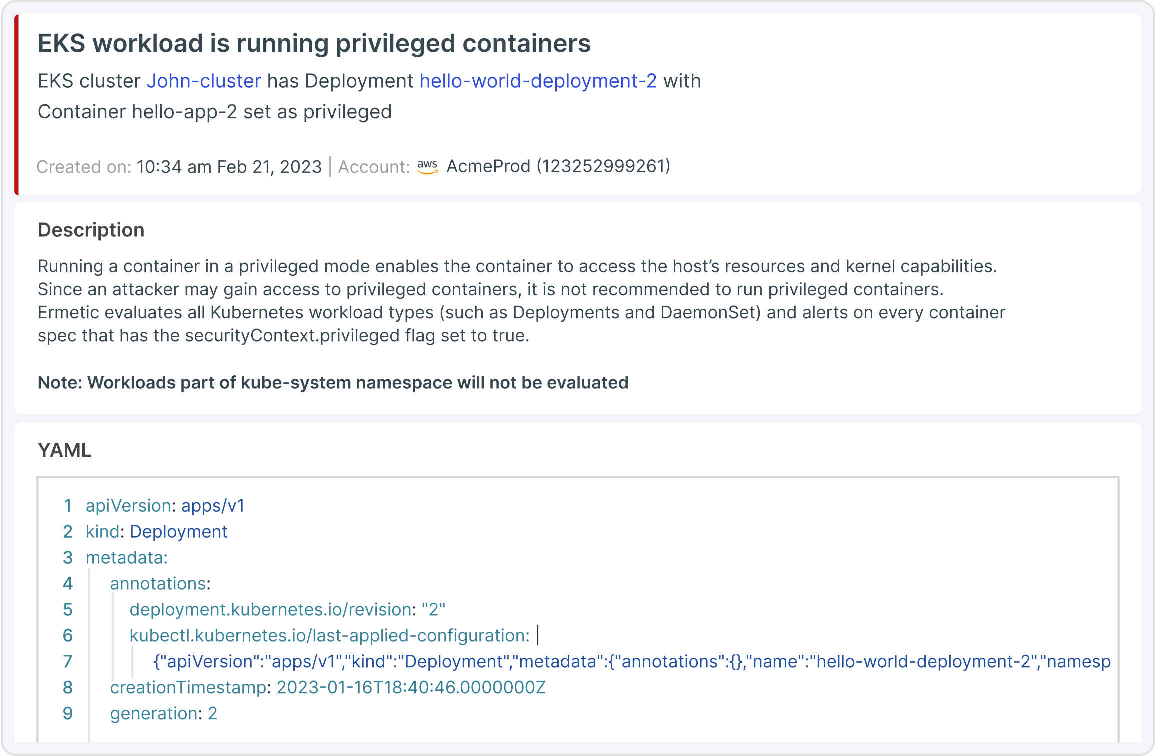
- **Role-based access control.** See deeply into K8s RBAC including identities, permissions and policies; remediate access risks and ensure least privilege

- **Prioritization and remediation.** Prioritize security gaps across K8s, workloads, identities, cloud configurations, and send alerts and how-tos via standard workflows

- **Network configuration.** See into network related issues such as API access, misconfigured unauthorized access between pods and insecure communications

- **Compliance and governance.** Continuously audit compliance against standards and benchmarks including CIS for Kubernetes; govern access with fine-grained policies

The Ermetic user experience tames security complexity and empowers DevOps stakeholders to maximize Kubernetes innovation with confidence.



EKS workload is running privileged containers

EKS cluster John-cluster has Deployment hello-world-deployment-2 with Container hello-app-2 set as privileged

Created on: 10:34 am Feb 21, 2023 | Account: aws AcmeProd (123252999261)

Description

Running a container in a privileged mode enables the container to access the host's resources and kernel capabilities. Since an attacker may gain access to privileged containers, it is not recommended to run privileged containers. Ermetic evaluates all Kubernetes workload types (such as Deployments and DaemonSet) and alerts on every container spec that has the securityContext.privileged flag set to true.

Note: Workloads part of kube-system namespace will not be evaluated

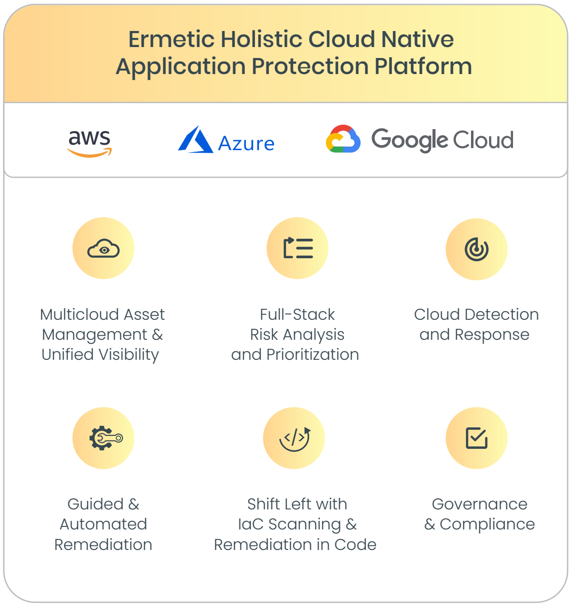
YAML

```
apiVersion: apps/v1
kind: Deployment
metadata:
  annotations:
    deployment.kubernetes.io/revision: "2"
    kubectl.kubernetes.io/last-applied-configuration: |
      {"apiVersion":"apps/v1","kind":"Deployment","metadata":{"annotations":{},"name":"hello-world-deployment-2","namesp
  creationTimestamp: 2023-01-16T18:40:46.0000000Z
  generation: 2
```

Ermetic accurately prioritizes Kubernetes security gaps and accelerates remediation with how-tos integrated in standard engineering workflows

The Ermetic Platform - CNAPP

Ermetic offers Kubernetes security posture management (KSPM) as part of its comprehensive cloud-native application protection platform (CNAPP) for AWS, Azure and GCP. The platform automates security and compliance from development to runtime. Its capabilities include best-in-class cloud infrastructure entitlement management (CIEM) as well as cloud security posture management (CSPM), cloud workload protection (CWP), Kubernetes security (KSPM) and infrastructure as code (IaC) security.



Ermetic Holistic Cloud Native Application Protection Platform

aws Azure Google Cloud

Multicloud Asset Management & Unified Visibility

Full-Stack Risk Analysis and Prioritization

Cloud Detection and Response

Guided & Automated Remediation

Shift Left with IaC Scanning & Remediation in Code

Governance & Compliance

What Customers Are Saying

> Ermetic is giving [us] IAM security, cloud expertise and cloud posture security. It is an independent tool providing transparency and deep, unified insight into our cloud architecture.
>
> Andreas Pfau
> Tribe Lead Business Solutions at Bilfinger

Contact us!

To learn more or schedule a demo: **info@ermetic.com**