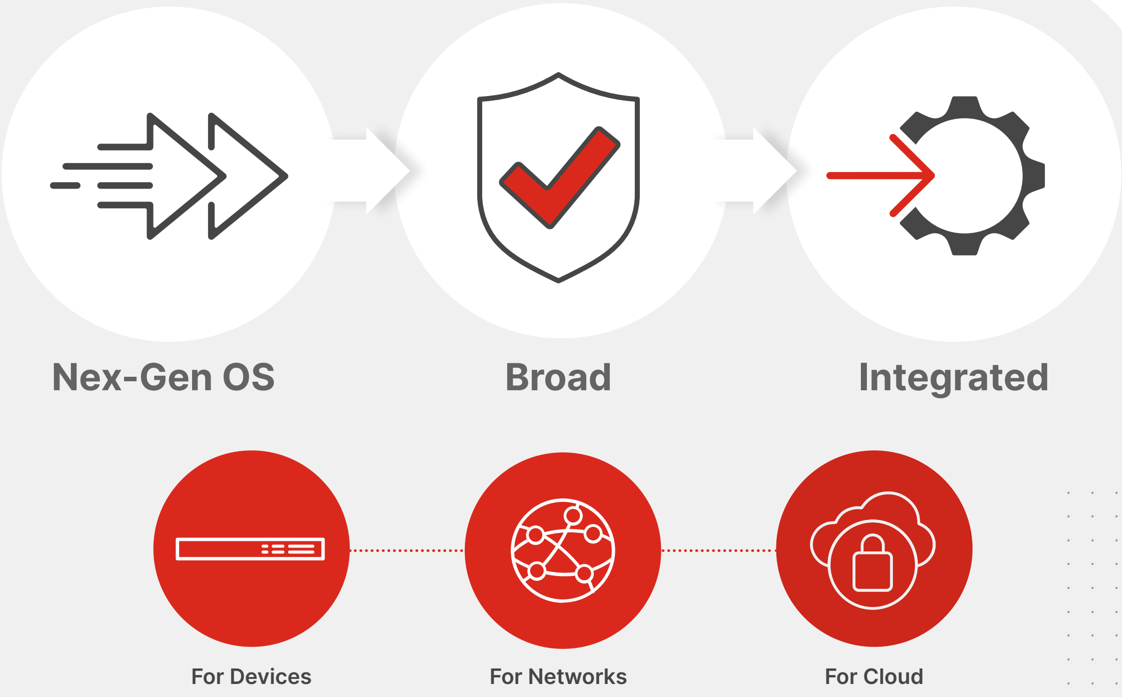
Data Sheet

Container FortiOS



Nex-Gen OS

Broad

Integrated

For Devices

For Networks

For Cloud

Highlights

NGFW

- Firewalling, Routing, NAT
- IPsec VPN

NGIPS

- Application control
- Antivirus
- Intrusion prevention
- Botnet protection
- Web filtering
- IPAM

CMDB

- Policy and automation engine
- Logging and reporting
- REST API

Consolidated Security for Container Platforms

Container technologies are rapidly expanding as an application infrastructure and services platform. However, the risks they introduce are often not adequately addressed by traditional security tools.

It is essential for organizations deploying applications and services on any container infrastructure, whether on a device, network, or cloud, to have access to a comprehensive security solution compatible with a broad range of container platforms and orchestration systems.

Container FortiOS (cFOS) provides enterprise-grade network security from FortiOS, tailored to suit the requirements of container platforms. With its lightweight and modular architecture, network administrators can efficiently deploy only the necessary network security functionalities for an application or service, reducing resource requirements and management complexity, thus ensuring the security of the business.

FortiOS Everywhere

cFOS is built upon FortiOS, designed in a form factor that can scale and deploy as and where needed to meet the requirements of container-based applications and services.

Device manufactures deploy containerized applications and services to rapidly and dynamically bring new products to market. Securing these products is critical to market competitiveness and business risk management. cFOS helps device manufacturers get to market faster with industry-grade security optimized to meet application requirements.

Telcos and service providers need to rapidly scale services during peak demand. Securing these services is critical to minimizing business risk. cFOS helps service providers scale and deploy security as and where needed at the speed of business.

Cloud services rapidly deploy new capabilities using cloud-native applications. Security capability optimized to protect new services and capabilities provides necessary protection while minimizing risk due to unnecessary complexity. cFOS helps digital businesses optimize security for new capabilities while minimizing risk to other services.

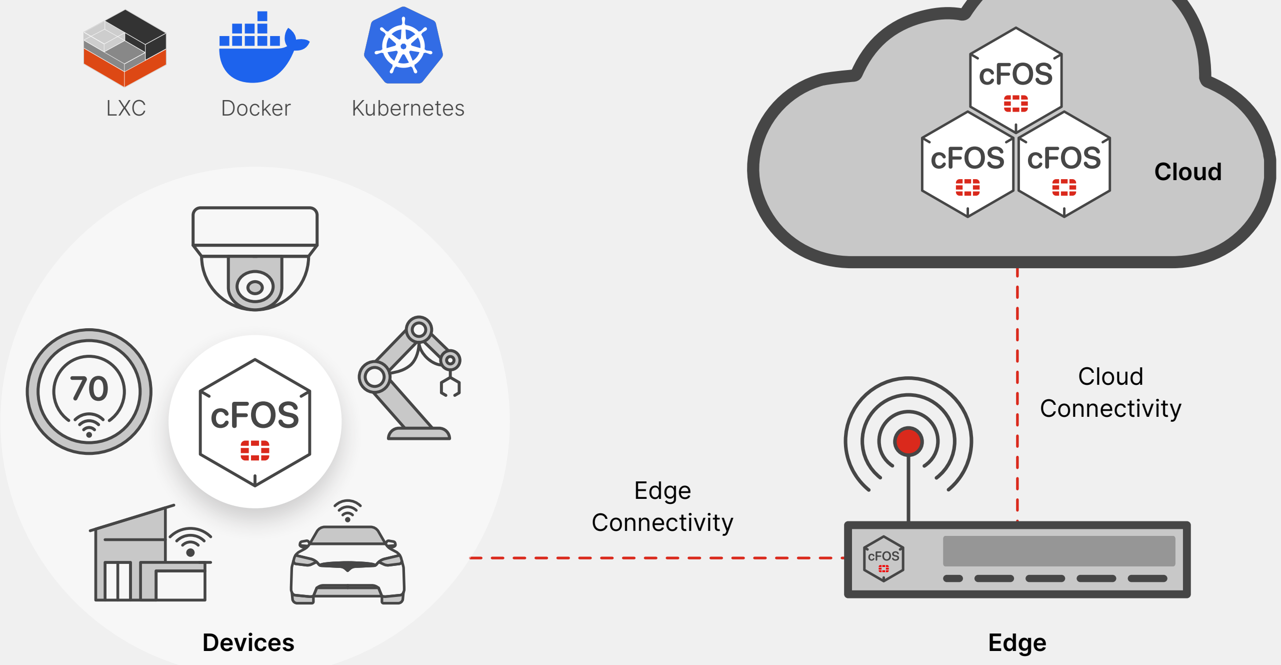
Available for:

LXC

Docker

Kubernetes

Deployment Architecture



Use Cases

Intrusion Prevention System

The intrusion prevention system (IPS) identifies, and blocks known malicious traffic from accessing critical or vulnerable systems within the network using deep packet inspection (DPI) and IPS signatures that are updated frequently throughout the day to include newly discovered threats.

Network Segmentation

Internal traffic can be segmented to ensure that permitted communication is allowed, while broadcast and multicast traffic are contained as appropriate.

Next-Generation Firewall

Traditional Layer 4 firewall capabilities block traffic between interfaces based on source or destination IP address and port. Furthermore, next-generation firewall (NGFW) deploys advanced security services.

SSL Inspection

SSL inspection can decrypt all encrypted traffic, providing other components of the security platform with complete visibility into network communications and preventing hackers from using encrypted SSL tunnels to deliver malware or steal data.

Virtual Patching

Virtual patching provides an immediate fix to address vulnerabilities that arise in container platforms. The IPS engine can prevent malicious traffic from exploiting the vulnerability, allowing OEMs and suppliers time to provide a software update.

Virtual Private Network

Secure communication between container platforms and external applications and services is ensured using IPsec VPN tunnels with high levels of encryption.

FortiGuard Services

Application Security

With FortiGuard Application Control, you can quickly create policies to allow, deny, or restrict access to applications or entire categories of applications running within the container platform. Application Control is available as part of the NGFW service in cFOS.

Botnet Protection

Block unauthorized attempts to communicate with compromised remote servers for both receiving malicious commands and extracting information. This prevents botnets and other threats from communicating with command & control servers to exfiltrate data or download malware.

Intrusion Prevention

With FortiGuard IPS Service deployed as part of your broader security infrastructure, cFOS can analyze the network traffic and deploy new intrusion prevention signatures in near real-time for coordinated network response.

Web Security

FortiGuard cloud-delivered web security services provide comprehensive protection to address threats including ransomware, credential-theft, phishing, spam, and other web-borne attacks.

FortiGuard Bundles

FortiGuard Labs delivers a number of security intelligence services to augment the FortiGate firewall platform. You can easily optimize the protection capabilities of your FortiGate with one of these FortiGuard Bundles.

Ordering Information

Product	SKU	Description
cFOS-vCPU01-S	FC1-10-CFOSV-<Support Bundle>-02-DD	Subscriptions license for Container FortiOS (1 vCPU core).
cFOS-vCPU02-S	FC2-10-CFOSV-<Support Bundle>-02-DD	Subscriptions license for Container FortiOS (2 vCPU core).
cFOS-vCPU04-S	FC3-10-CFOSV-<Support Bundle>-02-DD	Subscriptions license for Container FortiOS (4 vCPU core).
cFOS-vCPU08-S	FC4-10-CFOSV-<Support Bundle>-02-DD	Subscriptions license for Container FortiOS (8 vCPU core).
cFOS-vCPU16-S	FC5-10-CFOSV-<Support Bundle>-02-DD	Subscriptions license for Container FortiOS (16 vCPU core).
cFOS-vCPU32-S	FC6-10-CFOSV-<Support Bundle>-02-DD	Subscriptions license for Container FortiOS (32 vCPU core).
cFOS-vCPUUL-S	FC7-10-CFOSV-<Support Bundle>-02-DD	Subscriptions license for Container FortiOS (Unlimited vCPU core).

Note 1: The vCPU level is restricted at the OS-level in cFOS and based on the type of subscription license, required vCPU level will be enabled.
Note 2: Like FG-VM S-series, cFOS S-series doesn't have RAM restrictions on all vCPU levels.

Example of cFOS SKUs with service bundles for 1 vCPU		
Subscription License with Service Bundles for Container FortiOS **(1 vCPU)**	FC1-10-CFOSV-814-02-DD	Subscription license for Container FortiOS (1 vCPU) with Enterprise Bundle included.
	FC1-10-CFOSV-990-02-DD	Subscription license for Container FortiOS (1 vCPU) with UTP Bundle included.
	FC1-10-CFOSV-993-02-DD	Subscription license for Container FortiOS (1 vCPU) with ATP Bundle included.
	FC1-10-CFOSV-258-02-DD	Subscription license for Container FortiOS (1 vCPU) with only FortiCare included.

Note 1: DD is months for years 1, 3, and 5.

FortiCare Services

Fortinet prioritizes customer success through FortiCare Services, optimizing the Fortinet Security Fabric solution. Our comprehensive lifecycle services include Design, Deploy, Operate, Optimize, and Evolve. The FortiCare Elite, one of the service variants, offers heightened SLAs and swift issue resolution with a dedicated support team. This advanced support option includes an Extended End-of-Engineering-Support of 18 months, providing flexibility. Access the intuitive FortiCare Elite Portal for a unified view of device and security health, streamlining operational efficiency and maximizing Fortinet deployment performance.

Fortinet Corporate Social Responsibility Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy.

www.fortinet.com

June 18, 2024 11:30 AM

1234567-0-0-EN