Des choses étonnantes se produisent lorsque vous obtenez le soutien dont vous avez besoin.

Les organisations modernes de toutes les industries peinent à suivre le rythme des exigences d'un paysage axé sur la technologie, l'innovation et la connexion numérique.

Les équipes des TI sont aux prises avec d'anciennes infrastructures et des plateformes disparates tout en étant déchirées entre la gestion de l'entretien de la technologie au quotidien et la stimulation de l'innovation.

Les organisations d'aujourd'hui ont besoin de tout le soutien qu'elles peuvent obtenir, et ce, au moyen de services qui soulagent la charge de travail du personnel des TI, stimulent la croissance et aident les organisations à atteindre les résultats visés.

La technologie est le moteur des résultats organisationnels

La rapidité à établir des priorités numériques est essentielle à la réussite dans le marché concurrentiel d'aujourd'hui. Cependant, les complexités techniques peuvent ralentir les progrès. L'équipe des services d'ingénierie complets de CDW se concentre sur la transformation numérique (du code et des applications à l'infonuagique, aux données et à la sécurité) pour vous aider à accélérer l'innovation, à améliorer l'expérience utilisateur et à optimiser la collaboration, le tout avec agilité et rentabilité.

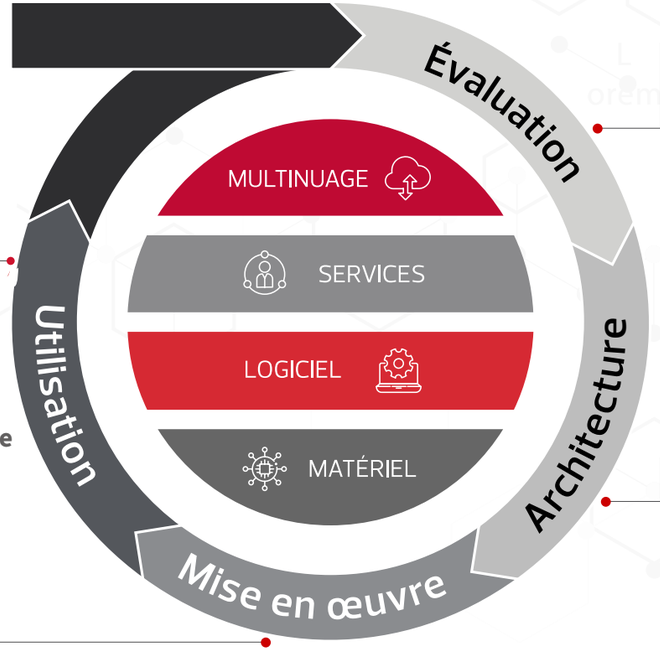
EMPILAGE COMPLET. CYCLE DE VIE COMPLET. RÉSULTATS COMPLETS.

Fonctionnement en continu

- Couverture en tout temps

Qualité démontrée

- Plus de 3 000 certifications
- Huit bureaux dans l'ensemble du Canada
- Couverture internationale



La confiance à l'échelle

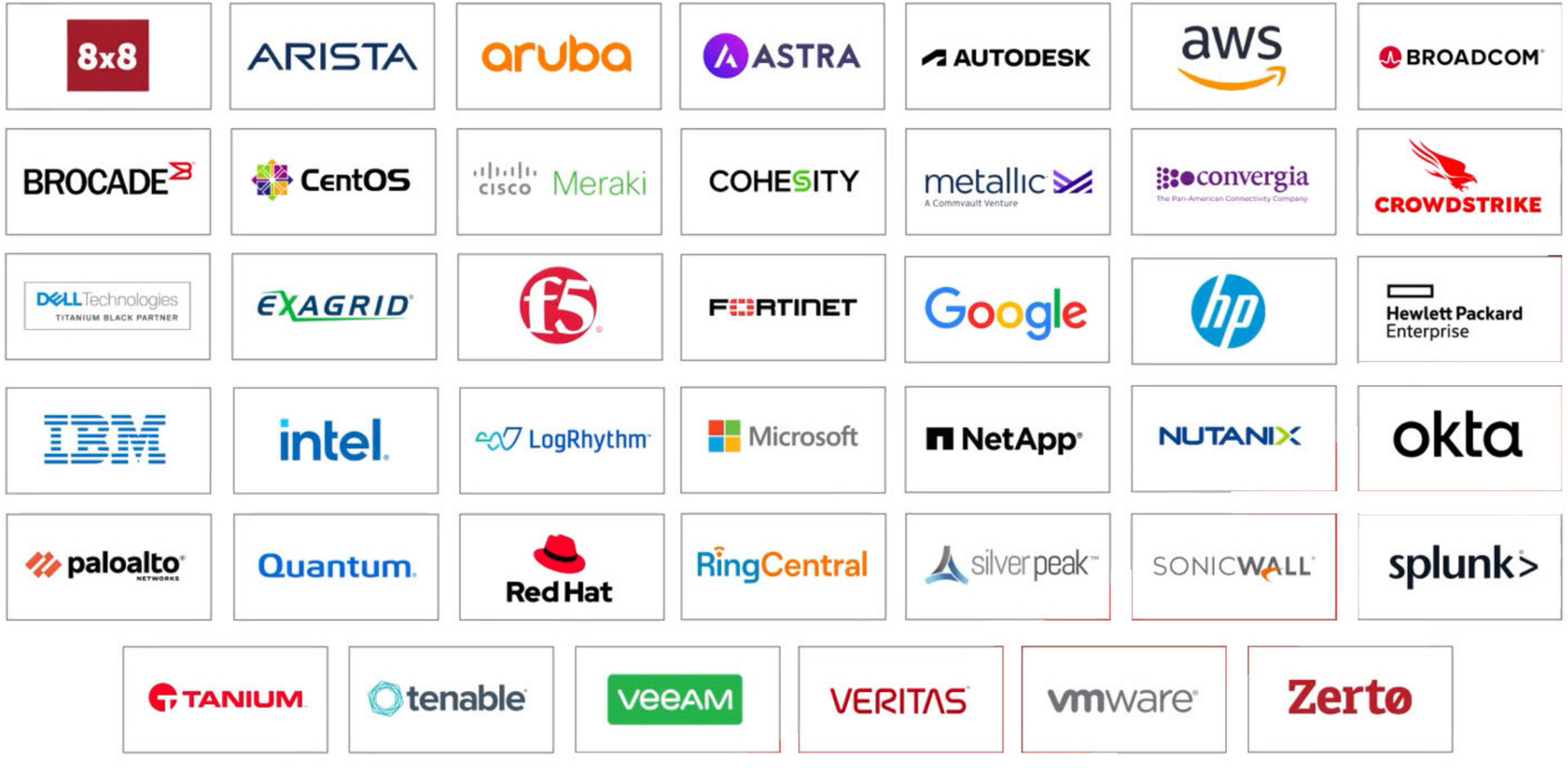
- Plus de 80 architectes de solutions
- Plus de 80 conseillers en prestation de services

Expertise hors pair

- Plus de 20 ans sur le marché canadien
- Plus de 900 collègues

DÉBUT DU DOCUMENT

Nos partenaires de services :



DÉBUT DU DOCUMENT

Tirez davantage parti de votre technologie

Nous connaissons les TI. C'est notre domaine. Lorsque vous vous associez avec nous, nous soulageons votre équipe des TI de la charge de travail supplémentaire. De cette façon, elle peut se concentrer sur les initiatives qui transforment les TI en avantage concurrentiel tandis que nous vous aidons à maximiser vos investissements en TI et à offrir une valeur réelle pour vos clients. Nos experts vous aident à **évaluer, à concevoir, à mettre en œuvre et à utiliser** votre environnement technologique.

ÉVALUATION

Nos experts certifiés fournissent une série de services d'évaluation pour aider les organisations à comprendre leur niveau de maturité actuel et à planifier des étapes pour poursuivre leur chemin vers un modèle d'exploitation de nuage hybride optimisé. Nous nous concentrons sur les domaines clés de croissance suivants : portabilité, facilité de gestion, observabilité, résilience et sécurité.

ARCHITECTURE

Nous allons vous aider à concevoir un plan pour former votre personnel, mettre à jour vos processus et mettre en œuvre des technologies pour accélérer votre capacité à répondre aux besoins technologiques actuels et futurs. Nous prenons les objectifs commerciaux et les transformons en plans et en architectures de mise en œuvre qui permettent à nos clients de réussir.

MISE EN ŒUVRE

CDW Canada dispose d'une foule de services pour aider les clients à former des compétences, à changer de processus et à mettre en œuvre des technologies qui répondent à leurs objectifs commerciaux. Des conseillers en prestation de services professionnels de premier plan aux services de renforcement du personnel, les services de CDW fournissent ce qui est nécessaire pour aider les clients à mener à bien leurs projets les plus complexes.

UTILISATION

Les services gérés sont au cœur de la capacité de CDW Canada d'aider les clients. De plus en plus d'organisations cherchent à consommer « en tant que service » et nos services gérés, le centre des opérations de sécurité et le centre national des opérations soutiennent les clients en assurant la couverture de leurs systèmes essentiels en tout temps.

DÉBUT DU DOCUMENT

Services d'infrastructure

Les services d'infrastructure de CDW Canada fournissent l'expertise, les outils et les ressources pour mettre à l'échelle votre infrastructure et la rendre durable. Nous vous aidons à mettre à niveau votre architecture existante et à vous préparer pour ce qui est à venir, que vous soyez sur place, en migration vers le nuage ou déjà dans le nuage.

Services d'infrastructure professionnels

Tandis que les pressions se font sentir pour que les services des TI fournissent plus de services plus rapidement, les infrastructures sont mises à rude épreuve. Notre équipe expérimentée de professionnels des infrastructures peut vous aider à découvrir des occasions cachées et à trouver les solutions qui conviennent le mieux à votre environnement.
[Explorer les services d'infrastructure gérés]

Centre de traitement des données

- **Pare-feu pour applications**
  Configurez le pare-feu pour applications pour permettre uniquement le trafic autorisé, grâce au module de gestion de pare-feu avancé.
  Fournisseurs pris en charge : F5

- **Stockage dans le nuage**
  Installez et configurez les services sur le nuage selon les exigences du client.
  Fournisseurs pris en charge : AWS Data Sync, AWS FSx, Azure NetApp Files, Backup (DR), CVO, NetApp Cloud Sync et NetApp Cloud Manager

- **Déploiement et mise à niveau d'une grappe de commutateurs**
  Modernisez votre système de stockage en passant d'une grappe sans commutateur à une grappe commutée, au moyen de commutateurs d'interconnexion en grappe. Mettez à niveau le logiciel et le matériel de commutation.
  Fournisseurs pris en charge : Broadcom

- **Construction et migration du centre de traitement des données**
  Pour les grandes entreprises qui souhaitent migrer vers des technologies de centres de traitement des données durables comme ACI ou NSX-T, nous fournissons des services professionnels garantissant une conception, un déploiement et une migration harmonieux. Pour les petites et moyennes entreprises, nous concevons et déployons un réseau robuste avec l'équipement et les technologies traditionnels.
  Fournisseurs pris en charge : Arista, Aruba, Cisco et VMware

- **Protection contre les attaques par déni de service distribué (DDoS)**
  Mettez en place une protection contre les attaques DDoS avec le module ASM.
  Fournisseurs pris en charge : F5

- **Conception et mise en œuvre de DNS**
  Conception et mise en œuvre du DNS BIG-IP.
  Fournisseurs pris en charge : F5

- **F5 en tant que fournisseur d'identité (FI)**
  Exécutez le BIG-IP en tant que fournisseur d'identité pour les applications en nuage ou sur place.
  Fournisseurs pris en charge : F5

- **F5 en tant que fournisseur de services (FS)**
  Exécutez le BIG-IP en tant que fournisseur de services pour avoir accès aux applications sur place.
  Fournisseurs pris en charge : F5

- **Démarrage rapide F5**
  Conception et mise en œuvre de la grappe BIG-IP. En nuage ou sur place.
  Fournisseurs pris en charge : F5

DÉBUT DU DOCUMENT

- **Mise en œuvre de l'infrastructure hyperconvergée**
  Déploiement de grappes à nœuds multiples, mises à niveau, migration de données de machines virtuelles et virtualisation.
  Fournisseurs pris en charge : Cisco UCS, FlexPod, NetApp et Nutanix

- **Calcul informatique de pointe**
  La puissance et la vitesse du calcul informatique de pointe (CIP) peuvent vous aider à traiter, trier et analyser de grands ensembles de données en une fraction de temps par rapport à l'informatique traditionnelle. CDW a l'expertise, les capacités et les ressources pour vous soutenir à toutes les étapes de votre parcours en matière de CIP. Nous pouvons vous fournir des solutions clés en main/de pointe ou des services professionnels pour vous aider à respecter les exigences particulières de votre environnement de CIP.

- **Kubernetes et applications**
  Déployez et configurez les nœuds de grappe Kubernetes et installez l'application nécessaire. Configurez le service de gestion du cycle de vie des données pour les applications à état en utilisant Astra.
  Fournisseurs pris en charge : Astra, Google K8s et NetApp

- **Actualisation du réseau RL/RE**
  Il s'agit de remplacer les appareils en fin de vie par les appareils les plus récents. Nous avons l'expertise pour travailler avec n'importe quel fournisseur de RL/RE, et nous sommes compétents dans la manipulation des environnements de fournisseurs hétérogènes.
  Fournisseurs pris en charge : Aruba, Brocade, Cisco, Dell, Fortinet, HPe et Meraki

- **Équilibreur de charge**
  Configurez un serveur virtuel pour équilibrer la charge et optimiser la séance de l'utilisateur sur plusieurs serveurs dorsaux.
  Fournisseurs pris en charge : F5

- **Évaluation du réseau**
  Évaluation approfondie du réseau RL/RE avec rapport détaillé sur les points sensibles, les préoccupations de sécurité, les incohérences de configuration et les recommandations.
  Fournisseurs pris en charge : Arista, Aruba, Cisco, Dell, Fortinet, HPe et Meraki

- **Déploiement du portail**
  Proposez un portail Web où les applications sont disponibles par l'intermédiaire d'un membre de groupe Active Directory (AD).
  Fournisseurs pris en charge : F5

- **Déploiement de commutateurs réseau SAN**
  Structurez des déploiements de solutions matérielles et logicielles grâce à la matrice SAN. Zonage et mise en service du SAN.
  Fournisseurs pris en charge : Brocade et Cisco

- **Conception et déploiement du SD-WAN**
  Services-conseils, conception et déploiement de solutions SD-WAN pour les petites et grandes entreprises. Cela comprend une intégration harmonieuse avec le réseau existant et la migration vers le nouveau réseau SD-WAN avec un minimum de temps d'indisponibilité.
  Fournisseurs pris en charge : Cisco, Fortinet, Meraki 1 et Silver Peak

- **Secure Remote Desktop**
  Offrez un accès sécurisé au bureau à distance au moyen du portail de gestion des portefeuilles d'applications (GPA).
  Fournisseurs pris en charge : F5

- **Accès sécurisé à l'infrastructure de bureau virtuel**
  Offrez un accès sécurisé à l'infrastructure de bureau virtuel par le portail de GPA.
  Fournisseurs pris en charge : F5

- **Évaluations du stockage**
  Analysez l'utilisation de la capacité de stockage, la performance, la qualité de service ainsi que l'intégrité et produisez des rapports avec des recommandations.
  Fournisseurs pris en charge : HPe, NetApp et Nutanix

- **Automatisation du stockage (Ansible)**
  Automatisez les tâches de stockage complexes avec la plateforme Ansible.
  Fournisseurs pris en charge : NetApp

- **Migration des données de stockage**
  Migrez des données de diverses plateformes vers NetApp, Nutanix, HPE, Cisco UCS et le nuage.
  Fournisseurs pris en charge : AWS, Azure, HPe, NetApp et Nutanix

- **Déploiements du stockage**
  Déploiement de grappes de matériel et de logiciels, mise à niveau ou déclassement, mise hors service, protection des données, consolidation et virtualisation.
  Fournisseurs pris en charge : Dell, HPE et NetApp

DÉBUT DU DOCUMENT

- **Amélioration et consolidation du stockage**
  Ajoutez des nœuds et des tiroirs disques à la grappe et éjectez le matériel en fin de vie.
  Fournisseurs pris en charge : HPE, NetApp et Nutanix

- **Solutions de bureau virtuelles**
  Nouveaux déploiements d'Horizon, mises à niveau des déploiements existants et évaluations de l'intégrité.
  Fournisseurs pris en charge : VMware Horizon/View

- **Virtualisation du réseau VMware**
  Le centre de traitement des données VMware NSX est la plateforme de virtualisation et de sécurité qui rend possible l'existence du réseau en nuage virtuel, une approche de réseautage définie par logiciel qui s'étend à travers les centres de traitement des données, les nuages, les points d'extrémité, etc.
  Fournisseurs pris en charge : VMware

- **Évaluation de l'intégrité vSphere**
  L'évaluation de l'intégrité couvre le réseau, la connectivité de stockage, les serveurs ESXi et l'intégrité de vCenter.
  Fournisseurs pris en charge : VMware

- **VxRail**
  Déployez de nouveaux appareils VxRail, mettez à niveau des appareils existants, mettez à l'échelle ou ajoutez des appareils.
  Fournisseurs pris en charge : Dell et VMware

- **Protection PAW**
  Appliquez la politique PAW pour protéger les applications contre les demandes malveillantes.
  Fournisseurs pris en charge : F5

- **Déploiement du réseau local sans fil**
  Conception et déploiement de réseaux locaux sans fil en repartant de zéro ou par évolution, pour les petites et les grandes entreprises.
  Fournisseurs pris en charge : Aruba, Cisco et Meraki

- **Relevé d'emplacement sans fil**
  Nos inspections d'environnements sans fil fournissent des données cruciales en vue de la réussite d'une planification du déploiement de réseaux Wi-Fi et du repérage de pannes et de problèmes dans ces réseaux, vous permettant de vous concentrer sur vos activités et résultats commerciaux plutôt que sur la complexité des infrastructures.
  Fournisseurs pris en charge : Aruba, Cisco et Wi-Fi 6

DÉBUT DU DOCUMENT

Protection des données

- **Migration des données de sauvegarde vers le nuage**
  Le déplacement des données de sauvegarde vers le nuage a été l'exemple parfait d'utilisation des ressources du nuage. De plus en plus d'entreprises abandonnent les sauvegardes sur bande et sur disque obsolètes pour passer au stockage infonuagique. CDW peut évaluer les besoins du client et mettre en œuvre une solution qui lui convient.
  Fournisseurs pris en charge : Commvault, Dell et Veeam

- **Migration de l'environnement de sauvegarde vers le nuage**
  La réduction des ressources sur place fait partie des priorités pour la plupart des clients. De nombreux clients envisagent de migrer l'environnement de sauvegarde vers le nuage et de conserver moins de ressources sur place. CDW peut évaluer l'environnement et les besoins des clients pour élaborer une solution qui utilisera les ressources infonuagiques en vue de protéger les données de sauvegarde.
  Fournisseurs pris en charge : Commvault, Dell et Veeam

- **Sauvegarde Commvault pour AWS**
  Les conseillers certifiés de CDW peuvent mettre en œuvre des mesures de protection pour les charges de travail AWS comme EC2 et EKS et les bases de données de plateforme en tant que service (PaaS) comme RDS et DocumentDB. CommVault Live Sync peut effectuer une réplication à partir de VMware et d'Hyper-V à AWS et d'AWS à VMware et Hyper-V et Azure. Les conseillers certifiés de CDW peuvent concevoir et mettre en œuvre une solution répondant à tous les besoins d'un client.
  Fournisseurs pris en charge : AWS et Commvault

- **Sauvegarde Commvault pour Azure**
  Les conseillers certifiés de CDW peuvent mettre en œuvre des mesures de protection pour les charges de travail Azure, les bases de données PaaS, SAP Hana sur Azure et SQL en utilisant Commvault. CommVault Live Sync peut effectuer une réplication à partir de VMware et d'Hyper-V à Azure et d'Azure à VMware et Hyper-V et AWS. Les conseillers certifiés de CDW peuvent concevoir et mettre en œuvre une solution répondant à tous les besoins d'un client.
  Fournisseurs pris en charge : Azure et Commvault

- **Mise en œuvre du logiciel de sauvegarde Commvault**
  Amélioration des services de mise en œuvre des environnements de sauvegarde de Commvault grâce aux meilleures pratiques de Commvault et aux conseillers en mise en œuvre certifiés de CDW. Pendant la mise en œuvre, CDW évaluera les exigences, concevra l'environnement et mettra en œuvre la solution de manière à répondre aux exigences d'audit de l'entente de niveau de service et à réduire la perte de données.
  Fournisseurs pris en charge : Commvault

- **Technologie Hyperscale de Commvault**
  Hyperscale est l'approche de Commvault comme solution de mise à l'échelle horizontale du stockage de données de sauvegarde. CDW peut mettre en œuvre ces dispositifs de sauvegarde dans le centre de traitement des données de production ou dans des emplacements éloignés comme une solution de stockage et calcul unique pour n'importe quel environnement afin de répondre à des exigences de résilience et de performance élevées.
  Fournisseurs pris en charge : Commvault

- **Migration des MV de Commvault vers le nuage**
  Les clients ont besoin d'une méthode sûre pour migrer les charges de travail sur place vers le nuage. CDW peut utiliser Commvault pour protéger dans un premier temps toutes les charges de travail de production, puis dans un deuxième temps copier ces données dans le nuage et répliquer les charges de travail dans la charge de travail de la plateforme infonuagique. Commvault répliquera les changements quotidiens jusqu'à ce que le basculement puisse être effectué. Une fois que vous êtes prêt à effectuer le transfert dans le nuage, utilisez la fonction de basculement pour arrêter les charges de travail sur place et faire tourner les charges de travail infonuagiques.
  Fournisseurs pris en charge : Commvault

- **Mise en œuvre de Dell Data Domain**
  Le Data Domain de Dell est un dispositif de deduplication des données très extensible pour le stockage de sauvegarde et il peut être étendu au stockage infonuagique au moyen d'un DDVE. Les conseillers certifiés de CDW peuvent concevoir et mettre en œuvre le périphérique de stockage dans n'importe quel logiciel de sauvegarde pour répondre aux exigences des clients.
  Fournisseurs pris en charge : Dell

- **Évaluation de la protection des données**
  Réalisez une configuration et une évaluation opérationnelle de l'environnement de protection des données existant du client. Cette évaluation sera fondée sur les meilleures pratiques de l'industrie. Un résumé de la configuration et des recommandations de mesures correctives seront fournis à titre de livrables du projet.
  Fournisseurs pris en charge : Tous les fournisseurs

- **Analyse de la stratégie de la plateforme de protection des données**
  Inspectez et évaluez l'environnement de protection des données actuel et les plans de la feuille de route des TI afin d'établir une stratégie autour des produits et architectures qui correspondraient le mieux à leurs exigences.
  Fournisseurs pris en charge : Tous les fournisseurs

DÉBUT DU DOCUMENT

- **Sauvegarde Dell pour Azure**
  La solution de protection des données intégrée (IDPA) de Dell est une interface de gestion unique pour sauvegarder tous types de charges de travail, y compris sur place, Azure et AWS. CDW peut introduire facilement cette solution rentable dans l'environnement pour gérer tous ses besoins dans le nuage en vue de sauvegarder les charges de travail PaaS et IaaS. Les conseillers certifiés de CDW peuvent concevoir et mettre en œuvre la solution pour protéger ces charges de travail.
  Fournisseurs pris en charge : Dell

- **Mise en œuvre du logiciel de sauvegarde Dell**
  Amélioration des services de mise en œuvre des environnements de sauvegarde Dell grâce aux meilleures pratiques de Dell et aux conseillers en mise en œuvre certifiés de CDW. Pendant la mise en œuvre, CDW évaluera les exigences, concevra l'environnement et mettra en œuvre la solution de manière à répondre aux exigences d'audit de l'entente de niveau de service et à réduire la perte de données.
  Fournisseurs pris en charge : Dell (IDPA, Avamar, Networker et PowerProtect)

- **Évaluation de l'état de préparation à une récupération après sinistre**
  Cette évaluation sert à évaluer l'état de préparation général du client à une récupération après sinistre et à recommander des améliorations.
  Fournisseurs pris en charge : Tous les fournisseurs

- **Réplication de la récupération après sinistre**
  Les conseillers en protection des données certifiés de CDW peuvent mettre en œuvre une solution de récupération après sinistre pour répondre aux besoins des clients soit dans un emplacement secondaire, soit dans le nuage. De nombreux clients ont remplacé leurs anciens sites physiques de récupération après sinistre par des sites de récupération après sinistre en nuage afin de réduire les coûts.
  Fournisseurs pris en charge : Commvault, Dell et Veeam

- **Mises à niveau matérielles de l'environnement**
  Le matériel de l'infrastructure de sauvegarde doit être remplacé à l'expiration des garanties afin de réduire les coûts d'entretien et de le maintenir en bon état de fonctionnement. Les conseillers en protection des données de CDW peuvent aider à mettre hors service les vieux appareils et à les remplacer par des plus récents.
  Fournisseurs pris en charge : Commvault, DELL et Veeam

- **Mises à niveau logicielles de l'environnement**
  Il convient de mettre à niveau les environnements de sauvegarde régulièrement pour y apporter les plus récentes améliorations sur le plan de la sécurité et du fonctionnement. Les conseillers certifiés de CDW peuvent mettre à niveau les environnements pour répondre aux exigences des clients.
  Fournisseurs pris en charge : Commvault, Dell et Veeam

- **Mise en œuvre d'ExaGrid**
  La solution de stockage de sauvegarde hiérarchisé ExaGrid est une solution de rechange de stockage de sauvegarde à très grande échelle qui utilise une zone d'atterrissage pour les nouvelles données de sauvegarde et un référentiel de rétention à long terme pour protéger les données. ExaGrid peut être utilisée avec n'importe quel logiciel de sauvegarde et mise en œuvre par nos conseillers CDW formés.
  Fournisseurs pris en charge : ExaGrid

- **Mise en œuvre de l'IDPA**
  L'IDPA de Dell est une solution de sauvegarde tout-en-un offrant de puissantes capacités de protection des données de niveau d'entreprise, quelle que soit la taille de l'environnement. Les conseillers formés et certifiés de CDW peuvent mettre en œuvre ces solutions dans n'importe quel environnement afin de protéger les charges de travail nécessaires.
  Fournisseurs pris en charge : DELL

- **Protection d'Office 365**
  Avec le modèle de responsabilité partagée Office 365, le client est responsable de la protection de ses données de production. Les conseillers certifiés de CDW peuvent concevoir et mettre en œuvre une solution pour conserver une copie de sauvegarde secondaire des données SharePoint, Teams, OneDrive et O365 Mail du client afin de répondre à ses exigences de vérification et de rétention.
  Fournisseurs pris en charge : Commvault, DELL, Metallic et Veeam

DÉBUT DU DOCUMENT

- **Mesures correctives**
  Dans tous les environnements, il existe des problèmes qui pourraient interférer avec les opérations de sauvegarde ordinaires et qui peuvent compromettre d'importantes ententes de niveau de service et exigences réglementaires en matière de protection des données. Nos conseillers certifiés peuvent vous aider à corriger les problèmes au sein de l'environnement.
  Fournisseurs pris en charge : Commvault, Dell, IBM, Veeam et Veritas

- **Intégration du niveau de stockage (instantané)**
  Les instantanés de niveau de stockage peuvent aider à réduire les fenêtres de sauvegarde avec les sauvegardes de plus en plus volumineuses. Les logiciels de sauvegarde peuvent gérer les instantanés, répertorier les données de sauvegarde et copier celles-ci du stockage vers les emplacements secondaires. CDW peut mettre en œuvre des instantanés pour la plupart des fournisseurs de solutions de stockage, en ramenant les temps de sauvegarde à quelques minutes seulement.
  Fournisseurs pris en charge : Commvault, Dell et Veeam

- **Mise en œuvre de la bibliothèque de bandes**
  Les bibliothèques de bandes sont encore utilisées dans de nombreux environnements de clients et doivent être remplacées après la fin des périodes de garantie et d'entretien. CDW a une vaste expérience dans l'utilisation des bibliothèques de bandes et peut mettre en œuvre de nouvelles bibliothèques et migrer les données au besoin d'une ancienne bande vers une nouvelle. Notre conseiller certifié peut créer, installer, mettre à niveau et configurer n'importe quel logiciel de sauvegarde que le client utilise aujourd'hui.
  Fournisseurs pris en charge : Dell, HP, IBM et Quantum

- **Sauvetage Veeam**
  Les conseillers certifiés de CDW peuvent mettre en œuvre Veeam Backup for AWS ou Azure afin de protéger les charges de travail au moyen du stockage infonuagique. Pour ce faire, ils recueilleront des renseignements et des exigences, mettront en œuvre la solution, contrôleront les copies de sauvegarde et les essais de restauration, puis documenteront le résultat du projet.
  Fournisseurs pris en charge : AWS, Azure et Veeam

- **Mise en œuvre du logiciel de sauvegarde Veeam**
  Amélioration des services de mise en œuvre des environnements de sauvegarde de Veeam grâce aux meilleures pratiques de Veeam et aux conseillers en mise en œuvre certifiés de CDW. Pendant la mise en œuvre, CDW évaluera les exigences, concevra l'environnement et mettra en œuvre la solution de manière à répondre aux exigences d'audit de l'entente de niveau de service et à réduire la perte de données.
  Fournisseurs pris en charge : Veeam

- **Référentiel renforcé Veeam – Immuabilité**
  La protection du stockage de sauvegarde est aussi importante que la protection des données de production. Un référentiel renforcé Veeam protège les données de sauvegarde Veeam en créant une copie sécuritaire non modifiable et non supprimable afin d'éliminer le risque de chiffrage des données de sauvegarde par un rançongiciel. CDW peut mettre en œuvre le référentiel renforcé Veeam et l'ajouter à l'infrastructure de sauvegarde.
  Fournisseurs pris en charge : Veeam

- **Mise en œuvre du SOBR Veeam**
  Un référentiel de sauvegarde à mise à l'échelle horizontale (SOBR) se compose d'un ou de plusieurs référentiels de sauvegarde appelés niveau de performances et niveau de capacité. CDW constate une légère hausse de la mise en œuvre du SOBR Veeam en vue de l'augmentation de la taille des données de sauvegarde et du début de l'utilisation du stockage objet pour les données à long terme. CDW peut concevoir et mettre en œuvre un SOBR pour remplacer les anciennes configurations afin de répondre aux exigences de capacité sur place et dans le nuage.
  Fournisseurs pris en charge : Veeam

- **Mise en œuvre du logiciel de sauvegarde Veritas**
  Amélioration des services de mise en œuvre des environnements de sauvegarde de Veritas grâce aux meilleures pratiques de Veritas et aux conseillers en mise en œuvre certifiés de CDW. Pendant la mise en œuvre, CDW évaluera les exigences, concevra l'environnement et mettra en œuvre la solution de manière à répondre aux exigences d'audit de l'entente de niveau de service et à réduire la perte de données.
  Fournisseurs pris en charge : Veritas (NetBackup et Backup Exec)

- **DÉPLOIEMENT DE VMWARE CLOUD (VMC)**
  Installation et configuration des applications VMware suivantes : VMware Cloud et VMware HCX.
  Fournisseurs pris en charge : AWS et VMware

- **DÉPLOIEMENT DE VMWARE CLOUD (VMC) AVEC VCDR**
  Installation et configuration de VMware Cloud avec VMware Cloud disaster recovery (VCDR) dans l'environnement du client.
  Fournisseurs pris en charge : AWS et VMware

DÉBUT DU DOCUMENT

Services d'infrastructure gérés

Passez moins de temps à mettre à jour et à maintenir les systèmes et plus de temps à créer de la valeur commerciale. Obtenez de meilleures performances et subissez moins de temps d'indisponibilité avec les services d'infrastructure gérés de CDW Canada.

- **Services gérés Cisco Meraki**
  Chez CDW Canada, nous comprenons que le réseautage dans le nuage hybride est essentiel pour le fonctionnement efficace de votre entreprise. Avec les Services gérés Cisco Meraki par CDW, vous pouvez compter sur les meilleurs experts des TI pour surveiller, gérer et mettre à jour vos déploiements Cisco Meraki : des points d'accès sans fil aux solutions de sécurité MX.
  Fournisseurs pris en charge : Cisco Meraki

Protection des données

- **Sauvegarde en tant que service (BaaS)**
  La sauvegarde en tant que service de CDW vous permet de profiter de ressources et d'outils qui apporteront clairvoyance et tranquillité d'esprit à votre entreprise. Vos équipes de TI peuvent se concentrer sur l'ajout de valeur dans d'autres aspects, sachant qu'elles peuvent se fier à CDW pour gérer votre environnement de sauvegarde.
  Fournisseurs pris en charge : Commvault, Veeam, VMWare et Zerto

- **La récupération après sinistre en tant que service (DRaaS)**
  La récupération après sinistre en tant que service (DRaaS) de CDW vous permet de profiter de ressources et d'outils qui apporteront clairvoyance et tranquillité d'esprit à votre entreprise. Vos équipes de TI peuvent se concentrer sur l'ajout de valeur dans d'autres aspects, sachant qu'elles peuvent se fier à CDW pour gérer la réplication dans votre environnement de récupération après sinistre.
  Fournisseurs pris en charge : Azure, Commvault et Zerto

- **Sauvegarde hébergée**
  Pour les organisations qui utilisent actuellement la technologie Commvault pour leurs sauvegardes, CDW offre une solution de sauvegarde hébergée qui fournit un environnement Commvault CommCell clés en main permettant d'augmenter la capacité de sauvegarde actuelle ou faire office de copie hors site comme solution de rechange à la technologie des bandes, vieillissante.
  Fournisseurs pris en charge : Commvault

- **Calcul géré**
  Calcul géré par CDW : Le service d'hyperviseur vous permet de profiter de ressources et d'outils qui apporteront clairvoyance et tranquillité d'esprit à votre entreprise. Vos équipes de TI peuvent se concentrer sur l'ajout de valeur dans d'autres aspects, sachant qu'elles peuvent se fier à CDW pour gérer votre environnement d'hyperviseur.
  Fournisseurs pris en charge : Cisco, Dell, HPe, Hypervisor, Microsoft et RedHat

- **Commutation de réseau gérée**
  Le service de gestion de réseau assure la gestion au jour le jour des appareils de réseautage pour les clients. CDW offre l'expertise et les connaissances pour fournir des services de surveillance et de signalement, d'administration des appareils et de gestion de la capacité générale pour les systèmes inclus dans la portée.
  Fournisseurs pris en charge : Aruba, Cisco, Fortinet, HPE et Meraki

DÉBUT DU DOCUMENT

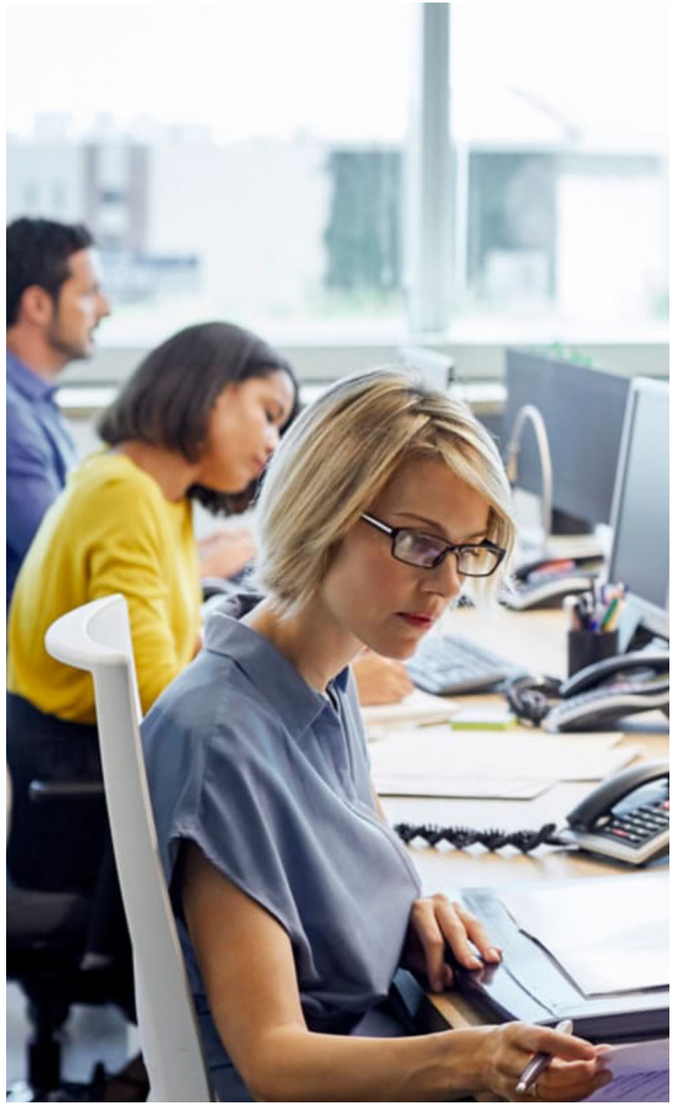
- **SD-WAN géré**
  Laissez vos équipes des TI internes se concentrer sur la performance de votre entreprise tandis que les experts de CDW assurent la gestion au jour le jour de vos appareils SD-WAN.
  Fournisseurs pris en charge : Cisco Meraki, Fortinet et Palo Alto

- **Stockage géré**
  Le service de stockage géré assure la gestion au jour le jour des périphériques de stockage pour les clients. CDW offre l'expertise et les connaissances pour fournir des services de surveillance et de signalement, d'administration des appareils et de gestion de la capacité générale pour les périphériques de stockage.
  Fournisseurs pris en charge : Dell, EMC, HPE Nimble et NetApp

- **Surveillance en tant que service**
  La surveillance en tant que service est une surveillance de base pour une technologie (réseaux, serveurs, machines virtuelles, services additionnels) qui fournit des notifications au client. CDW exploite l'infrastructure du système de surveillance pour le compte du client, mais n'enquête pas sur la cause sous-jacente d'événements ou d'alarmes. CDW transmet des notifications au client pour que les équipes des opérations de ce dernier les traitent.

- **Gestion des correctifs de serveur**
  Dans l'environnement des TI d'aujourd'hui, il n'est pas rare que les administrateurs de systèmes subissent des pressions quant au fait de fournir continuellement une valeur ajoutée à l'entreprise. La réalité, c'est que les systèmes peuvent devenir vulnérables à cause de priorités concurrentes. CDW peut travailler avec vos administrateurs pour fournir un service de correctifs permettant de garantir que vos systèmes sont à jour et de réduire les risques pour votre entreprise.
  Fournisseurs pris en charge : Microsoft, Red Hat Linux et CentOS

- **Site Recovery Manager**
  Pour les clients VMware, CDW offre VMware Site Recovery Manager, qui fournit une réplication entièrement intégrée et automatisée hors site de l'infrastructure virtuelle dans le nuage.
  Fournisseurs pris en charge : VMware



DÉBUT DU DOCUMENT

Services infonuagiques

Au vu de la complexité supplémentaire des environnements publics et multinuagiques en constante évolution, une planification soignée et une gestion experte constituent une nécessité. CDW vous aide à concevoir et à augmenter vos capacités en nuage, à construire votre plateforme selon vos spécifications exactes et à gérer votre environnement infonuagique de façon efficace, sûre et transparente.

Services infonuagiques professionnels

CDW Canada collabore avec vous dans ce parcours en tenant compte soigneusement de vos objectifs commerciaux à la lumière des technologies infonuagiques éprouvées qui peuvent offrir une valeur commerciale réelle. Nous pouvons vous aider à élaborer une feuille de route précise vers la mise à niveau, l'amélioration des compétences et le comblement des écarts de compétences au fil de votre parcours infonuagique. Si vous êtes déjà dans le nuage, CDW Canada peut vous aider à élaborer une stratégie infonuagique axée sur les affaires pour vous aider à obtenir plus de valeur de votre investissement dans l'infonuagique.

[Explorer les services infonuagiques gérés]

AWS

- **Optimisation des coûts infonuagiques**
  Les experts de CDW vous aident à optimiser vos coûts infonuagiques en évaluant l'infrastructure infonuagique, les modes d'utilisation et les dépenses de votre organisation afin de cerner les possibilités d'économies et de formuler des recommandations concrètes, de meilleures pratiques et des stratégies pour réduire les dépenses inutiles et maximiser la rentabilité.
  Fournisseurs pris en charge : AWS

- **Test d'intrusion infonuagique**
  Le service de test d'intrusion infonuagique de CDW est utilisé pour découvrir, identifier et classifier les défaillances et les vulnérabilités potentielles dans les environnements infonuagiques des organisations et aider à évaluer la posture de sécurité connexe. Les conseillers en cybersécurité de CDW essaient d'identifier les vulnérabilités et de les exploiter pour simuler un auteur de menace, puis font des recommandations pour corriger les problèmes.
  Fournisseurs pris en charge : AWS

- **Service de découverte et d'évaluation des licences (LEADS)**
  Le service de découverte et d'évaluation des licences (LEADS) de CDW permet aux entreprises d'évaluer et d'optimiser leurs environnements actuels sur place et dans le nuage en se fondant sur les ressources et l'utilisation réelles et sur les licences fournies par des tiers. Il comporte trois axes stratégiques principaux : déterminer les économies réalisables avec les anciennes licences, l'évaluation du rendement technique et les résultats de l'évaluation LEADS.
  Fournisseurs pris en charge : AWS

Services Microsoft

- **Séance d'introduction de deux jours sur l'apprentissage automatique et l'IA avec Azure OpenAI**
  Un atelier de deux jours sur les tenants et aboutissants des services cognitifs Azure, du service Azure OpenAI et d'Azure OpenAI Studio.

- **Expertise en architecture et déploiement avec Azure Compute, le réseau, les équilibreurs de charge et les bases de données**
  Nous fournissons des conseils pour la conception et la construction de solutions sur Azure en utilisant les meilleures pratiques et l'architecture. Nous concevons des environnements avant-gardistes et flexibles qui permettent aux entreprises de déplacer leurs charges de travail vers le nuage et d'intégrer les technologies et services les plus récents afin de rationaliser la disponibilité et la prestation de services.

- **Protection de l'identité avec Azure AD**
  La protection de l'identité permet d'automatiser la détection et la correction des risques fondés sur l'identité, les enquêtes sur les risques et l'exportation des données de détection des risques vers d'autres outils.

- **Pare-feu Azure**
  Le pare-feu Azure est un service de sécurité pare-feu de réseau intelligent et infonuagique natif qui offre une protection contre les menaces pour vos charges de travail infonuagiques exécutées sur Azure. Il s'agit d'un pare-feu à état en tant que service avec une haute disponibilité intégrée et une capacité d'extensibilité dans le nuage sans restriction.

- **Évaluation de sécurité Azure**
  Nous réalisons une évaluation et nous nous assurons que les meilleures pratiques de sécurité infonuagique sont respectées ou dépassées. Nous examinons les déploiements existants et faisons des recommandations basées sur la rétroaction des conseillers expérimentés sur le terrain.

- **Cours intensif sur Azure OpenAI**
  Un cours sur les services Azure OpenAI. Découvrez les différences entre l'apprentissage automatique, l'IA et l'IA générative, étudiez des applications dans le monde réel et faites l'expérience de la rédactique interactive avec le terrain de jeu avec fonction de clavardage Azure.

DÉBUT DU DOCUMENT

- **Automatisation des processus opérationnels : Power Apps, Power Automate Flow et Azure Logic Apps**
  Évaluez votre posture de sécurité et votre situation de conformité dans votre environnement Microsoft 365 pour vous aligner sur les meilleures pratiques recommandées par Microsoft. Nous fournissons un rapport sur l'état actuel de votre locataire avec une liste de recommandations concrètes classées par ordre de priorité pour vous aider à identifier et corriger les problèmes de sécurité potentiels dans votre environnement.

- **Migration des services de fichiers**
  Migration des services sur place vers SharePoint, OneDrive ou les deux.

- **Ateliers MCI**

  - **Azure Defender for Cloud (anciennement le « Security Centre »)**
    Microsoft Defender for Cloud est une plateforme de gestion de la posture de sécurité infonuagique (CSPM) et de protection de la charge de travail infonuagique (CWPP) pour toutes vos ressources sur Azure, sur place et multinuagiques (Amazon AWS et Google GCP). Defender for Cloud répond à trois besoins essentiels dans le cadre de la gestion de la sécurité de vos ressources et de vos charges de travail dans le nuage et sur place : évaluer, sécuriser et défendre en permanence.

  - **Ateliers sur la sécurité et la gouvernance dans Azure**
    Aidez les clients à apprendre à maximiser la valeur de Teams en intégrant des applications et des flux de travail adaptés aux besoins de leurs entreprises. Les clients reçoivent un rapport contenant des recommandations concrètes qui orientent le déploiement et les étapes suivantes.

  - **Applications collaboratives (anciennement Applications et solutions Teams)**
    Examinez divers défis et problèmes auxquels font face les travailleurs de première ligne afin d'identifier les scénarios prioritaires pour l'effectif de première ligne des clients. Les clients reçoivent un rapport contenant des recommandations concrètes qui orientent le déploiement et les étapes suivantes.

  - **Défense contre les menaces avec SIEM Plus XDR (anciennement Threat Protection)**
    Nous comprenons les objectifs de sécurité des clients, puis nous identifions les véritables menaces de sécurité à travers le courriel, l'identité et les données dans leur environnement de production pour mettre en valeur l'expérience Microsoft Sentinel et Microsoft 365 Defender. Les clients reçoivent un rapport contenant des recommandations concrètes qui orientent le déploiement et les étapes suivantes.

  - **Habilitation des intervenants de première ligne**
    Nous présentons la valeur de Microsoft Endpoint Manager pour montrer aux clients comment gérer les appareils, les applications et les identités des utilisateurs de partout. Les clients reçoivent un rapport contenant des recommandations concrètes qui orientent le déploiement et les étapes suivantes.

  - **Gestion des points d'extrémité**
    Montrez le potentiel des expériences de réunions hybrides et des salles de réunion de Microsoft Teams qui permettent aux gens de travailler de n'importe où, en tout temps. Les clients reçoivent un rapport contenant des recommandations concrètes qui orientent le déploiement et les étapes suivantes.

  - **Réunions et salles hybrides (anciennement Hybrid Meetings)**
    Nous aidons les clients au tout début de leurs transformations infonuagiques à envisager des scénarios de travail agiles et à imaginer une façon d'habiliter leurs employés à travailler de manière productive et en toute sécurité avec Microsoft 365. Les clients reçoivent un rapport contenant des recommandations concrètes qui orientent le déploiement et les étapes suivantes.

  - **Microsoft 365 Main-d'œuvre numérique (anciennement Transition to Cloud)**
    Nous découvrons les scénarios d'affaires uniques des clients, soulignons l'expérience de transformation des employés et mettons en valeur le potentiel de la suite Viva avec ses composantes Topics, Connections ou Learning. Les clients reçoivent un rapport contenant des recommandations concrètes qui orientent le déploiement et les étapes suivantes.

  - **Microsoft Sentinel**
    Nous démontrons la façon dont Microsoft Sentinel aide les organisations à utiliser les analyses de sécurité intelligentes et les renseignements sur les menaces pour déceler et arrêter rapidement les menaces actives.

  - **Microsoft Viva**
    Nous aidons les clients à découvrir comment Microsoft Viva Insights permet à l'effectif, aux gestionnaires et aux responsables d'obtenir des indications personnalisées et des recommandations concrètes qui contribuent à l'épanouissement de tous au sein d'une organisation. Les clients reçoivent un rapport contenant des recommandations concrètes qui orientent le déploiement et les étapes suivantes.

DÉBUT DU DOCUMENT

- **Ateliers MCI**

  - **Microsoft Viva Insights**
    Nous aidons les clients à évaluer leurs besoins en téléphonie et commutateurs privés, puis nous faisons une démonstration de l'expérience d'appel de bout en bout de Microsoft Teams pour mettre en valeur Microsoft Teams Phone comme solution téléphonique. Les clients reçoivent un rapport contenant des recommandations concrètes qui orientent le déploiement et les étapes suivantes.

  - **Atténuation des risques liés à la conformité et à la protection des renseignements personnels (anciennement Gestion des risques et enquêtes associées)**
    Nous démontrons la façon dont Microsoft Purview aide les clients à déceler les risques, enquêter et prendre des mesures pour les atténuer et assurer la conformité dans leur lieu de travail moderne. Les clients reçoivent un rapport contenant des recommandations concrètes qui orientent le déploiement et les étapes suivantes.

  - **Modernisation des communications**
    Nous obtenons une visibilité sur les objectifs informatiques professionnels hybrides de l'utilisateur final du client et faisons des démonstrations des solutions Windows 11, Windows 365 et Azure Virtual Desktop qui fournissent une expérience de bureau sûre à partir de presque n'importe où.

  - **Windows Nouvelle génération (anciennement Points d'extrémité de nouvelle génération)**
    Les clients reçoivent un rapport contenant des recommandations concrètes qui orientent le déploiement et les étapes suivantes.

  - **Protection et gouvernance des données sensibles (anciennement Découverte des données sensibles)**
    Nous aidons les clients à comprendre, gérer et atténuer les risques cachés en matière de confidentialité et de réglementation dans leur propre environnement avec Microsoft Purview. Les clients reçoivent un rapport contenant des recommandations concrètes qui orientent le déploiement et les étapes suivantes.

  - **Identités et accès sécurisés (anciennement Sécurisation des identités)**
    Nous aidons les clients à déceler et à atténuer les risques liés à l'identité et à protéger leur organisation avec une solution d'identité intégrée. Les clients reçoivent un rapport contenant des recommandations concrètes qui orientent le déploiement et les étapes suivantes.

  - **Sécurisation des environnements multinuagiques (anciennement Sécurité infonuagique hybride)**
    Nous aidons les clients à identifier les risques actuels et continus pour leur environnement infonuagique à l'aide de Microsoft Defender for Cloud et d'Azure Network Security afin de définir les prochaines étapes en vue d'accélérer leur parcours de sécurité. Les clients reçoivent un rapport contenant des recommandations concrètes qui orientent le déploiement et les étapes suivantes.

  - **Microsoft Defender for Endpoint, Office 365 et Identity Protection**
    Nous aidons les clients à gérer leurs appareils sur place. Solutions également disponibles : déploiement du système d'exploitation et des applications, mises à jour, application de correctifs, organisation des politiques en plusieurs couches et application de politiques, mesures correctives et rapports, cogestion avec Intune et 365 Endpoint Manager.

  - **Microsoft Intune/Gestion des appareils mobiles**
    Cette plateforme aide les clients à gérer, à analyser, à automatiser et à comprendre leurs données et à les utiliser pour atteindre plus rapidement leurs objectifs commerciaux.

  - **Déploiement de Microsoft Teams**
    Migrez les fichiers de votre serveur de fichiers réseau vers SharePoint Online et OneDrive for Business dans un stockage infonuagique sécurisé hébergé par Microsoft pour avoir accès à vos fichiers à partir de n'importe quel appareil avec une connexion Internet à l'intérieur et à l'extérieur de votre réseau d'entreprise sans avoir besoin de RPV.

  - **Microsoft Teams Voice – VoIP en nuage**
    Déployez Microsoft Teams pour travailler avec des coéquipiers par clavardage dans un espace de travail sécurisé, organisez des réunions par vidéoconférence, collaborez avec des documents et bénéficiez d'un stockage infonuagique intégré et d'une solution d'intégration d'applications.

DÉBUT DU DOCUMENT

- **Microsoft Viva : Viva Topics, Viva Insights, Viva Connections et Viva Learning**
  Nous emmenons votre système téléphonique dans le nuage avec Teams Voice, en ajoutant des capacités d'appel téléphonique à des logiciels de collaboration modernes, permettant aux organisations d'avoir des réceptions automatisées, des files d'attente d'appels et des numéros de conférence.

- **Évaluations des meilleures pratiques Microsoft/Office 365**
  Demandez à un ingénieur-conseil en prestation de services de CDW d'évaluer votre environnement Microsoft 365 pour vous assurer que Teams, SharePoint, OneDrive ainsi que les contrôles, politiques et paramètres de base du centre d'administration de Microsoft 365 sont configurés de façon à s'aligner sur les meilleures pratiques recommandées par Microsoft. Nous fournissons un rapport sur l'état actuel de votre locataire avec une liste de recommandations concrètes classées par ordre de priorité pour vous aider à identifier et corriger les problèmes potentiels dans votre environnement.

- **Migration vers Microsoft/Office 365 : Exchange, SharePoint, OneDrive, Lync/SFB vers Teams**
  Migrez vos courriels, vos fichiers et vos messages instantanés dans Microsoft 365 pour exploiter la puissance des applications et services infonuagiques avec un accès n'importe où et depuis n'importe quel appareil.

- **Authentification multifactorielle/accès conditionnel**
  Renforcez votre sécurité pour protéger les actifs de votre organisation en instaurant l'authentification multifactorielle; les personnes souhaitant accéder à votre environnement devront au préalable confirmer leur identité au moyen de plusieurs facteurs, et non plus seulement avec un mot de passe. Utilisez les politiques d'accès conditionnel pour appliquer les contrôles d'accès appropriés au besoin et assurer la sécurité de votre organisation.

- **SCCM/gestionnaire des points d'extrémité Microsoft**
  Microsoft Power Platform est une puissante gamme d'applications qui permettent aux clients d'automatiser les processus, de concevoir des solutions, d'analyser des données et de créer des agents virtuels.

- **Mise en œuvre de SharePoint/OneDrive**
  Déployez les modules de la suite Microsoft Viva dans Microsoft Teams pour améliorer le bien-être des employés avec Viva Insights; mobilisez et informez les employés avec un contenu personnalisé dans Viva Connections; créez un système de gestion des connaissances qui associe, gère et protège les connaissances et l'expertise avec Viva Topics; et créez un centre d'apprentissage où les employés peuvent explorer, partager, recommander et apprendre avec Viva Learning.

- **Évaluation de la solution – Évaluation de la sécurité infonuagique**
  Nous évaluons votre posture de sécurité dans votre environnement infonuagique afin de l'aligner sur une liste de recommandations concrètes classées par ordre de priorité pour vous aider à identifier et corriger les risques de sécurité potentiels.

- **Windows Hello for Business**
  Windows Hello for Business remplace les mots de passe utilisés sur les appareils par une authentification forte à deux facteurs. Cette authentification consiste en un nouveau type de certificat d'utilisateur lié à un appareil et utilisant un code biométrique ou un NIP.

DÉBUT DU DOCUMENT

Services multinuagiques

- **Automatisation – Démarrage rapide**
  Une approche simplifiée de l'automatisation d'une charge de travail, conçue pour se concentrer sur une charge de travail prédéterminée et tirer parti des principes modernes d'automatisation pour mettre en place rapidement et facilement une solution entièrement automatisée dans le nuage.
  Fournisseurs pris en charge : Azure

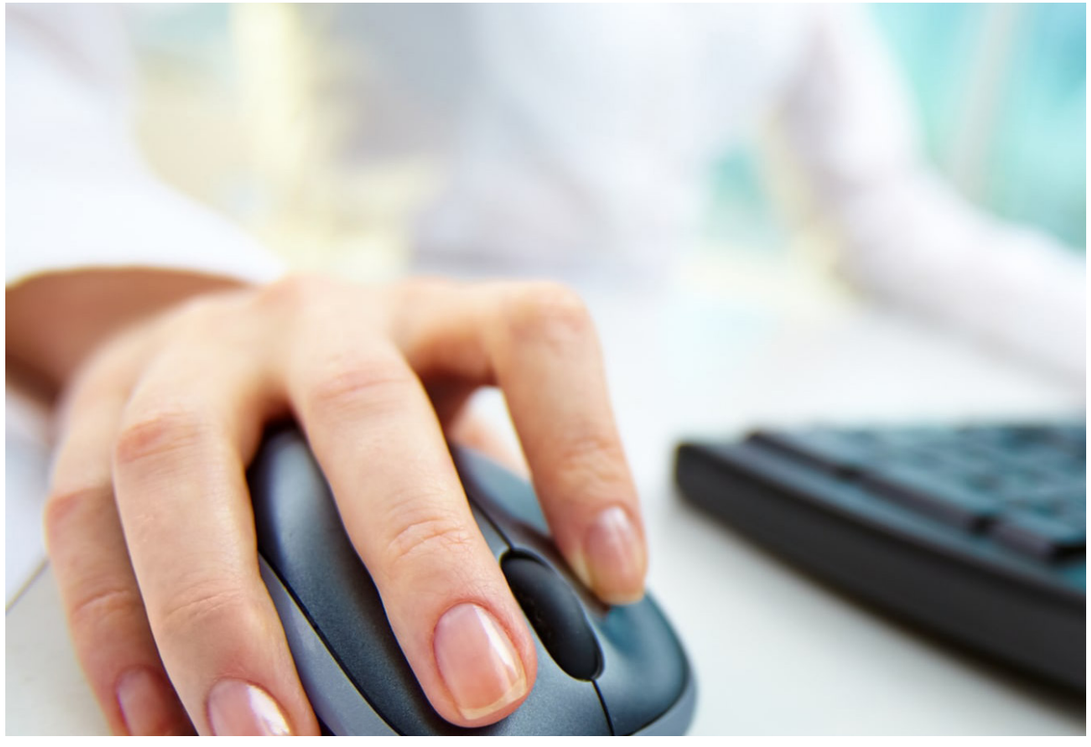
- **CIS – Évaluation des meilleures pratiques**
  Nous examinons en profondeur l'environnement infonuagique actuel du client pour nous assurer qu'il répond aux exigences du cadre. Nous recommandons des mesures correctives.
  Fournisseurs pris en charge : AWS et Azure

- **Communauté virtuelle**
  Profitez des affaires internationales de CDW tout en conservant votre réseau et vos données ici au Canada, avec des services tels que les communications unifiées en tant que service (UCaaS), la sauvegarde en tant que service (BUaaS), la récupération après sinistre en tant que service (DRaaS) et la connectivité.
  Fournisseurs pris en charge : 8x8, Convergia et RingCentral

- **Récupération après sinistre dans le nuage (DRaaS)**
  Nous déployons, adoptons et intégrons la protection des données dans le nuage public de façon sécuritaire. Nous mettons votre environnement à l'échelle au besoin, vous tenons au courant de tout changement et vous aidons à maximiser le rendement du capital investi (RCI) dans le nuage et à atteindre plus rapidement vos résultats commerciaux.
  Fournisseurs pris en charge : AWS, Azure et Commvault

- **Zone d'atterrissage infonuagique**
  Mobilisez des services professionnels pour élaborer les exigences et les services de base d'un environnement infonuagique. Ces services de base garantissent que le client est prêt à réussir dans les activités infonuagiques et la croissance future de son entreprise.
  Fournisseurs pris en charge : AWS et Azure

- **Migration infonuagique – Démarrage rapide**
  Un engagement programmatique conçu pour aider rapidement et facilement les clients dans leur migration vers le nuage.
  Fournisseurs pris en charge : AWS et Azure



DÉBUT DU DOCUMENT

- **Évaluation de l'état de préparation à la migration vers le nuage**
  Examen approfondi des facteurs techniques et commerciaux qui auront une incidence sur l'état de préparation de la charge de travail au nuage public. Il fournit aux clients l'analyse financière et technique de chaque charge de travail et recommande l'état à prévoir à l'avenir qui répondra aux exigences du client.
  Fournisseurs pris en charge : AWS et Microsoft

- **Évaluation pour une migration de base de données**
  Évaluation des données existantes sur place pour migrer dans le nuage (par exemple SQL ou MySQL).
  Fournisseurs pris en charge : AWS et Azure

- **Migration du courriel Microsoft Office 365**
  Services d'intégration et services complets de migration de boîte aux lettres électronique pour Microsoft Office 365 (courriel, éléments de l'agenda, tâches, données, fichiers PST locaux et publics).
  Fournisseurs pris en charge : Microsoft

- **Programme d'accès en ligne à distance Jumpstart pour Microsoft 365 Business Voice**
  Déploiement de base de Business Voice au moyen de Microsoft Teams.
  Fournisseurs pris en charge : Microsoft

- **Atelier sur la sécurité de Microsoft 365**
  Atelier d'habilitation visant à garantir que le client choisit les bons produits à mettre en œuvre dans O365 (comme Microsoft Defender pour O365).
  Fournisseurs pris en charge : Microsoft

- **État de préparation aux réunions Microsoft Teams**
  Évaluation de l'environnement du client pour déterminer si la solution Microsoft Teams peut être adoptée.
  Fournisseurs pris en charge : Microsoft

DÉBUT DU DOCUMENT

- **Veeam – Démarrage rapide**
  Évaluation des composantes actuelles du client sur le plan de l'environnement, de l'architecture, de l'installation et de la configuration de la solution Veeam Availability Suite, y compris Veeam Backup and Recovery et Veeam One Server.
  Fournisseurs pris en charge : Veeam

- **Projet pilote de bureau virtuel**
  Projet pilote et déploiement d'Enterprise Production sur Azure Virtual Desktop (AVD).
  Fournisseurs pris en charge : Microsoft

- **Un cadre bien structuré**
  L'examen bien structuré est une approche systématique d'évaluation des architectures infonuagiques et peut vous aider à identifier et corriger les problèmes potentiels concernant votre environnement.
  Fournisseurs pris en charge : AWS et Azure

- **Réunions et Voix avec l'adoption**
  Évaluez l'environnement existant en vue d'adopter Microsoft Teams.
  Fournisseurs pris en charge : Microsoft

- **Évaluation de Windows Autopilot (Intune)**
  Permet d'automatiser l'intégration et la personnalisation d'un appareil qui est expédié directement à l'utilisateur final.
  Fournisseurs pris en charge : Microsoft

- **Évaluation de Windows Autopilot et préprovisionnement avec Intune**
  Évaluation Intune pour garantir que les clients sont prêts à recevoir des services de pointe.
  Fournisseurs pris en charge : Microsoft

DÉBUT DU DOCUMENT

Services infonuagiques gérés

À mesure que les environnements d'informatique en nuage (infonuagiques) gagnent en complexité, vous avez besoin du bon fournisseur de services doué des compétences et de l'expérience requises pour faire passer vos applications et services en nuage au rang supérieur. CDW a acquis des années d'expérience dans la gestion de plateformes en nuage et la fourniture à nos clients du discernement, des perspectives, du soutien et du savoir-faire en nuage dont vous avez besoin pour garder une longueur d'avance sur le marché. Appelez l'équipe responsable de votre compte pour discuter de la façon dont CDW peut vous aider à atteindre vos objectifs commerciaux à l'aide de l'infonuagique.

- **Services AWS gérés**
  Avec la croissance des services et des infrastructures infonuagiques, les entreprises ont plus de difficulté à gérer les technologies complexes. CDW vous aidera à adopter et à intégrer AWS en toute sécurité et fournira un soutien continu; CDW peut également gérer votre environnement pour vous. CDW peut vous aider à mettre les environnements à l'échelle au besoin, et vous tenir au courant de tout changement. Elle vous aide à maximiser le rendement du capital investi (RCI) dans la solution AWS et à atteindre plus rapidement vos résultats commerciaux.

- **Services Azure gérés**
  La gestion d'un environnement infonuagique en constante évolution exige des compétences précises, particulièrement lorsque la production ou les systèmes critiques pour l'entreprise doivent rester en ligne sans interruption. Notre gamme complète de services gérés de prochaine génération pour Azure est appuyée par plus de 20 ans d'expérience en soutien de services gérés. En faisant appel à CDW, un partenaire reconnu et de confiance, vous aidez votre entreprise à maintenir un fonctionnement optimal.

DÉBUT DU DOCUMENT

Espace de travail numérique

À CDW, nous pouvons vous permettre de tirer parti de la technologie pour habiliter vos employés, servir vos clients et créer des expériences exceptionnelles. Explorez nos solutions d'espaces de travail numériques qui vont du point d'extrémité à l'espace de travail en passant par la productivité et la collaboration.

- **Automatisation des processus opérationnels : Power Apps, Power Automate Flow et Azure Logic Apps**
  Évaluez votre posture de sécurité et votre situation de conformité dans votre environnement Microsoft 365 pour vous aligner sur les meilleures pratiques recommandées par Microsoft. Nous fournissons un rapport sur l'état actuel de votre locataire avec une liste de recommandations concrètes classées par ordre de priorité pour vous aider à identifier et corriger les problèmes de sécurité potentiels dans votre environnement.

- **Migration du courriel Microsoft Office 365**
  Services d'intégration et services complets de migration de boîte aux lettres électronique pour Microsoft Office 365 (courriel, éléments de l'agenda, tâches, données, fichiers PST locaux et publics).

- **Programme d'accès en ligne à distance Jumpstart pour Microsoft 365 Business Voice**
  Déploiement de base de Business Voice au moyen de Microsoft Teams.

- **Microsoft Intune/Gestion des appareils mobiles**
  Cette plateforme aide les clients à gérer, à analyser, à automatiser et à comprendre leurs données et à les utiliser pour atteindre plus rapidement leurs objectifs commerciaux.

- **État de préparation aux réunions Microsoft Teams**
  Évaluation de l'environnement du client pour déterminer si la solution Microsoft Teams peut être adoptée.

- **Déploiement de Microsoft Teams**
  Migrez les fichiers de votre serveur de fichiers réseau vers SharePoint Online et OneDrive for Business dans un stockage infonuagique sécurisé hébergé par Microsoft pour avoir accès à vos fichiers à partir de n'importe quel appareil avec une connexion Internet à l'intérieur et à l'extérieur de votre réseau d'entreprise sans avoir besoin de RPV.

- **Microsoft Teams Voice – VoIP en nuage**
  Déployez Microsoft Teams pour travailler avec des coéquipiers par clavardage dans un espace de travail sécurisé, organisez des réunions par vidéoconférence, collaborez avec des documents et bénéficiez d'un stockage infonuagique intégré et d'une solution d'intégration d'applications.

- **Microsoft Viva : Viva Topics, Viva Insights, Viva Connections et Viva Learning**
  Transférez votre système téléphonique dans le nuage avec Teams Voice, en ajoutant des capacités d'appel du système téléphonique à un logiciel de collaboration moderne, permettant aux organisations d'avoir des répondeurs automatiques, des files d'attente d'appels et des numéros de conférence.

- **Évaluations des meilleures pratiques Microsoft/Office 365**
  Demandez à un ingénieur-conseil de CDW d'évaluer votre environnement Microsoft 365 pour garantir que vos contrôles, politiques et paramètres de base de Teams, de SharePoint, de OneDrive et du Centre d'administration Microsoft 365 sont configurés pour s'aligner sur les meilleures pratiques recommandées par Microsoft. Nous fournissons un rapport sur l'état actuel de votre locataire avec une liste hiérarchisée de recommandations exploitables pour vous aider à identifier et à résoudre les problèmes potentiels dans votre environnement.

- **SCCM/Microsoft Endpoint Manager**
  Microsoft Power Platform est un ensemble d'applications puissantes qui permettent au client d'automatiser des processus, de construire des solutions, d'analyser des données et de créer des agents virtuels.

- **Pilote de bureau virtuel**
  Déploiement pilote et de production d'entreprise d'Azure Virtual Desktop (AVD).

- **Solutions de bureau virtuel**
  Déploiements New Horizon, mises à niveau de déploiements existants et évaluations de l'état de santé.

- **Voix et réunions avec adoption**
  Évaluation de l'environnement existant pour passer à l'adoption de Microsoft Teams.

- **Démonstration de faisabilité de Windows 11**
  Windows 11 comporte de nombreuses nouvelles fonctionnalités pour aider les entreprises à être plus sûres, plus mobiles et plus productives. Une démonstration de faisabilité de Windows 11 vous aide à évaluer l'état de préparation de votre environnement et à déployer Windows 11 avec un impact minimal sur l'entreprise.

- **Évaluation de Windows Autopilot (Intune)**
  Permet d'automatiser l'intégration et la personnalisation d'un appareil livré directement à l'utilisateur final.

DÉBUT DU DOCUMENT

- **Évaluation de Windows Autopilot et préprovisionnement avec Intune**
  Évaluation Intune pour garantir que les clients sont prêts à recevoir des services de pointe.

- **Windows Hello for Business**
  Windows Hello for Business remplace les mots de passe utilisés sur les appareils par une authentification forte à deux facteurs. Cette authentification consiste en un nouveau type de certificat d'utilisateur lié à un appareil et utilisant un code biométrique ou un NIP.

Copilot

- **Atelier sur l'état de préparation à Copilot for Microsoft 365**
  L'atelier de CDW sur l'état de préparation à Copilot for Microsoft 365 aidera les décideurs de votre entreprise à planifier l'itinéraire spécifique que vous allez emprunter dans le cadre de votre parcours avec Copilot for Microsoft 365 et à visualiser en combien de temps vous pourrez atteindre la destination désirée.

- **Évaluation de la gouvernance de Copilot for Microsoft 365**
  Lors de l'évaluation de la gouvernance de Copilot for Microsoft 365, nos conseillers en infonuagique pour Microsoft 365 appuieront votre équipe Copilot avec leur expérience et leurs conseils avisés. Nous examinerons vos systèmes en profondeur et vous donnerons des conseils détaillés sur la façon dont vous pouvez préparer votre infrastructure Microsoft 365, la gouvernance des données, la sécurité et la conformité.

Point d'extrémité (AV, EDR, XDR)

- **Vérification de l'intégrité des points d'extrémité**
  Nous examinons la conception et la mise en œuvre de la technologie de point d'extrémité et fournissons des conseils sur les améliorations qui peuvent être apportées.

- **Migration/Mise en œuvre des points d'extrémité**
  Nouveau déploiement : le déploiement se fait à partir de rien; aucune technologie de point d'extrémité existante n'est utilisée. Migration : si le client estime que la technologie de point d'extrémité est inefficace ou que son entretien pour la maintenir efficace est coûteux, CDW la retire et la remplace par une technologie plus appropriée.

Ateliers MCI

- **Azure Defender for Cloud (anciennement le « Centre de sécurité »)**
  Nous examinons la conception et la mise en œuvre de la technologie de point d'extrémité et fournissons des conseils sur les améliorations qui peuvent être apportées.

- **Applications collaboratives (anciennement Applications et solutions Teams)**
  Examinez divers défis et problèmes auxquels font face les travailleurs de première ligne afin d'identifier les scénarios prioritaires pour l'effectif de première ligne des clients. Les clients reçoivent un rapport contenant des recommandations concrètes qui orientent le déploiement et les étapes suivantes.

- **Défense contre les menaces avec SIEM Plus XDR (anciennement Threat Protection)**
  Nous comprenons les objectifs de sécurité des clients, puis identifions les véritables menaces de sécurité à travers le courriel, l'identité et les données dans leur environnement de production pour mettre en valeur l'expérience Microsoft Sentinel et Microsoft 365 Defender. Les clients reçoivent un rapport contenant des recommandations concrètes qui orientent le déploiement et les étapes suivantes.

- **Habilitation des intervenants de première ligne**
  Nous présentons la valeur de Microsoft Endpoint Manager pour montrer aux clients comment gérer les appareils, les applications et les identités des utilisateurs de partout. Les clients reçoivent un rapport contenant des recommandations concrètes qui orientent le déploiement et les étapes suivantes.

- **Gestion des points d'extrémité**
  Montrez le potentiel des expériences de réunions hybrides et des salles de réunion de Microsoft Teams qui permettent aux gens de travailler de n'importe où, en tout temps. Les clients reçoivent un rapport contenant des recommandations concrètes qui orientent le déploiement et les étapes suivantes.

- **Réunions et salles hybrides (anciennement Réunions hybrides)**
  Nous aidons les clients au tout début de leurs transformations infonuagiques à envisager des scénarios de travail agiles et à imaginer une façon d'habiliter leurs employés à travailler de manière productive et en toute sécurité avec Microsoft 365. Les clients reçoivent un rapport contenant des recommandations concrètes qui orientent le déploiement et les étapes suivantes.

- **Microsoft 365 Digital Workforce (anciennement Transition vers le nuage)**
  Nous découvrons les scénarios d'affaires uniques des clients, soulignons l'expérience de transformation des employés et mettons en valeur le potentiel de la suite Viva avec ses composantes Topics, Connections ou Learning. Les clients reçoivent un rapport contenant des recommandations concrètes qui orientent le déploiement et les étapes suivantes.

- **Microsoft Viva**
  Nous aidons les clients à découvrir comment Microsoft Viva Insights permet à l'effectif, aux gestionnaires et aux responsables d'obtenir des indications personnalisées et des recommandations concrètes qui contribuent à l'épanouissement de tous au sein d'une organisation. Les clients reçoivent un rapport contenant des recommandations concrètes qui orientent le déploiement et les étapes suivantes.

- **Microsoft Viva Insights**
  Nous aidons les clients à évaluer leurs besoins en téléphonie et commutateurs privés, puis faisons une démonstration de l'expérience d'appel de bout en bout de Microsoft Teams pour mettre en valeur Microsoft Teams Phone comme solution téléphonique. Les clients reçoivent un rapport contenant des recommandations concrètes qui orientent le déploiement et les étapes suivantes.

- **Modernisation des communications**
  Nous obtenons une visibilité sur les objectifs informatiques professionnels hybrides de l'utilisateur final du client et faisons des démonstrations des solutions Windows 11, Windows 365 et Azure Virtual Desktop qui fournissent une expérience de bureau sûre à partir de presque n'importe où.

- **Windows Nouvelle génération (anciennement Points d'extrémité de nouvelle génération)**
  Les clients reçoivent un rapport contenant des recommandations concrètes qui orientent le déploiement et les étapes suivantes.

DÉBUT DU DOCUMENT

Services de sécurité

Les services de sécurité de CDW Canada fournissent des évaluations indépendantes de votre posture de sécurité et ils vous aident à mieux gérer vos faiblesses. Nos experts certifiés conçoivent des stratégies et des solutions complètes de protection et de réaction.

Services de sécurité professionnels

Vous pouvez compter sur notre équipe d'experts pour mettre en œuvre et examiner vos services de sécurité professionnels. Nous disposons également de centres de formation autorisés pour aider votre équipe interne à tirer parti au maximum de vos technologies de sécurité.

[Explorer les services de sécurité gérés]

- **Centre de formation autorisé**
  CDW est le seul centre de formation autorisé pour F5 et Palo Alto Networks. Plusieurs cours et dates sont disponibles et peuvent être réservés en conséquence sur le portail des centres de formation autorisés de CDW.
  Fournisseurs pris en charge : F5 et Palo Alto

- **Évaluation de la posture de sécurité infonuagique**
  Nous aidons les clients à obtenir une visibilité en ce qui concerne les mauvaises configurations possibles dans le nuage public IaaS ou PaaS dans AWS, Azure ou GCP. Ce service tire parti d'un outil de gestion de la posture de sécurité infonuagique pour interroger le nuage public ciblé et fournir des conclusions et des recommandations pour tous les écarts et risques identifiés. Le but est de stimuler les ventes d'outils de gestion de la posture de sécurité infonuagique et les mesures de correction potentielles du nuage.
  Fournisseurs pris en charge : AWS, Azure et GCP

POINT D'EXTRÉMITÉ (AV, EDR, XDR)

- **Vérification de l'intégrité des points d'extrémité**
  Nous examinons la conception et la mise en œuvre de la technologie de point d'extrémité et fournissons des conseils sur les améliorations qui peuvent être apportées.
  Fournisseurs pris en charge : CrowdStrike, Cylance, Microsoft et Palo Alto

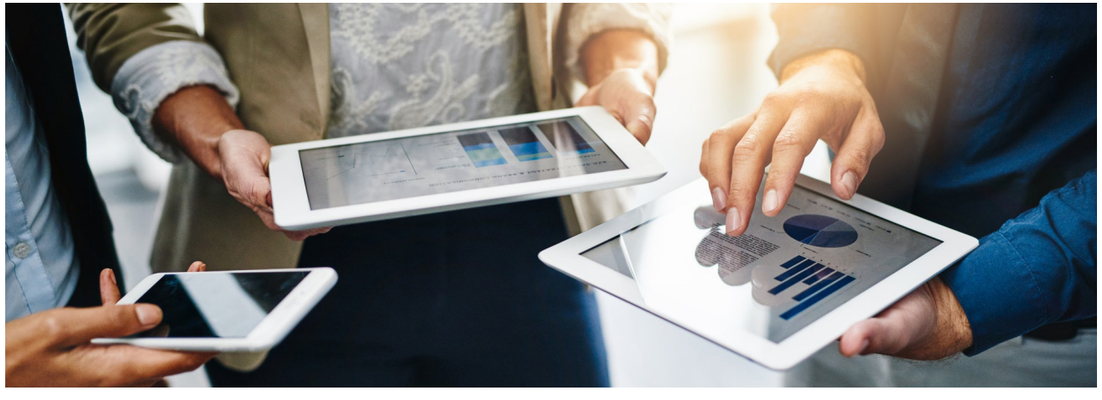
- **Migration/Mise en œuvre des points d'extrémité**
  Nouveau déploiement : le déploiement se fait à partir de rien; aucune technologie de point d'extrémité existante n'est utilisée. Migration : si le client estime que la technologie de point d'extrémité est inefficace ou que son entretien pour la maintenir efficace est coûteux, CDW la retire et la remplace par une technologie plus appropriée.
  Fournisseurs pris en charge : CrowdStrike, Cylance, Microsoft et Palo Alto

GESTION DES IDENTITÉS ET DES ACCÈS

- **IAM/SSO/Migration/Mise en œuvre**
  Certains clients souhaitent mettre en œuvre la gestion de l'identité sans solution actuellement en place. Intégration du protocole LDAP (lightweight directory access protocol)/AD (active directory) et intégration de l'authentification unique (SSO) dans les applications de l'entreprise.

  Certains clients cherchent à remplacer leur solution de gestion de l'identité par une solution IAM actuellement en place. Amélioration de la technologie et de l'architecture grâce à une configuration LDAP/AD et SSO déjà en place.
  Fournisseurs pris en charge : Centrify, Microsoft et Okta

- **Vérification de l'intégrité des solutions IAM/SSO**
  Nous examinons la mise en œuvre actuelle des solutions IAM/SSO et fournissons un rapport pour indiquer des domaines d'amélioration possibles.
  Fournisseurs pris en charge : Centrify, Microsoft et Okta



DÉBUT DU DOCUMENT

SÉCURITÉ DU RÉSEAU

- **Services de déploiement rapide des pare-feu de nouvelle génération (NGFW)**
  Déploiement rapide pour mettre en œuvre une solution nouvelle de NGFW ou pour effectuer une migration à l'identique entre les plateformes de pare-feu des fournisseurs.
  Fournisseurs pris en charge : Fortinet et Palo Alto Networks

- **Vérification de l'intégrité des pare-feu de nouvelle génération (NGFW)**
  Examen approfondi du débit du pare-feu NGFW, de son architecture, de sa conception et de sa disponibilité pour assurer un fonctionnement stable.
  Fournisseurs pris en charge : Cisco, Fortinet, Palo Alto Networks et SonicWall (avec le soutien des partenaires)

- **Services de mise en œuvre des pare-feu de nouvelle génération (NGFW)**
  Conception et mise en œuvre d'une solution nouvelle de NGFW ou migration à l'identique entre les plateformes de pare-feu des fournisseurs.
  Fournisseurs pris en charge : Cisco, Fortinet et Palo Alto Networks

- **Mise en œuvre du SD-WAN**
  Découverte, conception et mise en œuvre d'une solution de réseau étendu défini par logiciel (SD-WAN), en commençant par la compilation des besoins des clients, l'identification des infrastructures actuelles et la conception d'une solution de SD-WAN. Tout ceci est suivi d'une migration par étapes des services de production.
  Fournisseurs pris en charge : Cisco, Fortinet et Palo Alto Networks

- **Service de déploiement rapide de la solution SASE**
  Déploiement rapide pour la mise en oeuvre d'une nouvelle solution SASE (Secure Access Service Edge).
  Fournisseurs pris en charge : Cisco, Fortinet et Palo Alto Networks

- **Services de déploiement rapide de FortiGate**
  Déploiement rapide pour mettre en œuvre une solution nouvelle de pare-feu NGFW ou pour effectuer une migration à l'identique entre les plateformes de pare-feu des fournisseurs.
  Fournisseurs pris en charge : Fortinet

- **Actualisation de NGFW Palo Alto Networks**
  Gérer le vieillissement du matériel informatique ne doit pas forcément être un défi à relever. L'équipe des services de sécurité professionnels de CDW possède l'expertise et l'expérience voulues pour vous aider à actualiser le matériel pour votre infrastructure Palo Alto Networks existante.
  Fournisseurs pris en charge : Palo Alto Networks

- **Services de mise à niveau de PAN-OS**
  Les arrêts de production causés par les mises à niveau peuvent coûter cher à votre entreprise. Notre équipe a l'expertise et l'expérience pour vous aider à planifier et à corriger votre infrastructure Palo Alto Networks afin d'éviter les temps d'indisponibilité et de garantir que vos mises à niveau se font de la façon la plus harmonieuse possible.
  Fournisseurs pris en charge : Palo Alto Networks

- **Mise en œuvre de la solution SASE**
  Découverte, conception et mise en œuvre d'une solution SASE (Secure Access Service Edge), en commençant par la compilation des besoins des clients, l'identification des infrastructures actuelles et la conception d'un cadre SASE. Tout ceci est suivi d'une migration par étapes des services de production.
  Fournisseurs pris en charge : Palo Alto Networks

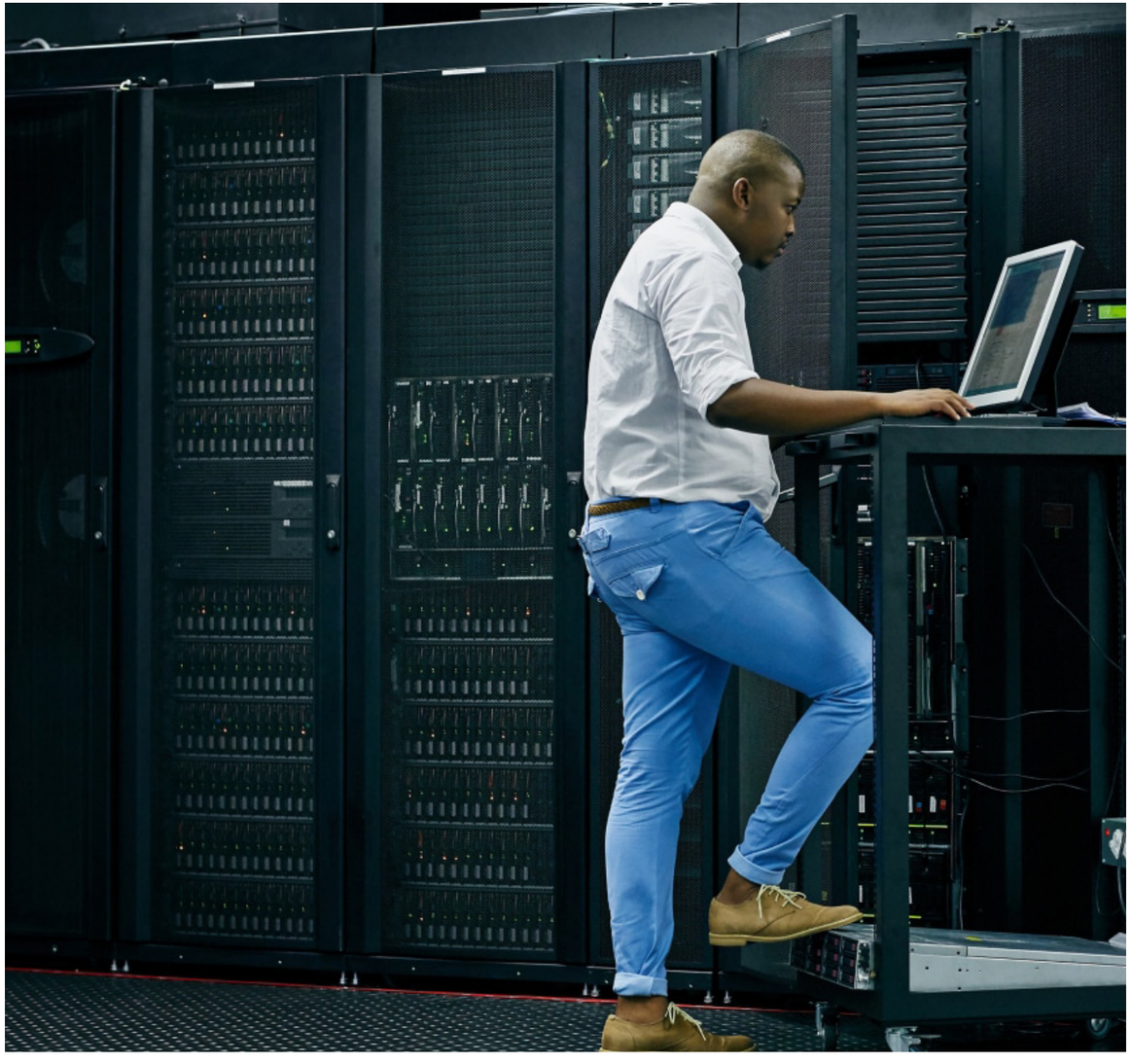
DÉBUT DU DOCUMENT

SIEM ET ANALYSES

- **Vérification de l'intégrité de la solution SIEM**
  Nous examinons une plateforme existante pour nous assurer que sa configuration lui permet de fonctionner de manière optimale et qu'elle renferme le bon contenu et les bonnes sources de journalisation pour prendre en charge une surveillance de sécurité appropriée.
  Fournisseurs pris en charge : LogRhythm et Splunk

- **Migration/Mise en œuvre de la solution SIEM**
  Conception et mise en œuvre d'une solution SIEM à partir de rien, y compris l'installation et la configuration de logiciels, l'intégration des sources de journalisation, ainsi que la mise en œuvre de cas d'alertes et d'utilisation, de rapports et de tableaux de bord, selon les exigences du client.
  Dans le cas des migrations, nous travaillons en étroite collaboration avec le client pour comprendre ce qu'il faut transférer de la solution existante pour le conserver et ce qui peut être déclaré obsolète.
  Fournisseurs pris en charge : LogRhythm et Splunk

- **Mise à niveau de la solution SIEM**
  Examen du système et vérification de l'intégrité de fonctionnement d'une plateforme existante, suivis de la planification et de l'exécution d'une mise à niveau de la plateforme. Selon l'ancienneté de la plateforme, de nombreuses mises à niveau pourraient être nécessaires, ainsi qu'un examen des exigences en matière de mémoire, de calcul et de stockage pour les dernières versions logicielles.
  Fournisseurs pris en charge : LogRhythm et Splunk



DÉBUT DU DOCUMENT

SÉCURITÉ MICROSOFT

- **Déploiement rapide de la solution IAM Azure Active Directory**
  Microsoft Entra est une suite de solutions d'identité basées sur le nuage qui fournissent un ensemble de capacités de gestion des identités et des accès. Azure AD, solution de base de Microsoft Entra, fournit l'identité en tant que caractéristiques et capacités de service, y compris la gestion de l'identité unifiée dans le nuage, l'authentification unique, l'accès conditionnel, la protection de l'identité et la gestion du cycle de vie de l'identité. Ce déploiement rapide, optimisé pour les petites et moyennes entreprises, permet aux clients de concrétiser rapidement la valeur de leur investissement dans Azure AD.

- **Déploiement avancé de la solution IAM Azure AD**
  Ce service est une extension de l'offre de service de déploiement rapide; il inclut la configuration des politiques d'accès conditionnel avancé, la fourniture d'applications, le déploiement de serveurs mandataires d'applications et le provisionnement distant d'applications sur place.

- **Déploiement rapide de M365 Defender**
  Microsoft 365 Defender est une solution XDR qui coordonne nativement la détection, la prévention, les enquêtes et les réponses entre les points d'extrémité, les identités, les courriels et les applications. Ce déploiement rapide, optimisé pour les petites et moyennes entreprises, permet aux clients de rentabiliser leur investissement dans la sécurité de Microsoft 365.

- **Déploiement avancé de M365 Defender**
  Comme le service de démarrage rapide, cette solution fournit des services d'installation et de configuration de base pour Defender for Endpoint, Defender for Identity et Defender for O365. Elle comprend également la configuration de fonctionnalités avancées telles que les règles de détection personnalisées, les politiques d'alerte personnalisées, le filtrage de contenu Web, les simulations d'hameçonnage et l'intégration de la solution SIEM.

- **Déploiement rapide de la protection contre la perte de données Microsoft Purview**
  Microsoft Purview est une plateforme avancée de gouvernance, de risques et de conformité des données qui permet aux organisations de régir, de protéger et de gérer leurs données. Avec les capacités de prévention des pertes de données de Microsoft Purview, les organisations peuvent définir des profils d'informations sensibles et les détecter dans les informations pour les protéger contre l'échange non intentionnel ou accidentel d'informations sensibles. Ce déploiement rapide, optimisé pour les petites et moyennes entreprises, permet aux clients de concrétiser rapidement la valeur de leur investissement dans la prévention des pertes de données avec Microsoft Purview.

- **Déploiement de la découverte et de la classification des données**
  Microsoft Purview Information Protection est un ensemble de fonctionnalités qui peuvent être mises à profit pour découvrir, classer et appliquer une protection à des données sensibles. Ce service comprend la configuration des étiquettes de sensibilité, des types d'informations sensibles personnalisées, des politiques d'étiquettes de sensibilité et le déploiement de lecteurs sur place.

- **Déploiement avancé de la prévention des pertes de données**
  Ce service est une extension de l'offre de service de démarrage rapide; il inclut la configuration des types d'informations sensibles personnalisées, des politiques de prévention de pertes de données avancées, des conditions des politiques de prévention de pertes de données personnalisées et le déploiement de lecteurs sur place.

- **Déploiement rapide de Sentinel**
  Microsoft Sentinel est une plateforme avancée d'analyse de sécurité, de renseignements sur les menaces, de chasse aux menaces et d'automatisation qui permet aux organisations de corréler les signaux de menace de multiples sources pour accroître la détection des attaques, augmenter la visibilité des menaces et accélérer la réaction face aux incidents. Ce déploiement rapide, optimisé pour les petites et moyennes entreprises, permet aux clients de réaliser rapidement la valeur de leur investissement dans Microsoft Sentinel.

DÉBUT DU DOCUMENT

Services de sécurité gérés

De nombreuses organisations canadiennes ne sont pas confiantes en ce qui concerne leur capacité à détecter des atteintes à la cybersécurité et à y répondre. Une expertise interne non adéquate et un nombre d'employés compétents insuffisant sont les deux raisons principales mentionnées par les répondants pour expliquer pourquoi ils ne peuvent pas gérer leur posture de sécurité efficacement. Les services de sécurité gérés de CDW vous permettent de tirer profit des compétences, de la technologie et de l'expertise très spécialisées de CDW, celles-ci étant directement adaptées en fonction des besoins de votre entreprise pour un coût mensuel prévisible.

- **Solution Defender gérée**
  La gestion par CDW de la détection et de la réponse avec Defender for Endpoint permet une détection avancée des menaces grâce à la corrélation automatique des événements, pour une qualification des incidents, une réponse et un endiguement des menaces plus rapides.
  Nous associons les capacités de détection, de prévention, d'enquête et de réponse de Defender for Endpoint à un analyste responsable de la surveillance, de l'analyse et de la correction des menaces en tout temps.
  Fournisseurs pris en charge : Microsoft

- **NGFW (pare-feu de nouvelle génération) géré**
  Avec la croissance des services et des infrastructures infonuagiques, les entreprises ont plus de difficulté à gérer les technologies complexes. CDW vous aidera à adopter et à intégrer un NGFW en toute sécurité et fournira un soutien continu; CDW peut également gérer votre environnement pour vous. CDW peut vous aider à mettre les environnements à l'échelle au besoin, et vous tenir au courant de tout changement.
  Elle vous aide à maximiser le rendement du capital investi (RCI) dans la solution NGFW et à atteindre plus rapidement vos résultats commerciaux.
  Fournisseurs pris en charge : Cisco, Fortinet et Palo Alto

- **Services gérés de Palo Alto Networks**
  La surveillance continue de la disponibilité et de la performance des solutions de Palo Alto Networks est plus facile avec les services gérés de CDW. Nos services sont gérés par des experts certifiés pour fournir une analyse approfondie et une réponse.
  Fournisseurs pris en charge : Palo Alto

  - **Cortex XDR géré**
    Permet une détection avancée des menaces grâce à la corrélation automatique des événements à travers les solutions réseau, infonuagiques et de points d'extrémité, pour une qualification des incidents, une réponse et un endiguement des menaces plus rapides. Assure en tout temps la surveillance et la gestion des menaces, la gestion du changement et de la configuration ainsi que la production de rapports de service mensuels. Simplification de la détection des menaces, de la corrélation et de la réponse en une seule solution complète.
    Fournisseurs pris en charge : Palo Alto

- **Services SASE gérés (Prisma Access)**
  Le produit SASE géré (Prisma Access) de CDW réunit en une seule plateforme toutes les capacités de réseautage et de sécurité dont les organisations ont besoin, assurant la sécurité de tout utilisateur et de toutes les applications, de partout. Cette solution comporte deux couches : la sécurité en tant que service (SaaS) et le réseau en tant que service (NaaS).
  Fournisseurs pris en charge : Palo Alto

- **Solution SD-WAN gérée (Prisma SD-WAN)**
  La solution Prisma SD-WAN est une solution qui privilégie le nuage et qui élimine les coûts des solutions réseau de commutation multiprotocole par étiquette (MPLS) coûteuses, améliore l'expérience de l'utilisateur final et offre une évolutivité pour moderniser la performance et la sécurité du réseau.
  Fournisseurs pris en charge : Palo Alto

DÉBUT DU DOCUMENT

- **SIEM géré**
  Managed Cloud SIEM fournit à nos clients un référentiel central des événements, où les données pour tous les événements de sécurité au sein d'une organisation sont stockées, analysées et exploitées. Ce service haut de gamme axé sur les renseignements est appuyé par notre équipe d'analystes des menaces qui procèdent à des analyses de sécurité détaillées et détectent les menaces.
  Fournisseurs pris en charge : Log Rhythm et Splunk

- **Sentinel géré**
  Managed Sentinel offre en tout temps à nos clients des systèmes évolués de détection des menaces, de surveillance des incidents, d'enquête, de recours et de rapports en plus de Microsoft Sentinel. Ce service haut de gamme axé sur les renseignements est appuyé par une équipe d'analystes très compétents qui procèdent à des analyses de sécurité détaillées et détectent les menaces.
  Fournisseurs pris en charge : Microsoft

- **SIEM en tant que service géré**
  Nous améliorons la posture de sécurité globale en identifiant rapidement les cybermenaces à travers le réseau et les environnements infonuagiques, en fournissant aux clients la stratégie de réponse appropriée pour se défendre contre ces menaces. La solution SIEM en tant que service offre aux clients une vue d'ensemble de la sécurité dans leur environnement en exploitant des outils de pointe. Les menaces de sécurité sont corrélées en un seul emplacement dans l'écosystème de sécurité.
  Fournisseurs pris en charge : Log Rhythm

DÉBUT DU DOCUMENT

Services-conseils en matière de risques

Les conseillers en chef de CDW peuvent vous aider à déceler les vulnérabilités de votre organisation, à créer un plan pour minimiser le cyberrisque et à orienter votre entreprise sur la façon de se conformer à la législation gouvernementale sur la protection des renseignements personnels.

Gouvernance, risque et conformité

- **Évaluation des conséquences sur l'entreprise**
  Une évaluation des conséquences sur l'entreprise vise à analyser les répercussions sur l'entreprise de la perturbation des processus et des fonctions clés. L'évaluation mettra l'accent sur l'identification des processus essentiels dans chaque secteur d'activité, l'évaluation de l'impact de la perturbation sur ces processus et la détermination des besoins en ressources pour chaque secteur d'activité.
  Le but de cet engagement est d'aider l'organisation du client à hiérarchiser la reprise des services en établissant des objectifs de reprise pour chaque secteur d'activité et ses processus associés.

- **Évaluation des écarts**
  Les évaluations des écarts fournissent aux clients une comparaison et une analyse des contrôles techniques, physiques et administratifs qui composent leur programme de sécurité ou de protection de la vie privée par rapport à une norme particulière de l'industrie. L'équipe Cyberrisque est capable d'effectuer des évaluations des écarts par rapport à diverses normes de sécurité et de protection de la vie privée de l'industrie. Voici quelques exemples des normes les plus courantes pour l'évaluation des écarts.
  Cadres de sécurité : CIS Top 20 (anciennement SANS TOP 20), ISO 27001, ISO 27017, ISO 27018 et NIST CSF

- **Évaluation globale de la sécurité**
  Une évaluation globale de la sécurité combine une évaluation des menaces et des risques avec des tests d'intrusion afin de comprendre la posture de sécurité d'une organisation de manière générale. Contrairement à ces services indépendants, l'évaluation globale de la sécurité comprend un rapport intégré, qui tire parti des données des deux évaluations pour apporter plus de contexte.

- **Développement d'un plan d'intervention en cas d'incident, développement d'un dossier d'exploitation et exercice de simulation**
  Le développement d'un plan d'intervention en cas d'incident et les exercices de simulation sont conçus pour aider à évaluer le plan d'intervention existant d'une organisation ou à en concevoir un nouveau. L'élaboration de ce plan comprend à la fois les exigences organisationnelles pour gérer le programme d'intervention, comme la définition des rôles et responsabilités, l'établissement des processus d'autorisation et de déclaration d'incident, ainsi que des dossiers d'exploitation techniques qui décrivent les plans d'intervention approuvés de l'organisation pour des scénarios de menace particuliers (comme l'infection par rançongiciel ou l'arnaque au président). À la suite de l'établissement du plan d'intervention et des dossiers d'exploitation techniques connexes, les conseillers en cyberrisque de CDW animent une séance de discussion avec les parties prenantes du client pour décrire un scénario d'incident et simuler la réaction à un scénario de menace pertinent.

- **Audit interne**
  Des audits internes sont réalisés afin de préparer les clients pour les audits de certification externes. Les audits internes facilitent le maintien des certifications par rapport aux normes ISO 27001, ISO 27017, ISO 27018 et NIST CSF. L'objectif est de faire effectuer un audit interne par un tiers du programme de sécurité du client afin de déceler toute non-conformité à la norme et de recommander des mesures correctives.
  Cadres de sécurité : contrôles CIS, ISO 27001, ISO 27017, ISO 27018 et NIST CSF

- **Évaluation initiale PCI DSS**
  Une évaluation de conformité initiale PCI vise à aider les organisations à comprendre leurs exigences de conformité liées à la norme PCI et à établir une feuille de route de conformité.
  Cadres de sécurité : PCI DSS

DÉBUT DU DOCUMENT

- **Évaluation des facteurs relatifs à la vie privée**
  On effectue des évaluations des facteurs relatifs à la vie privée afin de s'assurer que les risques d'atteinte à la vie privée sont abordés dans les pratiques de traitement de l'information d'un client. L'objectif de cette évaluation est de cerner, d'évaluer et de hiérarchiser les lacunes dans les pratiques actuelles de protection de la vie privée par rapport aux obligations du client en matière de protection de la vie privée, afin de déterminer la conformité aux exigences réglementaires requises et adressables, ainsi que les risques connexes en cas d'écarts de conformité.
  Cadres de sécurité : LPRPDE, HIPAA et RGPD

- **Évaluation des risques**
  Les évaluations des risques sont réalisées pour aider les clients à comprendre les menaces de sécurité, les vulnérabilités et les risques connexes qui peuvent influer sur la confidentialité, l'intégrité et la disponibilité des données des clients, des infrastructures/systèmes de soutien et des applications essentielles. Les évaluations des risques comprennent une évaluation des écarts par rapport aux normes de sécurité de l'industrie pour identifier les vulnérabilités dans l'environnement du client. L'évaluation des risques se concentre sur les personnes, les processus et les technologies qui interagissent avec les informations sensibles du client.
  Cadres de sécurité : contrôles CIS, ISO 27001, ISO 27017, ISO 27018 et NIST CSF

- **État de préparation à la certification par un tiers**
  Cette évaluation fournit des conseils sur l'adoption du cadre ISO et permet de cerner les lacunes, de déterminer la conformité et d'adopter les contrôles manquants. Il peut s'agir d'une première étape utile vers l'adoption et éventuellement la certification ISO 27001.
  Cadres de sécurité : contrôles CIS, ISO 27001, ISO 27017, ISO 27018 et NIST CSF

- **Évaluation de la menace et des risques**
  Les évaluations de la menace et des risques sont effectuées afin de fournir un contexte supplémentaire à une analyse de la menace; chose que ne fait pas une évaluation des risques fondée sur des normes. En plus de ce qui est couvert dans une évaluation des risques, une évaluation de la menace et des risques apporte un contexte supplémentaire lié à divers vecteurs de menaces qui pourraient toucher l'organisation ciblée.
  Cadres de sécurité : contrôles CIS, ISO 27001, ISO 27017, ISO 27018 et NIST CSF

- **Préparation à la certification d'un programme de sécurité/de protection de la vie privée**
  La préparation à la certification d'un programme de sécurité/de protection de la vie privée aide les clients à certifier leur programme en fonction d'une norme de l'industrie. La préparation à la certification comprend une évaluation des écarts et des risques pour déterminer les contrôles supplémentaires à mettre en œuvre et identifier les risques pour l'organisation; la mise en œuvre du programme; un audit interne pour s'assurer que les contrôles sont alignés avec la norme; ainsi que la gestion et le soutien de l'audit externe. Voici quelques exemples des normes les plus souvent utilisées.
  Cadres de sécurité : contrôles CIS, ISO 27001, ISO 27017, ISO 27018 et NIST CSF

- **Mise en œuvre d'un programme de sécurité/de protection de la vie privée**
  La mise en œuvre d'un programme de sécurité/de protection de la vie privée comprend la personnalisation des contrôles techniques, administratifs et physiques afin de protéger les renseignements sensibles et la vie privée d'un client. Les services comprennent la mise en œuvre des politiques, des procédures et des formulaires, l'établissement d'un comité de gouvernance, la formation de sensibilisation à la sécurité de l'information, la gestion des risques et les indicateurs du programme. Dans le cadre de la mise en œuvre du programme, l'on a souvent recours à une norme de sécurité de l'industrie comme base de mise en œuvre. Voici quelques exemples des normes les plus utilisées.
  Cadres de sécurité : contrôles CIS, ISO 27001, ISO 27017, ISO 27018 et NIST CSF

- **Mandat de maintien de certification du programme de sécurité/de protection de la vie privée**
  Le service de mandat de maintien de certification du programme de sécurité/de protection de la vie privée est axé sur les clients qui ont obtenu une certification par rapport à une norme de l'industrie et qui ont besoin d'un soutien continu pour le maintien de la certification. Le mandat comprend, entre autres, l'évaluation annuelle des risques, l'audit interne annuel, la gestion de l'audit externe, les réunions du comité de gouvernance et une consultation ponctuelle sur la sécurité et la protection de la vie privée.

- **Vérification de l'état de sécurité**
  La vérification de l'état de sécurité de CDW évaluera le programme de sécurité de votre organisation pour vous aider à comprendre votre posture de sécurité et déterminer les grandes vulnérabilités de votre environnement que des acteurs malveillants pourraient exploiter. Cette solution rentable vous aidera à établir un plan pour aborder les cinq risques les plus critiques pour votre environnement, fournira des recommandations personnalisées pertinentes pour vos activités et tracera un chemin d'amélioration continue de la sécurité pendant que vous développez vos affaires.

- **Chef de la sécurité de l'information virtuelle**
  Le chef de la sécurité de l'information virtuelle est un programme sur demande qui répond aux besoins uniques d'un client pour soutenir ses fonctions de gouvernance de la sécurité, de risque et de conformité. Ce programme permet de profiter des connaissances et de l'expérience d'un service de sécurité d'entreprise, de conformité et de vérification interne en sous-traitance tout en évitant la charge financière d'un service complet. Le groupe Cyberrisque de CDW agit comme un conseiller de confiance pour renforcer et maintenir la sécurité de l'information du client et sa posture de risque.

DÉBUT DU DOCUMENT

Test d'intrusion

- **Test d'intrusion et simulation d'attaque**
  Ces activités aident le client à mieux comprendre les risques d'exposition auxquels il est exposé afin qu'il soit mieux outillé pour prendre des décisions d'affaires éclairées. Nous mettons au jour des vulnérabilités de sécurité dans son environnement, comprenons la posture de sécurité de l'entreprise et testons son état de préparation face à une véritable cyberattaque.

  - **Test d'intrusion dans les interfaces de programmation d'applications (API)**
    Test d'intrusion axé sur l'identification des vulnérabilités dans les points d'extrémité et les protocoles des API qui pourraient être exploitées pour compromettre la confidentialité, l'intégrité et la disponibilité des données associées.

  - **Test d'intrusion infonuagique**
    Le service de test d'intrusion infonuagique de CDW est utilisé pour découvrir, identifier et classifier les défaillances et les vulnérabilités potentielles dans les environnements infonuagiques des organisations et aider à évaluer la posture de sécurité connexe. Les conseillers en cybersécurité de CDW essaient d'identifier les vulnérabilités et de les exploiter pour simuler un auteur de menace, puis font des recommandations pour corriger les problèmes.

  - **Ingénierie sociale par courriel**
    L'hameçonnage par courriel, un type d'ingénierie sociale, est une technique courante des auteurs de menaces lorsqu'ils visent une organisation pour obtenir des renseignements sensibles ou un accès au réseau. Les campagnes d'ingénierie sociale par courriel évaluent la sensibilisation à la sécurité des employés d'une organisation face à ces types d'attaques, et ce, en mesurant le taux de clics de liens, l'exécution de liens malveillants ou la saisie d'éléments d'identification sur un portail de connexion compromis.

  - **Test structurel d'une application**
    Test structurel d'une application logicielle pour découvrir, identifier et classer toutes les faiblesses potentielles du code source, de l'infrastructure ainsi que de l'intégration de l'application avec les systèmes externes. Le test comprend une analyse du code source dans les tentatives d'exploiter toute vulnérabilité découverte, dans le but d'évaluer la posture de sécurité.

  - **Test d'intrusion dans des applications mobiles**
    Test d'intrusion qui simule une attaque contre une application mobile pour identifier les vulnérabilités côté client, y compris, mais sans s'y limiter, l'insécurité du stockage des données, les erreurs de configuration et les contrôles de sécurité insuffisants concernant l'ingénierie inverse.

  - **Test d'intrusion du réseau (interne ou externe)**
    Un test d'intrusion externe comprend une analyse de l'infrastructure orientée vers l'extérieur d'une organisation pour identifier les vulnérabilités, vérifier manuellement les problèmes et les exploiter pour faire la démonstration de ce qui pourrait être accompli par un auteur de menaces.

    Un test d'intrusion interne démontre ce qu'un attaquant externe pourrait accomplir après avoir violé le périmètre d'une organisation. Le test d'intrusion du réseau interne comprend l'analyse, la validation et l'exploitation des vulnérabilités découvertes, ainsi qu'un sondage manuel du réseau à la recherche de vecteurs d'attaques supplémentaires qui ne sont pas habituellement identifiés avec des lecteurs automatisés.

  - **Évaluation de la vulnérabilité du réseau (interne ou externe)**
    Une évaluation des vulnérabilités repose sur des outils automatisés et des techniques manuelles pour identifier et valider les vulnérabilités au sein d'une infrastructure réseau interne ou externe.

  - **Évaluation issue du renseignement de sources ouvertes (OSINT)**
    Le renseignement de sources ouvertes (OSINT) est une forme de collecte de renseignements qui consiste à trouver, sélectionner et acquérir de l'information à partir de sources publiques et à l'analyser afin de produire des renseignements exploitables. La collecte de renseignements est effectuée afin de déterminer les points d'entrée dans une organisation, qu'ils soient physiques ou électroniques, afin de mettre en évidence l'information que l'organisation rend publique et la manière dont elle peut être utilisée par un attaquant déterminé.

  - **Ingénierie sociale par téléphone**
    L'ingénierie sociale par téléphone (ou hameçonnage vocal) est une technique utilisée par les auteurs de menaces pour essayer d'obtenir des informations sensibles ou de persuader un utilisateur d'entreprendre une action qui pourrait mener à une atteinte à la sécurité par message texte ou appel téléphonique. Les missions d'ingénierie sociale par téléphone évaluent la sensibilisation des employés à la sécurité face aux attaques vocales ou textuelles qui pourraient mettre l'organisation en danger.

  - **Ingénierie sociale en personne**
    L'ingénierie sociale en personne sert à évaluer les contrôles de sécurité physique et environnementale d'un site ainsi que les protocoles de sécurité, comme la confirmation de l'identité du personnel et des visiteurs, la prévention de l'accès non autorisé, etc. Parfois, l'ingénierie sociale en personne est également combinée à des services de test d'intrusion tels que la découverte d'une clé USB malveillante et l'attaque subséquente si la clé venait à être branchée à un appareil sur le réseau ciblé.

DÉBUT DU DOCUMENT

- **Évaluation de l'équipe rouge**
  Une évaluation recommandée pour les organisations ayant une pratique de sécurité ancrée; les missions d'une équipe rouge consistent essentiellement à tester les capacités de détection et d'intervention d'une organisation face à des scénarios d'attaque réels. Ces évaluations plus longues imitent un auteur de menaces qui tente de mettre un pied dans une organisation en exploitant les vulnérabilités techniques ou en utilisant divers types d'ingénierie sociale afin d'atteindre un objectif prédéterminé sans se faire détecter sur le réseau.

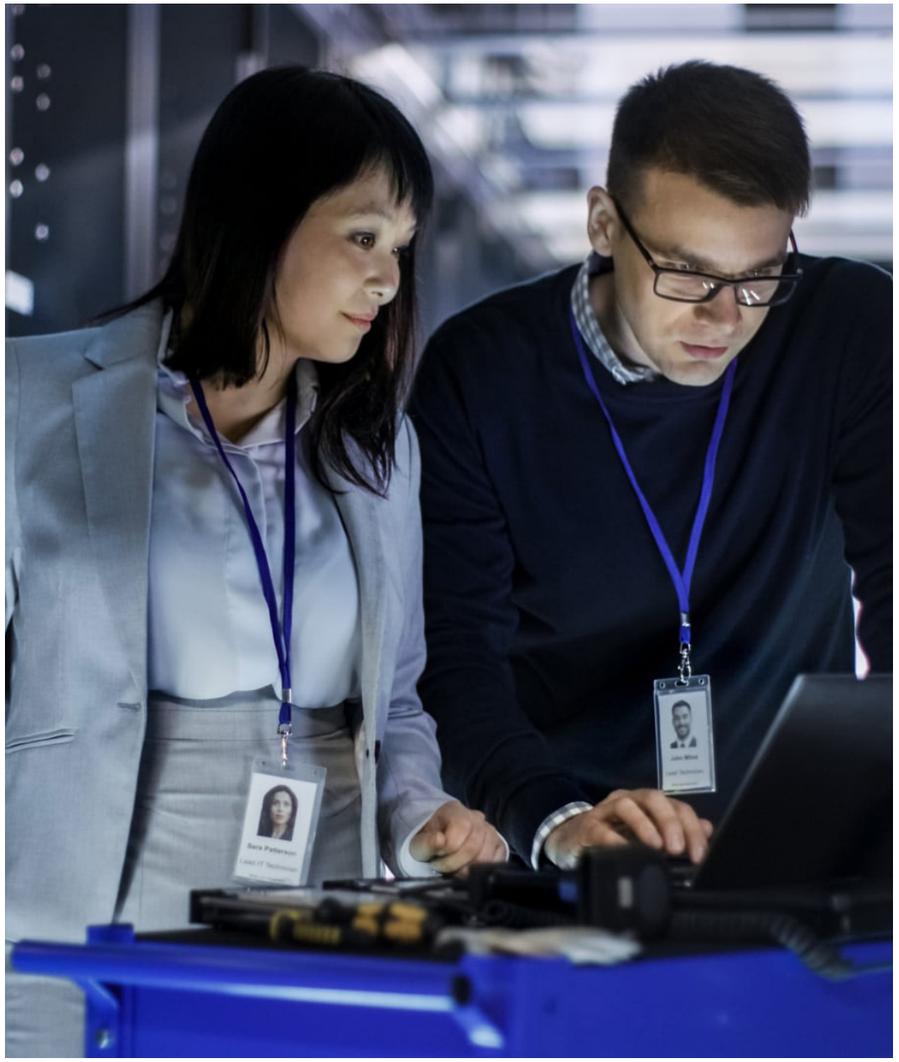
- **Test d'intrusion à partir d'un scénario**
  Test d'intrusion axé sur un scénario et un objectif particuliers (c.-à-d. imitation d'un auteur de menaces qui a compromis un poste de travail interne). Ce test d'intrusion est généralement fondé sur le temps et vise à identifier les vulnérabilités et les lacunes qui seraient exploitées par les auteurs de menaces dans le monde réel dans un scénario donné et il n'est pas conçu pour être une évaluation complète de l'intégralité de l'infrastructure réseau.

- **Test d'intrusion par attaque ciblée**
  Test d'intrusion limitée axé sur les voies d'attaque typiques utilisées à mauvais escient par les auteurs de menaces du point de vue d'un réseau externe. Ce test comprend une mission ponctuelle d'ingénierie sociale à partir de scénarios préconçus pour mesurer le taux de clics, la saisie d'éléments d'identification ou l'exécution de charges malveillantes.

- **Test d'intrusion dans des applications Web**
  On effectue ce type de test d'intrusion afin d'identifier et d'exploiter les vulnérabilités de l'application Web et de ses composants au moyen de techniques manuelles et automatisées.

Gestion des vulnérabilités

Le service géré de CDW offre une visibilité continue et des renseignements de sécurité utiles sur les environnements clients et le risque associé aux vulnérabilités. Cela permet au client de gérer sa surface d'attaque en identifiant les vulnérabilités, en les hiérarchisant puis en les validant.
Le service professionnel de CDW aide les clients à évaluer leur programme et leurs outils de gestion des vulnérabilités actuels, à trouver des possibilités d'amélioration, ainsi qu'à élaborer des processus et des politiques robustes pour gérer leur programme de manière harmonieuse.



DÉBUT DU DOCUMENT

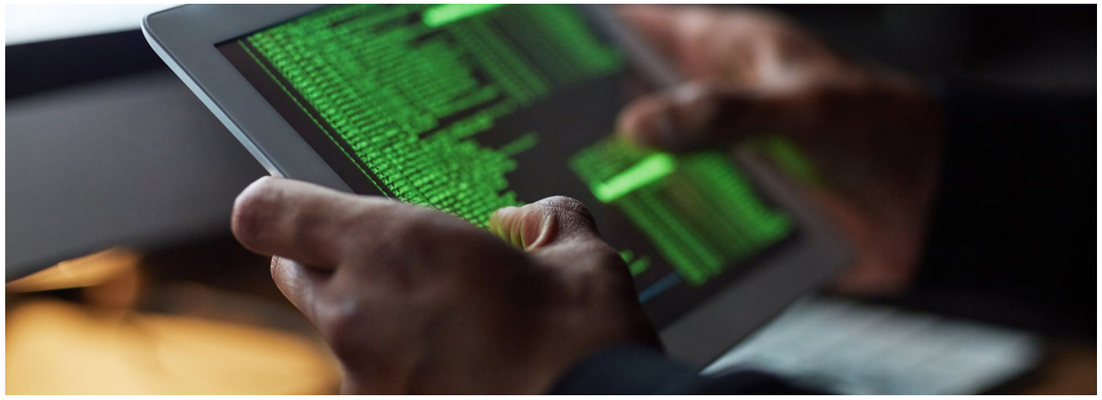
ServiceNow

La gestion de services de TI et les plateformes de flux de travail numérique deviennent les pierres angulaires des TI. En tant que partenaire ServiceNow®, CDW vous aide à optimiser la valeur de votre investissement dans ServiceNow® et à épurer les TI à la grandeur de votre organisation.

Gouvernance, risque et conformité (GRC) électronique

Se conformer à la réglementation requiert un investissement considérable en temps, en efforts et en argent consacrés à la création et à l'adoption d'un cadre bien planifié. La maintenance de ce cadre se révèle être un véritable défi. Le service de Gouvernance, risque et conformité (GRC) électronique de CDW est optimisé par ServiceNow et répond à ce problème en s'assurant que des contrôles en cours sont toujours présents à l'esprit, que des mesures peuvent être prises, et, qui plus est, que ce problème est consigné facilement.

- **Services de mise en œuvre**
  - **Gestion du service à la clientèle**
    La solution de gestion du service à la clientèle de ServiceNow permet de corriger et de prévenir les problèmes de façon permanente en connectant le service à la clientèle aux autres services et en automatisant les processus à travers les équipes pour accélérer la résolution des problèmes. Avec cette solution, vous pouvez résoudre les problèmes en rapprochant le guichet, le bureau intermédiaire et l'arrière-guichet, en gérant ainsi les problèmes des clients de manière proactive et en traitant instantanément leurs demandes.
  - **Gestion opérationnelle des TI**
    Les organisations adoptent une stratégie hybride ou qui privilégie le nuage dans leur poursuite de la transformation numérique. Cela offre une agilité sans précédent, mais crée également de nouveaux défis pour les TI. La solution de gestion opérationnelle des TI de ServiceNow vous permettra de les surmonter. Le produit ITOM Visibility crée un dossier exact et actuel de tout votre environnement et des services connexes. Le produit ITOM Health élimine le bruit dans les données en utilisant la puissance de l'intelligence artificielle appliquée à l'exploitation informatique ainsi que de l'automatisation pour vous aider à détecter, diagnostiquer et corriger rapidement les problèmes de service. Le produit ITOM Optimization aide à réduire les dépenses infonuagiques en identifiant et en opérationnalisant les optimisations des coûts et en créant un modèle d'exploitation standard à travers plusieurs nuages, offrant une gouvernance adaptative efficace.
  - **Gestion des services de technologies de l'information (GSTI)**
    Notre solution GSTI de ServiceNow propose des flux de travail évolutifs pour gérer les services de TI et les fournir à vos utilisateurs à travers une plateforme infonuagique unique appelée NOW. La solution GSTI peut aider à augmenter la productivité de vos agents, résoudre les problèmes rapidement et améliorer la satisfaction des utilisateurs. Grâce à cette solution optimisée par l'IA native de la plateforme, vous pouvez rapidement accélérer les changements technologiques, visualiser les actions recommandées pour les demandes ou billets entrants, et stimuler le libre-service et l'automatisation à travers la technologie d'agent conversationnel d'entreprise.
  - **Opérations de sécurité**
    La solution Opérations de sécurité de ServiceNow regroupe les données sur les incidents de vos outils de sécurité dans un moteur d'intervention structuré qui utilise des flux de travail intelligents, l'automatisation et une connexion profonde avec les TI pour hiérarchiser et résoudre les menaces en fonction de leur impact sur votre organisation.



DÉBUT DU DOCUMENT

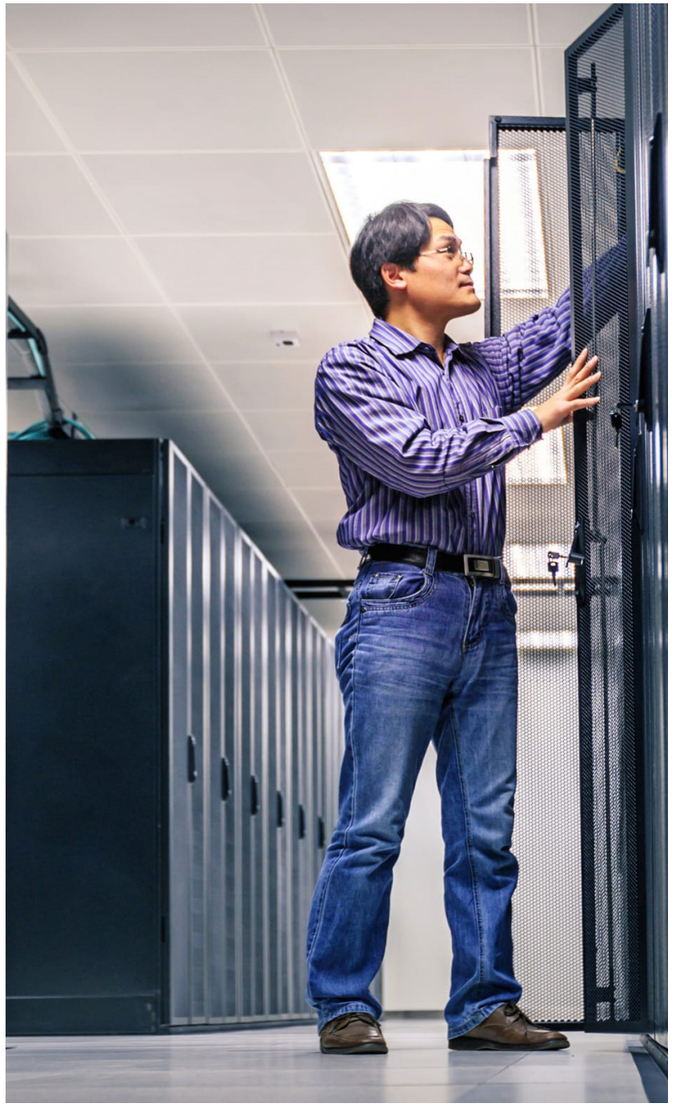
- **Feuille de route et évaluation de la maturité**
  Assurez la maturité continue et l'adoption de votre instance ServiceNow avec notre évaluation de maturité spécialisée. Cette évaluation trace un chemin de transition sur le moment, de l'état actuel à un état futur recommandé, décrivant le parcours qui vous est le mieux adapté. Il s'agit d'une mission menée par les services de conseil qui infuse une vision de l'avenir fondée sur les meilleures pratiques, intègre une approche fondée sur les affaires et conçoit ensuite un plan personnalisé pour la GSTI et la maturité d'un ensemble d'outils.

- **SmartCIP**
  En utilisant les principes d'amélioration continue du service, SmartCIP se concentre sur l'amélioration de la gestion du service dans votre organisation. Nos conseillers en services de soutien viennent à votre rencontre pour fournir les ressources et la motivation nécessaires et responsabiliser vos équipes suffisamment pour empêcher les initiatives d'amélioration de se perdre parmi les nombreuses exigences de votre temps.

- **Modules supplémentaires ServiceNow : SmartScan**
  À mesure que le nombre d'applications mises en œuvre dans votre plateforme ServiceNow augmente, il convient de continuer à optimiser l'instance (croissance et mise à l'échelle) sans en compromettre les performances. SmartScan réalise une évaluation complète de votre plateforme ServiceNow pour vérifier que les meilleures pratiques sont en place afin de vous apporter le plus haut retour sur investissement possible.

- **Modules supplémentaires ServiceNow : Aide à la mise à niveau**
  Nous utilisons l'approche éprouvée en six phases de ServiceNow pour mettre à niveau votre instance de ServiceNow jusqu'à la prochaine version séquentielle. Nous vous aiderons à planifier, à vous préparer et à migrer avec succès vers une nouvelle version de ServiceNow, à vérifier les applications personnalisées en cours de route ou à en mettre en œuvre de nouvelles au besoin.

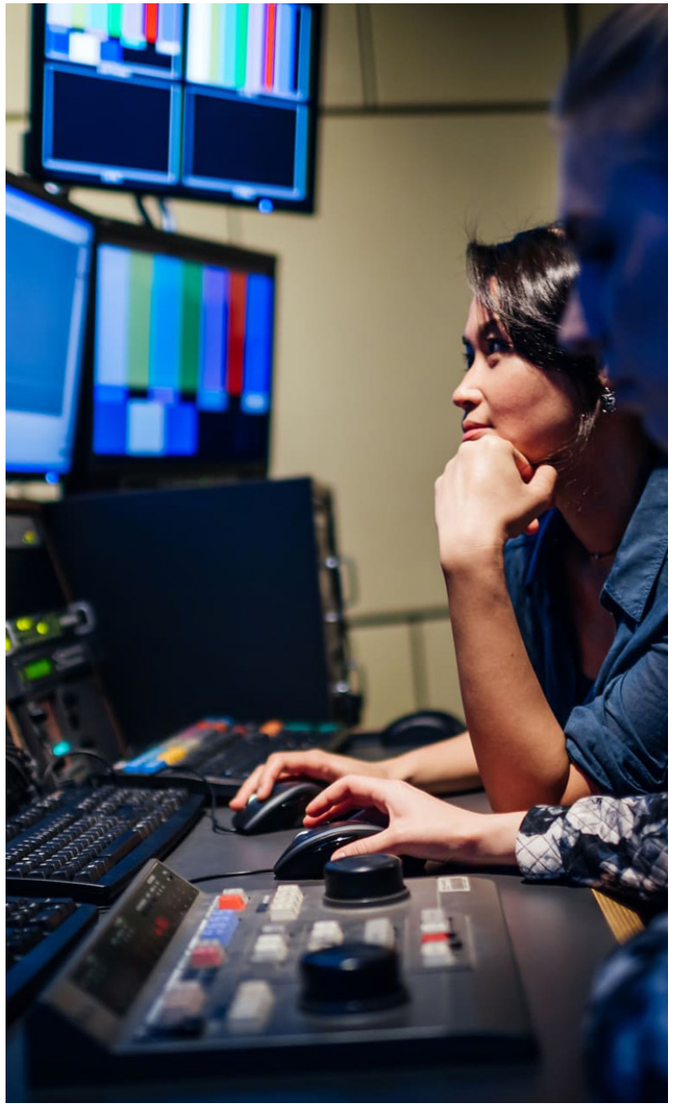
- **Ajustement de la feuille de route ServiceNow**
  Alors que votre utilisation de la plateforme ServiceNow s'adapte et se développe, il est essentiel d'examiner votre feuille de route actuelle pour décider si elle représente encore un plan exploitable qui peut continuer à se développer avec vous. L'ajustement de la feuille de route est un exercice au cours duquel les conseillers de CDW mèneront un examen axé sur la mise à jour de votre évaluation de maturité initiale pour fournir un aperçu pluriannuel en plusieurs phases où il faudra déterminer les occasions, les avantages et les niveaux d'investissement et, par la suite, concevoir une approche recommandée pour la maturité continue et l'adoption de votre plateforme ServiceNow.



DÉBUT DU DOCUMENT

Médias et divertissement

CDW est le chef de file du secteur des fournisseurs de solutions logicielles au Canada pour l'industrie des médias et du divertissement. Nous avons des milliers de clients allant de travailleurs autonomes et d'entreprises en démarrage à certains des plus grands studios de l'industrie.
Nos experts des médias et du divertissement travaillent étroitement avec les équipes de sécurité, de l'infonuagique et d'infrastructure afin de vous fournir les solutions optimales qui vous permettent de réaliser vos projets à temps, en toute sécurité et en respectant vos budgets.



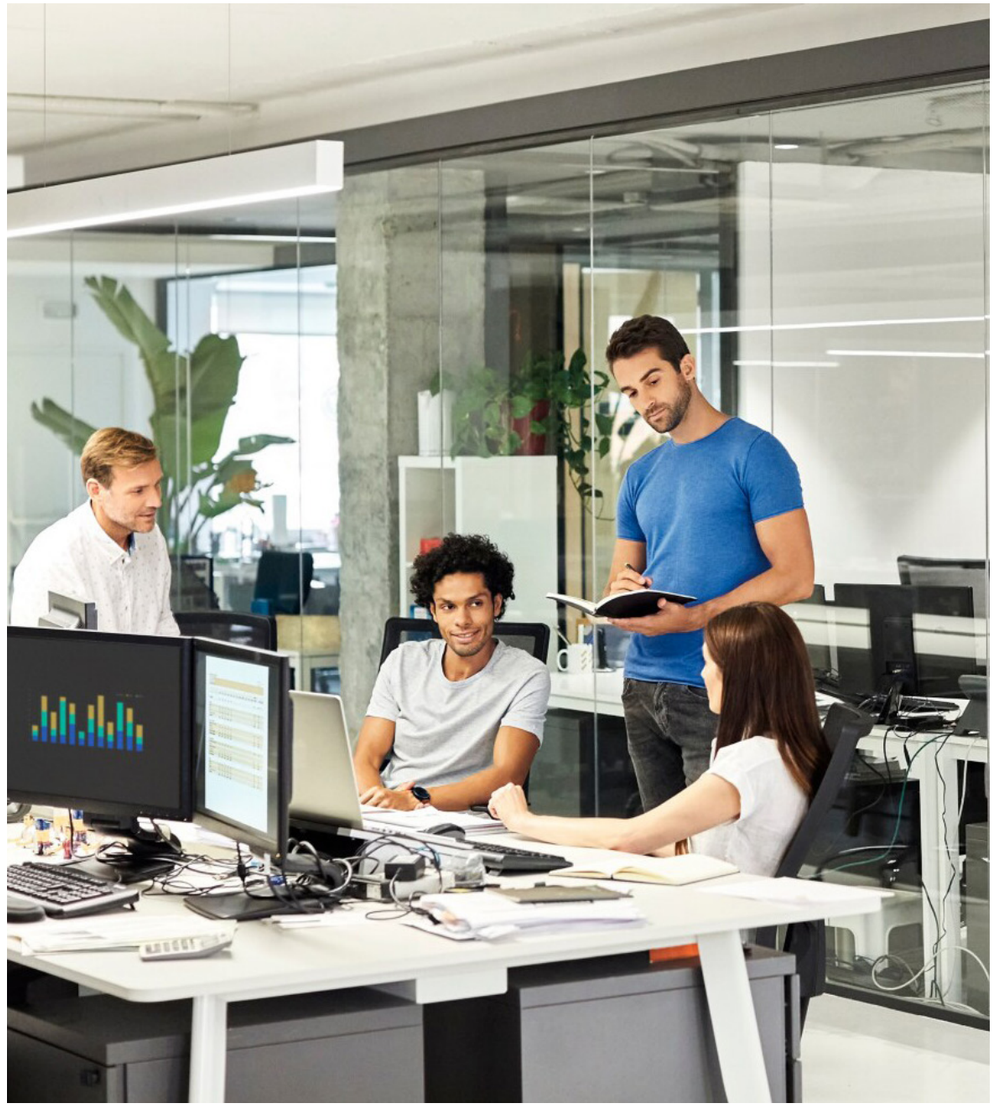
- **Solutions informatiques Médias et divertissement**
  Ces services comprennent StudioCloud, une communauté virtuelle pour l'industrie des médias numériques offrant des solutions informatiques sur demande aux studios. Les modèles de coûts par utilisation et prévisibles de StudioCloud permettent aux studios d'économiser de l'argent ainsi que des actifs et de gagner du temps en faisant correspondre l'accessibilité aux ressources informatiques avec les demandes et les calendriers des projets.
  Fournisseurs pris en charge : Autodesk, Dell, EMC et Intel

- **StudioCloud**
  Nous avons nivelé le terrain de jeu et créé StudioCloud, optimisé par Intel, une solution parfaitement sécurisée, complètement gérée, évolutive à l'infini et personnalisée selon vos besoins. Sélectionnez le nombre de nœuds et la durée du contrat dont vous avez besoin pour un projet précis. Mieux encore, nous offrons un environnement répondant aux lignes directrices de la MPAA pour toutes les tailles de studio! De plus, nos établissements proposent un service complètement géré, avec une surveillance en tout temps et le soutien des ingénieurs de StudioCloud, soutenu par notre propre réseau et notre centre des opérations de sécurité.
  Fournisseurs pris en charge : Autodesk et Intel

DÉBUT DU DOCUMENT

Services de dotation stratégique

CDW offre un vaste éventail de services de dotation. Aujourd'hui, nous aidons nos clients à trouver de la main-d'œuvre qualifiée partout au pays en ayant recours à la même équipe que celle que nous utilisons pour la dotation en personnel de nos projets internes. Dans le contexte actuel de plus en plus concurrentiel pour ce qui est de trouver de la main-d'œuvre en TI, CDW vous donne accès à un réseau profond de conseillers techniques éprouvés. Nous sommes ici pour soutenir votre entreprise en fournissant du personnel à temps plein ou spécialisé afin de répondre à vos besoins – sur le long terme ou pour des projets ponctuels.



DÉBUT DU DOCUMENT