SOLUTION BRIEF

Secure Container Ecosystems with Container FortiOS

Executive Summary

Whether running on bare-metal servers, virtual machines, or in containers, network services are susceptible to cyberthreats. To compete in today's markets, businesses need enterprise-grade network security to minimize risk to their services. However, container environments and the dynamic nature of container-based services present new challenges for IT, OT, and cloud teams that need to implement effective network security. Securing container-based services requires robust network security that is container-ready and customizable to meet the unique security requirements of specific services.

Designed for securing container-based deployments, Container FortiOS is a flexible container firewall that provides customizable, enterprise-grade network security that is container-aware and enterprise-ready. While container-based deployments can be secured with traditional firewalls, Container FortiOS offers several advantages over traditional firewalls.

33% of respondents believe that their existing container and Kubernetes security solution slows down development.[1]

Securing Container-Based Deployments

The rise of cloud-native development and microservices architectures necessitates a more agile and efficient approach to services delivery. Containerization can help foster faster development cycles, improve resource utilization, and provide greater application portability.

Threat actors are continuously hunting for opportunities to breach infrastructure, and containerized applications and services are no exception. Issues such as vulnerability exploits, container traffic interception, modification, or malware injection can lead to the corruption of services, data loss, and significant business harm. Container FortiOS is ideal for securing applications and services in container-based environments because of its:

- **Scalability:** Container FortiOS is highly scalable and can easily be deployed alongside containerized applications and services.
- **Portability:** Because containers are designed to be portable, Container FortiOS, along with its rules and policies, can be easily moved, for example, from development to production environments.
- **Microsegmentation:** Container FortiOS can provide fine-grained control, such as microsegmentation within the service architecture, which helps limit the attack surface if one container is compromised.
- **Visibility:** To deliver more granular and context-aware policies, Container FortiOS provides deep visibility into the traffic within containers.

Key Container FortiOS Benefits

Container FortiOS helps organizations get to market faster with enterprise-grade security optimized to meet security requirements and helps ensure application and data compliance. Key features and benefits include:

- **Consolidation:** Consolidate multiple technologies into a single policy and management framework. Container FortiOS is built on the Fortinet FortiOS operating system, which is the foundation of the Fortinet Security Fabric.
- **Network security:** Secure container applications and traffic with comprehensive network security that includes a firewall, VPN, segmentation, SSL inspection, intrusion protection services, and virtual patching.

- **Networking:** Improve security and access resources outside the container environment. Networking features are included with the firewall, such as routing, network address translation (NAT), and switching. Routing allows containers to access resources outside the container environment, like databases or APIs. NAT enables sharing of a single public IP across multiple containers while maintaining individual connections. Converging networking and security enables security features such as traffic segmentation and setting up granular security policies.
- **FortiGuard AI-Powered Security Services:** Get proven protection against even the newest and most sophisticated threats with FortiGuard AI-Powered Security Services. Real-time threat intelligence and updates protect against the latest viruses, exploits, and other security threats.
- **Modular architecture:** Minimize the codebase footprint and resource requirements. The Container FortiOS modular architecture enables DevOps teams to quickly and easily add only those security capabilities necessary to protect a containerized services.
- **Secure by design:** To ensure the products adhere to the highest security assurance standards, Container FortiOS solutions are secure by design and follow the Fortinet secure development life cycle, which includes code and product security incident response team review.
- **Support for major containers:** Secure any popular container platform, including Linux Containers (LXC), Docker, Kubernetes, and other custom container platforms based on LXC.

67% of organizations delayed or slowed down deployment due to Kubernetes security concerns.[2]

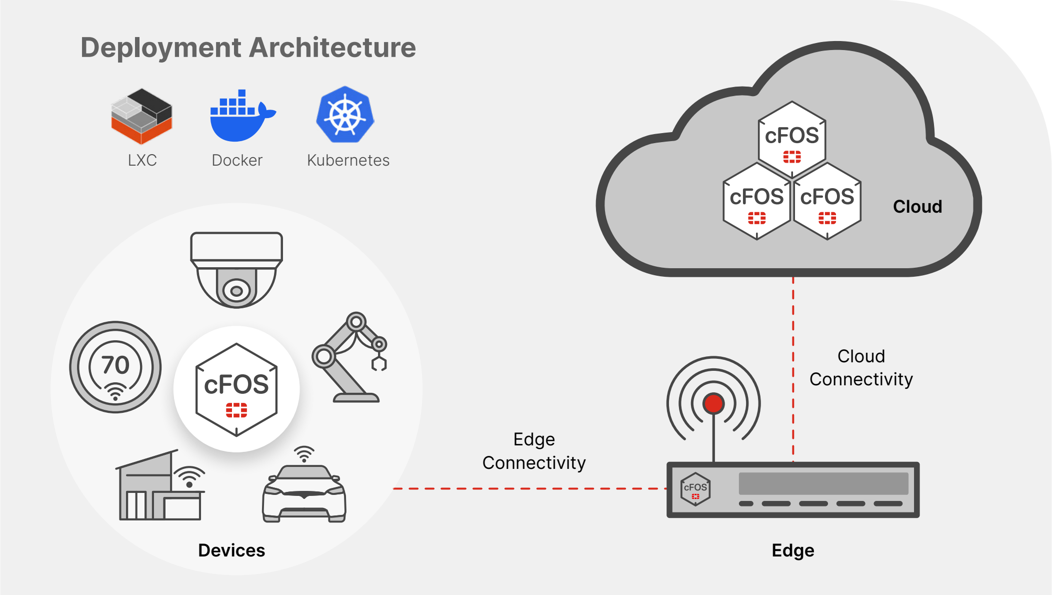

Figure 1: Container FortiOS deployment architecture

Superior Protection, Optimization, and Speed

As a container-based firewall, Container FortiOS protects containerized applications and services more efficiently and effectively than traditional firewalls. With Container FortiOS, security teams can secure systems by instantiating only necessary network security functions to ensure the application is secure while minimizing the risk of disruption to other services. DevOps teams can meet their security and time-to-market requirements by taking advantage of Fortinet's security expertise, container-ready technology, and a customized Container FortiOS solution.

Container FortiOS Advantages	FortiGate Next-Generation Firewall Advantages
■ **Scalability:** Container-based firewalls are highly scalable and can easily be deployed alongside containerized network applications and services, scaling up or down as needed. ■ **Portability:** Because containers are designed to be portable, the firewall and its rules and policies can be easily moved across environments from development to production. ■ **Microsegmentation:** Container firewalls can provide fine-grained control, allowing for microsegmentation within the service architecture, which limits the attack surface if one container is compromised. ■ **Visibility:** Container-based firewalls provide deep visibility into the traffic within containers for more granular and context-aware security policies. ■ **Lightweight:** To reduce overhead and improve performance, container firewalls typically only include a subset of the full firewall feature set.	■ **Mature and proven technology:** Traditional firewalls like FortiGate Next-Generation Firewalls have a long history of production use. ■ **Ease of use:** Container firewalls often don't include a graphical user interface and can only be managed programmatically or through the command line interface. ■ **Performance:** Hardware-based firewalls, especially those utilizing custom ASICs, offer higher performance and the ability to offload traffic encryption and decryption or SSL processing so they can better manage demand bursts and denial-of-service attacks. ■ **Features:** Traditional firewalls usually have a deeper and more complete feature set. ■ **Fabric integration:** Traditional firewalls are more likely to be integrated into a broader security fabric.

Protect Container-Based Services from the Latest Threats

The acceleration of digital business is driving the growth of container-based services, and securing these services is critical to the success of many organizations. Container FortiOS enables security teams to implement enterprise-grade security optimized for containers, giving businesses the agility to rapidly add new capabilities while being protected from the latest security threats.

[1] The state of Kubernetes security report: 2024 edition, Red Hat, June 11, 2024.

[2] Ibid.