When comparing the Total Cost of Ownership between OpenShift and a cloud specific Kubernetes solutions, it's important to consider **Direct Costs** and **Indirect Costs**.

This example is from an actual customer solution that compared OpenShift Performance Platform on AWS to Elastic Kubernetes Service (EKS) on AWS for a 3 Year TCO.

Table of Contents

3 Year TCO Savings with OpenShift in Comparison to EKS -$1,173,74

OpenShift 3 Year TCO Savings over AWS EKS for a 4 Kubernetes/OpenShit Cluster Infrastructures	-$1,173,749

These savings do not include the additional significant indirect savings from:

- Unplanned and planned downtime
- OpenShift's integrated security features that greatly reduced security vulnerabilities
- Application DevOps Engineer productivity estimated to increase at least 20%.
- Additional savings when a customer has a multi-cloud or hybrid infrastructure.

Direct and Identifiable OpenShift TCO Savings

Description	OpenShift	AWS EKS	Cost of OpenShift in Comparison to EKS
OpenShift Management Cluster & Ansible Automation AWS EKS Control Plane (No Central Management or Automation)	$30,030	$10,512	+$19,518
OpenShift Management Cluster and Master and Infrastructure Nodes AWS "Infrastructure" Nodes - non-EC2 Software and Services - Estimated	$159,300	$159,300	$0
OpenShift Application Worker Nodes AWS EKS Application Worker Nodes (Sames as OpenShift)	$79,650	$79,650	$0
OpenShift Subscription for Worker Nodes	$541,233	$0	+$541233
Implementation Services	$359,000	$748,000	-$389000

These are the costs for the Customer resources necessary to support a 4 Cluster Kubernetes/OpenShift Solution. This difference increases as the amount of Kubernetes clusters increases, where at 20 Clusters EKS would require at least 10 times the resources required by OpenShift. A Kubernetes Sr. Site Reliability Engineer (SRE) will have extensive Kubernetes and AWS experience although they will still need additional time for EKS setup and maintenance compared to OpenShift. - OpenShift: 20 hrs/week - EKS: 40 hrs/week EKS requires significant effort for security configuration, integration with AWS services, and potentially third-party tools. OpenShift's built-in security features significantly reduce the security engineer's workload. - OpenShift: 20 hrs/week - EKS: 80+ hrs/week EKS architecture design and integration with AWS services require more cloud architect involvement compared to OpenShift. - OpenShift: 5 hrs/week - EKS: 40+ hrs/week **OpenShift: 45 total hours per week** **EKS: 160 total hours per week** **Resource Cost: $75/Hour for 3 Years**	$526,500	$1,872,000	-$1345500

What Customer-required functionality is provided by OpenShift and what non-EKS products would need to be added to reduce planned and unplanned downtime?

OpenShift Platform Plus offers a comprehensive, integrated solution for containerized application deployment and management. To achieve a similar level of reliability and reduced downtime compared to AWS EKS, CUSTOMER would need to implement several additional AWS services and third-party tools:

1. Self-Healing and High Availability:

- **OPP:** OpenShift comes with built-in self-healing capabilities. It automatically detects and recovers from node failures, ensuring application availability. OPP also supports high availability configurations with multiple control plane nodes and etcd replicas.
- **EKS:** Requires additional configuration for high availability and self-healing. You need to set up multiple control plane nodes across Availability Zones, configure load balancers, and implement health checks. Additionally, you might consider using third-party tools like Kube-state-metrics and Prometheus Operator for monitoring and alerting to automate recovery actions.

2. Rolling Updates and Rollbacks:

- **OPP:** OpenShift provides a robust mechanism for rolling updates and rollbacks of applications and cluster components. This minimizes downtime during upgrades and allows for quick recovery in case of issues.
- **EKS:** Rolling updates and rollbacks can be achieved using Kubernetes native mechanisms, but they require careful planning and scripting. Tools like ArgoCD or Flux can automate these processes, but they need to be integrated and configured separately.

3. Monitoring and Observability:

- **OPP:** Includes integrated monitoring and logging tools (Prometheus, Grafana, Elasticsearch) that provide comprehensive visibility into cluster health, application performance, and resource utilization. This enables proactive identification and resolution of issues before they cause downtime.
- **EKS:** Requires integration with AWS CloudWatch, X-Ray, and potentially third-party tools like Datadog or New Relic to achieve similar levels of monitoring and observability.

4. Automated Scaling:

- **OPP:** Provides built-in autoscaling capabilities based on CPU utilization, memory usage, or custom metrics. This ensures that applications can handle varying workloads and prevents downtime due to resource constraints.
- **EKS:** Requires the use of Kubernetes Horizontal Pod Autoscaler (HPA) or Cluster Autoscaler (CA). While these are native Kubernetes features, they need to be configured and fine-tuned for optimal performance.

5. Disaster Recovery:

- **OPP:** Supports disaster recovery through features like etcd backup and restore cluster replication and multi-cluster management. This enables faster recovery from major incidents and minimizes data loss.
- **EKS:** Requires additional setup and configuration for disaster recovery. You need to implement mechanisms like EBS snapshots, cluster backups with Velero or Kasten K10, and multi-region replication for data resilience.

What vulnerabilities are reduced by OpenShift's integrated security features?

Red Hat OpenShift and AWS EKS are robust Kubernetes platforms, but OPP offers distinct advantages in integrated security, while EKS requires additional services for comparable protection.

OpenShift Security Advantages:

1. Kubernetes-Native Security:

OPP incorporates security throughout the entire Kubernetes stack, from the operating system (Red Hat Enterprise Linux CoreOS) to the container runtime (CRI-O) and networking (OVN-Kubernetes). This unified approach provides a more cohesive and consistent security posture.

2. Advanced Cluster Security for Kubernetes (ACS):

OPP includes Red Hat Advanced Cluster Security for Kubernetes (formerly StackRox), a comprehensive solution for threat detection, vulnerability management, network segmentation, compliance, and risk profiling. ACS's deep integration with Kubernetes allows for enhanced visibility into application behavior and potential risks, outperforming basic Kubernetes security measures.

3. Secure Software Supply Chain:

OPP integrates with Red Hat Quay, a secure container registry, and Red Hat Advanced Cluster Security for Kubernetes (ACS) to ensure the integrity and security of container images throughout their lifecycle. This helps to mitigate the risk of supply chain attacks through vulnerability scanning, image signing, and policy-based deployments.

4. Open Policy Agent (OPA) Integration:

OPP leverages Open Policy Agent (OPA) for fine-grained authorization and policy enforcement within Kubernetes clusters. This allows for greater flexibility and customization in defining security policies beyond the capabilities of basic RBAC.

AWS EKS Security – Additional Services Required for Comparable Security:

To achieve a security posture comparable to OPP, AWS EKS requires the following additional services and integrations:

1. Kubernetes-Native Security:

- **Amazon VPC CNI:** While not a direct replacement for OPP's OVN-Kubernetes, it provides networking capabilities within your Amazon Virtual Private Cloud (VPC) environment.

- **Calico or Cilium:** These third-party network plugins offer more advanced network policy enforcement and micro-segmentation capabilities similar to OPP's integrated networking.

2. Threat Detection and Vulnerability Management:

- **Amazon GuardDuty:** This service can monitor EKS audit logs and Kubernetes events, but it lacks the depth and Kubernetes-specific insights of OPP's ACS.
- **Sysdig Falco or Aqua Security:** These third-party tools provide runtime security and threat detection within your Kubernetes workloads, offering features similar to ACS.
- **Trivy or Clair:** Integrate these open-source vulnerability scanners to identify and remediate vulnerabilities in container images, similar to what Quay and ACS offer in OPP.

3. Secure Software Supply Chain:

- **Amazon ECR:** While ECR provides image scanning, it lacks the advanced policy-based deployments and image signing features of Quay.
- **Notary or Cosign:** These third-party tools can be integrated with ECR to enhance image signing and verification capabilities.

4. Policy Enforcement and Authorization:

- **Open Policy Agent (OPA) or Kyverno:** These policy engines offer similar fine-grained authorization and policy enforcement capabilities as OPA in OPP.

What are the typical work areas where a customer can expect to see productivity improvement for DevOps engineers working on containerized cloud applications, as a result of working with OpenShift?

Overall, OpenShift OPP can significantly improve the productivity of DevOps engineers by simplifying deployment, enhancing security, improving developer experience, providing hybrid cloud flexibility, and streamlining monitoring and troubleshooting. These improvements can translate into faster time to market, reduced operational costs, and improved application performance and reliability.

OpenShift OPP offers several key advantages over AWS EKS that can lead to significant productivity improvements for DevOps engineers working on containerized cloud applications. Here's a detailed look at the typical work areas where these improvements can be seen:

1. Simplified Deployment and Management:

- **OPP:** Streamlines the deployment of containerized applications with its built-in tooling and automation. The OperatorHub provides a curated collection of operators that simplify the

installation, configuration, and management of complex applications. Additionally, the OpenShift console offers a user-friendly interface for managing clusters, applications, and resources.

- **EKS:** Requires more manual configuration and scripting to set up and manage clusters and applications. DevOps engineers may need to use various tools and services like Helm charts, Terraform, and AWS CloudFormation to automate these processes.

Productivity Improvement:

DevOps engineers can save significant time and effort on initial setup, configuration, and ongoing maintenance tasks. This allows them to focus on more strategic activities like application development, optimization, and innovation.

2. Enhanced Security and Compliance:

- **OPP:** Offers robust security features that are integrated into the platform. This includes features like Red Hat Advanced Cluster Security for Kubernetes, image scanning, network policies, and security context constraints. OPP also provides compliance certifications for various industry standards, helping organizations meet regulatory requirements more easily.
- **EKS:** Relies on a combination of AWS security services and third-party tools for security and compliance. This can lead to increased complexity and potential for misconfigurations.

Productivity Improvement:

DevOps engineers can spend less time on manual security configuration and troubleshooting. The integrated security features of OPP also help reduce the risk of security breaches, saving time and resources on incident response and remediation.

3. Improved Developer Experience:

- **OPP:** Provides a comprehensive developer experience with tools like CodeReady Workspaces, which offers cloud-based development environments for Kubernetes applications. OPP also integrates with popular CI/CD tools like Jenkins and Tekton, enabling seamless automation of the build, test, and deployment processes.
- **EKS:** Requires more manual setup and configuration to integrate with developer tools and CI/CD pipelines. DevOps engineers may need to build custom scripts and workflows to streamline these processes.

Productivity Improvement:

Developers can get up and running quickly with pre-configured development environments and integrated CI/CD pipelines. This leads to faster iteration cycles, quicker feedback loops, and ultimately, faster time to market for applications.

4. Hybrid Cloud Flexibility:

- **OPP:** Supports hybrid cloud deployments, allowing organizations to run applications on-premises, in public clouds, or in a combination of both. This provides flexibility to choose the best environment for each workload based on cost, performance, and compliance requirements.
- **EKS:** Primarily designed for running Kubernetes applications on AWS. While it can be extended to other environments with tools like AWS Outposts, this requires additional configuration and management overhead.

Productivity Improvement:

DevOps engineers can manage applications across multiple environments from a single platform, reducing the complexity and overhead of managing hybrid cloud deployments. This allows them to focus on optimizing application performance and availability across different environments.

5. Streamlined Monitoring and Troubleshooting:

- **OPP:** Includes integrated monitoring and logging tools that provide visibility into the health and performance of clusters, applications, and resources. The OpenShift console also provides a centralized view of logs and metrics, making it easier to identify and troubleshoot issues.
- **EKS:** Requires integration with AWS monitoring and logging services like CloudWatch and Elasticsearch Service. This may involve additional configuration and setup to achieve the same level of visibility as OPP.

Productivity Improvement:

DevOps engineers can quickly identify and resolve issues with the help of integrated monitoring and logging tools. This leads to faster incident response times and reduced downtime for applications.