Rapport d'exposé de Sécurité

Windows 10

Avantages Et Inconvénients

Réalisé par :

Guermah Maamar Walid

Zaidi Imene

SOMMAIRE

Introduction

Introduction

Microsoft Corporation

Microsoft Corporation est une multinationale américaine, fondée par Bill Gates et Paul Allen, principalement active dans le développement et la vente des systèmes d'exploitation et des logiciels.

Le siège social de Microsoft se situe à Redmond, près de Seattle, et ses meilleures ventes sont le système d'exploitation Windows et la suite bureautique Microsoft Office.

Microsoft est le plus large producteur de software au monde mesuré par son revenu, elle est aussi une des entreprises les plus précieuses au monde.

Produits Microsoft

Microsoft depuis son apparition a réussi d'imposer sa présence au sein de la vie quotidienne et professionnelle de ses clients à travers le monde entier.

Et cela en produisant une large variété de logicielles et services permettant d'harmoniser l'expérience utilisateur par toutes les innovantes fonctionnalité que ses produits assurent.

Parmi les produits et services qui ont conquis le marché informatique on peut citer :

- Windows
- Office
- Xbox
- Skype
- Microsoft Store

Microsoft Windows

Windows été au départ une interface graphique unifiée produite par Microsoft, qui est devenue ensuite une gamme de systèmes d'exploitation à part entière, principalement destinés aux ordinateurs compatibles PC.

Ce système est passé par plusieurs versions à travers l'histoire de l'informatique commençant par Windows 1.x, 2.x, 3.x, 95, 2000, XP, Vista ..... 7, 8, pour arriver à Windows 10 qui est, actuellement, déployé sur plus de 200 millions appareils dans 192 pays différents a travers le monde.

Dans ce qui suit on va voir une présentation globale sur ce système d'exploitation et de ce qui rapporte de nouveau en matière logicielle, ainsi que ses principales avantages et inconvénient dans le domaine de sécurité informatique.

Présentation Générale

Présentation Générale

Présentation

Windows 10 est un système d'exploitation de la famille Windows NT développé par Microsoft. Officiellement présenté le 30 septembre 2014, il est disponible publiquement depuis le 29 juillet 2015.

Windows 7[2]	
Depuis l'édition	Vers l'édition
Windows 7 Édition Starter	Windows 10 Famille
Windows 7 Édition Familiale Basique	
Windows 7 Édition Familiale Premium	
Windows 7 Professionnel	Windows 10 Professionnel
Windows 7 Édition Intégrale	

Windows 8[3]	
Depuis l'édition	Vers l'édition
Windows Phone 8.1[5]	Windows 10 Mobile
Windows 8.1[4]	Windows 10 Home
Windows 8.1 Professionnel	Windows 10 Professionnel
Windows 8.1 Pro Étudiants	

La mise à jour vers Windows 10

Microsoft propose gratuitement la mise à jour vers Windows 10 pour les appareils dotés d'une version de Windows 7 ou de Windows 8/8.1 authentique et éligible

Présentation Générale

Editions

1. Windows 10 Famille
2. Windows 10 Professionnel
3. Windows 10 Mobile
4. Windows 10 Enterprise

Après la mise à jour, vous conserverez la même édition de Windows. À titre d'exemple, Windows 7 Édition Familiale Premium fera place à Windows 10 Famille.

Exigence matérielle et logiciels

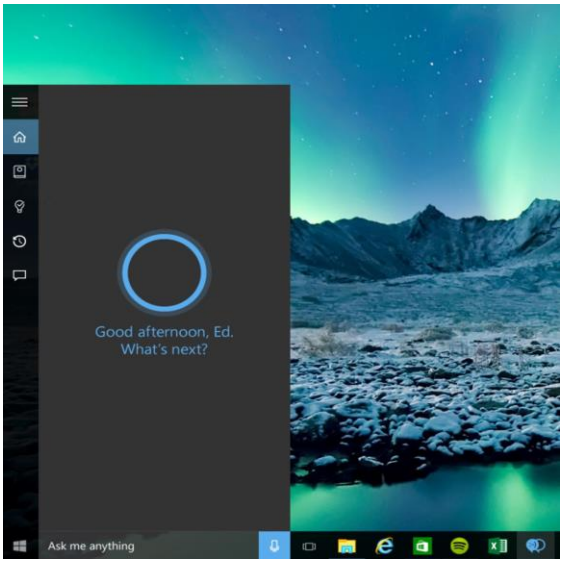
Pour procéder à la mise à jour vers Windows 10 sur PC ou tablette, voici ce qu'il faut :

- Dernier système d'exploitation : Utilisation de la dernière version de Windows 7 SP1 ou Windows 8.1.
- Processeur : Processeur de 1 GHz ou plus rapide ou SOC
- RAM : 1 gigaoctet (Go) pour système 32 bits ou 2 Go pour système 64 bits
- Espace sur le disque dur : 16 Go pour système 32 bits ou 20 Go pour système 64 bits
- Carte graphique : DirectX 9 ou version ultérieure avec pilote WDDM 1.0
- Écran : 800x600

Quoi de neuf ?

Quoi de neuf ?

Cortana

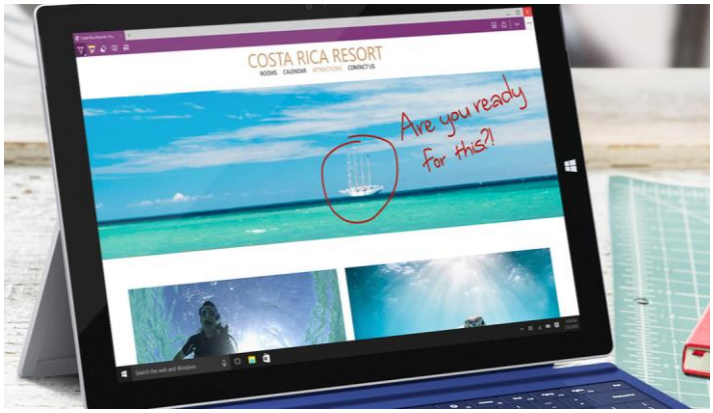


Cortana est un assistant personnel. Cortana fonctionne mieux lorsqu'il connaît les activités de son utilisateur et cela en utilisant les données depuis son appareil, son compte Microsoft personnel, des services tiers et d'autres services Microsoft

Et donc pour permettre son bon fonctionnement Cortana accède aux différentes informations suivantes :

1. Services de localisation.
2. Messages textes et e-mail.
3. Historique des communications.
4. Personnalisation vocale et des entrées.
5. Applications et services Microsoft
6. Services tiers.
7. Historique de navigation.
8. Historique de recherche.

Microsoft Edge



Microsoft Edge est le nouveau navigateur de Microsoft pour Windows 10.

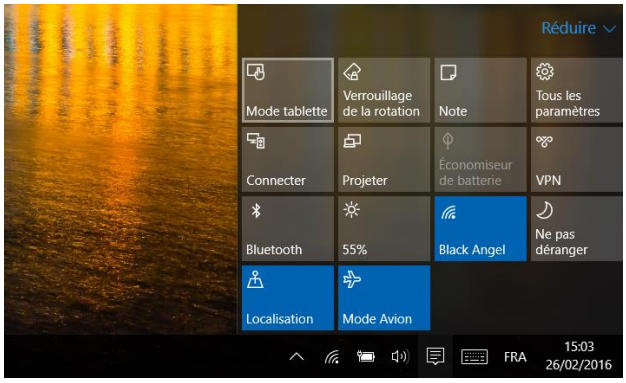
Lors de l'utilisation du navigateur pour accéder à Internet, des données à propos de l'appareil (l'adresse IP, la langue, les temps d'accès) sont envoyées aux sites web consulté et aux services en ligne utilisés

Microsoft Edge utilise les requêtes de recherche et l'historique de navigation pour fournir une navigation plus rapide et des résultats de recherche pertinents

1. Recherche automatique et suggestions de recherche.
2. Prédiction de page.
3. Sites suggérés.

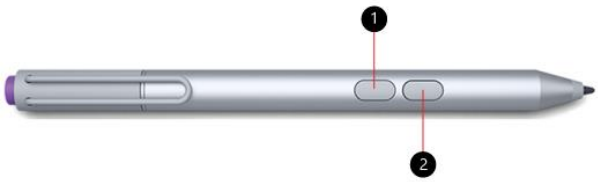
Quoi de neuf ?

Le Continuum



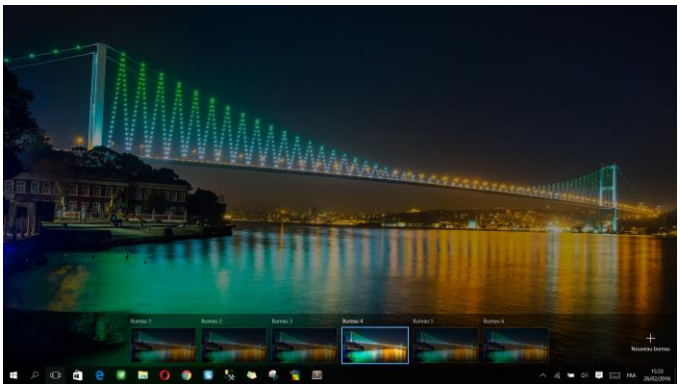
Windows 10 permet le passage du clavier vers le tactile et vice-versa et cela par sa faculté de détecter la présence d'un clavier physique afin d'ajuster automatiquement l'affichage du menu Démarrer et lors de l'utilisation d'une saisie tactile, ce menu se transforme alors en une interface Modern UI

En mode tablette l'utilisateur peut faire tout ce qu'il peut faire en mode normal avec un simple balayage vers une direction donnée.



Il peut même utiliser un stylet qui est plus confortable et naturelle, et n'a jamais été aussi proche de celle d'un stylo avec du papier.

Le Multitâche



Cette fonctionnalité permet de créer plusieurs bureaux virtuels et afficher les tâches ouvertes en un seul affichage ainsi de basculer facilement de l'un à l'autre.

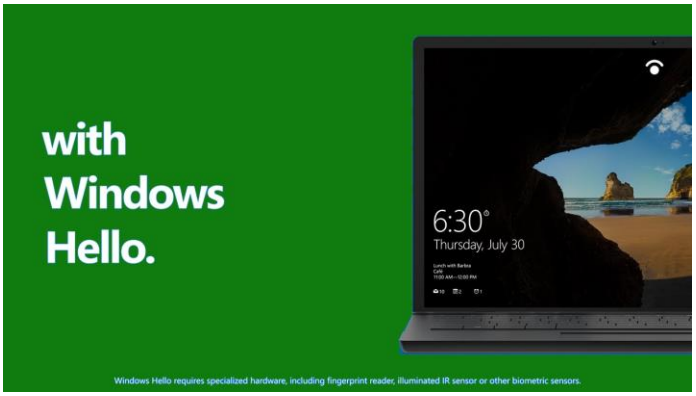
Elle permet à l'utilisateur d'attribuer certaines applications à un bureau, d'autres à un autre bureau.

Très pratique au quotidien, chaque bureau pouvant être enrichi, déplacé et supprimé selon le besoin utilisateur.

La sécurité

Sécurité : Avantage

Windows Hello



Windows Hello fournit un accès instantané aux appareils par identification biométrique.

Si l'utilisateur l'active, Windows Hello utilisera son visage, son empreinte digitale ou son iris pour l'identifier, sur la base de points ou de caractères uniques extraits de l'image et stockés sur son appareil comme modèle.

Les données de vérification biométrique utilisées lors de la connexion ne sortent pas de l'appareil et peuvent être supprimées au niveau des Paramètres.

Pour l'exploitation de cette fonctionnalité il faut que l'appareil soit doté d'une webcam RealSense 3D qui permet de faire du tracking d'objet dans l'espace et qui est équipée d'infrarouge pour que ça puisse fonctionner peu importe la luminosité.

Device Guard

Device Guard est une nouvelle fonctionnalité de Windows 10 exclusive a la version entreprise, il vise à lutter contre les malwares et les logicielles non autorisés de manière efficace.

Lors du chargement d'une application, Windows 10 se charge de vérifier si elle est approuvée ou pas par la politique d'entreprise et avertit l'utilisateur.

Pour avoir un haut niveau de sécurité Microsoft recommande d'utiliser Device Guard avec la sécurité basée sur la virtualisation, pour cela l'appareil doit disposer de matériel spécifique pour prendre en charge les fonctions de virtualisation hyper-v.

La sécurité basée sur la virtualisation est un mécanisme qui isole les processus critiques et la mémoire associée du reste du système d'exploitation.

Lorsque la protection est activée, les processus critiques s'exécutent dans un mode utilisateur isolé.

Le composant qui détermine si l'application est approuvée se nomme CODE INTEGRITY.

Le fonctionnement de device guard CODE INTERGRITY est le suivant :

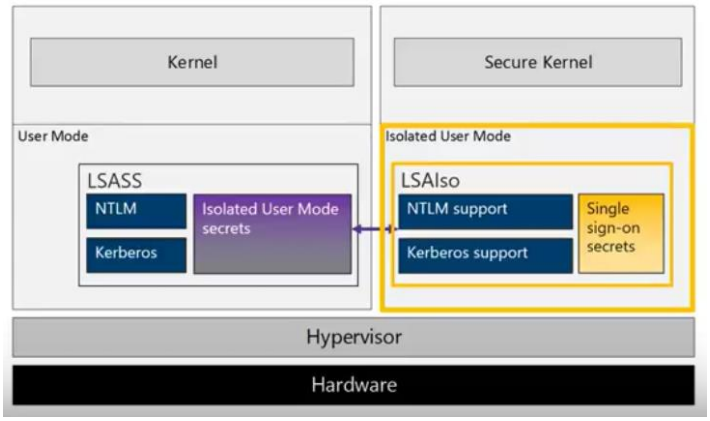
Avant qu'une application ou un driver soit chargé il faut que les pages mémoires soient marquées comme exécutables, ces pages mémoire ne sont marquées comme exécutable qu'après validation par CODE INTEGRITY.

Sécurité : Avantage

Credential Guard

Credential Gaurd est une fonctionnalité exclusive à Windows 10 Entreprise qui permet de protéger l'utilisateur contre le vol des informations d'authentification en rendant inopérant les outils de type MimiKatz par exemples qui sont fréquemment utilisés lors des cybers attaques pour l'extraction des mots de passe Windows

Credential Gaurd utilise l'environnement d'exécution sécurisé hyper-V pour isoler les données d'authentification du reste du système d'exploitation.



LSASS est le service d'authentification dans Windows qui permet de déterminer l'identité d'un utilisateur qui se sert d'un mot de passe ou de Windows hello ou une carte a puce.

Credential Guard isole les secrets précédemment stockés dans l'autorité de sécurité locale LSA en utilisant la sécurité basée sur la virtualisation.

Le processus LSASS communique avec LSAIso en utilisant des appels de procédures à distance

Les données stockées en utilisant la sécurité basée sur la virtualisation ne sont plus extractibles depuis le système d'exploitation.

Entreprise Data Protection

EDP vise principalement les utilisateurs qui accèdent sur le même appareil Windows 10 à des données privées et des données Entreprises, cela en leur permettant de différencier entre les deux types et apporter plus de sécurité aux données Enterprise ainsi d'éviter les fuites d'informations en copiant par exemple un fichier entreprise dans un dossier privé.

Les données Entreprises sont protégées par chiffrement au niveau du fichier et sont visiblement identifiable par une icone spécifique au niveau de l'interface

La protection du fichier est conservée même si le fichier est copié par exemple sur une clé USB

Les données sont classées comme Entreprise si elles proviennent d'une source ou destination définie comme Entreprise (Ex : intranet) ou d'une source Cloud de type OneDrive For Business.

Sécurité : Inconvénient

Two step forward, One step back

James Forshaw, qui est actuellement chercheur en sécurité chez Google Company (Spécialité Windows) et qui a pu découvrir comment compromettre Windows 8.1, lors d'une conférence informatique a fait un discours très contrasté, entre éloges et critiques. Il a d'ailleurs intitulé sa présentation : « Deux pas en avant, un pas en arrière».

Ce dernier a bien souligné la sécurité mise en place dans le nouveau système Windows 10 cependant il annonce qu'il est devenu exposé à une plus grande surface d'attaque.

James Forshaw explique qu'en effet, il y a 150 services système et 238 pilotes activés par défaut dans Windows7, 169 et 253 dans Windows 8.1, et 196 et 291 dans Windows 10, un nombre plus important synonyme en réalité d'une plus grande surface d'attaque.

Ce qui est encore plus grave c'est que seulement 11,11% des services sont démarré sous Windows 7 et 31,28% le sont sous Windows 10, ce qui signifie que les vecteurs d'attaque sont toujours présents et encore plus nombreux qu'avant.

Et pour terminer, Forshaw affirme que le nouveau navigateur Microsoft Edge préfigure l'avenir de la sécurité en matière de navigateur en activant par défaut la navigation privée, cependant il intègre une version de Flash Player qui est vue comme une véritable passoire sur le plan sécurité.

Confidentialité

Confidentialité

Le passage de Microsoft à Windows 10 a permis à de nombreuses personnes de se pencher sur les conditions d'utilisation de ce nouveau système d'exploitation, clairement plus orienté Cloud que ses prédécesseurs.

L'outil de tracking via la télémétrie implémentée dans Windows 10 a notamment été accusé de récolter des informations bien plus nombreuses et étendues que ce qui avait été jusque-là annoncé. De ce fait, de nombreux attentistes ont déclaré vouloir rester sur Windows 7 ou 8.1 en attendant que cette situation puisse se clarifier.

Qu'est-ce que la télémétrie ?

Selon Wikipédia, la télémétrie est une technologie qui permet la mesure à distance et la journalisation d'informations d'intérêt vers le concepteur du système ou un opérateur. Ces systèmes requièrent des instructions et des données à envoyer dans le but de réaliser l'exploitation requise.

Microsoft définit la télémétrie comme « données systèmes qui sont téléchargées par le composant Connected User Experience et Telemetry », également connu sous le nom de Universal Telemetry Client, ou service UTC.

Les données personnelles recueillies ?

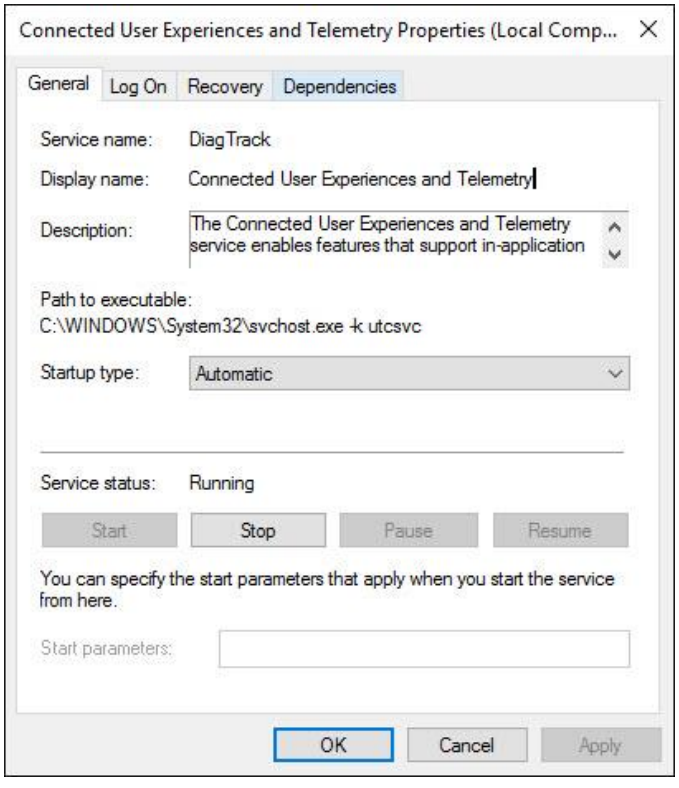
Dans la Déclaration de confidentialité de Microsoft, Microsoft explique quelles données personnelles sont recueillies, ces données sont :

- Nom et données du contact prénom, nom de famille, adresse e-mail, adresse postale, numéro de téléphone et d'autres données de contact similaires.
- Informations d'identification les mots de passe, les indices de mot de passe et des informations de sécurité similaires utilisées pour l'authentification.
- Données démographiques les données telles que l'âge, le sexe, le pays et la langue préférée.
- Centres d'intérêt et favoris.
- Données de paiement comme le numéro de moyen de paiement (par exemple, un numéro de carte de crédit) et le code de sécurité associé au moyen de paiement.
- Données d'utilisation comme les fonctionnalités utilisées, les articles achetés, les pages web consultées, les termes de recherche entrés …
- Contacts et relations
- Données de localisation, qui peuvent être soit précises soit imprécises. Les données de localisation précises peuvent être des données GPS (Global Position System), ainsi que des données identifiant des antennes-relais à proximité et des points d'accès Wi-Fi. Les données de localisation imprécises comprennent, par exemple, une localisation dérivée de l'adresse IP, Il peut notamment s'agir d'une ville ou d'un code postal.

Confidentialité

Comment se fait la collecte de données ?

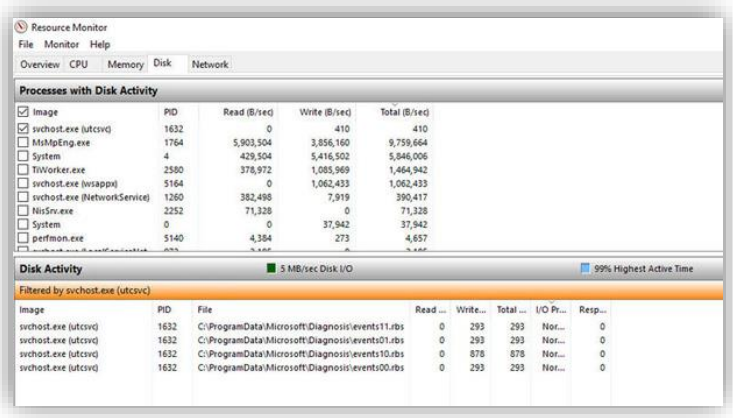
Windows 10 embarque un logiciel appelé **Connected User Experience and Telemetry**, également connu sous le nom de **Universal Telemetry Client** (UTC). Il fonctionne comme un service Windows avec le nom d'affichage DiagTrack et le nom de service utcsvc.



Pour trouver l'ID de processus (PID) de ce service, regarder l'onglet Services dans le Gestionnaire des tâches de Windows. Cette information est utile pour tous ceux qui veulent suivre les activités du service DiagTrack avec d'autres outils logiciels.

On va présenter ici le test effectué Par Ed Bott, ZDNet.com

En suivant ce PID pour surveiller l'activité du service DiagTrack sur une période de plusieurs jours, et ce en utilisant l'outil de suivi des ressources sur une machine virtuelle exécutant Windows 10 Enterprise avec un compte local et le niveau de télémétrie positionné sur « Basic ».



Cette capture d'écran montre le composant DiagTrack réaliser exactement ce que la documentation dit qu'il fait : une mesure initiale de la performance, puis la vérification du contenu de quatre fichiers de log toutes les 15 minutes. Parce qu'on ne faisait rien avec ce système de test, il n'y avait pas d'accidents ou d'installations d'applications à signaler, de sorte que ces fichiers de log ne changent pas au cours de la période que j'ai mesuré.

Confidentialité

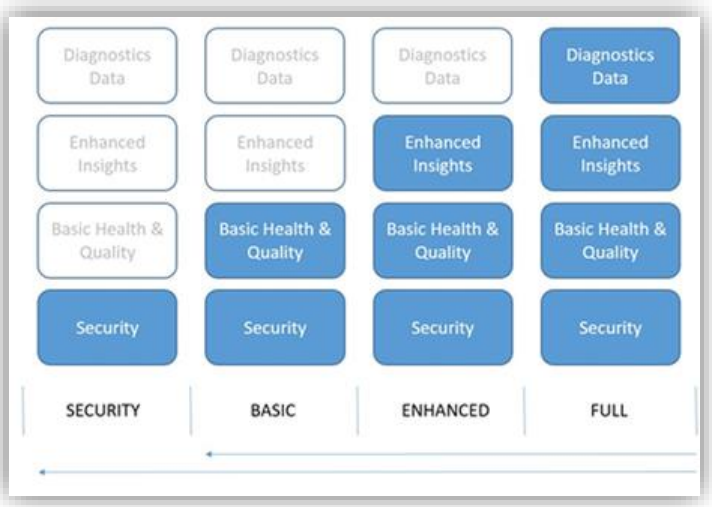
Sur ce système de test alimenté par secteur, sont plus ou moins 32 connexions qui sont effectuées toutes les huit heures. Si vous faites la même expérience avec l'option connexion réseau limitée, Microsoft affirme qu'aucune donnée n'est transmise. Et si le test est réalisé sur un ordinateur portable fonctionnant sur batterie, la vérification est effectuée toutes les quatre heures.

Niveaux de télémétrie dans Windows 10

Les différents niveaux de télémétrie dans Windows 10.

- Sécurité. Informations nécessaires pour préserver la sécurité de Windows, notamment concernant les paramètres du client de télémétrie, l'outil de suppression de logiciels malveillants et Windows Defender. Ce niveau est disponible uniquement sous Windows 10 Entreprise, Windows 10 Éducation et IoT Standard.
- De base. Informations de base sur l'appareil, à savoir : données relatives à la qualité, à la compatibilité des applications et au niveau de sécurité.
- Améliorée. Éclaircissements supplémentaires, à savoir : modes d'utilisation et de fonctionnement de Windows et des applications Windows, informations avancées sur la fiabilité, et informations des niveaux De base et Sécurité.
- Complète. Toutes les informations nécessaires pour identifier et résoudre des problèmes, ainsi que les informations des niveaux De base, Améliorée et Sécurité.

Sous forme de diagramme :



La quantité et le type de données de télémétrie que UTC recueille est déterminé par le choix d'un des quatre niveaux de télémétrie proposé. Trois d'entre eux (Basic, Enhanced et Full) peuvent être configuré en utilisant les réglages. Le quatrième niveau (dit Security) est disponible pour les PC uniquement sous licence Windows 10 Entreprise et Education et ne peut être réglé qu'a l'aide des outils d'administration tels que Group Policy ou celui de gestion des périphériques mobiles.

Les données de télémétrie comprennent des informations sur l'appareil et comment il est configuré (y compris les attributs matériels comme le processeur, la mémoire installée, et le stockage), ainsi que des renseignements relatifs à la qualité tels que la disponibilité, le nombre d'accidents ou de blocages. Des informations basiques sont également transmises, telles que la liste des applications et les pilotes installés.

Confidentialité

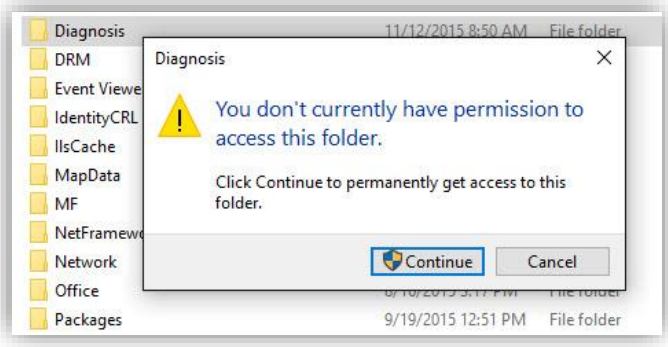
Pour les systèmes où la télémétrie est réglée à un niveau supérieur que celui de base, les informations recueillies comprennent des événements qui analysent l'interaction entre l'utilisateur, le système d'exploitation et les applications

Le niveau proposé par défaut dans Windows 10 Home et Pro est « Full » et « Enhanced » pour l'édition Enterprise. (Sur un périphérique qui exécute une édition Insider Preview, cette valeur est positionnée sur « Full » et ne peut être modifié que par l'installation d'une version finale.)

Les organisations qui ont besoin de se protéger un minimum des connexions réseau et des transferts de données devraient regarder avec attention le niveau « Secutity », mais seulement si elles ont les ressources IT pour mettre en place leur propre infrastructure de mise à jour. (A ce niveau de collecte de données minimale, Windows Update ne fonctionne pas.)

Où stocker les données de télémétrie ?

Sur un ordinateur équipé de Windows 10, les données de télémétrie sont stockées dans des fichiers chiffrés dans le dossier caché %ProgramData%\Microsoft\Diagnosis.



Les fichiers et dossiers positionnés à cet endroit ne sont pas accessibles aux utilisateurs normaux et il faut avoir les autorisations nécessaires ce qui rend délicat cette recherche. Et même si vous pouviez regarder dans le contenu de ces fichiers, il n'y a rien à y voir, parce que les fichiers sont chiffrés.

Le client UTC se connecte à settings-win.data.microsoft.com, fournit son ID de périphérique (générée aléatoirement et qui n'est associée à aucune donnée personnelle), ainsi que quelques autres détails de configuration, et télécharge un fichier de paramètres. Ensuite, le client de télémétrie utilise ce fichier de paramètres pour se connecter au service de gestion des données de Microsoft à l'adresse v10.vortex-win.data.microsoft.com et télécharge les données qui sont en attente d'être envoyées. La transmission a lieu via des connexions HTTPS chiffrées.

Comment Microsoft utilise les données ?

Microsoft conserve les données de télémétrie potentiellement sensibles « dans espace de stockage séparé, verrouillé, et accessible uniquement à un petit nombre d'employés de Microsoft du groupe Windows Device ». En outre, mentionne l'entreprise, « Seuls ceux qui peuvent démontrer un besoin métier valide peuvent accéder à l'information de télémétrie ».

Confidentialité

Ces données sont compilées dans des rapports pour analyse à l'usage des équipes chargées de la correction des bugs et de l'amélioration de la performance du système d'exploitation et des services associés. Seules « des informations de télémétrie anonymes et agrégées » sont mentionnées dans les rapports qui sont partagés avec les partenaires.

Il n'y a aucune règle concernant le temps de conservation des données. Toutefois, Microsoft affirme que son objectif est de stocker des données « aussi longtemps que cela est nécessaire pour fournir un service ou une analyse ». Une déclaration un peu vague mentionne que « la plupart de l'information sur la façon dont Windows et les applications fonctionnement est supprimée dans les 30 jours ».

Microsoft utilise les données recueillies dans trois buts essentiels :

1. Faire fonctionner ses activités et assurer la fourniture de ses services.
2. Pour envoyer des communications, y compris des communications promotionnelles.
3. Pour afficher de la publicité.

Partage des données personnelles

Dans la déclaration de confidentialité de Microsoft nous trouvons la façon dont les informations de l'utilisateur sont exploitées

« Nous accéderons à, divulguerons et préserverons les données personnelles, notamment votre contenu (comme le contenu de vos e-mails dans Outlook.com, ou des fichiers de dossiers privés dans OneDrive), lorsque nous pensons de bonne foi qu'il est nécessaire de le faire :

1. Lorsque cela est exigé par la loi en vigueur ou pour répondre à des requêtes légales valides, notamment celles émanant des organismes d'application de la loi et d'autres organismes gouvernementaux ;
2. Pour protéger nos clients, pour éviter le spam ou les tentatives d'escroquer des utilisateurs des services, ou pour empêcher les pertes de vie ou des blessures graves ;
3. Pour utiliser et assurer la sécurité de nos services, notamment prévenir ou arrêter une attaque sur nos systèmes ou réseaux informatiques ;
4. Pour protéger les droits ou la propriété de Microsoft, y compris l'application des conditions d'utilisation des services — toutefois, si nous recevons des informations indiquant qu'une personne utilise nos services pour un trafic de biens physiques ou intellectuels volés appartenant à Microsoft, nous n'inspecterons pas nous-mêmes le contenu privé d'un client, mais nous pourrons saisir les autorités judiciaires. »

Conclusion

Aujourd'hui les systèmes d'exploitation jouent un rôle très important dans l'environnement de l'entreprise et constituent le cœur de son système d'information ainsi que celui de toute décision à prendre dans la vie professionnelle ou privée de l'individu.

C'est pourquoi, il est dans l'intérêt de l'individu de savoir choisir quel système va convenir au mieux au type d'information traitée afin de pouvoir protéger cette derniere et garder sa conformité et sa fiabilité.

Parmi ces systèmes, nous avons vu Windows 10 qui proposent toute une panoplie de services de sécurité jugé robustes pour la protection des données, néanmoins il faut rester vigilant et prendre ses gardes en ce qui concerne la confidentialité de ces données vue la manière dont elles sont exploitées par Microsoft.

Bibliographie

Déclaration de confidentialité de Microsft

- **https://privacy.microsoft.com/fr-fr/privacystatement**

Articles

- **http://www.zdnet.fr/actualites/windows-10-et-la-telemetrie-une-analyse-reseau-simple-pour-faire-la-lumiere-39832840.htm**
- **http://www.theregister.co.uk/2015/10/26/windows_10_gets_penciled_security_tick_from_top_google_hacker/**
- **http://www.memoclic.com/393-windows/18463-nouvelle-version.html**

Vidéos

- **Présentation de Device Guard, Credential Guard, et Entreprise Data Protection par Arnaud Jumelet ingénieur en informatique de la la Direction Technique et Sécurité de Microsoft France**