Forcepoint

# Commercial Solutions for Classified Programs: Forcepoint NGFW

## Overview:

Federal agencies and contractors are increasingly turning to Commercial Solutions for Classified (CSfC) programs to secure sensitive and classified data. Forcepoint's Next-Generation Firewall (NGFW) solutions are ideally positioned to play a critical role in a CSfC solution, delivering robust security that meets the stringent compliance requirements necessary to protect classified information.

## What is CSfC?

The CSfC program, managed by the National Security Agency (NSA), enables agencies to use commercially available technologies in layered security solutions that meet the protection requirements for classified data. This program allows agencies to rapidly deploy secure communications without relying solely on costly, traditional government-approved solutions, while still maintaining the highest standards of data protection.

Forcepoint NGFW solutions provide a critical building block for secure, compliant CSfC implementations, ensuring that federal agencies and contractors can protect classified data while meeting the rigorous requirements set forth by the NSA. Forcepoint NGFW solutions enable organizations to deploy effective, future-proof security for their most sensitive data.

**Learn about the Forcepoint NGFW solution**

Read more about **CSfC programs**

## Why Forcepoint NGFW Matters in a CSfC Solution:

### FIPS FIPS 140-3 Compliance:

Forcepoint NGFW integratesFIPS 140-3 validated cryptographic modules, ensuring that sensitive government and defense data is securely encrypted both in transit and at rest.

### Comprehensive Data Protection:

Forcepoint NGFW combines advanced threat protection, application control and deep packet inspection with strong encryption capabilities to safeguard classified information.

### Layered Security Architecture:

As part of a CSfC solution, Forcepoint NGFWs integrate seamlessly with other commercial technologies, such as secure routers and endpoint protection, to form a layered defense architecture. This layered approach enhances resilience against advanced persistent threats (APTs) and sophisticated cyberattacks.

### Scalability and Flexibility:

Forcepoint NGFW solutions are highly scalable, enabling federal agencies and contractors to tailor their security posture to meet specific mission requirements. This flexibility is essential when deploying CSfC solutions across diverse environments and geographies.

### Operational Efficiency and Compliance Reporting:

Forcepoint's centralized management allows agencies to efficiently manage security policies, monitor traffic and generate compliance reports. This ensures that the solution helps maintain regulatory compliance and audit trails for CSfC certification.

### Zero Trust Access:

Forcepoint NGFW with VPN and Endpoint Context Agent enables Zero Trust Application Control, ensuring secure, context-aware access. By enforcing strict policies and real-time device intelligence, it supports Zero Trust Network Access, protecting sensitive data and reducing risks across the network.

forcepoint.com/contact