CHEAT SHEET

Why Kubernetes Security Is Mission-Critical

To continuously launch leading applications and new technologies, organizations are eagerly adopting containers and Kubernetes so they can become more agile and quicken time-to-market. However, the rise in the adoption of Kubernetes is hindered by genuine security concerns.

In a recent **survey** of more than 500 DevOps professionals, 55% delayed an application release because of security issues, 94% experienced at least one Kubernetes security incident in the past year, and 59% said security is their biggest concern with regard to continued use of Kubernetes and containers.

Kubernetes offers many advantages, but also poses some unique security challenges that can be difficult to address. If organizations don't make the necessary investment in security strategies and tooling, it can quickly cause delays in production and expose intellectual property, personnel files, and other at-risk assets that can have a direct impact on the bottom line. Organizations with weaker security also risk losing partnering opportunities.

86% of organizations manage some portion of their container workloads using Kubernetes.

<50% of organizations have an adequate investment in container security.

$4.24M was the average cost of a data breach in 2021, a 10% rise from the average cost in 2019.

60% of organizations will use cybersecurity risks as a "primary determinant" in choosing who they conduct business with.

Kubernetes Security Challenges and Best Practices

The following are some of the major security challenges facing Kubernetes production deployments, as well as guidelines from the National Security Agency (NSA) and Cybersecurity and Infrastructure Security Agency (CISA) for hardening the security of Kubernetes implementations.

Compromised Container Images and Image Registries

While the use of container images and registries enable developers to deploy services independently, images and their dependencies might contain vulnerabilities. To ensure the highest protection, organizations should implement strong governance policies to ensure that images are built using preapproved and secure base images and stored in trusted image registries. In addition, to standardize this process, organizations should create a list of image registries that are allowed for use.

NSA/CISA Guideline: Scan container images for possible vulnerabilities or misconfigurations.

Compromised Containers or Malicious Traffic

Containers need to communicate with one another to perform required actions. However, unrestricted communication between containers can be exploited by attackers. A breached container can also affect other containers and pods.

NSA/CISA Guideline: Run containers and pods with the least privileges possible. In addition, use network separation to control the amount of damage a compromise can cause.

Unsecure Default Configurations

Although Kubernetes provides a variety of controls to secure clusters and applications, it does not provide secure configurations out of the box.

NSA/CISA Guideline: Use strong authentication and authorization to limit user and administrator access, as well as firewalls to limit unneeded network connectivity and encryption to protect confidentiality.

Lack of Visibility

Visibility is critical to ensure that security is maintained. However, it can be particularly challenging to monitor containers to detect attacks or malicious activity, especially in distributed, heterogeneous environments.

NSA/CISA Guideline: Use log auditing so that administrators can monitor activity and be alerted to potential malicious activity.

Compliance Challenges

Compliance is a critical concern for many organizations and government agencies. However, the distributed nature of containerized environments makes it difficult for businesses to meet compliance requirements.

NSA/CISA Guideline: Periodically review all Kubernetes settings and use vulnerability scans to help ensure risks are appropriately accounted for and security patches are applied.

The Four C's of Cloud-Native Kubernetes Security

Cloud-native security adopts a defense-in-depth approach that is implemented across four key layers, known as the 4 C's of cloud-native security by the Cloud Native Computing Foundation (CNCF):

Code

Security measures that protect the code, such as vulnerability scanners and secure coding practices.

Containers

Security measures at the container level, such as restricting access to network ports and encrypting data in transit.

Clusters

Security measures at the cluster level, such as defining network security policies and hardening all master nodes.

Cloud or Enterprise Data Centers

Security measures that protect infrastructure. This is usually implemented by a cloud provider or on-premise.

Moving from a "Trust But Verify" to a "Never Trust, Always Verify" Kubernetes Security Model

Years ago, firewalls, passwords, and antivirus were deployed to protect internal business systems and assets from malicious actors. This traditional network security followed a "trust but verify" model in which internal users and endpoints within the organization's network were automatically trusted once their log-in credentials were validated. However, once on the network, users are free to move laterally within the systems and access or exfiltrate any data to which they are not limited. This can include threat actors and malicious insiders.

As business infrastructures have grown increasingly complex and the number of cybersecurity attacks have escalated, the "trust but verify" approach has proven ineffective in protecting against malicious attacks and security breaches.

Rooted in the principles of "never trust, always verify," zero trust security means that no one is trusted, by default, from inside or outside the network, and verification is required from anyone trying to gain access to resources on the network.

Zero trust is designed to protect modern digital environments by leveraging network segmentation, preventing lateral movement, and simplifying granular user access controls.

Concepts of Zero Trust

The zero trust model is based on three fundamental concepts:

Secure Network

Always verify access, assuming that external and internal threats exist on the network at all times.

Secure Resources

Resources in the network should be securely accessed, regardless of the location. Implement checks in a way in which the locality of the resource is not sufficient in deciding trust in a network.

Authenticate

Every user, device, and traffic must always be authenticated. In the zero trust model, trust is not to be taken for granted, but is based on observation and regular authentication to help limit risks. Essentially, a zero trust approach aims to wrap security around every user, device, and connection, every time.

Applying a Zero Trust Approach to Enterprise Kubernetes Deployment

The distributed nature of cloud computing architectures means workloads are running in different locations and networks, and often are running across multiple clouds and on-premise infrastructures. As more cloud-native systems are being deployed on Kubernetes, a new system is needed to provide greater protection to businesses.

Zero-trust principles can be used to secure the individual pillars of a container infrastructure. These include the following:

GitOps

Most digital projects are used to working with GitHub and GitLab repositories. However, moving to GitOps requires that teams adopt a declarative approach to how code is pushed. Tooling like Flux helps achieve the necessary deployment from Git to Kubernetes.

DevOps

As previously explained, zero trust means taking a shift-left approach to security and expanding into DevSecOps. Security operations cannot operate in silos, which means security teams must leave behind traditional processes and tooling and give importance to code source.

Service Mesh

Most companies are only learning the complexities of managing and securing Kubernetes. Service meshes like Itsio have become a standard in Kubernetes to secure north-south traffic and east-west traffic.

Service Identity

Service identity should be implemented using certificate-based authentication. Existing API and microservices architecture should be rearchitected to implement a service mesh design.

Policy Management

Policy management infrastructure is fundamental in managing white lists and attributing level access controls. Automation and real-time auditing of each service identity is required.

All of these are challenges that need to be—and should be—addressed for organizations and government agencies to deploy a zero-trust-based architecture in a cloud-native environment.

The D2iQ Enterprise Kubernetes Security Difference

The D2iQ Kubernetes Platform (DKP) provides the most advanced, secure, feature-rich, easy-to-deploy, easy-to-manage, and cost-effective Kubernetes platform available. DKP's security posture can be broken down into four concepts:

Security Traffic Flows	External cluster traffic Internal cluster traffic
Access and Identity Management	Authentication integration Authorization implementation Secret management
Logging, Monitoring, and Compliance	Logging architecture Monitoring architecturew Compliance as a code
Operating and Maintaining the Cluster	Configuration management Image management Migration and deployment management Contingency planning

Trusted Solutions and Benefits

Enterprise-Scale Tests

DKP goes through a rigorous testing and review process where it's scanned against Center for Internet Security (CIS) benchmarks, common vulnerabilities, and exposures (CVEs), and then deployed and soaked for up to 10,000 hours with mixed workload testing.

Release Cycle

D2iQ relies on upstream Kubernetes, which currently maintains community support for up to N-2 versions. This time period tends to amount to nine months of upstream support for any given minor version of Kubernetes, or a new minor release of Kubernetes every three months.

Upstream Base Technology Leadership

D2iQ can, and has, submitted enhancements and fixes for the underlying components included in DKP. This work has included triage, root cause analysis, and fixes for upstream open-source projects. Our engineering teams are actively contributing to a wide range of these projects, from a code and technical leadership perspective. Those efforts include Kubernetes itself, Kubefed, Kubecost, Cluster API, and many more.

Supply-Chain Management

As cyberattacks continue to escalate, there has been increased focus on ensuring a reliable and transparent supply chain, especially for open-source software. At D2iQ, we provide an opinionated Kubernetes distribution while remaining transparent about each piece of code integrated into our platform.

Kubernetes Security Vulnerabilities

D2iQ is a part of the Kubernetes embargo community, meaning we are given early builds of Kubernetes under confidentiality to test and package in advance of the official release. This status gives us the opportunity to give you critical CVE patches very quickly, usually the day they are announced.

DKP Security Vulnerabilities

Ensuring security to the best of our abilities underlies everything we do. D2iQ will perform both open-source software licensing and container image security scanning for releases. Image vulnerability scanning is performed on a continuous basis as part of D2iQ's standard continuous integration and continuous delivery CI/CD process.

Air-Gapped Deployments

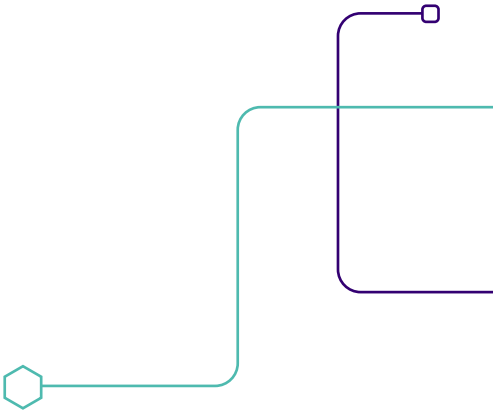
DKP is infrastructure- agnostic and has a proven track record of running in a variety of environments, including those that are fully air-gapped from the Internet.

FIPS Compliant

Many government agencies in the United States require Federal Information Processing Standards (FIPS) compliance or validation for deployed software. D2iQ works with many government agencies and has a history of delivering FIPS-compliant platforms as part of these partnerships. In addition, DKP is FIPS 140-2 certified, which is the more stringent of the two standards. With FIPS 140-2 validation, U.S. public sector organizations can have peace of mind that their DKP products and workloads have been certified secure by an independent laboratory in compliance with government standards.

Don’t Let Kubernetes Security Be an Afterthought

Breaches, disruptions, and data thefts are serious cybersecurity issues that organizations and government agencies shouldn’t take lightly. The good news is that DKP meets all the NSA/CISA guidelines, giving D2iQ customers the assurance that their environments provide military-grade security protection.



To learn how your business can future-proof its infrastructure with DKP, visit the d2iq.com website, speak with the D2iQ experts, or see DKP in action by requesting a demo.