7 POINTS CLÉS
À PRENDRE EN COMPTE POUR LA SÉCURITÉ DE SES ENDPOINTS

Beaucoup de choses brouillent la frontière entre la gestion des terminaux et la sécurité. Par exemple ? Gérer un endpoint. Le configurer. Effectuer la gestion des applications et des logiciels. Et le patcher. Le fait est que la gestion et la sécurisation d'un appareil sont si interdépendantes qu'il est logique que ces deux fonctions soient réunies dans une plate-forme unique capable d'accomplir ces tâches, ainsi que d'autres tâches nécessaires dans votre organisation informatique.

1 | Découverte et visibilité

La première étape est de savoir ce qui se trouve sur votre réseau. Ne pas savoir quel logiciel est installé sur les appareils signifie que vous ne savez pas s'il a reçu les correctifs nécessaires, si l'appareil doit être renforcé, etc. Obtenir une vision complète de tous les appareils connectés sur l'ensemble du réseau, s'ils sont connectés au réseau de l'entreprise en permanence ou si un appareil se met en marche temporairement, peut-être pendant quelques minutes environ, puis disparaît, vous devez être en mesure de le voir.

2 | Gestion de la conformité

Il n'y a pas si longtemps, la gestion de la conformité garantissait que les appareils étaient protégés par un mot de passe. Aujourd'hui, nous avons affaire à des cryptages des appareils, d'authentification multi facteur, de suivi des appareils, de gestion à distance, la liste est longue. Ajoutez maintenant la nécessité de superposer les politiques du gouvernement ou des commissions de réglementation dans lesquelles une violation ou un non-respect de la conformité pourrait entraîner des amendes ou des frais et menacer l'entreprise.

3 | Gestion des correctifs

Les correctifs sont devenus beaucoup plus étendus et constituent l'une des mesures les plus efficaces à mettre en place pour prévenir la vulnérabilité des appareils et empêcher la violation de votre environnement. Il est nécessaire d'avoir une visibilité sur les endpoints qui en ont besoin et sur ceux qui ont été patchés, non seulement les périphériques connectés au réseau de l'entreprise mais aussi ceux qui sont hors du réseau de l'entreprise. Si vous examinez les principales vulnérabilités répertoriées régulièrement, bon nombre d'entre elles se trouvent également dans des applications. Il faut être capable d'analyser une large liste d'applications, ainsi que des systèmes d'exploitation, voir ce qui doit être corrigé ou mis à jour, et peut être configuré pour appliquer automatiquement les mises à jour dès qu'elles sont disponibles.

4 | Contrôle des applications

Avec le contrôle des applications, l'équilibre que vous essayez de trouver se situe entre la réduction des risques et l'augmentation de la productivité, en protégeant les systèmes et les utilisateurs tout en leur permettant de faire leur travail le plus efficacement possible. Et c'est là qu'intervient le contrôle des applications.
Nous sommes tous confrontés aux possibilités d'applications menaçantes inconnues s'exécutant sur nos réseaux d'entreprise. Le contrôle des applications permet non seulement d'identifier les applications exécutées sur les appareils, mais également de restreindre l'accès. Ce contrôle peut également empêcher l'exécution des applications indésirables. Optez pour une solution complète pour la gestion des applications, de son installation au contrôle de son utilisation en passant par son blocage et sa suppression.

5 | Gestion des privilèges

L'une des batailles auxquelles doit faire face l'informatique est de savoir si un utilisateur doit avoir ou non des droits administrateurs sur son ordinateur. La gestion des privilèges peut aider à résoudre ce dilemme. Attribuer les droits d'utilisateur de base du compte utilisateur, élever certains privilèges de système d'exploitation ou d'application selon les besoins, puis réduire ou réinitialiser ces privilèges une fois que les besoins de l'utilisateur sont satisfaits. Ces capacités et droits spécifiques permettent à l'utilisateur d'effectuer des actions qu'il souhaiterait faire mais qu'il ne peut pas exécuter avec ses droits utilisateurs de base. Parfois, cependant, un utilisateur doit être configuré en tant qu'administrateur, ce que requièrent certaines capacités nécessaires du système d'exploitation. La gestion des privilèges permet de restreindre des droits d'administrateur spécifiques, en réduisant les élévations ou en ajustant les privilèges.

6 | Accès distant sécurisé

Aujourd'hui, le nombre de Endpoints que les services informatiques doivent gérer est de plus en plus important. De plus avec le télétravail, nous avons d'importants effectifs à distance qui ont plus que jamais besoin d'un accès à distance sécurisé. Il est essentiel d'établir des règles et des politiques pour la gestion de tous ces périphériques distants, puis d'être sûr que, quel que soit l'endroit où se trouve ce périphérique, il est correctement géré. Des outils peuvent gérer les appareils distants pour s'assurer qu'ils sont correctement configurés et toujours à jour. Ils peuvent également identifier les appareils compromis ou non conformes et les empêcher d'accéder à des données, des services spécifiques ou même au réseau de l'entreprise. Il est impératif de maintenir une connexion à l'appareil et le mettre à jour afin qu'il soit conforme et qu'il dispose d'un accès nécessaire.

7 | Réinitialisation complète du système

Lorsque nous parlons de réinitialisation complète du système, nous ne parlons pas seulement de réinitialiser le système d'exploitation ou de supprimer des données, mais également de le réimaginer dans un scénario de résolution de panne ou lorsqu'un appareil doit être réutilisé.
Avec une solution adéquate, vous pouvez réinitialiser l'appareil, le réimaginer à l'image de votre société et installer les applications précédentes de l'utilisateur. Vous pouvez également remettre les informations de profil et les données utilisateur sur l'appareil. Et en réinitialisant rapidement l'appareil, vous pouvez le remettre en état de marche rapidement - dans de nombreux cas plus tôt qu'il n'en faudrait pour exécuter plusieurs outils essayant de nettoyer l'appareil et en espérant que le risque soit entièrement corrigé.

Afin de répondre à tous ces points essentiels et faire gagner du temps à votre département Informatique, optez pour une seule interface qui gère tous vos périphériques et profils utilisateurs. Consolidez la gestion et renforcez la sécurité du poste client et du poste de travail, répondez aux attentes croissantes des utilisateurs et simplifiez vos processus de gestion, à l'aide d'une seule suite de gestion unifiée du poste client.

N'hésitez plus ! Contactez Cegedim Outsourcing pour mettre en place une expérience utilisateur optimale tout en boostant la productivité et en renforçant la sécurité.

www.cegedim-outsourcing.fr | cegedim Outsourcing