Companies are transforming their software development processes by shifting from monolithic applications to cloud-native microservices, leveraging containers and Kubernetes. As more containers are deployed, maintaining adequate monitoring and security of these new cloud-native infrastructure components becomes more difficult. Companies often list security and monitoring as their top concerns for deploying containers at scale. Containers provide a great level of portability and isolation, but it is hard to see what’s inside to monitor and secure them.

Sysdig has partnered with Hewlett Packard Enterprise to enable HPE Ezmeral Container Platform users to ship and deploy container applications faster and at scale by embedding security, compliance, and performance into their DevOps workflow. Using Sysdig, HPE Ezmeral Container Platform users can scan containers for vulnerabilities and have deep insights on anomalous behavior and application health issues. Users can resolve issues quickly by analyzing granular data with Kubernetes context collected by both Sysdig and HPE Ezmeral Container Platform.

Sysdig complements and enhances HPE Ezmeral Container Platform toward the application development process, providing insight across the cloud-native lifecycle, shifting security left and enabling more control at the developer level. Sysdig provides centralized visibility and security when operating HPE Ezmeral Container Platform at scale, where Sysdig can scale to 10,000+ nodes to help secure and monitor containers and applications. This gives customers the confidence to accelerate and securely expand deployment of their cloud-native applications on HPE Ezmeral Container Platform.

Confidently run HPE Ezmeral Container Platform with Sysdig Secure DevOps

FIGURE 1. Sysdig Secure DevOps workflow on HPE Ezmeral Container Platform
UNIFIED MONITORING AND SECURITY

With Sysdig, get insight into performance and security to deliver secure, reliable microservices more effectively on HPE Ezmeral Container Platform. Sysdig’s unified solution provides support for multicloud and multicluster monitoring and security.

COMPLIANCE AND AUDIT REPORTING

Sysdig ensures the HPE Ezmeral Container Platform meets regulatory compliance standards (for example, Payment Card Industry Data Security Standard [PCI-DSS], General Data Protection Regulation [GDPR], and National Institute of Standards and Technology [NIST] 800-190) with compliance checks and file integrity monitoring (FIM). It also continuously validates cloud compliance for environments built on containers and Kubernetes across the entire application lifecycle.

FORENSICS AND AUDITS

The DevOps workflow conducts forensics and incident response for your HPE Ezmeral Container Platform deployment to understand security issues, meet compliance requirements, and recover quickly. Sysdig Secure provides deep insights into all activity in the container ecosystem before, during, and after an incident.

BENEFITS

Sysdig and HPE Ezmeral Container Platform together deliver powerful insights to identify vulnerabilities, stop threats, and speed incident response.

- Runtime security: Protect containers in production with behavioral profiles that ensure the uptime of these services
- Image scanning: Define and execute comprehensive container image scanning policies to fail builds and prevent vulnerabilities
- Compliance and audit reports: Visualize and audit activity events, patterns, and trends for your HPE Ezmeral Container Platform deployment across the entire application lifecycle
- Customizable alerts: Customize actionable alerts for any scope or threshold for HPE Ezmeral Container Platform and integrate with downstream tools such as Slack, PagerDuty, and ServiceNow
- Configuration validation: Help ensure configurations at every HPE Ezmeral Container Platform logical layer meet security best practices based on CIS Benchmarks
- Microservice performance management: Dynamically map services, trace service response times, and understand relationships

Sysdig provides a unified security, compliance, and monitoring environment for HPE Ezmeral Container Platform. This unified data platform enables DevOps teams to accurately triage an incident, quickly determine if the incident is caused by a misconfiguration or malicious attempt, and perform forensics even after the container is gone.

HPE has partnered with Sysdig to help companies confidently run cloud-native workloads on Kubernetes and containers, in production, across private, hybrid, and multicloud environments. By automating security, compliance, and monitoring for a secure DevOps workflow, developers and platform teams can help maximize their application release velocity on HPE Ezmeral Container Platform.

LEARN MORE AT
hpe.com/containerplatform
sysdig.com