SOLUTION BRIEF

D2iQ Security Solution

Overview

Security remains a top issue for businesses. Smart cloud-native application architectures and DevOps processes enable more data, intelligence, and agility to be applied to business processes to deliver better outcomes. But this is an even more tempting target for bad actors working to penetrate out-of-date security technologies, processes, and implementations not designed for this smart cloud-native world.

According to Tigera[1]:

- 94% experienced at least one Kubernetes security incident in the past year.
- 55% delayed an application release due to security issues.
- 59% said security is their biggest concern with regard to the continued use of Kubernetes and containers.

A strategy to overcome these issues is to develop a comprehensive Kubernetes security strategy to meet the requirements of organizations with the most stringent security requirements, such as the military and intelligence agencies. Getting to a military-grade security posture isn't easy, but it does not have to be overly expensive or complex. Indeed, unnecessary complexity increases security risks.

A successful Kubernetes security involves people, processes, and technology.

People

The employees, partners, customers, and other stakeholders accessing your company's applications are a key focus area for strong security. They need to be trained in best practices from password management to understanding the nature of various online scams.

Process

Your security processes support the good actors in maintaining strong security and prevent the bad actors from accessing your data and applications. Some of these processes include password management, active review of network management, firewall checklists, and scanning containers and software images regularly. Operational processes associated with air-gapped deployments are a key focus.

[1] Kubernetes Security: Risks, Security Controls & Best Practices – Tigera

Technology

The basic technologies that enable authentication, authorization, detection, and prevention should be deployed. Air-gapped deployments are the most secure, coupled with the right processes.

To keep pace with the latest security technology and best practices, follow the Cloud Native Computing Foundation (CNCF) open-source communities that have more people looking at the code and finding and fixing security issues faster. A vendor-backed team focused on making sure their technology (Kubernetes, operational software) is secure, coupled with that active community, is the best of both worlds.

Security Solution - D2iQ Kubernetes Platform (DKP) and Services

D2iQ helps customers attain military-grade security for smart cloud-native applications within the D2iQ Kubernetes Platform (DKP), which consists of the following products:

- **DKP Essential—**a single-cluster entry-level Kubernetes platform.
- **DKP Enterprise—**a multi-cluster enterprise Kubernetes platform.
- **DKP Edge/IoT—**Kubernetes platform optimized for managing edge devices.

DKP Kaptain AI/ML (add-on)—A DKP add-on that simplifies AI/ML operations.

DKP Insights (technology preview)—A DKP self-service capability that embeds D2iQ's intelligent automation expertise in Kubernetes operations.

Military-Grade Security

DKP is security hardened by following enterprise security best practices, including access control through single sign-on, encrypted data addresses, and a network policy. DKP can be configured to meet NSA/CISA Kubernetes security guidelines and validates Federal Information Processing Standards (FIPS) 140-2 compliance. The container images that are shipped as part of the platform, including platform applications (which enable Day 2 readiness), are scanned for Common Vulnerabilities and Exposures (CVE) before every major and minor release.

Air-Gapped Deployments

DKP is designed from the ground up with air-gapped security in mind to enable an easy and successful production-grade experience for complex deployment patterns. D2iQ offers a unique portfolio of military-grade technology, professional services, training, and support offerings that enable you to deliver the security, compliance, and scale for mission-critical workloads from the edge to the cloud.

Support Services

D2iQ provides a wide range of Kubernetes 24/7 support offerings to help you quickly resolve issues for core Kubernetes and its supporting platform services. Our team delivers a unique mixed workload testing methodology that ensures your stack of technologies are initially and continuously tested to ensure the security and interoperability of key services.

Professional Services

D2iQ's professional services team provides expert guidance, including a focus on security that includes people, process, and technology solutions from Day 0 design to Day 2 operations—and beyond.

Advise: Our Advisory Services answer your most pressing questions and guide your wide-ranging cloud-native endeavors to achieve secure enterprise-grade outcomes.

Activate: Our Activation Services are tailored to ensure that Kubernetes is customized to meet your cloud-native application needs for scalability, efficiency, security, and speed.

Adopt: Our Adoption Services are designed to help with Day-2 operations enablement and continuous support and improvement in the lifecycle of your applications.

Training Services

D2iQ is a Certified Kubernetes Training Partner (KTP) and delivers instructor-led courses that can equip your staff with the skills and knowledge needed to successfully plan, build, secure, and operate on Day 2 in production, both for Kubernetes and its supporting platform services. Our training services address the people challenges of secure Kubernetes deployments.

The DKP Difference

As the leading independent platform for Kubernetes in production, DKP provides a holistic approach and a complete set of enterprise-grade technologies, services, training, and support to build and run applications in production securely and at scale. Together, we help you address the people, processes, and technology challenges to get to a military-grade security posture.

Built around the open-source Cluster API, DKP becomes the single, centralized point of control for your organization's application infrastructure, empowering you to more easily deploy, manage, secure, and scale Kubernetes workloads in Day-2 production environments. DevSecOps efficiency and productivity are maximized through continuous delivery and agile development. Multi-tenant logging and role-based policy enable your organization to allocate responsibility. enable your organization to allocate responsibility.

To learn more about about how D2iQ can be your partner in the cloud native journey, go to D2iQ.com