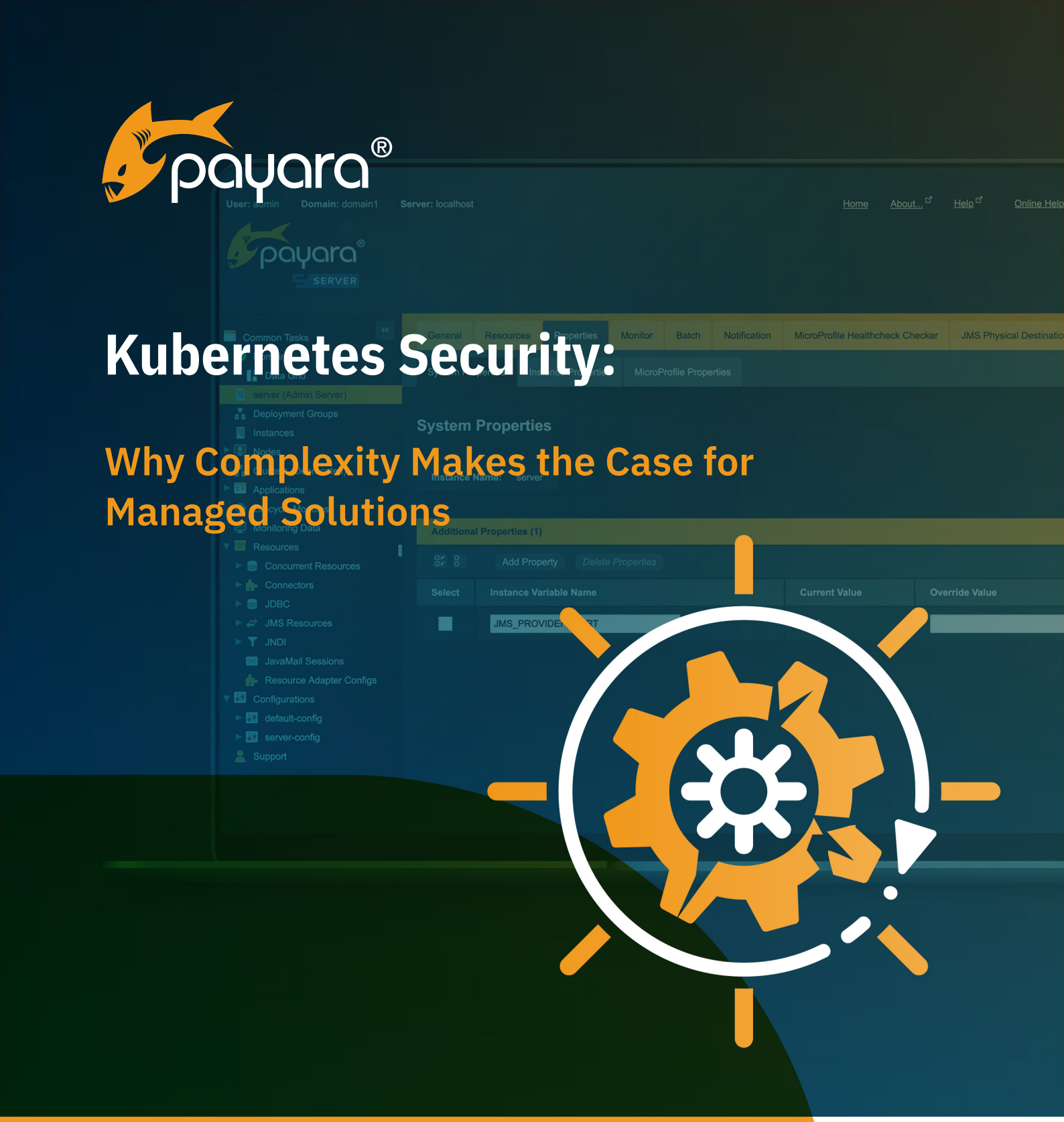
Kubernetes Security:

Why Complexity Makes the Case for Managed Solutions



Power Up Your Jakarta EE

Executive Summary

Kubernetes has become the backbone of modern cloud-native infrastructure, enabling organizations to build, scale and deploy applications faster than ever before. However, its complexity introduces significant security and operational challenges that many enterprises are unprepared to manage at scale.

The *CrowdStrike Complete Guide to Kubernetes Security* (2025) underscores the challenges that Kubernetes security presents and the potential vast attack surface, from misconfigurations and supply chain vulnerabilities to insecure network policies and compromised credentials. As organizations increasingly adopt Kubernetes, they must also confront a sobering reality: securing it effectively demands deep expertise, continuous vigilance and a holistic security strategy across the entire software development lifecycle (SDLC).

For most C-suite leaders in organizations using Java, the question isn't whether Kubernetes is valuable, it's how to reap its benefits without exposing the business to undue risk or operational overhead. This whitepaper explores why a managed abstraction like Payara Cloud represents a strategic evolution for enterprises. A solution of this kind can help organizations seeking agility, security and scalability while simplifying Kubernetes security, as teams don't have to master the intricacies of the technology itself.

The Rise of Kubernetes and Its Strategic Importance

Kubernetes has rapidly become the de facto standard for container orchestration. According to the 2023 Cloud Native Computing Foundation (CNCF) Annual Survey, 84% of organizations are using or evaluating Kubernetes, up from 81% in 2022. Kubernetes' ability to automate deployment, scaling and management of containerized applications has made the technology indispensable for digital transformation.

However, as adoption grows, so do the risks. The Red Hat 2024 State of Kubernetes Security Report found that two-thirds of organizations experience delayed deployments due to Kubernetes security concerns. Despite built-in advantages, such as isolation and rollback capabilities, Kubernetes environments are inherently complex and dynamic. As such, they can be hard to secure and maintain.

Navigating Security Risks in Self-Managed Kubernetes Environments

Kubernetes offers powerful functionalities, but with these comes a steep learning curve and an expanded threat landscape. Key challenges include:

Complexity and Configuration Risks

Kubernetes architecture involves multiple components — API servers, etcd, kubelet, controllers — each serving critical roles and all requiring precise configuration. Missteps in any area can lead to vulnerabilities, unauthorized access or service disruptions.

Supply Chain Vulnerabilities

Containers often rely on third-party images and dependencies. Typosquatting attacks, whereby attackers publish malicious packages under lookalike names, are increasingly common and difficult to detect without reliable scanning and validation tools.

Identity and Access Management

Kubernetes uses a sophisticated RBAC model, but improper configurations can grant overly permissive access. Managing least privilege across teams, services and clusters becomes a full-time job in itself.

Network Exposure

Without strict network policies, internal communications between containers and pods may be exposed. Attackers can exploit these pathways to move laterally within a cluster once initial access is gained.

Secrets Management

While Kubernetes has native secrets management, securing those secrets through encryption, rotation and access control is far from trivial. Improper handling can lead to data exposure and credential theft.

These issues aren't theoretical. They are real threats that have led to breaches, downtime and reputational damage for companies worldwide.

The Cost of DIY Kubernetes Management

Managing Kubernetes internally requires not only technical know-how, but also ongoing investment in monitoring, tooling, training and incident response. Organizations face several hidden costs:

- **Operational Overhead:** Running Kubernetes at scale demands dedicated DevOps and security teams.
- **Security Gaps:** Without continuous integration of security into CI/CD pipelines, vulnerabilities slip through undetected.
- **Delayed Time-to-Market:** Manual processes and misconfigurations slow down deployments and innovation cycles.
- **Increased Risk Exposure:** Unpatched vulnerabilities, outdated base images and insecure IaC templates present persistent risks.
- **Higher Total Cost of Ownership (TCO):** Maintaining clusters, patching nodes and ensuring uptime can outweigh the cost savings of self-managed infrastructure.

As CrowdStrike notes in its latest report, fixing issues in production can be up to 640 times more expensive than addressing them during development. For executives, this means investing early in secure, scalable solutions is more than just prudent, it's a financial imperative.

Moving Beyond the Infrastructure Layer: Embracing Managed Abstractions

Given the operational burden and security complexities associated with self-managed Kubernetes, forward-thinking organizations are shifting toward fully managed platforms and higher-level abstractions. These are platforms that provide the power of Kubernetes without requiring in-depth knowledge of its inner workings.

Introducing Payara Cloud

Payara Cloud is a fully managed application platform built specifically for enterprise Java developers. It abstracts away the underlying Kubernetes infrastructure, allowing businesses to focus on deploying, scaling and managing Jakarta EE and MicroProfile applications rather than infrastructure.

Key Advantages of Payara Cloud for Enterprise Leaders

Feature	Benefit
No Cluster Management Required	Eliminates the need to configure, monitor or maintain Kubernetes clusters.
Built-In Security by Design	Includes hardened configurations, secure image scanning and automated policy enforcement.
Seamless Integration with Developer Workflows	Enables rapid deployment without requiring deep DevOps or security expertise.
Reduced Operating Cost	Lowers infrastructure, staffing and maintenance costs.
Faster Time-to-Market	Streamlines CI/CD pipelines and reduces friction in releasing updates.

By using a platform like Payara Cloud, organizations can:

- Reduce their team's cognitive load
- Minimize misconfiguration risks
- Shift security left in the SDLC
- Focus resources on core business value

This approach aligns perfectly with the CrowdStrike recommendation to "shift left" and "shield right," embedding security throughout the development and runtime lifecycle.

Aligning Kubernetes Security with Business Strategy

Security should never be a bottleneck to innovation. In fact, when done right, it enables innovation by reducing risk, improving confidence in deployments and accelerating trusted delivery. CIOs, CISOs and CTOs must ask themselves:

- Are we investing in infrastructure or innovation?
- Are we hiring experts to manage Kubernetes or to build products?
- Can we afford to absorb the growing complexity and threat landscape of self-managed K8s?

If the answer leans towards overhead, distraction and risk, then the path forward is clear: move up the stack and adopt managed, secure, enterprise-grade abstractions over Kubernetes.

Recommendations for C-Suite Leaders

To future-proof your organization's cloud-native strategy while mitigating risk and reducing complexity, consider the following executive actions:

Reassess Your Kubernetes Strategy

Evaluate whether your current Kubernetes implementation supports your business goals or acts as a drag on innovation and security.

Invest in Platforms, Not Just Tools

Choose a platform that abstracts complexity, integrates security natively and empowers both developers and DevOps teams.

Shift Left, But Don't Overburden Developers

Embed security practices early in the SDLC, but use tools and platforms that automate compliance, scanning and policy enforcement.

Consolidate Tools to Reduce Operational Debt

Avoid fragmented toolchains. Opt for a unified platform that offers visibility, governance and protection across the entire application lifecycle.

Partner with Experts

Collaborate with a vendor who brings both domain expertise and operational maturity in cloud-native security. In addition, choosing a partner that operates on a shared responsibility model can be extremely beneficial.

Conclusions: The Future Belongs to Abstraction

Kubernetes will continue to be foundational to cloud-native computing. But as the CrowdStrike guide makes clear, its complexity introduces risks that many organizations are ill-equipped to handle.

Rather than trying to master every layer of the stack, smart organizations are choosing to abstract away the complexity and focus on what matters most: delivering secure, scalable applications that drive business outcomes.

A platform like Payara Cloud exemplifies this shift — offering the performance, flexibility and resilience of Kubernetes without the burden of managing it. For C-suite leaders, this represents not just a technical decision, but a strategic one.

In a world defined by speed, agility and security, choosing simplicity through abstraction is essential.

About Payara Cloud

Payara Cloud is a fully managed application platform built for modern Java developers. Running on Kubernetes under the hood, it delivers an enterprise-grade environment for deploying, scaling and securing Jakarta EE and MicroProfile applications — without the complexity of managing clusters.

With built-in security controls, seamless CI/CD integration and zero-cluster-management overhead, Payara Cloud empowers your team to focus on what matters: building and delivering high-quality applications faster and more securely.

Ready to eliminate the operational burden of Kubernetes? Start your 14-day free trial today — no credit card required. Get Started Now

sales@payara.fish

UK: +44 800 538 5490
Intl: +1 888 239 8941

www.payara.fish