

# Solutions commerciales pour les agences gouvernementales : Forcepoint NGFW

## Vue d'ensemble:

Les agences fédérales et les sous-traitants se tournent de plus en plus vers les programmes Commercial Solutions for Classified (CSfC) pour sécuriser les données sensibles et classifiées. Les solutions NGFW (Next-Generation Firewall) de Forcepoint sont idéalement positionnées pour jouer un rôle essentiel dans une solution CSfC, en offrant une sécurité robuste qui répond aux exigences de conformité strictes nécessaires pour protéger les informations classifiées.

## Qu'est-ce que CSfC?

Le programme CSfC, géré par la National Security Agency (NSA) aux Etats Unis, permet aux agences d'utiliser les technologies commerciales disponibles dans des solutions de sécurité en couches qui répondent aux exigences de protection des données classées confidentielles. Ce programme permet aux agences de déployer rapidement des communications sécurisées sans dépendre uniquement des solutions coûteuses et traditionnelles approuvées par le gouvernement, tout en maintenant les normes les plus élevées de protection des données.

Les solutions Forcepoint NGFW fournissent une composante essentielle pour des mises en œuvre CSfC sécurisées et conformes, garantissant que les agences fédérales et les sous-traitants peuvent protéger les données classifiées tout en répondant aux exigences rigoureuses établies par la NSA. Les solutions Forcepoint NGFW permettent aux organisations de déployer une sécurité efficace et pérenne pour leurs données les plus sensibles.

**En savoir plus sur la solution Forcepoint NGFW**  
En savoir plus sur les **programmes CSfC**

## Pourquoi Forcepoint NGFW est important dans une solution CSfC:

### Conformité FIPS FIPS 140-3:

Forcepoint NGFW intègre des modules cryptographiques validés FIPS 140-3, garantissant que les données sensibles du gouvernement et de la défense sont chiffrées en toute sécurité, à la fois en transit et stockées.

### Protection complète des données :

Forcepoint NGFW combinent une protection contre les menaces avancées, le contrôle des applications et l'inspection approfondie des paquets avec de fortes capacités de chiffrement pour sauvegarder les informations classifiées.

### Architecture de sécurité en couches :

Dans le cadre d'une solution CSfC, les pare-feux NGFW de Forcepoint s'intègrent parfaitement à d'autres technologies commerciales, telles que les routeurs sécurisés et la protection des terminaux, pour former une architecture de défense en couches. Cette approche en couches améliore la résilience contre les menaces persistantes avancées (APT) et les cyberattaques sophistiquées.

### Évolutivité et flexibilité :

Les solutions Forcepoint NGFW sont hautement évolutives, permettant aux agences fédérales et aux entrepreneurs d'adapter leur posture de sécurité pour répondre aux exigences spécifiques de leur mission. Cette flexibilité est essentielle lors du déploiement de solutions CSfC dans divers environnements et régions.

### Rapports sur l'efficacité opérationnelle et la conformité :

La gestion centralisée de Forcepoint permet aux agences de gérer efficacement les politiques de sécurité, de surveiller le trafic et de générer des rapports de conformité. Cela permet de s'assurer que la solution contribue à maintenir la conformité réglementaire et les pistes d'audit pour la certification CSfC.

### Accès Zero Trust :

Forcepoint NGFW avec VPN et Endpoint Context Agent permet un contrôle d'application Zero Trust et assure un accès sécurisé et contextuel. En appliquant des politiques strictes et des informations en temps réel sur les appareils, il prend en charge le Zero Trust Network Access, protégeant les données sensibles et réduisant les risques sur l'ensemble du réseau.