Papier blanc

Quand « Aussi sécurisé que possible » ne suffit pas :

Pourquoi est-il temps de passer à Microsoft 365 E5

Vous pensez peut-être que vos données et vos systèmes sont aussi sécurisés que possible avec votre licence Microsoft 365® E3 actuelle, mais êtes-vous vraiment prêt(e) à affronter les menaces et les défis en évolution du paysage numérique actuel? Dans quelle mesure avez-vous confiance en votre capacité à prévenir, détecter et réagir face aux cyberattaques, à protéger vos informations confidentielles, et à vous conformer aux exigences réglementaires? Combien de temps et d'argent investissez-vous dans la gestion de multiples solutions de sécurité qui peuvent ne pas s'intégrer harmonieusement ou couvrir tous vos besoins?

Si vous n'êtes pas certain(e) des réponses à ces questions, ou si vous vous craignez les risques et les coûts associés à une faille de sécurité, envisagez de passer à Microsoft® 365 E5. Cette offre constitue la solution de sécurité la plus avancée et complète de Microsoft, conçue pour vous aider à adopter une approche de sécurité à confiance nulle (Zero Trust) en matière d'identité, de périphériques, de données, d'applications et d'infrastructure.

Avec M365 E5, vous bénéficiez des avantages suivants :

Amélioration de la protection contre les menaces
avec Microsoft Defender pour point de terminaison, Office 365® et Identity, qui misent sur l'IA, l'analyse comportementale et la mise à l'échelle du nuage pour fournir une défense proactive et unifiée contre les attaques sophistiquées

Prévention de la perte de données (DLP) et gouvernance
avec Microsoft Information Protection, Cloud App Security et Compliance Manager, qui vous aident à classer, étiqueter, protéger et surveiller vos données confidentielles sur l'ensemble des appareils, applications et services infonuagiques; et simplifient la conformité aux normes et réglementations de l'industrie;

Gestion simplifiée de la sécurité et des opérations
avec Microsoft Secure Score, le centre de sécurité Microsoft 365 et le centre de conformité Microsoft 365, qui vous offrent un tableau de bord centralisé et intégré pour évaluer votre posture de sécurité, prioriser les recommandations et automatiser les flux de travail

Simplification et réduction des coûts
avec un seul fournisseur une seule licence et un seul contrat de soutien, ce qui élimine le besoin de multiples solutions de sécurité et de fournisseurs et réduit votre coût total de possession. lowers your total cost of ownership

Les données sont l'un des actifs les plus précieux pour toute organisation, mais elles s'accompagnent également de nombreux défis et risques. Comment pouvez-vous protéger vos données confidentielles contre un accès non autorisé ou une utilisation abusive? Comment pouvez-vous vous conformer aux réglementations et aux normes de protection des données de votre industrie ou de votre région? Comment pouvez-vous surveiller et vérifier vos activités de données et les journaux d'accès, et générer des rapports et des alertes à des fins de conformité et de gouvernance?

Les questions suivantes vous aideront à évaluer comment votre approche actuelle se compare aux pratiques exemplaires et aux références.

Pouvez-vous affirmer en toute confiance que les identifiants de votre entreprise n'ont jamais été compromis? Et si elles ont été compromises, disposiez-vous d'un moyen automatisé pour surveiller et atténuer la situation?

Si votre entreprise utilise M365 E3, vous n'êtes peut-être pas conscient des risques de sécurité potentiels qui existent dans votre environnement. M365 E3 repose sur des politiques de mot de passe de base et l'authentification multifacteur pour protéger vos identifiants, mais ces mesures ne suffisent pas pour prévenir ou détecter le vol et l'abus d'identifiants. Les pirates informatiques peuvent utiliser des attaques par hameçonnage, des logiciels malveillants ou des attaques par force brute pour obtenir vos mots de passe et contourner vos défenses.

M365 E5 offre un niveau de sécurité supérieur pour vos identifiants avec Microsoft Entra™ ID Premium P2, qui comprend des fonctionnalités avancées telles que :

- **Protection de l'identité :** Cette fonctionnalité utilise l'apprentissage automatique pour détecter les activités suspectes et les connexions risquées en fonction du comportement, de l'emplacement, de l'appareil et du réseau de l'utilisateur. Elle fournit également des alertes et des recommandations en temps réel pour vous aider à répondre et à remédier aux problèmes.
- **Gestion des identités privilégiées :** Cette fonctionnalité vous permet de gérer et de surveiller l'accès des utilisateurs ayant des privilèges élevés, tels que les administrateurs, les propriétaires ou les contributeurs. Vous pouvez mettre en place des politiques d'accès juste-à-temps et juste-assez, exiger une authentification multifacteur et des flux d'approbation et examiner les journaux et les rapports d'audit pour garantir la conformité et la responsabilité.

Avec M365 E5, vous pouvez affirmer en toute confiance que les identifiants de votre entreprise sont protégés par la solution de gestion des identités et des accès la plus avancée et la plus complète du marché. Vous pouvez également bénéficier d'une approche automatisée et proactive pour surveiller et atténuer les menaces, et réduire la complexité et les coûts associés à la gestion de plusieurs solutions de sécurité et fournisseurs.

Êtes-vous pleinement conscient(e) de la nature et de l'emplacement de toutes vos données confidentielles, et avez-vous une compréhension claire de la manière dont vos données confidentielles sont protégées contre une exposition potentielle?

La licence M365 E5 avec Purview de Microsoft peut vous aider à obtenir plus de visibilité et de contrôle sur vos données confidentielles au sein des applications et services Microsoft 365, tels que SharePoint®, OneDrive® et Exchange. Contrairement à M365 E3, qui ne propose que des fonctionnalités de base de protection et de conformité des donnée, M365 E5 et Purview peuvent analyser et classer vos données sur différents emplacements et appareils, et appliquer automatiquement des politiques et des étiquettes cohérentes en fonction des besoins de votre entreprise et des réglementations de l'industrie. Vous pouvez également utiliser Purview pour découvrir et cartographier vos sources et flux de données, et surveiller et vérifier l'accès et l'utilisation de vos données confidentielles.

Avec M365 E5 et Purview, vous pouvez vous assurer que vos données confidentielles sont protégées contre une exposition et un usage abusif potentiel, et que vous avez une compréhension claire de la façon dont elles sont stockées, traitées et partagées.

Dans quelle mesure votre système est-il efficace pour catégoriser les données confidentielles et comment garantissez-vous qu'elles sont sécurisées contre tout accès non autorisé?

M365 E5 et Purview vous permettent de découvrir, classer et protéger les données confidentielles dans l'ensemble de votre environnement de données hybride, y compris sur site, dans le nuage et dans des environnements multinuages. Vous pouvez utiliser des classificateurs intégrés ou personnalisés pour identifier plus de 100 types de données confidentielles, telles que les informations personnellement identifiables (PII), les données financières ou les dossiers de santé. Vous pouvez également appliquer des étiquettes de sensibilité et le chiffrement à vos données au repos ou en transit, garantissant que seuls les utilisateurs autorisés peuvent y accéder.

Vous utilisez peut-être des solutions de DLP, mais peuvent-elles répondre et limiter l'accès en fonction des comportements à risque? Comment surveillez-vous et détectez-vous les comportements à risque sur vos sources de données et appareils?

M365 E5 et Purview offrent des solutions DLP avancées qui peuvent détecter et répondre aux comportements à risque sur l'ensemble de vos sources de données et appareils. Vous pouvez définir des stratégies et des règles pour bloquer, mettre en quarantaine ou notifier automatiquement les utilisateurs lorsqu'ils tentent de partager ou de transférer des données confidentielles en dehors de votre organisation ou à des destinataires non fiables. Vous pouvez également exploiter l'analyse comportementale et l'apprentissage automatique pour identifier et corriger les menaces internes, telles que l'exfiltration de données, le sabotage ou le vol.

M365 E5 et Purview offrent une visibilité et des informations complètes sur vos activités et risques liés aux données. Vous pouvez utiliser le Centre de conformité Microsoft 365 pour surveiller et auditer vos événements de données, tels que la création, l'accès, la modification, la suppression ou le partage. Vous pouvez également utiliser Microsoft Cloud App Security pour découvrir et évaluer l'utilisation et le niveau de risque de vos applications et services infonuagiques. En outre, vous pouvez utiliser Microsoft Defender pour point de terminaison pour détecter et enquêter sur les activités malveillantes ou anormales sur vos points de terminaison, telles que les logiciels malveillants, les rançongiciels ou les attaques par hameçonnage.

Comment appliquez-vous des politiques et des contrôles granulaires pour prévenir l'accès non autorisé, le partage ou la fuite de données confidentielles?

Avec M365 E5, vous pouvez appliquer des politiques et des contrôles granulaires pour empêcher l'accès non autorisé, le partage ou la fuite de données confidentielles en utilisant les capacités d'étiquetage et de protection de sensibilité de Purview. L'étiquetage de sensibilité vous permet de classer et d'étiqueter vos données en fonction de leur sensibilité et de leur valeur commerciale, et d'appliquer le chiffrement, les restrictions d'accès et les marquages visuels pour les protéger tout au long de leur cycle de vie. Vous pouvez également utiliser l'étiquetage de sensibilité pour analyser et découvrir automatiquement vos données confidentielles dans vos environnements infonuagiques et sur site, et leur appliquer des stratégies et des contrôles cohérents. Avec Purview et M365 E5, vous pouvez également couvrir d'autres sources de données et scénarios, tels que Microsoft Teams®, Outlook®, Word, Excel®, PowerPoint®, Power BI®, les appareils Windows® 10, les applications infonuagiques tierces et les serveurs de fichiers et les partages réseau sur site. Vous pouvez également tirer parti de politiques et de règles de la perte de données (DLP) plus sophistiquées et personnalisables, telles que la correspondance exacte des données, les classificateurs entraînables ou les types d'informations confidentielles, pour détecter et protéger vos données avec une précision accrue.

M365 E5 et Purview offrent des solutions de DLP plus avancées et complètes que M365 E3, qui comprend uniquement des fonctionnalités de base de DLP pour Exchange Online, SharePoint Online et OneDrive Entreprise. En outre, vous pouvez intégrer vos solutions de DLP avec d'autres outils de sécurité et de conformité, tels que Microsoft Compliance Manager ou Microsoft Secure Score, pour renforcer la protection et la gouvernance de vos données. Vous pouvez également utiliser Microsoft Endpoint Manager, inclus dans M365 E5, pour gérer et sécuriser vos appareils Windows 10 et appliquer des politiques de conformité.

Comment réagissez-vous aux incidents et aux violations de données en temps réel et comment les corrigez-vous efficacement?

L'un des principaux avantages de M365 E5 et Purview est qu'ils vous permettent de réagir aux incidents et aux violations de données en temps réel et de les corriger efficacement. Avec M365 E5 et Purview, vous pouvez :

- **Surveiller et auditer vos activités et événements de données** dans l'ensemble de vos environnements infonuagiques et sur site en utilisant le journal d'audit unifié et les fonctionnalités avancées d'audit.
- **Recevoir des alertes et des notifications** lorsqu'un incident ou une violation de données se produit, par exemple lorsqu'un utilisateur tente d'accéder, de partager ou d'extraire des données confidentielles, ou lorsqu'un acteur malveillant tente de compromettre vos données.
- **Enquêter et analyser l'incident ou la violation de données** en utilisant l'aide du Centre de sécurité Microsoft 365, le Centre de conformité Microsoft 365 et la carte de données Purview. Vous pouvez également tirer parti des fonctionnalités avancées de eDiscovery et de Advanced Threat Protection (ATP) de M365 E5 pour recueillir et préserver des preuves, identifier et suivre l'origine et l'étendue de l'incident ou de la violation de données, et évaluer l'impact et le niveau de risque de l'incident ou de la violation de données.
- **Remédier à l'incident ou à la violation de données,** en utilisant les actions et les flux de travail intégrés de M365 E5 et Purview. Vous pouvez également utiliser les fonctionnalités de Microsoft Defender for Cloud Apps et Microsoft Defender pour point de terminaison de M365 E5 pour bloquer ou révoquer l'accès, mettre en quarantaine ou supprimer des données, appliquer ou supprimer des étiquettes de sensibilité, appliquer des stratégies de chiffrement ou de protection, ou instaurer un processus de notification de violation de données.

M365 E5 et Purview offrent plus de valeur et une sécurité améliorée que M365 E3, qui ne comprend pas les fonctionnalités avancées d'audit, d'eDiscovery, d'ATP, de Defender for Cloud Apps ou de Defender pour point de terminaison. M365 E3 a également des capacités limitées pour surveiller, enquêter et remédier aux incidents et aux violations de données sur plusieurs sources de données et scénarios.

Comment assurez-vous la conformité aux réglementations et normes de confidentialité et de sécurité des données?

Pour garantir la conformité aux réglementations et normes de confidentialité et de sécurité des données, vous devez adopter une approche complète et cohérente pour gérer et protéger vos données confidentielles dans l'ensemble de votre organisation. M365 E5 et Purview peuvent vous aider à y parvenir en offrant les avantages suivants :

- **M365 E5 et Purview vous permettent de découvrir et de classer vos données confidentielles sur diverses sources de données,** telles que SharePoint, OneDrive, Exchange, Teams, Azure®, les applications infonuagiques tierces et des serveurs sur site, en utilisant des étiquettes de sensibilité intégrées ou personnalisées et des politiques de classification des données. Vous pouvez également utiliser la carte de données de Purview pour obtenir une vue d'ensemble de votre paysage de données et de sa généalogie, et identifier tout problème de qualité, de gouvernance ou de conformité des données.
- **M365 E5 et Purview vous permettent d'appliquer et de faire respecter des politiques de protection et de rétention des données** basées sur vos étiquettes de sensibilité et vos exigences de conformité. Vous pouvez utiliser les fonctionnalités de protection des informations de Microsoft Purview® et de gestion de la conformité de Microsoft de M365 E5 pour chiffrer, restreindre ou limiter l'accès à vos données confidentielles, ainsi que surveiller et remédier à toute violation ou à tout conflit de politique. Vous pouvez également utiliser les fonctionnalités d'analyse des données et de catalogue de données de Purview pour suivre et faire un rapport sur l'utilisation et l'état de conformité de vos actifs de données.
- **M365 E5 et Purview vous aident à répondre et à vous adapter aux évolutions des réglementations et normes de confidentialité et de sécurité des données,** telles que le RGPD, le CCPA, l'HIPAA ou l'ISO 27001. Vous pouvez utiliser les fonctionnalités de Microsoft Compliance Score et Microsoft Privacy Assessment M365 E5 pour évaluer votre posture de conformité actuelle et identifier les lacunes ou les risques éventuels. Vous pouvez également utiliser les fonctionnalités Purview Data Policy Management and Data Access Governance pour créer et mettre à jour vos politiques et permissions de données conformément aux dernières pratiques réglementaires et industrielles.

M365 E5 et Purview offrent plus de valeur et une sécurité améliorée par rapport à M365 E3, qui ne propose pas le même niveau de découverte, de classification, de protection, de rétention, de surveillance, de rapport et de gouvernance des données. M365 E3 offre également un soutien limité pour les scénarios de conformité aux données transversaux et interapplications, et ne comprend pas les fonctionnalités avancées de Purview qui vous permettent de gérer et de sécuriser vos données à grande échelle et sur des environnements hybrides.

Comment mesurez-vous et améliorez-vous l'efficacité et l'efficience de vos solutions de DLP?

Pour mesurer et améliorer l'efficacité et l'efficience de vos solutions de prévention de la perte de données (DLP), vous devez disposer d'une vue complète et cohérente de vos données dans l'ensemble de votre organisation. Vous devez également être en mesure de suivre et de faire un rapport sur l'état de conformité et les actions prises sur vos données, ainsi que d'évaluer l'impact de vos politiques et contrôles. M365 E5 et Purview vous permettent de le faire en fournissant les fonctionnalités suivantes :

- **Tableau de bord de prévention des pertes de données :** Ce tableau de bord vous offre un endroit centralisé pour gérer et surveiller vos politiques et alertes de DLP à travers les applications et services Microsoft 365, tels qu'Exchange Online, SharePoint Online, OneDrive for Business, Teams et Power Platform®. Vous pouvez également vous connecter à des sources de données tierces, telles que Box, Dropbox, Google Drive, Amazon® S3 et Salesforce, en utilisant le connecteur Microsoft Cloud App Security. Le tableau de bord vous fournit des informations sur les types, les emplacements et les volumes de données confidentielles dans votre organisation, ainsi que sur l'exposition potentielle et les niveaux de risque. Vous pouvez également voir les tendances et les schémas d'incidents de perte de données et de violations, et approfondir les détails et le contexte de chaque événement. Vous pouvez utiliser ces informations pour peaufiner vos politiques et règles et prendre des mesures correctives pour prévenir ou atténuer la perte de données.
- **Purview Data Insight :** Cette fonctionnalité vous permet de découvrir, cataloguer et classer vos données sur l'ensemble de votre environnement de données hybride, y compris dans les environnements sur site, infonuagique et multinuage. Vous pouvez utiliser Purview pour analyser et indexer vos sources de données, telles que SQL Server®, Azure SQL Database, Azure Synapse Analytics, Azure Data Lake Storage, Azure Blob Storage, Azure Cosmos DB, Power BI, et bien plus encore. Vous pouvez également utiliser la carte de données de Purview pour visualiser la généalogie et les relations de vos données à travers différents systèmes et applications. Purview Data Insight vous aide à comprendre la nature, la sensibilité et la valeur de vos données, et à appliquer les politiques de protection et de rétention des données appropriées en fonction de vos besoins commerciaux et de conformité.
- **Gouvernance des données Purview :** Cette fonctionnalité vous permet de définir et de faire respecter vos politiques et permissions de données sur l'ensemble de votre environnement de données, et de garantir que vos données sont accessibles et utilisées conformément à vos normes et principes de gouvernance des données. Vous pouvez utiliser Purview pour créer et attribuer des rôles et responsabilités liés aux données, tels que les propriétaires, les responsables, les utilisateurs et les experts des données, et gérer leurs droits d'accès et privilèges. Vous pouvez également utiliser Purview pour mettre en place des règles de qualité des données et des vérifications de validation, et surveiller l'état de conformité et la santé de vos actifs de données. La gouvernance des données Purview vous aide à garantir que vos données sont précises, fiables et sécurisées, et que vous pouvez démontrer la conformité aux réglementations et normes internes et externes.

M365 E5 et Purview offrent plus de valeur et une sécurité améliorée par rapport à M365 E3, qui ne propose pas le même niveau de découverte, de classification, de protection, de rétention, de surveillance, de rapport et de gouvernance des données. M365 E3 offre également un soutien limité pour les scénarios de conformité aux données transversaux et interapplications, et ne comprend pas les fonctionnalités avancées de Purview qui vous permettent de gérer et de sécuriser vos données à grande échelle et sur des environnements hybrides. En passant à M365 E5 et à Purview, vous pouvez améliorer vos solutions de DLP et réduire le risque de violations de données et de conformité.

Pouvez-vous détecter et répondre aux incidents et aux violations de données sur plusieurs appareils, plateformes et applications en temps réel?

Voici quelques-unes des façons dont M365 E5 et Purview vous aident à détecter et à répondre aux incidents et aux violations de données sur plusieurs appareils, plateformes et applications en temps réel.

- **Purview Data Map :** Cette fonctionnalité vous offre une vue globale et actualisée de votre paysage de données, y compris où vos données sont stockées, comment elles circulent, qui y accède et ce qu'elles contiennent. Vous pouvez utiliser la carte de données pour découvrir et cataloguer vos données source, analyser et classer vos actifs de données, et suivre la généalogie et les dépendances de vos données. La carte des données s'intègre également à Microsoft Purview pour appliquer des politiques et des étiquettes cohérentes à vos données, et faire respecter les règles de protection des données et de conformité.
- **Centre de conformité M365 :** Cette fonctionnalité vous permet de gérer et de surveiller votre posture de conformité des données à travers M365 et d'autres services infonuagiques, tels qu'Azure, AWS®, Salesforce et Google Workspace. Vous pouvez utiliser le centre de conformité pour créer et attribuer des politiques et actions de conformité, telles que la rétention, la suppression, le chiffrement et l'audit, et les appliquer à vos données en fonction de leur type, de leur emplacement, de leur sensibilité et des exigences réglementaires. Vous pouvez également utiliser le centre de conformité pour générer des rapports et des tableaux de bord qui montrent votre état de conformité et vos performances, et identifier les lacunes ou les problèmes qui nécessitent votre attention.
- **Purview Audit (Premium) :** Cette fonctionnalité vous permet de capturer et de conserver des journaux d'audit plus détaillés et à plus long terme de vos activités et de l'utilisation de vos données, et de les analyser à des fins d'investigation et de recherche. Vous pouvez utiliser l'audit avancé pour accéder à jusqu'à 10 ans de données d'audit, rechercher et filtrer selon différents critères, tels que l'utilisateur, l'appareil, l'application et l'action, et exporter les résultats pour une analyse plus poussée. Vous pouvez également utiliser l'audit avancé pour configurer des alertes et des notifications pour des événements ou des modèles spécifiques, tels que l'exfiltration de données, l'accès non autorisé ou les violations de politique, et déclencher des réponses automatisées ou des flux de travail pour y remédier.
- **Purview Insider Risk Management :** Cette fonctionnalité vous aide à détecter et à atténuer les menaces internes, telles que les fuites de données, le vol, le sabotage ou la fraude, en utilisant des analyses avancées et l'apprentissage automatique pour identifier les comportements et les activités des utilisateurs à risque ou malveillants. Vous pouvez utiliser la gestion des risques internes pour définir des indicateurs et des seuils de risque, tels que le mouvement des données, la fréquence d'accès ou les anomalies réseau, et surveiller vos utilisateurs pour détecter tout écart ou violation. Vous pouvez également utiliser la gestion des risques internes pour enquêter et résoudre les incidents internes, et fournir des preuves et de la documentation pour des actions légales ou disciplinaires.

En passant à M365 E5 et Purview, vous pouvez tirer parti de ces fonctionnalités et capacités pour améliorer la sécurité et la conformité de vos données, et protéger vos données contre les menaces internes et externes.

Comment puis-je m'assurer que mes données sont chiffrées, classifiées, étiquetées et protégées en fonction de leur sensibilité et de leur valeur?

Pour garantir que vos données sont chiffrées, classifiées, étiquetées et protégées en fonction de leur sensibilité et de leur valeur, vous pouvez utiliser la prévention de la perte de données (DLP) de Microsoft 365 E5. Cette fonctionnalité vous aide à prévenir la fuite accidentelle ou intentionnelle de vos données confidentielles, telles que les informations personnelles, les données financières ou la propriété intellectuelle, en détectant et en bloquant les potentielles violations de données à travers les services Microsoft 365, tels qu'Exchange Online, SharePoint Online, OneDrive for Business, Teams et Outlook. Vous pouvez utiliser le DLP pour définir des règles et des politiques basées sur le contenu et le contexte de vos données, tels que les étiquettes de sensibilité, les destinataires ou l'emplacement, et appliquer des actions telles que la notification, le blocage, le chiffrement ou la rétention. En utilisant le DLP, vous pouvez protéger vos données contre un partage non autorisé ou inapproprié et vous conformer aux normes et réglementations de l'industrie.

Comparé à Microsoft 365 E3, qui offre des capacités de DLP limitées pour Exchange Online, SharePoint Online et OneDrive for Business, Microsoft 365 E5 propose des fonctionnalités avancées et complètes de DLP pour l'ensemble des services Microsoft 365, y compris Teams et Outlook. De plus, Microsoft 365 E5 inclut Microsoft Defender for Cloud Apps, qui étend le DLP aux applications infonuagiques tierces, telles que Dropbox, Box ou Salesforce. Microsoft 365 E5 vous permet également d'utiliser le marquage automatique par les points de terminaison, ce qui vous permet d'appliquer automatiquement des étiquettes de sensibilité à vos données en fonction du contenu et des métadonnées, et d'appliquer des politiques de chiffrement et de protection sur vos appareils, tels que Windows 10, iOS® ou Android.

Enfin, considérez les difficultés potentielles que vous pourriez rencontrer sans la proposition de valeur de sécurité de Microsoft M365 E5 :

- Vous **pourriez perdre la visibilité et le contrôle sur vos données confidentielles** sur différents appareils, plateformes et applications, et exposer vos données à un accès non autorisé ou à un mauvais usage.
- Vous **pourriez ne pas être en conformité avec les réglementations et normes de protection des données** de votre industrie ou région, telles que le RGPD, l'HIPAA ou le PCI DSS, et encourir des pénalités légales ou des dommages à la réputation.
- Vous **pourriez subir des violations ou fuites de données** compromettant la confidentialité, l'intégrité et la disponibilité de vos données, et entraînant des pertes financières ou le mécontentement des clients.
- Vous **pourriez passer à côté des opportunités d'optimiser** votre gouvernance et gestion des données, et d'améliorer la qualité, la sécurité et la valeur de vos données.
- Vous **pourriez ne pas être en mesure de détecter et de répondre aux menaces avancées basées sur l'identité,** telles que les comptes compromis, les risques internes ou les applications malveillantes, ou d'atténuer les dommages potentiels à vos données et systèmes.
- Vous **pourriez ne pas être en mesure d'appliquer des politiques d'accès granulaires et conditionnelles** basées sur l'utilisateur, l'appareil, l'emplacement et les facteurs de risque, ou d'empêcher l'accès non autorisé ou risqué à vos données et ressources.
- Vous **pourriez ne pas être en mesure de protéger vos données confidentielles** contre un partage, une suppression ou une altération accidentels ou malveillants, ou d'appliquer des politiques de prévention de la perte de données (DLP) sur l'ensemble de vos environnements infonuagique et sur site.
- Vous **pourriez ne pas être en mesure de découvrir, classer, étiqueter et protéger vos données confidentielles** tout au long de leur cycle de vie, ou de vous conformer aux exigences et réglementations de protection des données de votre industrie ou région.
- Vous **pourriez ne pas être en mesure de surveiller et d'auditer** vos activités de données et les journaux d'accès, ou de générer des rapports et des alertes à des fins de conformité et de gouvernance.

Insight.

Stimuler l'innovation grâce à la transformation numérique

Chez Insight, nous aidons nos clients à favoriser l'innovation avec une approche qui englobe les personnes, les processus et les technologies. Nous croyons que le meilleur chemin vers la transformation numérique est intégratif, réactif et aligné de manière proactive sur les exigences de l'industrie. Notre approche axée sur le client offre des solutions sur mesure à travers une gamme de services, comprenant l'environnement de travail moderne, les applications modernes, les infrastructures modernes, la périphérie intelligente, la cybersécurité et les données et l'IA.

En savoir plus à ca.insight.com

À propos de l'auteur

Norm Andersch est un architecte principal en cybersécurité au sein de l'équipe de l'environnement de travail moderne d'Insight. Son objectif est de créer des services professionnels et gérés spécifiquement pour la sécurité et la conformité afin d'aider les clients à renforcer leurs programmes de sécurité. Norm détient de nombreuses certifications Microsoft pour la sécurité Azure, Azure AD et l'ensemble des solutions Microsoft Defender.