

1. Identification Du produit

<i>Organisation éditrice</i>	Blancco Ltd.
<i>Lien vers l'organisation</i>	www.blancco.com
<i>Nom commercial du produit</i>	Blancco - Data Cleaner+
<i>Numéro de la version évaluée</i>	Version 4.8
<i>Catégorie de produit</i>	Effacement de données

2. Description du Produit

a. Description générale du produit

Le logiciel Blancco - Data Cleaner+ est une solution d'effacement « irréversible » des informations contenues dans des disques durs sur des architectures Intel x86. Les cas typiques d'utilisations de ce logiciel sont :

- lors de la réaffectation d'un disque dur d'une personne à une autre.
- Lors de la mise à la réforme d'un disque.

L'effacement se fait par réécriture des secteurs du disque dur selon un mode opératoire défini, soit par une norme de suppression (cf. §1) soit par l'utilisateur lui-même. La fonction de réécriture est indépendante du système d'exploitation et du BIOS de la machine sur laquelle se trouve le disque à effacer.

Après l'effacement des disques durs, le logiciel génère automatiquement un rapport détaillé de la suppression incluant un inventaire complet du matériel et indiquant le nombre de secteurs défectueux physiquement. Le logiciel peut traiter l'effacement simultané de 4 disques durs par ordinateur.

Les disques durs dont les données ont été supprimées par le logiciel peuvent être réutilisés. Le logiciel n'a aucun effet sur les fonctions mécaniques du disque dur. Il peut automatiquement effectuer un formatage « logique » du disque dur après l'effacement et en faire des partitions pour une réutilisation rapide et facile. Le reformatage logique est disponible en NTFS, FAT16 ou FAT32.

Le produit est disponible en 3 versions différentes :

- Standalone : Le produit est gravé sur un CD ou présent dans une disquette. Il n'est dépendant d'aucune autre installation. Il nécessite la disponibilité d'un support externe au PC pour sauvegarder les rapports d'effacement.
- Network : Le produit peut être gravé ou initié à partir du réseau. Il est dépendant du serveur de gestion de Blancco assurant la gestion des effacements et leur audit. Ce serveur peut être local (Blancco LAN Server ou Blancco WAN Server) ou hébergé par Blancco (www.blanccoservice.com).
- Combined : Cette version est un mixte des deux précédentes. Si la machine sur laquelle s'installe le logiciel ne détecte pas de serveur Blancco dans le réseau de la machine il passe en mode standalone.

b. Description de la manière d'utiliser le produit

Il est supposé que toutes les données utiles contenues sur le disque à effacer ont été préalablement sauvegardées avant le lancement de la procédure d'effacement.

Le logiciel Blancco - Data Cleaner+ dispose de son propre système de démarrage (boot). L'ordinateur cible démarre par pré installation, à partir d'une disquette, d'un CD-ROM ou du réseau (PXE¹).

Par pré installation, le logiciel est livré sous format MSI (Microsoft Installer). Ceci est un exécutable qui va installer le logiciel sur le disque dur. Pour démarrer l'effacement, l'administrateur clique sur Blancco dans le menu de démarrage de Windows. Cette action va changer l'ordre de démarrage du PC et va mettre Blancco - Data Cleaner+ comme premier choix de démarrage. L'administrateur devra confirmer cette action à deux reprises. Le système d'exploitation Windows va s'éteindre et le PC va redémarrer avec le logiciel Blancco - Data Cleaner+. Après l'effacement le rapport peut être sauvegardé sur un support amovible tel qu'une disquette ou une clé USB.

En mode standalone et combined le rapport est sauvegarder sur un système amovible tel qu'une disquette ou une clé USB

En mode réseau (PXE), l'ordinateur client va solliciter le serveur Blancco LAN Server pour récupérer une image du système de démarrage. L'ordinateur client peut alors démarrer depuis le système Blancco. Dès lors, l'utilisateur a la possibilité de choisir les disques à effacer selon un standard prédéfini, ou choisi par lui. Lors du lancement de l'effacement, l'ordinateur client interroge le serveur pour vérifier s'il reste suffisamment de licences pour effectuer l'effacement. Si la réponse est positive, l'effacement commence. A partir de là, l'ordinateur client peut-être isolé du serveur, l'effacement ce fera jusqu'à la fin (sauf intervention de l'utilisateur). Quand l'effacement est terminé, l'ordinateur client envoie un rapport au serveur. Si le serveur est indisponible (faille du réseau), l'utilisateur a la possibilité de sauvegarder ce rapport sur un système amovible.

La gestion de la suppression se fait de manière intuitive à la souris et au clavier. Ceci se déroule principalement en 4 écrans.

- Confirmation de la licence d'utilisation
- Sélection des disques à effacer : l'agent peut modifier toutes les configurations par défaut de l'image client.
- Procédure d'effacement : barres d'avancement de la procédure et possibilité d'arrêter l'effacement.
- Affichage et sauvegarde du rapport : sauvegarde sur le serveur ou sur média amovible

Ces quatre écrans sont modifiables selon la personnalisation de l'image par l'administrateur Ceci allant d'une image complètement dépendante de l'agent d'effacement à une image client complètement automatisée (nécessitant seulement la sélection de l'image à utiliser et l'extinction de la machine après l'effacement).

¹ PXE : **P**re-**X**ecution **E**nvironment : permet à une station de travail de démarrer à partir d'une image de système d'exploitation qui se trouve sur un serveur.

Cible de Sécurité - Blancco DataCleaner+ v4.8

c. Description de l'environnement prévu pour son utilisation

- Blancco – Data Cleaner+ doit être lancé sur une machine dont la configuration doit être gérée par l'administrateur. Il n'y a pas de dépendance par rapport au système d'exploitation.
- Blancco – LAN Server s'installe sur les plateformes Windows Server 2000 ou 2003.

d. Description des hypothèses sur l'environnement

Blancco – Data Cleaner+ doit être lancé sur une machine en bon état de marche. Ce produit est destiné à des utilisateurs avertis ayant les droits et autorisations nécessaires sur les machines à effacer.

Le réseau utilisé doit être sain et géré en appliquant les procédures classiques d'administration et d'exploitation. Ses administrateurs sont considérés comme non hostiles.

- Rapports

Il est supposé que l'administrateur lit les certificats d'effacement afin de confirmer le bon fonctionnement de Blancco – Data Cleaner+.

- Réseau

Dans le cas des versions Network et Combined, il est supposé que l'administrateur dispose des droits d'accès à l'infrastructure réseau qui accueillera le serveur d'effacement Blancco, autant au niveau physique (câblage, matériel d'interconnexion, etc.) qu'au niveau logiciel.

L'administrateur doit aussi disposer de connaissances suffisantes dans le domaine de l'administration du système et des services nécessaires au déploiement de la solution, tels que:

- Active Directory
- DNS – Domain Name Server
- DHCP – Dynamic Host Configuration Protocol
- RIS – Remote Install Services ou WDS – Windows Deployment Service (PXE)
- IIS - Internet Information Services

L'administration du serveur se fait au travers d'une interface web. De ce fait une présence physique sur le serveur est inutile, mais est toutefois possible. Cette application site est protégée contre une utilisation non autorisée selon le schéma suivant :

- Une section utilisateur, permettant seulement l'interaction avec le serveur et en AUCUN cas la modification de ce dernier ou de son contenu.
- Une section administrateur, accessible seulement aux personnes autorisées par l'administrateur dans la configuration d'IIS. Les moyens de contrôle d'accès supportés sont ceux proposés par IIS, tels que ACL ou Active Directory.

Cible de Sécurité - Blancco DataCleaner+ v4.8

- Environnement de travail

Les machines des utilisateurs sont dans un environnement de confiance, le logiciel d'effacement ne disposant d'aucun mécanisme visant à assurer sa propre sécurité (intégrité...). Il peut s'agir typiquement d'un environnement bureautique. .

- e. Description des dépendances par rapport à des matériels, des logiciels et/ou des microprogrammes du système qui ne sont pas fournis avec le produit

Blancco - Data Cleaner+ supporte les disques durs sur des architectures Intel x86.

La machine cible doit être configurée pour démarrer sur le support contenant le logiciel d'effacement (disquette, CD-Rom ou carte réseau supportant le PXE selon les cas)..

- f. Description des utilisateurs typiques concernés (utilisateurs finaux, administrateurs, experts...)
et de leur rôle particulier dans l'utilisation du produit

Ce produit est destiné à des utilisateurs avertis ayant les droits et autorisations nécessaires sur les machines à effacer : administrateur de la machine, agents d'effacement, utilisateurs avec droits d'accès au serveur d'administration.

- g. Définition du périmètre de l'évaluation, à savoir les caractéristiques de sécurité du produit concernées par l'évaluation

Le périmètre de l'évaluation concerne Le logiciel Blancco - Data Cleaner+ v4.8 complet, en version Network, Combined et Standalone, avec toutes ses fonctions de sécurité.

Le serveur Blancco – LAN Server est en dehors du périmètre de la cible mais devra être mis en œuvre pour évaluer les versions Network et Combined de logiciel Blancco - Data Cleaner.

3. Description de l'environnement technique dans lequel le produit doit fonctionner

- a. Data Cleaner a été conçu pour effacer les données stockées sur les supports suivants :

- Ordinateur compatible IBM avec un processeur 486DX ou mieux
- IDE, SCSI, SATA, USB
- Disquette de 1.44 MB ou CD-Rom

- b. Système d'exploitation compatible

- Blancco Data Cleaner fonctionne sur son propre système d'exploitation. Aucune compatibilité n'est donc nécessaire.

4. Description des biens sensibles que le produit protéger

Les biens sensibles sont les données stockées sur le disque dur à effacer.

5. Description des menaces

L'agent menaçant est toute personne non autorisée qui tenterait de récupérer des données sur les disques durs de l'ordinateur ayant fait l'objet d'un effacement par le logiciel.

6. Description des fonctions de sécurité du produit

Blancco - Data Cleaner+ fournit une fonction d'effacement de données secteur par secteur en réécrivant la totalité du disque. Cette réécriture est régie de deux façons différentes.

1. Standards Prédéfinis : Certifiés par des agences de sécurité et des gouvernements, leur configuration varie en fonction des pays et standards de sécurité dans lesquels ils ont été validés (voir ci-après).
2. Standards Personnalisés : l'utilisateur choisit comment se passera l'effacement.

Ces deux types de standard sont régis par une configuration à deux paramètres points :

- Le nombre de passages, c'est à dire le nombre de fois que le disque sera complètement réécrit.
- Le motif d'écrasement, c'est à dire la valeur hexadécimale qui sera écrite dans chaque secteur du disque.

Certains des standards prédéfinis définissent aussi si une vérification est obligatoire ou optionnelle après l'effacement. Cette vérification est faite par Blancco – Data Cleaner+ après chaque effacement et est confirmé dans le rapport d'effacement.

Les standards prédéfinis présents dans le logiciel sont :

Les standards prédéfinis	Nombre de réécritures	Vérification
Air Force System Security Instructions 5020	4	Obligatoire
Bruce Shneider's algorithm	7	/
HMG Infosec Standard No: 5 (baseline)	1	Optionnel
HMG Infosec Standard No: 5 (enhanced)	3	Obligatoire
Navy Staff Office Publication (NAVSO P-5239-26) for RLL	3	Obligatoire
OPNAVINST 5239.1A	3	Obligatoire
Peter Gutmann's algorithm	35	/
The National Computer Security Center (NCSC-TG-025)	4	Obligatoire
U.S. Department of Defense Sanitizing (DOD 5220.22-M)	3	Obligatoire
U.S. Army AR380-19	3	Obligatoire
German Standard BSI/VSITR	7	/
National Security Agency 130-1	3	Obligatoire
U.S. Department of Defense Sanitizing (DOD 5220-22-M ECE)	7	Obligatoire

En outre, Blancco - Data Cleaner+ dispose d'outils de détection permettant la suppression de données dans des zones normalement inaccessibles tels que HPA (Host Protected Areas) et DCO (Device configuration Overlay), ainsi que le support des secteurs altérés et remappés.