# Renforcer la défense à l'aide d'une plateforme unifiée

**Principaux avantages :**

- Résilience complète du cœur stratégique à la périphérie tactique
- Plateforme cohérente pour les applications essentielles dans les environnements déconnectés
- Approche unifiée de l'autonomie et de la sécurité

## Combler les lacunes en matière de résilience, du cœur stratégique à la périphérie tactique

Les organismes publics de défense font face à un enjeu crucial : assurer la fiabilité de l'exploitation dans l'ensemble de l'environnement, du cœur stratégique à la périphérie tactique. Ce besoin essentiel d'agilité, de sécurité et d'autonomie stratégique accélère la transformation du secteur de la défense. Les organismes évoluent et remplacent leurs datacenters traditionnels et centralisés par des architectures hautement distribuées et adaptées à leur mission. Ils doivent opérer une transformation profonde pour parvenir à la maîtrise des décisions, c'est-à-dire la capacité pour tous les décisionnaires d'identifier, de comprendre, de décider et d'agir plus rapidement que tous les adversaires dans tous les domaines.

### L'importance de la résilience opérationnelle de bout en bout

Les missions modernes passent par le cloud hybride, qui englobe des clouds privés air gap, des mini-datacenters déployés ainsi que des appareils tactiques renforcés tels que des drones et des systèmes embarqués. L'architecture est essentielle pour exécuter des opérations multidomaines qui exigent une intégration et une coordination complexes des ressources dans les airs, sur terre, en mer, dans l'espace, dans le cyberespace ainsi que dans le champ électromagnétique.

Cependant, l'expansion des domaines crée également des vulnérabilités critiques et accroît considérablement la complexité technique. Les technologies isolées et les environnements disparates peuvent nuire à la continuité de l'exploitation, tandis que les menaces de sécurité se multiplient sur une vaste surface d'attaque. La dépendance vis-à-vis d'une connectivité permanente représente un sérieux point de défaillance. Dans les environnements soumis à des contraintes, les appareils d'edge computing doivent fonctionner de manière autonome et synchroniser les données uniquement lorsque des liens intermittents et fiables sont disponibles. Le principal défi consiste à atteindre une véritable résilience de bout en bout. La souveraineté dans un datacenter centralisé ne suffit pas si la périphérie tactique n'est pas en mesure de fonctionner de manière indépendante.

## Les principaux défis de la transformation numérique dans le secteur de la défense

Bien que l'infrastructure hybride offre une flexibilité indéniable, les organismes de défense rencontrent plusieurs obstacles majeurs au cours de leur transformation numérique :

- **Cyberattaques :** les organismes de défense sont particulièrement préoccupés par la menace croissante que représentent les chaînes d'approvisionnement sophistiquées et les cyberattaques. Par exemple, il est possible de compromettre la sécurité de flottes entières de drones ou de véhicules en injectant du code malveillant dans des bibliothèques Open Source. De même, les attaques de type « homme du milieu » (ou MitM pour « man-in-the-middle » en anglais) peuvent altérer les mises à jour de micrologiciels en transit vers des appareils stratégiques, et ainsi potentiellement saboter d'importantes missions.
- **Structures technologiques isolées :** les différents environnements (datacenter, cloud et périphérie) reposent souvent sur des piles technologiques incompatibles. Cette incompatibilité oblige les entreprises à recréer des solutions pour chaque déploiement, une approche qui entraîne une fragmentation des outils. En conséquence, les troupes et les équipes d'ingénierie doivent maîtriser plusieurs plateformes, comme Amazon Web Services (AWS), Microsoft Azure ou des systèmes d'exploitation tactiques spécialisés, ce qui ralentit considérablement la préparation aux missions.
- **Complexité :** l'utilisation de processus manuels engendre naturellement une augmentation de la complexité. Par exemple, le déplacement de données entre le datacenter et la périphérie du réseau nécessite des workflows personnalisés, ce qui rallonge les délais de déploiement. En parallèle, les modèles de sécurité traditionnels peinent à s'adapter aux architectures distribuées et laissent des failles critiques que des adversaires pourraient exploiter.

## Adopter une approche unifiée

Les organismes de défense ont besoin de toute urgence d'une structure ouverte et unifiée, qui renforce l'autonomie et la sécurité à tous les niveaux. La solution idéale est une plateforme cohérente pour exécuter les applications essentielles dans un cloud privé, traiter les charges de travail d'IA à la périphérie du réseau et prendre des décisions en temps réel concernant les appareils d'edge computing sur le terrain. La véritable résilience moderne repose sur la capacité à opérer en assurant une intégrité à toute épreuve, dans tous les environnements.

## Nos solutions

Les organismes de défense ont besoin d'une base unifiée et d'un conseiller de confiance pour réunifier leur espace numérique fragmenté et garantir la résilience du cœur stratégique à la périphérie tactique. Chez Red Hat, nous proposons cette plateforme essentielle et cohérente. Grâce à notre approche « déployer une fois, exécuter partout », nous accélérons la préparation aux missions et offrons aux équipes des outils familiers dans tous les environnements. En plus de fournir une expérience cohérente, nos solutions sont basées sur des normes ouvertes. La plateforme évite toute dépendance vis-à-vis d'un fournisseur et améliore les intégrations grâce à une solution évolutive et flexible.

**Sécurité de niveau militaire :** nous intégrons des normes de sécurité renforcées en veillant à ce que nos plateformes de base, telles que Red Hat® OpenShift®, respectent des normes de conformité strictes. La gamme de produits Red Hat Trusted Software Supply Chain assure la sécurité en permanence, grâce à une approche globale et continue. Elle intègre des pratiques DevSecOps pour renforcer la chaîne de contrôle et garantir le respect des normes officielles en matière de sécurité, de conformité, de confidentialité et de transparence.

**Souveraineté de l'assurance :** l'attestation de chiffrement permet de vérifier que le micrologiciel et les mises à jour critiques n'ont pas été modifiés, et d'assurer dans le même temps la souveraineté de l'assurance. Ce processus garantit l'intégrité et la fiabilité des systèmes numériques. Il fait partie intégrante de notre stratégie de plateforme qui vise à valider la chaîne d'approvisionnement des logiciels et à réduire le risque d'injection de code malveillant.

**Automatisation déconnectée :** l'automatisation déconnectée s'intègre aux processus déjà en place et permet d'appliquer des correctifs aux appareils sur le terrain sans connexion à Internet. Avec Red Hat Ansible® Automation Platform, les organismes peuvent mettre en œuvre une exploitation fiable et autonome pour une défense moderne. Cette plateforme permet de gérer les appareils confrontés à des problèmes de réseau (refus, déconnexion, intermittence et faible bande passante) sans dépendre d'une connectivité externe vulnérable. Cette autonomie protège l'investissement à long terme dans les ressources logicielles déployées, minimise les risques de sécurité associés à des injections de code malveillant et garantit la continuité des missions importantes lorsqu'il est impossible de recevoir une aide extérieure.

Au niveau du datacenter, les solutions fiables telles que Red Hat OpenShift offrent une infrastructure souveraine et évolutive. À la périphérie du réseau, les clusters OpenShift compacts traitent les charges de travail de renseignement et d'intelligence artificielle (IA) essentielles. Sur le terrain, la solution légère Red Hat Device Edge permet d'effectuer des opérations déconnectées et ultraportables sur des systèmes renforcés.

## Cas d'utilisation éprouvés dans le secteur de la défense

Plusieurs organismes de défense ont réussi à mettre en œuvre des solutions Red Hat pour relever d'importants défis liés à l'exploitation et réaliser des avancées significatives.

**Optimisation des opérations sur le terrain :** l'armée de l'air d'un pays européen subissait d'incessantes interruptions causées par des pannes de réseau lors de ses opérations sur le terrain. Avec la mise en œuvre de Red Hat OpenShift dans des datacenters portables d'edge computing, son service informatique a adopté des fonctionnalités de traitement de l'IA en local qui ont permis d'assurer la continuité des opérations quel que soit l'état de la connectivité, tout en réduisant considérablement les besoins en matière de bande passante.

**Mises à jour logicielles en vol pour les systèmes aériens sans pilote :** un grand sous-traitant de la défense a démontré sa capacité à effectuer des mises à jour logicielles en vol sur des systèmes aériens sans pilote. Avec Red Hat Device Edge, cette entreprise est parvenue à déployer des mises à niveau du modèle d'IA sur des drones en cours de mission, améliorant ainsi les capacités de reconnaissance de cible en temps réel, le tout, sans interruption de mission ni temps d'arrêt du système.

**Accélération de l'infrastructure et du déploiement :** un organisme de défense nationale a obtenu des gains d'efficacité considérables en automatisant ses processus PaaS (Platform-as-a-Service) à l'aide des solutions Ansible Automation Platform et Red Hat OpenShift. Les délais de déploiement de l'infrastructure ont été réduits de plusieurs semaines à 24 heures seulement, la rendant ainsi prête pour les opérations de combat. En parallèle, sa capacité de développement a été multipliée par quatre en un an, tout en respectant des protocoles de sécurité stricts.

## Pour se lancer

Contactez un représentant Red Hat pour découvrir comment protéger vos systèmes de défense, du datacenter à la périphérie du réseau.

### À propos de Red Hat

Red Hat aide ses clients à standardiser leurs environnements, à développer des applications cloud-native et à intégrer, automatiser, sécuriser et gérer des environnements complexes en offrant des services d'assistance, de formation et de consulting primés.

facebook.com/redhatinc
@RedHatFrance
linkedin.com/company/red-hat

**EUROPE, MOYEN-ORIENT ET AFRIQUE (EMEA)**
00800 7334 2835
europe@redhat.com

**FRANCE**
00 33 1 41 91 23 23
fr.redhat.com

fr.redhat.com
#3134353_1225