Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

Check Point GO: un espace de travail sécurisé virtuel

Livre blanc technique

Table des matières

Problématiques des travailleurs

Les entreprises connaissent depuis ces dernières années une augmentation significative de la mobilité de leurs travailleurs. Les employés se connectent aujourd'hui régulièrement à leur bureau à partir de leur PC personnel via VPN, utilisent des points d'accès Wifi dans les aéroports, et reçoivent leurs e-mails professionnels sur leur smartphone. Cette mobilité conduit à une productivité sans précédent pour les entreprises, leurs employés restant connectés à tout moment et en tout lieu.

Un nombre croissant d'entreprises utilise le télétravail comme alternative viable pour leurs employés. Certains employés travaillent plusieurs jours par semaine depuis leur domicile, tandis que d'autres travaillent à distance à temps plein. Selon une étude de *World at Work*, 42% des employeurs américains ont permis à leurs employés de travailler à distance en 2008. Ce chiffre était de 30% l'année précédente. Ces employés se connectent typiquement depuis un ordinateur portable appartenant à leur entreprise, ou depuis leur ordinateur personnel, via une connexion VPN directe.

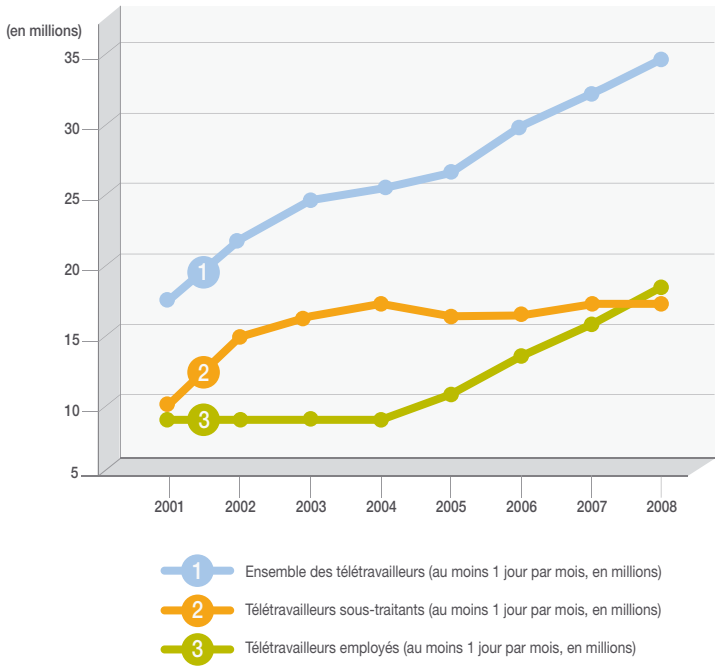

Figure 1. Tendances du télétravail.
Source : Telework Trendlines 2009, WorldatWork.

Les entreprises sont également amenées à fournir des accès contrôlés et protégés à leurs sous-traitants et partenaires. Selon le Ponemon Institute, plus de 44 % des cas de failles de sécurité cette année sont dûes à des erreurs de tiers. L'ouverture d'un accès instantané au réseau de l'entreprise pour les employés en déplacement devient également un besoin vital pour de nombreuses entreprises. La disponibilité des accès haut débit et l'efficacité des communications modernes ont accéléré la vitesse des échanges commerciaux. L'accès continu aux ressources de l'entreprise est devenu une nécessité.

En chiffres :

- 42% des employeurs américains favorisent le télétravail
- 34 millions d'employés télétravaillent au moins un jour par mois
- 43% d'augmentation du nombre de télétravailleurs

Fait :

Le nombre croissant de travailleurs mobiles augmente les risques de sécurité

Menaces et dangers pour les travailleurs mobiles

Bien que l'accès à distance sécurisé au réseau de l'entreprise pour les employés, les sous-traitants et les partenaires fournisse d'énormes avantages en termes de productivité et d'efficacité, il entraîne également des risques significatifs pour la sécurité de l'entreprise. Les ordinateurs portables contenant des données confidentielles sur l'entreprise ou ses clients peuvent être perdus ou volés. Les mots de passe, identifiants de connexion et fichiers confidentiels laissés sur des périphériques non sécurisés à la fin d'une session pourraient être exploités par les utilisateurs suivants. De plus, les employés qui se connectent à distance peuvent utiliser des machines non sécurisées, ou encore, des machines contenant des logiciels malveillants peuvent ouvrir un accès direct au réseau de l'entreprise et le rendre vulnérable à de nombreuses menaces.

Figure 2. Les attaques ciblent les données confidentielles à l'aide de différentes méthodes.

Pour ces raisons, les utilisateurs mobiles requièrent des niveaux de protection supplémentaires qui ne peuvent simplement pas être fournis par les solutions traditionnelles de sécurisation de poste.

Check Point GO fournit la solution

GO est une clé matérielle chiffrée contenant un logiciel de sécurité. GO chiffre les données sur son disque flash et fournit un accès à distance sécurisé par des règles spécifiques, ainsi qu'un environnement de travail sécurisé virtuel pour travailler sur des documents et des applications. Toutes les données confidentielles des utilisateurs sont chiffrées sur le disque flash, afin que les identifiants, les informations contenues dans les documents et autres données confidentielles restent protégées, même en cas de perte de GO.

Lorsque GO est connecté au port USB d'un PC, un nouveau bureau Windows contenant les raccourcis et les documents de l'utilisateur lui est présenté. GO utilise les logiciels installés sur le PC, tels que Microsoft Word et Microsoft Excel, mais les documents de l'utilisateur restent protégés dans l'environnement GO,

Les pertes de données sont une menace réelle :

- PC non administrés et non sécurisés
- Logiciels malveillants
- Enregistreurs de frappe

Une solution trois en un:

- Virtualisation sécurisée
- Connexion sécurisée
- Portable, plug-and-play

qui est un environnement sécurisé fonctionnant séparément en parallèle de l'environnement de l'hôte. GO ouvre un canal sécurisé avec les applications stockées sur l'hôte, ce qui lui permet d'utiliser les applications, mais aucune donnée n'est transférée ni mise à disposition sur l'hôte.

Les employés utilisent régulièrement des ordinateurs non sécurisés dans les hôtels et les aéroports, y compris des ordinateurs personnels. Il n'existe aucune garantie que ces systèmes soient équipés des tous derniers logiciels antivirus disposant de signatures de virus à jour, ou qu'ils ne contiennent pas de logiciels malveillants. Cela entraîne des risques significatifs pour la sécurité de l'entreprise. GO crée un environnement de travail sécurisé virtuel permettant une connexion sécurisée et distincte au réseau de l'entreprise. Aucun des processus du système de l'hôte ne peut y accéder, et aucune trace n'est laissée dans le système de l'hôte une fois la session terminée.

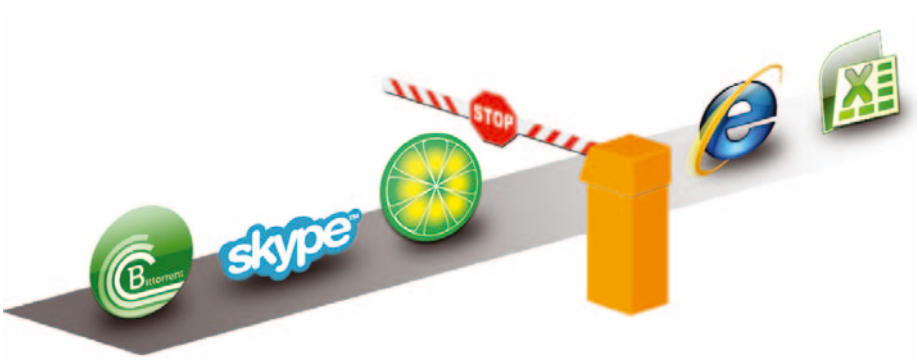

Figure 3. GO détermine les applications autorisées à fonctionner et celles qui ne le sont pas

Figure 4. Sécurité par ségrégation

*** Ces options peuvent être configurées par les administrateurs**

Fonctionnalités :

- Fonctionnement plug-and-play
- Espace de travail sécurisé virtuel
- Environnement utilisateur Windows standard
- Connectivité VPN intégrée
- Chiffrement logiciel et matériel actif en permanence
- Contrôle des transferts de fichiers
- Contrôle des applications
- Authentification des utilisateurs
- Administration centralisée

Sécurité par contrôle d'accès :

- Restriction d'accès granulaire à l'hôte
- Blocages possible des impressions

L'entreprise peut utiliser des règles de sécurité pour renforcer la protection, déterminer quelles applications sont autorisées à s'exécuter au sein de GO, et la manière dont les fichiers sécurisés doivent être traités. Les administrateurs peuvent également configurer des paramètres supplémentaires pour empêcher les utilisateurs d'imprimer ou d'accéder à l'hôte.

LA technologie GO

Un programme spécial est lancé dès que GO est connecté à un PC ou un ordinateur portable. Ce programme obtient l'accès au micro-logiciel du disque flash dans lequel les données confidentielles sont stockées. Un écran d'identification est présenté à l'utilisateur afin qu'il saisisse ses identifiants.

Une nouvelle instance d'explorer.exe est lancée dans l'environnement de travail sécurisé virtuel de GO une fois l'identifi cation validée. Tous les processus suivants sont lancés en temps que processus enfant de ce nouvel explorer, permettant ainsi à GO de contrôler les applications dans l'environnement sécurisé.

La bibliothèque NTDLL fait office de barrière entre l'environnement utilisateur et le noyau du système.

GO effectue un t ype spécifique d'accroche sur cette barrière pour intercepter l'exécution du code de l'application avant qu'elle n'atteigne NTDLL. L'entreprise peut appliquer des règles de sécurité spécifiques telles que l'interdiction de copier des fichiers de GO vers l'hôte ou vice-versa.

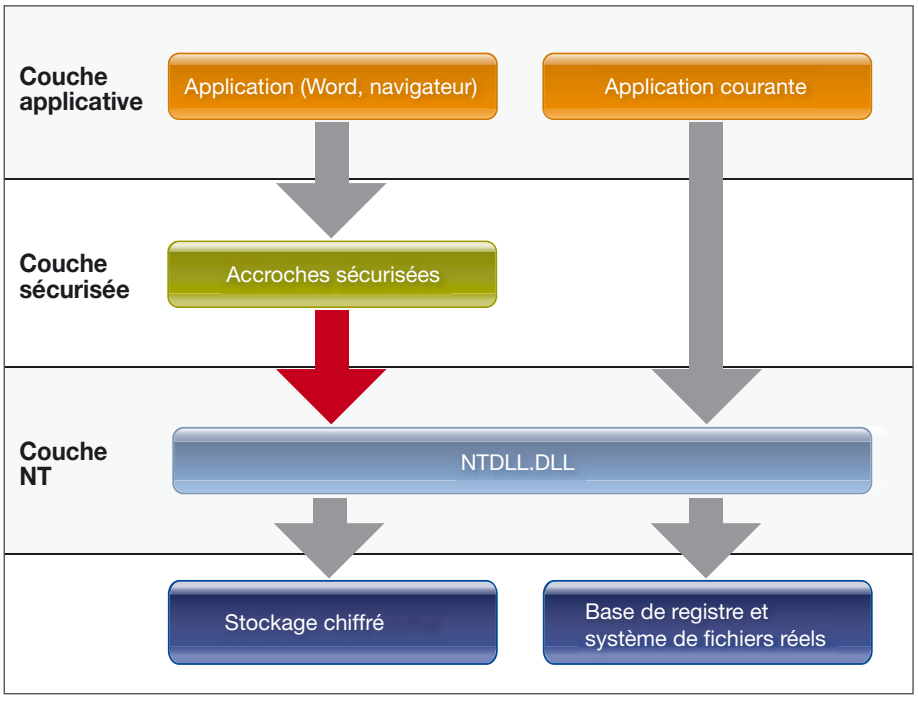

Figure 5. Architecture de Check Point GO

Espace de travail sécurisé virtuel :

- Utilisation du système d'exploitation de l'hôte – aucune licence séparée nécessaire
- Utilisation des applications permises sur le PC hôte
- Stockage chiffré

Architecture sécurisée :

La ségrégation de l'espace de travail utilisateur protège les données confidentielles

Toutes les opérations d'entrée/sortie sur les fichiers et la base de registre de l'application sécurisée fonctionnant dans GO sont redirigées sur le disque flash. En d'autres termes, les applications fonctionnant sur le bureau de GO (y compris le nouvel explorer) utilisent une base de registre et un système de fichiers virtuels. Les données de la base de registre et les fichiers virtuels sont instantanément écrits sur le disque flash et immédiatement chiffrés.

Lorsqu'une application demande la création d'un fichier dans GO, la fonction CreateFile de l'API Win32 est appelée. GO intercepte l'API et le fichier est créé dans le système de fichiers du disque flash. Des règles peuvent également interdire la création de fichiers dans GO, si nécessaire.

Cet accrochage spécial ne requiert pas l'installation d'un pilote spécifique, ce qui réduit considérablement le potentiel de conflits entre GO et les applications sur des ordinateurs non administrés. Dans cette architecture, l'espace mémoire des applications dans GO et celui des applications dans l'hôte ne sont pas séparés pour éviter les conflits de mémoire. D'autres bibliothèques Windows en plus de NTDLL sont exploitées de la même manière pour renforcer la sécurité.

GO intègre également un clavier virtuel pour protéger les applications de l'environnement sécurisé contre les logiciels malveillants de l'hôte qui enregistrent secrètement les frappes au clavier. De tels logiciels malveillants pourraient capturer les identifiants des utilisateurs et ainsi obtenir un accès non autorisé au réseau de l'entreprise.

Applications de la technologie GO(exemples d'utilisation)

Avec GO, les entreprises peuvent fournir à leurs employés, leurs sous-traitants et leurs partenaires, un espace de travail virtuel sécurisé, contrôlé, chiffré, cohérent et indépendant de l'ordinateur hôte. Les administrateurs ont la possibilité de contrôler l'accès aux fichiers stockés sur la partition chiffrée et protégée par mot de passe pour se conformer à la réglementation sur la protection de la vie privée.

Au travail

GO est portable et les utilisateurs peuvent l'emporter où qu'ils aillent. La totalité de l'environnement de travail, y compris les paramètres de sécurité, les signets, les documents, les raccourcis et la connectivité VPN, reste cohérente sur chaque PC.

Figure 6. Facilité d'accès pour les sous-traitants et les invités.

Mécanismes de protection :

- Clavier virtuel pour combattre les enregistreurs de frappe
- Contrôle des applications

Fait :

Une solution unique, plusieurs utilisations possibles

GO peut faciliter l'accès aux partenaires et aux invités, ou accorder un accès temporaire aux sous-traitants qui utilisent leurs propres ordinateurs. Dans tous les cas, les sous-traitants et les invités n'ont rien à installer sur leur ordinateur. Aucune ressource supplémentaire n'est requise, ce qui réduit considérablement les coûts de support.

À la maison

Le nombre croissant d'e-mails avec pour objet « En télétravail aujourd'hui » rend les administrateurs système nerveux. Il existe une corrélation négative entre le nombre d'employés travaillant à l'extérieur du pare-feu et le contrôle que l'entreprise a sur ses données. L'augmentation du nombre d'employés travaillant à domicile entraîne une augmentation égale du nombre potentiel de failles de sécurité.

Figure 7. GO facilite le travail à domicile en cas de catastrophe naturelle.

De simples chutes de neige peuvent conduire les travailleurs à rester chez eux pendant plusieurs jours. Une pandémie mondiale telle que la récente épidémie de grippe H1N1 peut forcer de nombreux employés à rester chez eux pendant plusieurs semaines. En conséquence, des outils de connexion à distance pratiques et sécurisés sont nécessaires pour maintenir la productivité sans sacrifier la sécurité.

Figure 8. GO fournit un espace de travail mobile.

En déplacement

Les employés tels que les commerciaux qui travaillent en déplacement ou à partir de leur domicile peuvent utiliser GO sur n'importe quel PC plutôt que de transporter un ordinateur portable. Ils peuvent également utiliser GO sur leur propre ordinateur portable pour combiner cohérence et sécurité.

Exemples d'utilisation :

- Travailleurs mobiles
- Accès partenaires, sous-traitants ou invités
- Plan de reprise d'activité

Solution idéale :

GO met votre bureau dans votre poche.

Résumé

GO fournit un accès sécurisé à l'espace de travail de l'entreprise tout en empêchant les pertes de données et les activités malveillantes à partir de systèmes distants, pour un coût nettement moindre que celui des solutions traditionnelles de sécurisation de poste.

A propos de Check Point Software Technologies Ltd.

Leader mondial de la sécurité sur Internet, Check Point Software Technologies Ltd. (www.checkpoint.com) est le seul acteur du marché à proposer des solutions de sécurité totale pour les réseaux, les données et les postes utilisateurs, via une plate-forme de gestion unifiée. Check Point assure aux clients un niveau optimal de protection contre tous types de menaces, simplifie l'installation et la maintenance des dispositifs de sécurité, et réduit leur coût total de possession. Précurseur de la technologie Firewall-1 et du standard de la sécurité des réseaux Stateful Inspection, Check Point est toujours à la pointe de la technologie. Grâce à sa nouvelle architecture dynamique Software Blade, Check Point offre des solutions à la fois fiables, flexibles et simples d'utilisation, qui peuvent être totalement personnalisées pour répondre aux besoins spécifiques de chaque entreprise ou de chaque environnement informatique. Check Point compte parmi ses clients les 100 sociétés figurant au classement des Fortune 100 ainsi que plusieurs dizaines de milliers d'entreprises et d'organisations de toute taille. Maintes fois primées, les solutions ZoneAlarm de Check Point protègent les PC de millions de particuliers contre les pirates, les logiciels espions et les vols d'identité.

Bureaux Check Point

Siège mondial
5 Ha'Solelim Street
Tel Aviv 67897, Israël
Tél. : +972 3 753 4555
Fax : +972 3 624 1100
email : info@checkpoint.com

Siège américain
800 Bridge Parkway
Redwood City, CA 94065
Tél. : +1 800 429 4391 ; +1 650 628 2000
Fax : +1 650 654 4233
URL : **http://www.checkpoint.com**

26 février 2010