Mission edge

Comment Red Hat peut aider le département de la Défense des États-Unis à accomplir plus vite ses missions

Red Hat

Sommaire

Introduction
Un changement radical du modèle informatique

Chapitre 1
L'atout militaire de la prise de décision stratégique

Chapitre 2
La mise en œuvre de la résilience

Chapitre 3
L'importance de l'interconnexion

Chapitre 4
Le partage des données : obtenir des renseignements utiles

Chapitre 5
L'approche de Red Hat pour l'edge computing appliqué aux missions

Pour en savoir plus

Introduction

Un changement radical du modèle informatique

Les divisions et services du département de la Défense des États-Unis utilisent des données opérationnelles et générées par les utilisateurs pour prendre des décisions stratégiques, résoudre les problèmes et garder le contrôle sur l'espace de bataille moderne. Les troupes actuelles doivent cependant composer avec l'évolution des méthodes de collecte, de partage et d'utilisation de ces données.

Pour intégrer et coordonner les processus de commande et de contrôle sur terre, en mer, dans les airs, l'espace et le cyberespace, les capacités numériques ne peuvent plus se limiter aux datacenters et aux environnements cloud traditionnels. Les équipes, les machines et les technologies qui en ont besoin doivent aussi y avoir accès à la périphérie du réseau.

Le département de la Défense des États-Unis est confronté à de nouveaux adversaires aux capacités comparables, qui émergent malgré les difficultés relatives à la distance, à l'océan, au temps et à l'échelle qui caractérisent le théâtre des opérations de l'USINDOPACOM (United States Indo-Pacific Command). Pour relever ces défis et affronter les adversaires de tous les théâtres, le département de la Défense a besoin de solutions qui offrent certaines possibilités :

Innover avec agilité

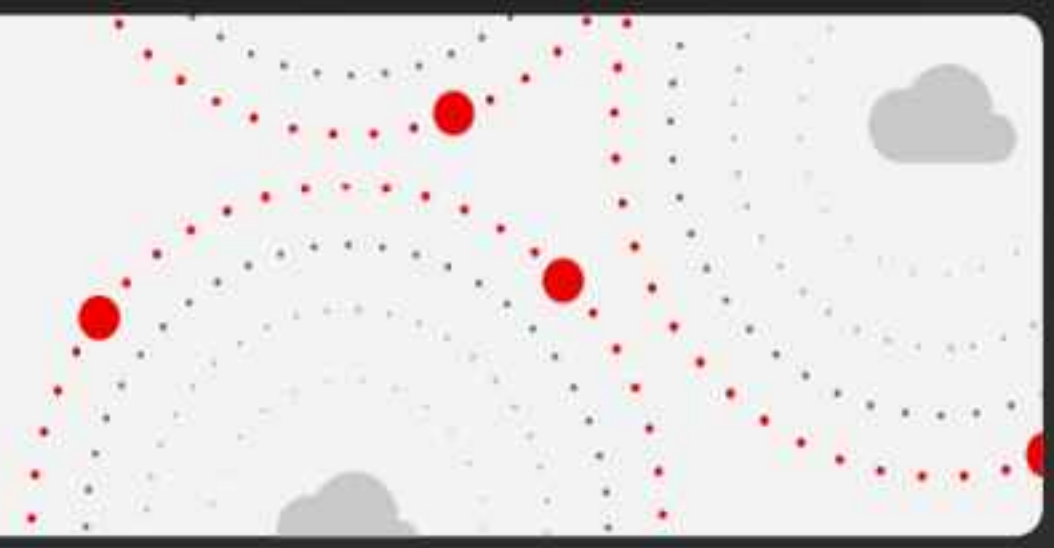
Conserver une posture de sécurité forte

Standardiser l'interopérabilité entre les divisions et les services

Exploiter les données

Garantir la préparation opérationnelle dans le cyberespace

L'objectif est de pouvoir agir plus vite, à moindre risque. L'approche Mission Edge, ou edge computing appliqué aux missions, est la clé pour y parvenir et accomplir plus facilement les missions au sein du département de la Défense des États-Unis. Elle repose sur une architecture informatique dynamique et décentralisée, composée d'équipements matériels et de charges de travail hétérogènes, qui relie les producteurs et les consommateurs de données.



Une nouvelle approche informatique pour l'espace de bataille moderne

Les systèmes de défense traditionnels sont à l'origine de systèmes monolithiques uniques et propres à un domaine que l'on retrouve dans la plupart des espaces de bataille classiques. En parallèle, les adversaires des États-Unis aux capacités quasi comparables bénéficient eux aussi des progrès technologiques. Aujourd'hui, l'enjeu est de réaliser l'intégration complexe des systèmes nécessaires pour coordonner, assurer et renforcer la sécurité de l'exploitation dans tous les domaines, et en particulier à la périphérie du réseau.

Toute stratégie de modernisation doit prendre en compte les environnements d'edge computing suivants :

Périphérie de l'entreprise : toutes les capacités que l'entreprise fournit à l'utilisateur via des environnements réseau et d'applications modernisés, standardisés et sécurisés. Il peut s'agir de la formation des militaires et du personnel de maintenance pour les déploiements tactiques.

Périphérie de l'exploitation : réseaux locaux d'appareils intelligents qui interagissent, offrant ainsi des capacités essentielles telles que la surveillance et le contrôle des processus, l'analyse prédictive et l'optimisation de la chaîne d'approvisionnement. Par exemple, lors de la fabrication d'un avion de combat F-35, chaque composant est équipé d'un dispositif de radio-identification qui est analysé, puis placé sur l'avion en production afin d'assurer un contrôle qualité maximal.

Périphérie du fournisseur : rapprochement entre le traitement informatique et l'utilisateur afin de limiter, voire d'éliminer les nombreux transferts d'informations aux datacenters, tels que l'AOC (Air Operations Center) et le DCGS (Distributed Common Ground System).

Périphérie des interactions : systèmes informatiques distribués dans le monde entier qui permettent aux utilisateurs d'interagir avec les applications. Dans le cadre d'une opération militaire, il peut s'agir de l'accès en temps réel aux données dont les troupes ont besoin pour prendre les meilleures décisions tactiques sur le champ de bataille.

Ces définitions peuvent aider à identifier les besoins à la périphérie du réseau pour accomplir les missions du département de la Défense des États-Unis.

Avec une approche de cloud hybride et des solutions complètes, Red Hat contribue non seulement à la modernisation des déploiements, mais aussi à la réalisation des objectifs du département de la Défense tout au long du processus. Plus précisément, Red Hat fournit une expertise et des technologies qui permettent de moderniser la prise de décision décentralisée, de renforcer la résilience des processus d'exploitation, ainsi que d'améliorer l'interconnexion et le partage des données.

Chapitre 1

L'atout militaire de la prise de décision stratégique

La réussite des missions repose sur l'utilisation de données de qualité qui permettent d'accéder en toute confiance à des informations fiables et pertinentes. Même si les données ont récemment été placées au centre de l'attention dans le secteur de la défense, elles s'inscrivent dans une stratégie plus large. Il est essentiel de transformer plus rapidement les données en informations exploitables pour rivaliser avec des adversaires aux capacités quasi comparables. Trois capacités sont au cœur de la prise de décision stratégique : la disponibilité des données, la prise de décision distribuée et l'interconnexion.

À mesure que les appareils connectés deviennent plus performants et plus présents, ils complexifient les réseaux connectés. La prise de décision décentralisée s'impose pour renforcer la résilience des processus d'exploitation tout en améliorant l'interconnexion et le partage de données. Cette pratique pose toutefois un certain nombre de défis.

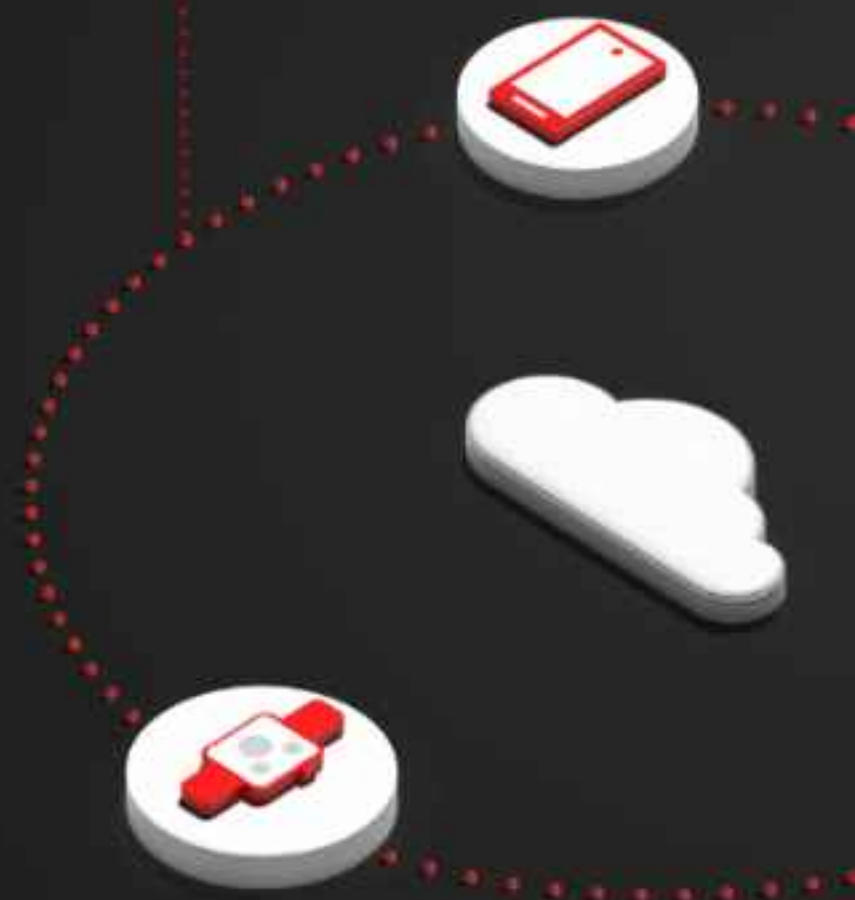
L'amélioration de la disponibilité, de la visibilité et de l'incidence des données

Les opérations multidomaines (MDO) et les initiatives technologiques, telles que l'approche CJADC2 (Combined Joint All-Domain Command and Control), permettent déjà au département de la Défense d'améliorer la disponibilité et l'intégration des données dans et entre les systèmes des différents services et partenaires.

Le développement de capacités MDO sur la base d'une architecture de cloud hybride et d'edge computing assure résilience, dynamisme, rapidité et efficacité lors de la distribution et de la gestion des charges de travail volumineuses issues d'un événement de convergence. Une infrastructure de cloud hybride et d'edge computing offre l'élasticité et la résilience nécessaires pour gérer le volume et la vitesse des données quand un tel événement a lieu.

Principaux défis liés à la prise de décision décentralisée :

- Les systèmes d'edge computing sont souvent difficiles d'accès et disposent d'une bande passante limitée.
- L'adoption d'une approche axée sur les logiciels s'avère complexe.
- Il convient de respecter des exigences Zero Trust, car l'isolement n'est plus une mesure de sécurité adaptée à la protection contre les menaces internes et externes.
- Pour relever ces défis, il faut notamment mettre en œuvre une stratégie de sécurité renforcée dans l'ensemble du cyberespace, afin de garantir l'authentification et la vérification de chaque appareil ou utilisateur en permanence. C'est ce qui permet au département de la Défense des États-Unis de mieux préparer l'ensemble de ses systèmes à toute éventualité.



Les principaux aspects d'une architecture de cloud hybride et d'edge computing

Normes ouvertes

L'utilisation de normes Open Source garantit la richesse des solutions et leur interopérabilité, et favorise la collaboration et l'innovation.

Réseaux tactiques

Toute convergence MDO nécessite des réseaux tactiques, tels que les capteurs, l'Internet des objets militaires et les réseaux 5G, afin de faciliter la transmission et l'extraction de données par des milliers d'appareils sur le champ de bataille.

Automatisation

Des processus automatisés d'ajout et de suppression des ressources offrent une reproductibilité cohérente pour ajouter et supprimer rapidement des capacités et des fonctions à la demande dans une zone de service.

Intégration agile

Compte tenu de la variété des données que les ressources MDO produisent et consomment, l'intégration agile permet d'extraire des renseignements basés sur la véracité et la valeur des données via des architectures de microservices orientées événements, dans le but d'alimenter la prise de décision des équipes et de l'intelligence artificielle (IA).

Gestion des données

Toutes les informations dépendent de l'analyse et de l'inférence des données. Les ressources mises à disposition varient d'une rencontre à l'autre. La gestion et l'intégration des systèmes doivent donc être suffisamment flexibles pour s'adapter à la nature dynamique des ressources disponibles.

Intelligence artificielle

L'IA représente un avantage vital pour la prise de décision stratégique. L'assistance d'un ordinateur allège la charge de travail de plus en plus lourde qui incombe aux décideurs pour extraire, classer et organiser des informations à partir des très nombreuses données produites dans l'espace de bataille. L'approche Mission Edge facilite considérablement la gestion du cycle complet de développement logiciel pour les charges de travail d'IA et d'apprentissage automatique (AA).

Exigences en matière de prise de décision stratégique

Pour faire reposer la prise de décision stratégique sur les fonctions CJADC2 dans tous les domaines, il convient de recourir à des conseils de planification, aux avancées du secteur et aux technologies modernisées qui utilisent et combinent des données nouvelles et existantes tout en adaptant les solutions commerciales aux exigences proprement militaires.

Chapitre 2

La mise en œuvre de la résilience

L'objectif des opérations multidomaines est de rassembler simultanément diverses ressources sur terre, en mer, dans les airs, l'espace et le cyberespace pour former une convergence, une fenêtre de capacité maximale servant à entraver la réponse de l'adversaire. Plus élevée que jamais, la demande de données et de charges de travail sur plusieurs appareils et ressources présente cinq caractéristiques clés, les « 5 V » :

Volume

Plus le nombre de ressources impliquées est élevé, plus le volume des données augmente à mesure que de nouveaux producteurs et consommateurs de données interviennent.

Variété

Ces ressources appartiennent à différents domaines et se concentrent sur différentes informations, ce qui augmente la variété des données produites et consommées.

Vitesse

Une fois la convergence atteinte, le nombre de producteurs et de consommateurs de données va connaître un pic, et la quantité de données que chaque ressource produit ou utilise va augmenter, accélérant ainsi le flux de données.

Véracité

La véracité des données devient de plus en plus essentielle à mesure de l'évolution de la convergence. Les données doivent être non seulement authentiques, mais aussi pertinentes et exploitables.

Valeur

La valeur des données dépend de leur véracité, de leur volume et de leur vitesse au moment de la prise de décision.

L'espace de bataille MDO est dynamique. Chaque mission est unique, et différentes ressources sont déployées selon les rencontres. La gestion et l'intégration des systèmes doivent donc être suffisamment flexibles pour s'adapter à la nature dynamique des ressources disponibles pour chaque bataille.

Un événement de convergence dans un théâtre d'opérations peut entraîner la production et la consommation de données par des milliers de ressources, notamment des capteurs embarqués, des systèmes satellites, ainsi que des cyberopérations offensives et défensives. Toutes ces données peuvent représenter un atout puissant pour les officiers, qui doivent ensuite les comprendre et agir en conséquence. Cependant, les systèmes traditionnels de communication sur le terrain ne sont pas capables de traiter le volume de données transmises et n'offrent donc pas la possibilité de fonder les choix de mission sur les données.

Les demandes de convergence MDO devront probablement s'appuyer sur des communications via le réseau 5G pour faciliter la transmission et l'extraction des données à partir des milliers d'appareils sur le champ de bataille.

À titre de comparaison, les grands événements sportifs qui accueillent des dizaines de milliers de passionnés, comme la Coupe du monde de football ou les Jeux olympiques, génèrent d'importants volumes de données dans un espace et un délai limités. Les opérateurs de télécommunications se préparent à ces événements en augmentant le nombre de ressources pour gérer l'intensification du trafic. Ils peuvent évoluer à la demande, car ils disposent d'une infrastructure basée sur une architecture extensible de cloud hybride et d'edge computing. Cette architecture fait toutefois partie d'un ensemble plus vaste. Pour évoluer rapidement et dynamiquement à la périphérie du réseau, il faut recourir à l'automatisation.

L'automatisation à la périphérie du réseau pour les missions

En adoptant une approche axée sur l'automatisation, les opérateurs de télécommunications peuvent ajouter et supprimer des ressources sans perdre en reproductibilité ni en rapidité. L'automatisation permet d'apporter des changements simples et reproductibles qui augmentent la flexibilité et la capacité. Si chacune de ces instances nécessitait une intervention manuelle, la capacité ne pourrait pas évoluer assez rapidement. De plus, la mise en œuvre de chaque intervention entraînerait des irrégularités et des erreurs.

Grâce au développement de capacités MDO sur une architecture de cloud hybride et d'edge computing, le département de la Défense des États-Unis bénéficie d'un haut niveau de résilience, de dynamisme et d'efficacité lors de la distribution et de la gestion des charges de travail volumineuses issues d'un événement de convergence.

L'automatisation pour mieux préparer les systèmes informatiques

L'intégration de l'automatisation dans les stratégies de préparation des systèmes informatiques permet au département de la Défense de sécuriser davantage les systèmes d'information, de réduire les surfaces d'attaque et de consolider les défenses. En outre, les capacités avancées des outils d'automatisation peuvent favoriser le bon déroulement des missions en veillant à la préparation opérationnelle et à l'adaptation continues aux nouvelles menaces dès leur apparition. Cette approche permet de maintenir une posture de sécurité plus robuste, avec à la clé une prise de décision améliorée ainsi que des processus de commande et de contrôle plus efficaces.

L'automatisation offre plusieurs moyens d'améliorer la préparation des systèmes informatiques :

Renforcement de l'efficacité pour détecter les menaces et y répondre
Automatiser la détection des menaces en temps réel pour y réagir et limiter les effets des attaques

Cohérence dans la sécurité de l'exploitation
Appliquer les protocoles de sécurité de manière uniforme, en limitant les erreurs humaines et les écarts de politiques

Évolutivité des opérations de sécurité
Compléter les capacités de sécurité efficacement pour répondre à l'évolution des besoins de l'entreprise

Réduction du nombre d'erreurs humaines
Atténuer les risques de failles dues aux erreurs manuelles

Amélioration de la surveillance de la conformité
Gérer et documenter systématiquement le respect des politiques, les demandes de tâches numériques et les évaluations de la préparation

Amélioration de la gestion des incidents
Réagir rapidement aux incidents et obtenir des informations détaillées pour une résolution plus rapide

Optimisation des ressources
Aider les équipes, notamment de défense et de cybersécurité, à concentrer leur attention sur les tâches d'exploitation stratégiques et l'innovation

Chapitre 3

L'importance de l'interconnexion

La périphérie du réseau ne correspond pas à un seul endroit bien précis. Elle se compose de systèmes et d'appareils interconnectés qui produisent et consomment des données de façon dynamique. Le flux de ces données détermine l'efficacité de l'exploitation. S'il est essentiel de recueillir des informations complètes sur les conditions en constante évolution d'un espace de bataille, la grande quantité de données à traiter et à analyser fait apparaître d'importants obstacles. Des difficultés se posent notamment lorsqu'il faut prendre des décisions critiques dans une situation d'urgence sur le champ de bataille.

Pour relever ce défi, l'approche C.JADC2 exploite des flux de données toujours plus nombreux et disparates dans tous les domaines, fournit des informations utiles grâce à des processus automatisés et basés sur l'IA, et présente les résultats aux troupes plus rapidement que jamais. L'objectif global est d'aider le département de la Défense des États-Unis à recueillir et comprendre les données, puis à agir en conséquence pour bénéficier d'un avantage et prendre des décisions stratégiques.

Par exemple, les technologies spatiales offrent un atout considérable en matière de communication, de reconnaissance et de navigation, des capacités essentielles pour les opérations militaires mondiales en temps réel. L'interopérabilité entre en jeu dans chaque aspect d'une mission, qu'il s'agisse du déploiement de satellites destinés à la sécurité des communications, de systèmes de géolocalisation précis, ou de capacités de surveillance pour détecter des menaces à grande distance.

Pour atteindre le niveau de rapidité, de stabilité et d'évolutivité nécessaire à la périphérie du réseau, il faut :

Obtenir des informations utiles en accélérant la prise de décision éclairée à la périphérie du réseau

La transmission des données depuis la périphérie tactique en vue de leur traitement entraîne beaucoup de retards. Lorsque les renseignements exploitables sont finalement renvoyés, la situation peut avoir complètement changé. Pour tirer parti des informations, il faut prendre des décisions au plus vite, directement à la périphérie du réseau.

Réduire le temps nécessaire pour observer, orienter, décider et agir

L'accélération de la prise de décision permet aux troupes de passer à l'action sans laisser le temps à l'adversaire d'analyser la situation et d'y réagir. L'idée est de prendre de meilleures décisions plus rapidement. Les troupes peuvent rassembler et comprendre les informations, puis agir en conséquence au plus vite grâce à une approche MOSA (Modular Open Systems Approach) appliquée à l'edge computing et à la science des données.

Assurer la disponibilité continue des données

De nombreux ordinateurs tactiques sont réservés à un but précis. Par exemple, si l'un des deux ordinateurs est détruit dans un tank, l'autre ne peut pas le remplacer. Pour continuer de prendre les décisions qui s'imposent, les troupes doivent être en mesure de réorienter les capacités de mission de tout ordinateur.

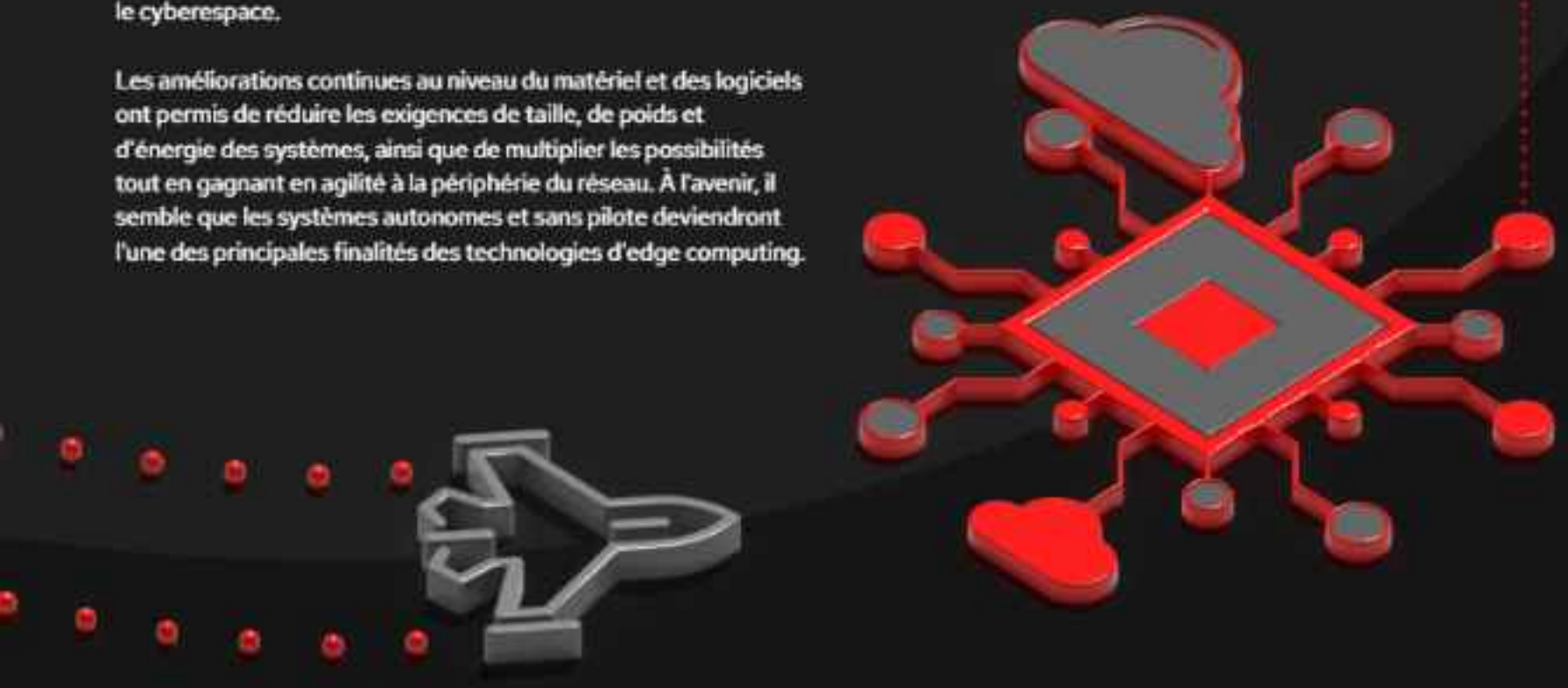
Partager les capacités d'IA et d'AA entre les forces

Aujourd'hui, chaque équipe chargée des systèmes de combat et des applications de mission développe des capacités logicielles sur mesure. Il en résulte des applications non interopérables et des doublons. Avec une interface de partage pour les capacités telles que les modèles d'AA et les algorithmes d'IA (sans divulgation d'autres propriétés intellectuelles), les troupes peuvent prendre de meilleures décisions.

Davantage d'innovation dans tous les domaines grâce à l'IA

En transformant les véhicules sans pilote et les outils de terrain, les technologies d'IA et d'AA améliorent les capacités dans tous les domaines, notamment dans les airs, sur terre, en mer et dans le cyberespace.

Les améliorations continues au niveau du matériel et des logiciels ont permis de réduire les exigences de taille, de poids et d'énergie des systèmes, ainsi que de multiplier les possibilités tout en gagnant en agilité à la périphérie du réseau. À l'avenir, il semble que les systèmes autonomes et sans pilote deviendront l'une des principales finalités des technologies d'edge computing.



Le renforcement de l'interconnexion au sein du département de la Défense concerne plusieurs domaines :

Gestion de flotte
L'IA peut optimiser le déploiement, la maintenance et l'acheminement des flottes militaires, notamment les avions, les navires et les véhicules, et améliorer ainsi l'efficacité et la préparation logistiques.

Entretien préventif
En analysant les données des capteurs et des journaux d'utilisation, il est possible de prévoir les pannes d'équipements avant qu'elles se produisent, ce qui contribue à réduire les temps d'arrêt et à prolonger la durée de vie du matériel militaire.

Surveillance et reconnaissance
Les systèmes basés sur l'IA peuvent surveiller de manière autonome de vastes zones à l'aide de véhicules sans pilote, tels que des drones et des satellites. Ils identifient les changements et les menaces avec plus de précision et de rapidité.

Cyberdéfense
L'utilisation d'algorithmes d'IA pour surveiller, détecter et traiter les cybermenaces en temps réel aide à protéger l'infrastructure et les données essentielles contre des attaques toujours plus sophistiquées.

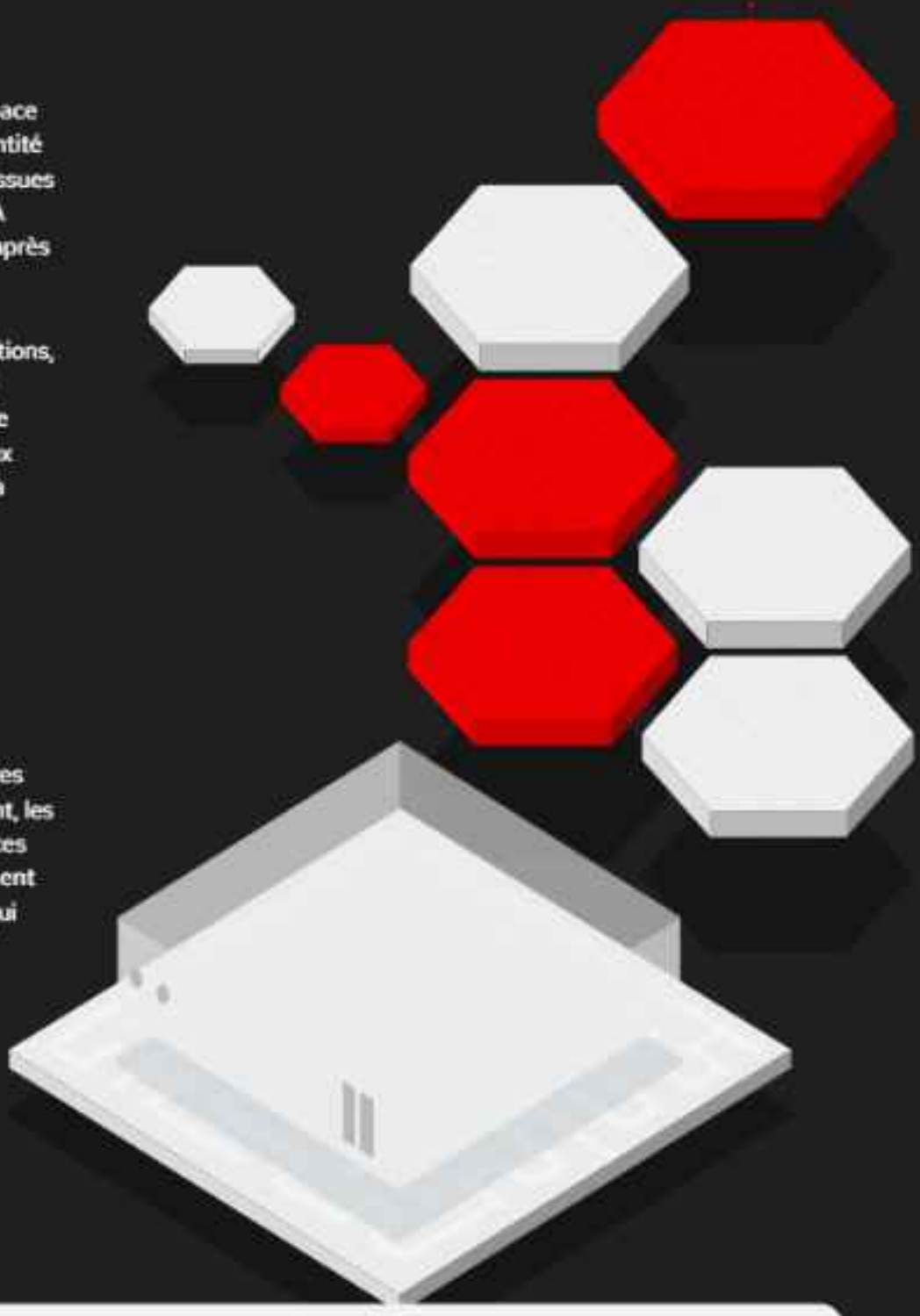
Entraînement et simulation
L'IA permet de créer des environnements d'entraînement et des simulations réalistes. Les troupes peuvent ainsi se préparer à diverses situations sans subir les risques liés à un entraînement sur le terrain ou parallèle au déploiement.

Chapitre 4

Le partage des données : obtenir des renseignements utiles

Face à l'importance croissante des données dans l'espace de bataille moderne, il faut garder à l'esprit que la quantité n'est pas toujours synonyme de qualité. Les données issues de sources telles que l'intelligence humaine, l'IA et l'AA fourniront uniquement des informations exploitables après un processus approprié de traitement et d'analyse.

L'exploitation de l'infrastructure, les fusions et intégrations, ainsi que le traitement des données en transit doivent reposer sur des normes ouvertes pour fournir le flux de données et les capacités de traitement nécessaires aux objectifs d'une convergence et à l'adaptation flexible à chaque événement dynamique.



Des normes ouvertes

La circulation libre des données entre les infrastructures numériques est une condition de réussite. Trop souvent, les données essentielles restent bloquées dans des services isolés ou déconnectés. Les normes ouvertes garantissent l'accessibilité et l'interopérabilité entre les solutions, qui peuvent ainsi fournir des informations exploitables.

L'élimination des obstacles entre les infrastructures numériques favorise la convergence

Collaboration
Laboratoire de combat doté d'une infrastructure multi-client, cohérente et standardisée

Rapidité
Accès fluide aux données de tous les domaines, accélération du prototypage, expérimentation et itération

Agilité
Création de capacités réorientables et déploiement dans tout type d'environnement grâce à l'intégration de données de tous les domaines et à des pratiques DevSecOps

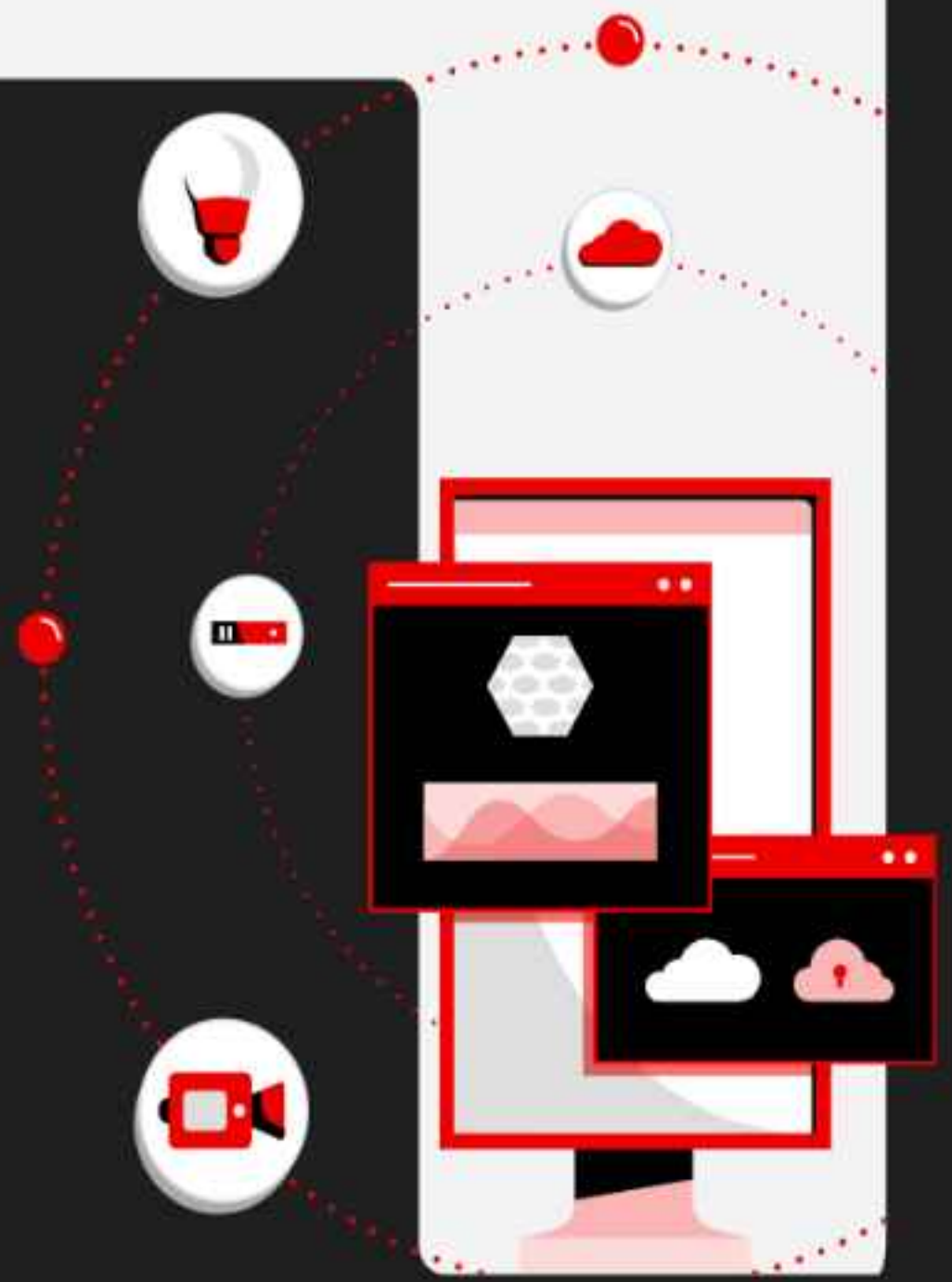
Flexibilité
Normes ouvertes pour les données et l'infrastructure dans les environnements de laboratoire et d'exploitation

Figure 1 : caractéristiques nécessaires pour obtenir des renseignements exploitables

L'utilisation d'une base logicielle

Une architecture réseau logicielle offre une base pour une infrastructure numérique commune à tous les domaines et axée sur la sécurité. Red Hat fournit cette base, qui couvre notamment la collecte, l'intégration, l'analyse et la syndication des données. L'objectif est de fournir aux troupes un environnement collaboratif qui leur permet d'accéder aux données géospatiales ainsi qu'aux modèles et outils d'analyse les plus récents.

Cette base englobe les principaux aspects liés à la sécurité, à la latence et à la rapidité lors des missions, dans toutes les topologies et de bout en bout. Elle enrichit les systèmes de transport, de communication et d'intégration pour contribuer à la réussite des missions. L'environnement collaboratif et les outils d'analyse aident les soldats à interagir avec les données, quel que soit leur échelon, selon le modèle CROP (Common Relevant Operational Picture).



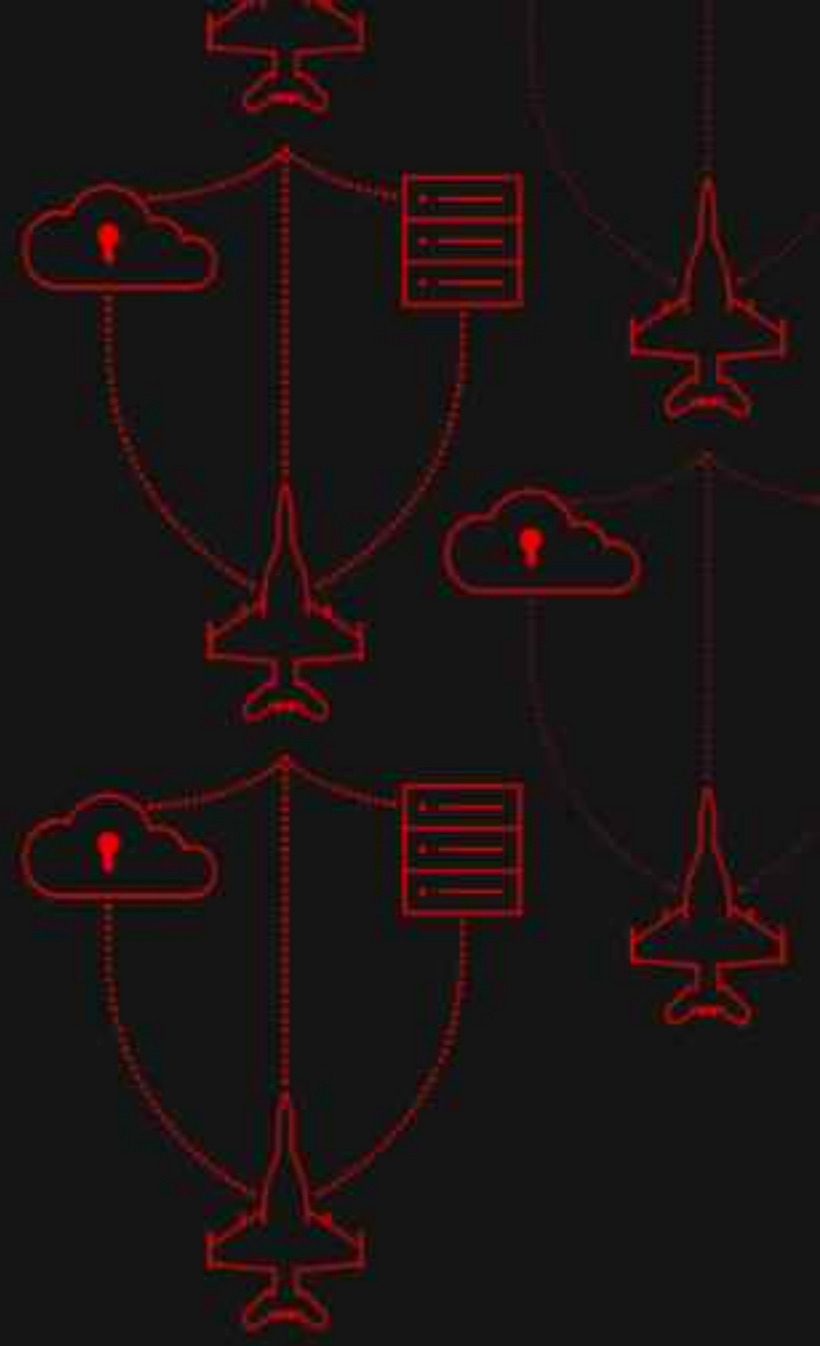
L'importance de la gestion

Bien que stratégiques, les systèmes d'IA/AA actuels sont si dynamiques qu'ils doivent être régulièrement mis à jour, modifiés et réglés pour optimiser la précision et la valeur des informations qu'ils fournissent. Les outils d'IA et d'AA doivent être axés sur la portabilité, la gestion des données et les déploiements configurables. La gamme de produits Red Hat offre la flexibilité nécessaire pour déployer des modèles en mettant l'accent sur la sécurité afin de générer, mettre à l'échelle, reproduire et partager rapidement des résultats d'IA/AA de manière cohérente avec une communauté d'intérêt.

Les technologies Red Hat® se distinguent par leur architecture de messagerie flexible qui permet d'évaluer la situation en temps quasi réel. Avec une infrastructure de messagerie robuste, l'échange de données est riche et efficace entre tous les nœuds des domaines CJADC2, et le traitement des énormes volumes de données est plus rapide. Les équipes peuvent ainsi relier les données entre des systèmes disparates, tout en les transformant et en les enrichissant à la périphérie du réseau.

Chapitre 5

L'approche de Red Hat pour l'edge computing appliqué aux missions



L'edge computing est le prolongement naturel de la stratégie de cloud hybride ouvert de Red Hat, qui consiste à rendre opérationnelles toutes les charges de travail dans tous les environnements, quel que soit l'emplacement. Aucun fournisseur ne peut toutefois répondre à tous les besoins dans ce domaine, pas même Red Hat.

Red Hat propose des solutions et une expertise qui s'appuient sur un vaste écosystème de partenaires fournisseurs de matériel et de logiciels pour aider les troupes à remplir leurs missions à la périphérie du réseau. Grâce à ce riche catalogue de partenaires certifiés pour le matériel, les logiciels et le cloud, le département de la Défense des États-Unis peut moderniser l'ensemble de ses ressources tout en préservant l'agilité, en maintenant sa posture de sécurité et en standardisant l'interopérabilité entre les divisions et les services.

Avec une plateforme d'applications moderne et basée sur des conteneurs, les troupes peuvent développer des applications, puis les déployer dans tout type d'environnement d'edge computing (base opérationnelle avancée, véhicule, système d'arme semi-autonome, etc.). Elles peuvent également migrer les charges de travail vers d'autres équipements si besoin.

Les atouts d'une plateforme d'applications basée sur des conteneurs

Limitation des coûts
Les conteneurs facilitent la réalisation des objectifs MDO et CJADC2 visant à créer une capacité de défense intégrée qui englobe les systèmes existants. Il n'est donc pas nécessaire de démonter et remplacer le matériel, ni de réécrire les applications existantes, car elles peuvent être déployées et gérées sur la même plateforme que les applications modernes basées sur des microservices.

Interopérabilité des données
Grâce aux technologies d'intégration, le département de la Défense peut transmettre immédiatement les informations nouvellement acquises à d'autres systèmes, sans dépendre d'une intervention manuelle. Les troupes peuvent ainsi communiquer rapidement entre elles et avec leurs supérieurs. Les unités déployées, les officiers et même le Pentagone disposent tous de la même COP (Common Operational Picture).

Agilité en mission
Avec des applications d'IA et d'AA basées sur des microservices, les équipes de développement du département de la Défense peuvent s'adapter rapidement aux changements en désintégrant, puis en réorientant les microservices, par exemple pour ingérer des données issues d'un nouveau type de capteur.

Résilience et capacité de survie au cours des missions
Tous les ordinateurs d'une ressource d'edge computing (comme un navire ou un tank) forment un MicroCloud. Si un ordinateur tombe en panne, l'équipe peut rapidement réorienter la capacité de mission d'un autre.

Les avantages des solutions Red Hat pour l'edge computing appliqué aux missions

L'adoption de l'edge computing pour la prise de décision stratégique dans tous les domaines implique de disposer de technologies, de techniques, de tactiques et de procédures adaptées.

Développement et déploiement dans tous les environnements

La solution Red Hat OpenShift® Container Platform aide les forces du département de la Défense des États-Unis à développer des applications pour les déployer ensuite dans tout type d'environnement, quel que soit l'échelon. Red Hat OpenShift renforce la sécurité à tous les niveaux de la pile de conteneurs. Les technologies Red Hat Integration facilitent l'adaptation aux changements inévitables des formats et des protocoles de données, en rassemblant les données des systèmes d'hier, d'aujourd'hui et de demain.

Gain d'efficacité dû à l'automatisation

L'efficacité des processus d'exploitation à la périphérie du réseau requiert également une mise en œuvre robuste et évolutive de l'automatisation qui garantit la cohérence et la rapidité du déploiement et de la gestion de l'infrastructure et des applications essentielles. Avec Red Hat Ansible® Automation Platform, le département de la Défense peut automatiser les tâches et configurations courantes pour réduire les interventions manuelles et ainsi limiter les erreurs et les temps d'arrêt dans les environnements distants et difficiles.

De plus, la solution Ansible Automation Platform applique automatiquement les politiques de sécurité et les exigences de conformité, ce qui garantit une posture de sécurité forte dans diverses conditions pour les appareils et les processus d'exploitation à la périphérie du réseau.

Solution aux défis de l'edge computing

Pour atteindre un haut niveau d'efficacité à la périphérie du réseau, il est nécessaire d'adopter des solutions légères et flexibles qui s'adaptent aux environnements d'edge computing. La plateforme Red Hat Device Edge permet de déployer et gérer des applications et services conteneurisés sur les appareils d'edge computing, pour des processus d'exploitation cohérents et efficaces même sur des sites distants aux ressources limitées.

Avec Red Hat Device Edge, le département de la Défense des États-Unis peut traiter et analyser les données en temps réel à la périphérie du réseau, ce qui réduit la latence et améliore les capacités de prise de décision. Les fonctions de sécurité robustes de cette plateforme renforcent la sécurité des déploiements à la périphérie du réseau pour protéger les systèmes contre les cybermenaces, et s'intègrent à l'infrastructure informatique existante pour faciliter les mises à jour et l'évolutivité. Le département de la Défense peut ainsi garantir un niveau élevé de fiabilité et d'agilité pour les processus d'exploitation essentiels, même dans des environnements complexes et dynamiques.

Red Hat peut aussi apporter son soutien lors de la transformation numérique des équipes qui adoptent une plateforme de cloud hybride et de nouveaux processus DevSecOps. Parce que la préparation des systèmes informatiques est essentielle pour la sécurité nationale, Red Hat fournit l'expertise technologique nécessaire pour aider le département de la Défense des États-Unis à protéger ses réseaux, systèmes et données contre l'activité numérique malveillante, et pour améliorer la préparation aux opérations militaires et les capacités opérationnelles.

Entreprise ancrée dans l'Open Source, Red Hat réunit les idées issues d'une communauté complexe et diversifiée, à l'image du département de la Défense. Les meilleures idées des communautés en amont sont mises en œuvre dans des solutions ciblées afin d'aider les clients à atteindre leurs objectifs.

Découvrez comment Red Hat aide le département de la Défense des États-Unis à remplir ses missions plus vite et à moindre risque.

Découvrez comment renforcer l'efficacité de l'exploitation plus rapidement.
Contactez un spécialiste Red Hat du département de la Défense.