sysdig IBM zSystems IBM **LinuxONE**

Unified visibility, security, and compliance with Sysdig Platform for IBM zSystems and IBM LinuxONE

As organizations expand into using containers, microservices, and cloud infrastructure, a new set of issues are emerging. Those challenges include container-based observability, security, and compliance, each of which now requires a different approach to security.

Mission-critical applications across the world rely on IBM zSystems to ensure continuous availability, reliability, and operation in an open hybrid cloud environment. Today, 45 of the top 50 banks, four of the top five airlines, seven of the top 10 global retailers, and 67 of the Fortune 100 rely on IBM zSystems as their core platform[1].

IBM zSystems and IBM LinuxONE are designed to prevent security threats and protect data across a hybrid cloud environment with certified multitenant workload isolation as well as transparent, pervasive encryption with optimized performance. The Sysdig Platform helps build a security-focused, Kubernetes-based foundation for developing, deploying, and managing applications in containerized and cloud environments.

Together, Sysdig and IBM deliver a cloud-native monitoring and security platform to confidently run containers, Kubernetes, Red Hat OpenShift Container Platform, Linux, and cloud services on IBM zSystems and IBM LinuxONE.

IBM zSystems and IBM LinuxONE provide a strong foundation built for security, resiliency, and availability:

- Integrated **FIPS 140-2 level 4** compliant hardware security module (HSM[2]).
- Leverage **Red Hat OpenShift** Container Platform to modernize applications.
- Multitenancy with full LPAR isolation and virtualization designed for the highest **EAL5+ security certification**[3].
- **IBM Cloud Hyper Protect Services** to provide data-at-rest and data-in-flight protection.
- Confidential computing through the implementation of **Trusted Execution Environment** (TEE) and **Secure Execution** on Linux on IBM Z and IBM LinuxONE.

1 IBM research and analysis: https://ibm.biz/App_Mod_IBM_Study
2 Source: https://www.ibm.com/security/cryptocards/highlights
3 Source: https://www.commoncriteriaportal.org/files/epfiles/1160c.pdf

Sysdig is driving the standard for cloud and container security and provides:

- Deep visibility across Red Hat OpenShift, Kubernetes, containers, and Linux.
- Radically simple to run and scale.
- Built on an open-source security stack.

Key Use Cases

Security Governance for Linux on IBM Z and IBM LinuxONE workloads

Set and enforce policies across containers, Kubernetes, Red Hat OpenShift Container Platform, and Linux hosts to maintain higher levels of security for IBM zSystems and IBM LinuxONE based applications.

Continuous Compliance

Ensure compliance across the container lifecycle for standards like NIST, PCI, GDPR, and HIPAA.

Image Scanning and Vulnerability Management

Scan and block container vulnerabilities in the CI/CD pipeline and identify vulnerabilities in running images across containers, Kubernetes, Red Hat OpenShift, and Linux workloads.

Configuration Validation

Ensure configurations at every logical layer of your infrastructure meet security best practices based on CIS Benchmarks for Kubernetes and Linux.

Prometheus based monitoring features for Linux on IBM Z and IBM LinuxONE that covers:

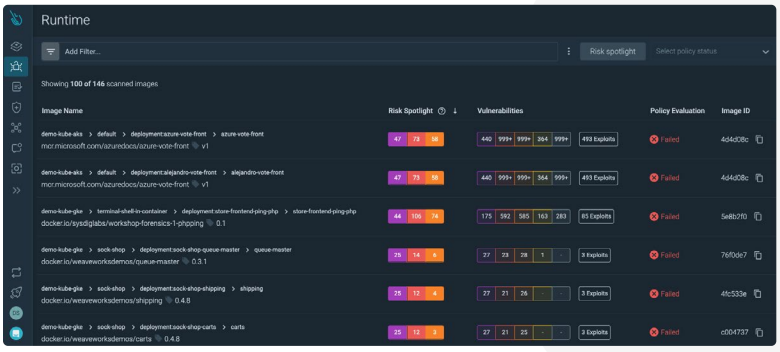
- Containers
- Kubernetes clusters
- Troubleshooting
- Customization of metrics

Audit and Forensics

Reconstruct system activities correlated with Kubernetes application context for forensics and incident response.

Runtime Security for workloads running on Red Hat OpenShift or Kubernetes

Detect anomalous behavior with the Falco engine and prevent threats using Kubernetes native controls such as Pod Security Policies.



Spotlight on vulnerabilities manifesting at Runtime

Sysdig + IBM zSystems and IBM LinuxONE: Better Together

The Sysdig Platform with the IBM zSystems and IBM LinuxONE helps CISOs, SREs, and DevOps professionals manage security, risk, and compliance at scale.

Solve your security challenges with a platform that responds immediately by blocking the execution of malicious processes, logging forensic information, and capturing telemetry about suspicious activity.

Contact your IBM or Sysdig representative for a free 30 day trial!