SupportAssist for Business Pcs : présentation de la sécurité

Réponses à cinq questions clés que vous vous posez peut-être au sujet de la sécurité offerte par SupportAssist.

SupportAssist vous permet d'automatiser le support de Dell Technologies en identifiant les problèmes matériels et logiciels sur l'ensemble de votre parc de PC. SupportAssist gère les problèmes de performances et de stabilisation du système, réduit les menaces de sécurité, surveille et détecte les défaillances matérielles et automatise le processus d'engagement du support technique Dell.

SupportAssist collecte aussi proactivement les données de télémétrie à partir de vos PC et fournit des renseignements sur l'utilisation des PC et les mesures correctives qui s'imposent en fonction de votre type de souscription au service.

Sommaire

I. Introduction

Une panne sur un ordinateur portable peut être source à la fois d'interruption et de frustration. Les problèmes de ce type peuvent considérablement affecter la productivité d'un collaborateur, et souvent, au pire moment. C'est pour cette raison que les DSI portent une attention croissante à la qualité et au temps d'activité de leur parc de PC.

Nombre d'entre eux se sont tournés vers la technologie la plus récente et la plus avancée. Celle-ci utilise les informations issues de la science des données pour traiter des milliards de points de données et aider les administrateurs IT à gagner en efficacité. Les informations relatives à l'état du système obtenues à partir des systèmes des utilisateurs finaux sont envoyées au département IT de l'entreprise ou à un fournisseur de matériel ou de logiciels afin de prévenir ou résoudre rapidement les problèmes. Dell ProSupport Plus, avec la technologie de connectivité SupportAssist, vous alerte en cas de défaillance du disque dur en fournissant une vue unique de l'ensemble de votre parc informatique à partir du portail TechDirect.

Bien que cette technologie soit nécessaire pour garantir le temps d'activité et l'efficacité, les DSI posent parfois des questions sur les informations collectées et sur la manière dont elles sont gérées.

Les questions suivantes sont considérées comme essentielles :

- Quelles données SupportAssist collecte-t-il ?
- Comment ces données sont-elles protégées lors de leur transmission au département IT de l'entreprise ou au fournisseur d'ordinateurs ?
- Une fois qu'elles sont arrivées à destination, ces données sont-elles stockées de manière à rester privées et sécurisées ?
- Comment Dell respecte-t-il le RGPD et d'autres normes ?

Ce document examine ces questions, ainsi que d'autres interrogations permettant d'évaluer les technologies reposant sur la science des données. Il fournit un bref aperçu de la façon dont SupportAssist, dans le cadre de l'offre ProSupport Suite for PCs, fournit un service de support complet, capable d'anticiper les problèmes et de les résoudre avant même qu'ils ne surviennent. Il détaille également la façon dont la division Dell Technologies Services sécurise les données sensibles dans le cadre de ses processus, de leur transport et de leur stockage.

II. À propos de SupportAssist

SupportAssist est la technologie de connectivité intelligente de Dell[1] qui permet à une organisation de recevoir un support technique automatisé pour l'ensemble de son parc de PC. Elle surveille les appareils des utilisateurs finaux, détecte proactivement les problèmes matériels et logiciels et fournit des informations sur l'utilisation du système.

Lorsqu'un problème est détecté, SupportAssist ouvre automatiquement un ticket auprès du support technique, en fonction du niveau de service souscrit. Le type de problème détermine si l'alerte déclenche une demande de support technique ou une expédition automatique de pièces. SupportAssist collecte des données matérielles et logicielles, utilisées par le support technique pour dépanner et résoudre l'anomalie.

Dell ProSupport Suite for PCs offre les fonctionnalités de support les plus complètes dans une solution unique, sans avoir à multiplier les services[2]. En savoir plus.

Fonctionnalités clés

- Détection proactive et prédictive à l'échelle du parc pour une résolution plus rapide des problèmes
- Analyse rapide des scores d'intégrité, d'expérience des applications et de sécurité sur un seul écran
- Bibliothèque de scripts créés par Dell pour automatiser les tâches et corriger les problèmes sur l'ensemble du parc
- Automatisation de la création et du déploiement de catalogues de mises à jour personnalisés pour le BIOS, le pilote, le firmware et les applications Dell
- Flexibilité pour personnaliser vos vues et tableaux de bord dans TechDirect

Les fonctionnalités disponibles varient en fonction du forfait de support souscrit pour un PC.

- Avec ProSupport Plus, les utilisateurs finaux bénéficient de l'ensemble des fonctionnalités de SupportAssist, y compris la détection prédictive des problèmes et la prévention des pannes.

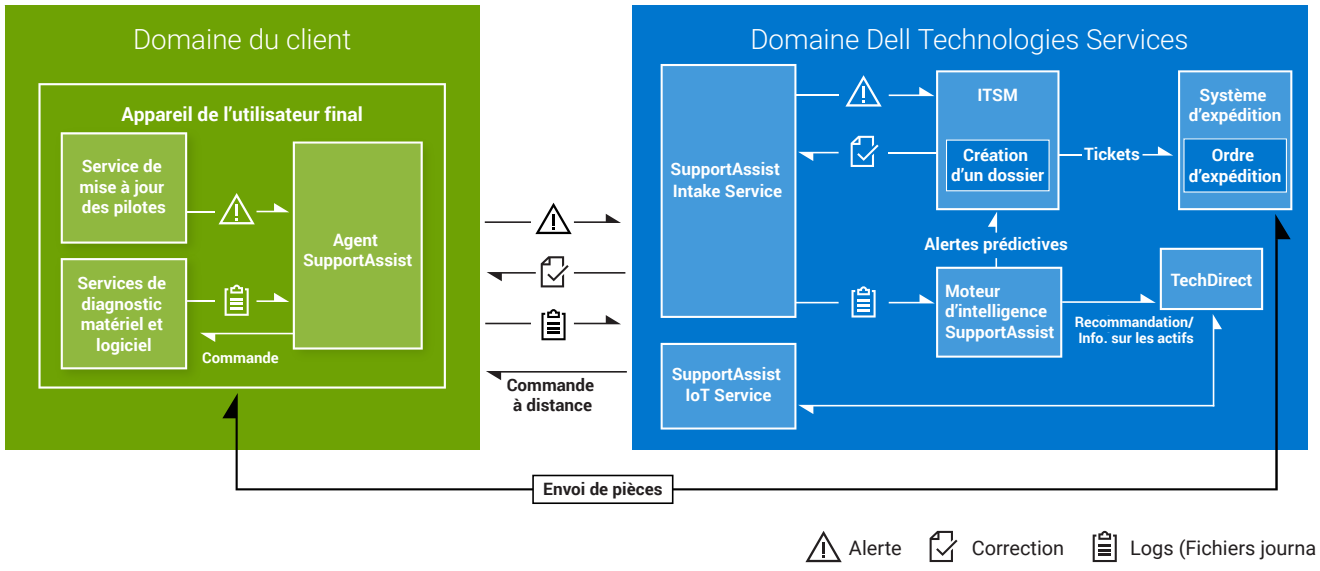
Pour obtenir la liste complète des fonctionnalités, consultez notre Guide de l'administrateur.

III. Architecture de SupportAssist

SupportAssist comprend un ensemble de services qui surveille les systèmes en continu et exécute des contrôles d'intégrité planifiés sur un appareil. Ces informations sont transmises aux serveurs Dell Technologies afin d'analyser les données et de formuler des recommandations.

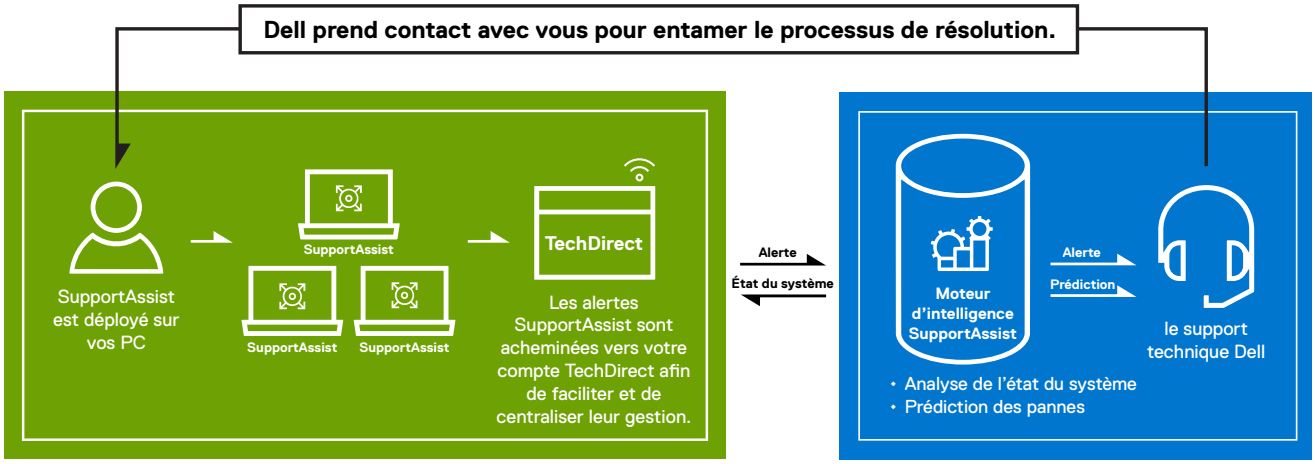
Consultez notre Guide de déploiement afin d'obtenir la liste complète des exigences en matière de réseau, de points de terminaison, de ports, de pare-feu ou de passerelles pour le déploiement et les mesures correctives de SupportAssist. Nos scripts correctifs sont développés par Dell, testés, signés puis confirmés avant leur exécution.

Architecture de SupportAssist



Gestion centralisée de SupportAssist à l'aide de TechDirect

Les alertes SupportAssist sont acheminées vers le compte TechDirect d'une organisation afin de faciliter et de centraliser leur gestion. Les organisations ayant souscrit au service ProSupport ou ProSupport Plus peuvent également choisir de transférer automatiquement les alertes à Dell Technologies Services.



Gestion centralisée de SupportAssist à l'aide de TechDirect (suite) :

SupportAssist Insights est un composant d'analyse particulièrement utile qui collecte des données d'utilisation du système consultables dans TechDirect. Il s'agit notamment de l'utilisation du processeur, de l'espace disque disponible, de la capacité maximale de la batterie, de l'autonomie de la batterie et de nombreuses autres informations utiles. TechDirect peut afficher ces informations pour tous les systèmes, pour les systèmes d'un groupe d'appareils spécifique ou pour un système individuel. Les clients sont en mesure d'identifier les problèmes de performances et de prendre de meilleures décisions commerciales (mettre à niveau ou remplacer le matériel, par exemple).

IV. Sécurité SupportAssist

Il peut arriver que le DSI ou le directeur de la sécurité d'une organisation se pose des questions sur les types de données collectées par SupportAssist et sur la façon dont ces données sont gérées. Cette section répond à ces questions, en montrant comment SupportAssist recueille uniquement les données nécessaires pour résoudre les problèmes des clients, puis gère ces données en assurant une sécurité optimale.

Quelles données SupportAssist collecte-t-il ?

Comment les scripts correctifs sont-ils sécurisés ?

Comment la technologie SupportAssist assure-t-elle la sécurité du stockage et du transfert des données ?

Comment le service SupportAssist utilise-t-il les données ?

Quelles sont les pratiques et politiques de sécurité de Dell Technologies ?

Quelles données SupportAssist collecte-t-il ?

SupportAssist collecte automatiquement les données nécessaires au dépannage d'un problème et les envoie en toute sécurité au support technique. Ces données nous permettent de fournir une expérience de support adaptative, intelligente et accélérée.

L'étiquette de service, nécessaire pour identifier l'appareil d'un utilisateur final spécifique, est la seule information sur la société collectée à partir des appareils. Lorsque SupportAssist détermine qu'une pièce doit être proactivement expédiée, Dell utilise les coordonnées existantes, lesquelles sont stockées en toute sécurité (par un chiffrement, l'application de règles de rétention, etc.) sur les serveurs Dell Technologies.

Les informations système suivantes sont collectées et expédiées une fois toutes les 24 heures dans le cadre de la surveillance du système de routine :

- **Version du schéma :** version du schéma utilisée pour la surveillance de routine du système
- **Version de l'agent :** version de SupportAssist déployée sur le système
- **Étiquette de service :** identifiant unique du système
- **Modèle de système :** nom de modèle du système
- **Informations d'enregistrement :** statut de l'enregistrement de SupportAssist
- **Version du système d'exploitation :** version du système d'exploitation en cours d'exécution sur le périphérique
- **Version SP :** correctif du système d'exploitation
- **Date UTC :** date et heure auxquelles les informations de surveillance du système de routine ont été transmises à Dell Technologies Services
- **Version du BIOS :** version du BIOS installée sur le système
- **État :** état de l'alerte en fonction de la gravité, par exemple, avertissement
- **Description :** informations sur la défaillance du système, par exemple, utilisation élevée du processeur
- **Espace libre sur le disque dur :** espace libre disponible sur le disque dur du système
- **Utilisation de la mémoire :** quantité de mémoire système utilisée
- **Utilisation du processeur :** quantité de processeur utilisée
- **Date locale :** date et heure du système
- **Dernière date de démarrage :** date et heure du dernier redémarrage du système
- **Date d'exécution de la mise à jour Windows :** date et heure de la dernière mise à jour Windows sur le système
- **Nombre de BSOD 24 h :** nombre d'occurrences d'écran bleu au cours des dernières 24 heures
- **Informations sur l'alerte :** ID unique de l'alerte

Pour plus d'informations sur les données de surveillance du système collectées à partir d'un système actif, veuillez consulter notre page Dell.com ici.

Toutes les informations sont transmises par des canaux sécurisés.

Comment les scripts correctifs sont-ils sécurisés ?

Avant d'être téléchargés sur la plateforme de mesures correctives, tous les scripts correctifs créés par Dell sont signés avec des certificats Dell, après quoi ils sont soumis à des tests approfondis et à une validation afin de s'assurer qu'ils fonctionnent comme prévu, sans produire de résultats inattendus. Ce processus sert de base à la vérification de l'authenticité du script avant son exécution. Par exemple, si un script est modifié ou remplacé sur le point de terminaison, la validation de la signature du certificat échoue et SupportAssist bloque l'exécution du script. Cela permet d'éviter l'exécution de code non autorisé ou potentiellement dangereux. Ces scripts ne peuvent pas être modifiés par des personnes extérieures à Dell, ce qui garantit leur intégrité. Il est recommandé de tester les scripts sur un groupe désigné de PC avant d'élargir leur déploiement.

Les scripts de workflow personnalisés suivent un autre processus. Lorsque les clients chargent leurs propres scripts, le système de mesures correctives accepte à la fois les scripts non signés et les scripts signés avec un certificat client. L'intégrité de ces scripts est préservée lors du transfert vers les PC et lorsqu'ils sont stockés au repos. Il est recommandé de tester les scripts personnalisés sur un groupe spécifique de PC avant d'élargir leur déploiement.

TechDirect Connect and Manage prend en charge la création de sites et de groupes, ce qui permet aux clients de valider à la fois les scripts créés par Dell et les scripts personnalisés sur les ordinateurs de test. Toutes les informations de la console de mesures correctives sont sécurisées dans les limites du domaine client dans TechDirect. Elles sont accessibles uniquement aux utilisateurs qui se sont vus attribuer des rôles appropriés par l'administrateur du client. Les résultats peuvent également être exportés dans un fichier CSV pour une analyse plus approfondie.

Comment la technologie SupportAssist assure-t-elle la sécurité du stockage et du transfert des données ?

Les données envoyées de SupportAssist à Dell Technologies Services sont chiffrées à l'aide d'un chiffrement 256 bits et transférées en toute sécurité via un protocole TLS (Transport Layer Security).

Une clé de chiffrement est générée au moment de l'exécution sur chaque machine lors de l'installation du package. La clé de chiffrement est utilisée, en complément du sel, pour chiffrer les informations installées. Un algorithme conforme aux normes du secteur est utilisé pour chiffrer les données au repos.

En cryptographie, le sel désigne des données aléatoires ajoutées à une fonction unidirectionnelle qui « hache » des données, un mot de passe ou une phrase secrète. La fonction principale des sels est de se défendre contre les attaques par dictionnaire ou leur équivalent haché, une attaque de table arc-en-ciel précalculée.

Toutes les clés de chiffrement sont générées à l'aide de générateurs de nombres aléatoires sécurisés. Les données en transit sont sécurisées à l'aide du protocole TLS par-dessus le protocole HTTPS (Hypertext Transfer Protocol Secure). Tous les algorithmes de chiffrement sont conformes aux normes du secteur, et les données au repos sont chiffrées.

Le protocole HTTPS est utilisé dans les communications hors zone pour les transmissions de commentaires fournis par l'utilisateur, les événements de télémétrie de diagnostic et l'interrogation d'une API sur Dell.com ou Microsoft Azure IoT Hub pour les informations système utilisées dans le processus de restauration. Un MQTT sécurisé est utilisé pour l'approche publication/abonnement.

Le protocole HTTPS standard est utilisé pour sécuriser les communications entre le client et l'infrastructure back-end lors de la transmission ou du téléchargement de contenu sur l'appareil de l'utilisateur final. Le protocole HTTPS ou MQTT sécurisé est utilisé pour sécuriser la transmission des données de télémétrie, la communication avec une API backend sur Dell.com ou Microsoft Azure IoT Hub, et le téléchargement du contenu récupéré à partir de Dell.com.

Tous les composants réseau sont situés derrière un pare-feu et sont gérés par une équipe de sécurité réseau. Le trafic réseau est étroitement contrôlé. Tout le trafic entrant est transmis via des ports spécifiques et uniquement envoyé aux adresses réseau de destination appropriées. SupportAssist utilise la bande passante réseau pour divers événements qui nécessitent une connectivité à l'infrastructure Dell Technologies Services. La bande passante utilisée peut varier en fonction du nombre de systèmes cibles surveillés par SupportAssist. Pour en savoir plus sur la consommation moyenne de données, reportez-vous au document Données collectées à partir de PC connectés.

Comment le service SupportAssist utilise-t-il les données ?

SupportAssist utilise les données collectées pour fournir un support automatisé, proactif et prédictif aux clients. En cas de problème avec un système, SupportAssist génère une alerte pour permettre à un agent du support technique de procéder au dépannage.

SupportAssist utilise également les données collectées pour prédire quand un composant est sur le point de tomber en panne, à l'aide d'un logiciel d'intelligence artificielle basé sur les données collectées à partir de dizaines de millions de systèmes Dell sur le terrain. Cette alerte prédictive peut être utilisée pour expédier une pièce avant qu'elle ne tombe en panne, ce qui optimise le temps d'activité du système et la protection des données.

Enfin, SupportAssist utilise les données pour détecter et supprimer les virus et les logiciels malveillants des systèmes utilisateur, pour optimiser les performances du système d'exploitation et pour fournir des recommandations sur les mises à jour du BIOS, des pilotes et du firmware.

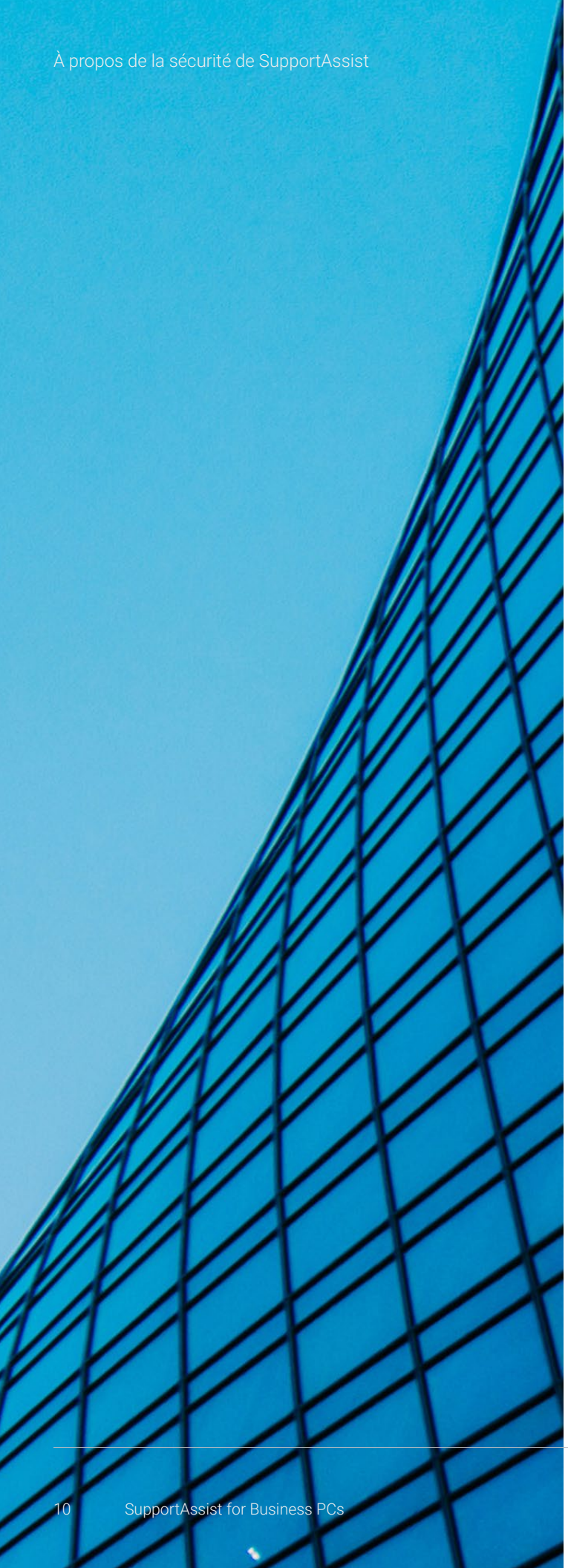
L'utilisation des applications système fournit des informations sur l'utilisation du système à l'aide du composant Insights.

Sécurité physique

Dell Technologies Services héberge les données SupportAssist, dont les informations relatives aux applications, systèmes et composants réseau et de sécurité, dans un datacenter situé aux États-Unis, conçu pour garantir des niveaux élevés de disponibilité et de sécurité. Les données SupportAssist sont protégées à l'aide d'un large éventail de mesures.

L'accès aux datacenters où se trouve l'infrastructure est limité au personnel autorisé. L'accès est contrôlé par carte à puce.

Les mesures de sécurité physiques et logiques protègent les données stockées.



Sécurité logique

Les données générées par SupportAssist sont stockées dans le respect de la Politique de confidentialité de Dell.

L'accès logique à l'infrastructure de Dell Technologies Services (serveurs, équilibreurs de charge, partages réseau, etc.) est limité par le biais d'outils internes audités et évalués conformément aux directives informatiques Dell Digital.

- **Audit :** les journaux des appareils surveillés sont tenus à jour et seules les infrastructures et/ou applications Dell Technologies Services y ont accès. Ces journaux consignent toutes les tentatives de connexion ou d'accès au système d'exploitation ou à la console du serveur Web SupportAssist.

Les builds gérés par l'IT sont renforcés à l'aide des contrôles recommandés par les pratiques d'excellence en matière de sécurité du Center for Internet Security (CIS).

Enfin, l'écosystème SupportAssist utilise à la fois la haute disponibilité locale au sein de son datacenter et une infrastructure identique dans un datacenter distinct. Les seules exceptions concernent les technologies qui présentent une haute disponibilité intrinsèque, telles que les clusters Big Data et les Clouds privés.

Pour l'analytique des données, Dell Technologies Services utilise les environnements Cloud que nous contrôlons et gérons entièrement, y compris les Clouds privés, hybrides et publics. Les bases de données relationnelles, les services de stockage simples et les entrepôts de données sont tous chiffrés et utilisent le moins de privilèges possible. Aucune base de données relationnelle n'est accessible au public. Les entrepôts de données sont sécurisés à l'aide du protocole HTTPS.

Quelles sont les pratiques et politiques de sécurité de Dell Technologies ?

Développement

Notre norme SDL (Secure Development Lifecycle Standard) interne est une base de référence pour les organisations produit Dell Technologies. Elle fournit des points de référence essentiels pour le développement sécurisé de produits et d'applications. Dell propose un catalogue de contrôle SDL défini basé sur la norme ISO/IEC 27034 et une norme basée sur le cadre de développement logiciel sécurisé (SSDF) du NIST. Ces outils aident les équipes Dell à créer des produits sécurisés pour les clients et à éviter l'introduction de failles et de faiblesses de sécurité dans les logiciels et le matériel développés et pris en charge par Dell. Les équipes d'ingénierie sont tenues de mettre en place ces contrôles lors du développement de nouvelles fonctionnalités. Ces contrôles englobent les activités d'analyse ainsi que des mesures normatives, appliquées de manière proactive et axées sur les principaux domaines de risque.

Les activités d'analyse, y compris la modélisation des menaces, l'analyse du code statique, l'analyse et les tests de sécurité, font partie intégrante de l'objectif d'identifier et d'atténuer les défauts de sécurité tout au long du cycle de développement. En outre, la norme SDL inclut des contrôles normatifs pour s'assurer que les équipes de développement traitent de manière proactive des problèmes de sécurité spécifiques, y compris ceux décrits dans les normes de l'industrie telles que l'Open Web Application Security Project (OWASP) Top 10 et le SANS Top 25.

SupportAssist for Business PCs s'aligne sur ce cadre SDL robuste, en utilisant le modèle de maturité SDL de Dell pour implémenter des contrôles de sécurité conformément aux normes du secteur. Le programme DevSecOps sécurise les processus modernes de développement et de déploiement de logiciels Dell en automatisant les contrôles SDL et en appliquant des règles de sécurité dans un environnement d'intégration et de déploiement continus (CI/CD). Ces outils CI/CD automatisent les processus de création, de test et de déploiement, ce qui garantit que les modifications de code sont intégrées et testées en continu dans le cadre du workflow de développement.

Les ingénieurs SDL effectuent des évaluations de sécurité SDL pour identifier les problèmes de sécurité et les vulnérabilités dans les logiciels et fournir des recommandations aux équipes de développement pour corriger ces constats de sécurité. C'est ainsi que l'on obtient de la visibilité sur la maturité de nos pratiques de sécurité et sur la posture de sécurité de nos logiciels et matériels.

Cette évaluation comprend les éléments suivants :

- L'évaluation des failles de sécurité à l'aide d'un test d'intrusion.
- Des tests de sécurité tiers effectués par des fournisseurs respectés tels que Secureworks.
- L'évaluation des solutions d'authentification, d'autorisation et de gestion des identités.
- L'analyse approfondie de toutes les bibliothèques et composants tiers à l'aide d'outils d'analyse de composition logiciels leaders sur le marché.
- La communication des conseils de sécurité Dell pour des améliorations de sécurité spécifiques.
- La classification rigoureuse des données en collaboration avec notre organisation de sécurité mondiale, et l'alignement des efforts de confidentialité et de sécurité pour protéger les données électroniques.
- La soumission de demandes d'audits de sécurité et de procédures de gouvernance.

RGPD

Chez Dell, nous avons mis en œuvre des mesures afin de nous assurer que nous disposons des processus et procédures nécessaires pour nous conformer aux obligations que nous impose le RGPD. Dell suit l'évolution des lois relatives à la protection de la vie privée dans le monde entier et veille à honorer ses obligations applicables en vertu de la législation en vigueur dans ce domaine. Lorsque la société Dell fait office de sous-traitant des données, elle se conforme à un formulaire mutuellement convenu ou à un formulaire de contrat de traitement des données standard. Pour plus d'informations, consultez les liens suivants :

- Résumé de la déclaration d'entreprise et des contrôles de Dell relatifs à la sécurité de l'information conformément au RGPD
- Engagement de Dell en matière de conformité au RGPD
- Questions fréquentes sur la conformité de Dell pour les clients Dell Technologies

Des processus sécurisés et des pratiques du secteur éprouvées maintiennent la sécurité de SupportAssist.

Tests de validation de la sécurité

Les évaluations de sécurité tierces sont effectuées régulièrement par rapport à l'application SupportAssist et à son infrastructure de prise en charge.

Les évaluations des applications incluent notamment le transport des données et la sécurité des API, l'analyse des codes source statiques et dynamiques, les vérifications croisées OWASP (Open Web Application Security Project) et les bibliothèques et produits tiers.

Les évaluations de l'infrastructure comprennent notamment les appareils, serveurs et prestataires de services internes et externes du réseau.

Gestion des changements

Le processus de gestion des changements de Dell Technologies suit les pratiques d'excellence ITIL Foundation, telles que dictées par le comité de gestion des changements dans l'entreprise. Toutes les modifications sont gérées via des tickets de demande de changement. Les personnes qui accèdent au système pour initier des modifications doivent suivre une formation ITIL et se familiariser avec la norme SDL. Toutes les mises à jour et mises à niveau appliquées à l'infrastructure back-end font l'objet d'un contrôle des versions à des fins de suivi et de traçabilité. L'équipe utilise un processus automatisé pour appliquer de nouveaux builds ou révoquer tout build ou correctif logiciel ayant été déployé.

Chaque version promue sur Dell.com/support contient des informations sur les changements apportés, avec toutes les limitations connues.

Toutes les nouvelles fonctionnalités et modifications sont préparées par notre équipe de gestion des produits et sont hiérarchisées à l'aide d'un processus de gestion des changements et d'un plan d'enregistrement.

Authentification

SupportAssist utilise Dell MyAccount pour l'authentification avec l'infrastructure ou l'application Dell Technologies Services, une clé symétrique aléatoire et les groupes de connexion du système d'exploitation/JWT pour l'authentification « on-the-box ».

Les groupes, tels que l'équipe d'administration de base de données et l'équipe de support opérationnel, qui ont accès aux composants de SupportAssist, se voient attribuer des tâches et des droits d'accès distincts. Toutes les mises à jour de l'environnement de production font l'objet d'une procédure de contrôle des changements définie, qui intègre des vérifications et des bilans.

Communauté sensibilisée à la sécurité

Dell propose un programme de formation à la sécurité basé sur les rôles pour sensibiliser les collaborateurs, nouveaux et existants, aux pratiques d'excellence en matière de sécurité spécifiques à leur poste et à l'utilisation des ressources pertinentes. Dell Technologies s'efforce de créer une culture de sensibilisation à la sécurité dans l'ensemble de sa communauté. En outre, la communauté de développeurs fait partie du programme Dell Security Champion, conçu pour favoriser la sécurité « Shift Left » dans les pratiques de développement logiciel.

Rapports sur les incidents

Chez Dell Technologies, tous les collaborateurs sont tenus de signaler rapidement toute activité suspecte, tout problème de cybersécurité ou toute menace à notre équipe de réponse aux incidents de sécurité informatique (CSIRT) par e-mail à l'adresse security@dell.com.

Réponse aux failles de sécurité

Dell Technologies s'engage à minimiser les risques associés aux failles de sécurité dans ses produits, ses applications et ses services Cloud. Pour mettre en œuvre rapidement des pratiques de réponse aux failles de sécurité, Dell respecte les directives décrites dans la norme Dell Technologies Vulnerability Response Standard (VRT). Dell participe activement à diverses initiatives communautaires, notamment les organisations FIRST (Forum of Incident Response and Response Teams) et SAFECode (Software Assurance Forum for Excellence in Code). Les processus et procédures de Dell sont conformes au cadre FIRST PSIRT Services Framework, ainsi qu'à d'autres normes, notamment ISO/IEC 29147:2018 et ISO/IEC 30111:2019.

Dell Technologies s'efforce de résoudre les failles de sécurité de ses produits, applications et services Cloud dans les délais les plus courts possibles du point de vue commercial. Les délais exacts peuvent varier en fonction de la vulnérabilité spécifique et de son impact, comme la complexité de l'effort/impact de sécurité à corriger. L'équipe PSIRT (Product Security Incident Response Team) coordonne la réponse et la divulgation de toutes les failles de sécurité des produits qui nous sont signalées. Toutes les divulgations relatives aux failles de sécurité des produits Dell Technologies sont disponibles en ligne sur la page Conseils, avis et ressources de sécurité Dell. Pour plus d'informations sur les pratiques de réponse aux failles de sécurité de Dell, reportez-vous à la Politique de réponse aux failles de sécurité de Dell.

Affiliations du secteur

Dell Technologies participe à plusieurs groupes du secteur afin de collaborer avec d'autres fournisseurs leaders dans la définition, l'évolution et le partage des pratiques d'excellence en matière de sécurité des produits et d'amélioration de la cause du développement sécurisé. Parmi les exemples de collaboration dans le secteur, citons : Voici quelques exemples de collaboration dans le secteur :

- Dell Technologies a cofondé et préside actuellement le conseil d'administration du Software Assurance Forum for Excellence in Code (SAFECode). Parmi les autres membres du conseil d'administration figurent des représentants de Microsoft, Adobe, SAP, Intel, Siemens, CA et Symantec. Les membres de SAFECode partagent et publient des pratiques et des formations en matière d'assurance logicielle.

Un leader du secteur dans la définition des pratiques d'excellence en matière de sécurité des produits et d'amélioration du développement sécurisé.

Affiliations du secteur - Suite

- Dell Technologies est un membre actif de l'organisation FIRST (Forum of Incident Response and Security Teams). FIRST est une organisation de premier plan et un leader mondial reconnu dans le domaine de la réponse aux incidents et aux failles de sécurité.
- Dell participe activement à l'Open Group Trusted Technology Forum (OTTF). L'OTTF dirige le développement d'un programme et d'un cadre pour l'intégrité de la chaîne logistique mondiale.
- Les employés de Dell ont été les membres fondateurs de l'IEEE Center for Secure Design, qui a été lancé dans le cadre de l'initiative de cybersécurité de l'IEEE afin d'aider les architectes logiciels à comprendre et à résoudre les failles de conception de sécurité les plus répandues.

Normes de sécurité du secteur

- Les collaborateurs de Dell sont activement impliqués dans les organismes de normalisation et les consortiums du secteur, qui se concentrent sur le développement de normes de sécurité et sur la définition de pratiques de sécurité à l'échelle du secteur, notamment :
- Cloud Security Alliance (CSA)
- The Forum of Incident Response and Security Teams (FIRST)
- The Open Group
- Software Assurance Forum for Excellence in Code (SAFECode)
- Storage Networking Industry Association (SNIA)

Dell Technologies est titulaire de la certification ISO 9001. Dell réalise régulièrement des audits trimestriels et des examens de conformité pour l'ensemble de ses centres de développement et de fabrication.

V. Conclusion

La technologie de connectivité SupportAssist offre des fonctionnalités intelligentes d'automatisation et de mesures correctives pour optimiser le temps d'activité du parc d'ordinateurs de bureau et d'ordinateurs portables Dell d'une organisation. La division Dell Technologies Services est en mesure de proposer cette technologie de pointe accompagnée d'une sécurité optimale grâce à la sécurisation des processus, de la transmission et du stockage des données.

Pour toute question et pour plus d'informations, rendez-vous sur **Dell.com/SupportAssist**

[1] Pour connaître la configuration requise et le système pris en charge, reportez-vous à notre guide de l'utilisateur (version SupportAssist for Home PCs pour un usage personnel) ou au guide de l'administrateur (version SupportAssist for Business PCs pour la gestion de parcs de PC) et cliquez sur « PC pris en charge ». Les fonctionnalités proactives et prédictives dépendent du service auquel vous avez souscrit et des règles commerciales de Dell Technologies. Pour en savoir plus sur les fonctionnalités de ProSupport Suite for PCs, consultez notre guide de l'administrateur et cliquez sur « Connexion et gestion des fonctionnalités et niveaux de service Dell ». Pour en savoir plus sur les fonctionnalités de Dell Care Suite, Premium Support Suite ou Alienware Care Suite for PCs, consultez le guide de l'utilisateur et cliquez sur « Fonctionnalités de SupportAssist et niveaux de service Dell ».

[2] D'après une analyse réalisée par Dell en décembre 2023.

© 2025 Dell Inc. Tous droits réservés. Des marques ou noms de produits peuvent apparaître dans ce document en référence aux entités revendiquant la propriété de ces marques et noms de produits ou à leurs produits. Les spécifications sont correctes à la date de publication, mais sont sujettes à disponibilité ou à modification sans préavis. Dell et ses sociétés affiliées ne peuvent en aucun cas être tenus responsables des erreurs et omissions de typographie ou de photographie. Les conditions générales de vente et de service Dell s'appliquent et sont disponibles sur demande. Les offres de services Dell n'affectent en aucun cas les droits légaux du client. Mars 2025 | KI