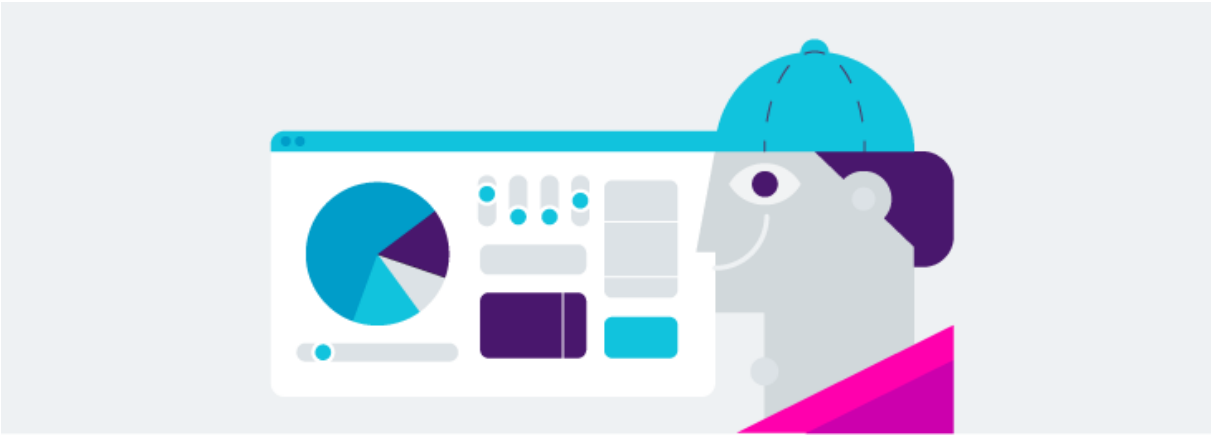

5 raisons de choisir Endpoint Protector

Inspiré de l'article de Andrada Coos 23 novembre 2018 Protection des clients lourds et légers, prévention contre les pertes de données

Bien que les solutions de prévention des pertes de données (DLP) soient devenues un élément de plus en plus courant dans les stratégies de conformité aux RGPD, HIPAA, GLBA, etc. Elles suscitent encore des craintes, en raison des longues et lourdes périodes de mise en œuvre souvent associées, leur impact potentiel sur la productivité des employés. Parce que les stratégies doivent être déployées à l'échelle du système, la complexité des outils DLP, combiné à une mise en œuvre complexe des politiques peuvent entraver plutôt que maintenir l'efficience de production.
Cela est certainement vrai pour certaines solutions DLP, nous ne sommes pas tous égaux... Chez Endpoint Protector, notre interface intuitive caractérise l'approche universelle de la prévention des pertes de données. Nous avons créé des outils puissants qui sont non seulement très efficaces pour protéger les données contre la perte et le vol, mais qui sont également faciles à mettre en œuvre et à utiliser. Voici les cinq principales raisons pour lesquelles Endpoint Protector est la solution DLP la plus efficiente et conviviale du marché :

Une véritable solution multiplateforme

Aujourd'hui, les réseaux d'entreprises fonctionnent avec des ordinateurs Windows, Mac OS, Linux. Les entreprises ont souvent du mal à trouver une solution DLP capable de gérer ces 3 OS concomitamment. Attirées par les promesses de solutions DLP multiplateformes qui s'avèrent inefficaces ou pire, contraintes de recourir à plusieurs solutions, chacune répondant aux besoins d'un seul OS.
Endpoint Protector est né d'une vision « solution multiplateforme ». Endpoint Protector est la solution DLP pour macOS la plus fiable au monde, EndPoint Protector est membre de la Linux Foundation. Nous sommes le seul éditeur au monde à proposer et à fournir une parité de fonctionnalités entre Windows, macOS et Linux. Endpoint Protector peut facilement être déployé sur tous les systèmes d'exploitation et géré par les administrateurs à partir d'un seul tableau de bord, éliminant le besoin de plusieurs panneaux de contrôle.

Déploiement facile et rapide

Chez Endpoint Protector, nous sommes fiers du fait que notre produit peut être opérationnel en 30 minutes. Ceci est dû à la grande flexibilité de nos méthodes de déploiement qui répondent aux besoins de toutes les infrastructures organisationnelles. Endpoint Protector peut être une Appliance virtuelle compatible avec les outils de virtualisation les plus répandus, ou une Appliance matérielle facile à utiliser, préinstallée avec une variété de modèles basés sur les besoins des clients, ou une solution de cloud pour Amazon Web Services, Microsoft Azure et Google Cloud.
Ces méthodes d'implémentation optimisées réduisent considérablement le temps nécessaire aux clients pour configurer Endpoint Protector sur leur réseau. Cela détruit complètement tous les mythes selon lesquels les solutions DLP sont difficiles à mettre en œuvre.

Politiques et paramètres granulaires

Lorsqu'il s'agit de maintenir l'efficience des employés tout en utilisant les solutions DLP, la flexibilité est essentielle. Les politiques granulaires de Endpoint Protector permettent aux administrateurs d'appliquer des politiques non seulement globalement, mais aussi en fonction des périphériques, des ordinateurs, des utilisateurs et des groupes. De cette façon, les besoins particuliers de chaque département peuvent être satisfaits sans avoir à appliquer les mêmes politiques à l'échelle de l'entreprise. De même, la rigueur d'une politique peut être ajustée en fonction de l'accès de chaque utilisateur aux données sensibles.
Endpoint Protector est livré avec une large base de données de politiques prédéfinies pour les types de données sensibles les plus courantes, tels que les informations personnelles identifiables, mais aussi des politiques destinées à soutenir les entreprises dans leurs efforts pour se conformer aux lois de protection des données telles que GDPR, HIPAA et GLBA.

Une approche modulaire du DLP

Endpoint Protector ne cesse d'évoluer, nous nous sommes appuyés sur nos 15 années d'expérience dans le domaine de la DLP, en travaillant avec des entreprises de toutes tailles, nous avons développé un format modulaire qui permet aux entreprises de combiner et d'assortir les bons outils afin de répondre à leurs besoins spécifiques.
L'entreprise adapte, simplifie, les ressources en fonction de ses besoins précis, l'élimination des modules inutiles permet de se concentrer sur les seuls domaines d'intérêt de l'entreprise. En même temps, les entreprises en quête d'une solution DLP complète, peuvent simplement choisir l'ensemble des modules. L'implémentation de deux modules ou de tous les modules n'affecte en rien la facilité de déploiement ou le temps nécessaire à la configuration d'Endpoint Protector.

Une interface intuitive et conviviale

Endpoint Protector possède une interface moderne et conviviale qui offre une courbe d'apprentissage courte et permet au personnel non spécialisé de comprendre et d'utiliser facilement notre solution, ce qui permet une transition plus rapide vers un environnement de travail plus sûr.
En conclusion, les mythes entourant les difficultés de mise en œuvre de la DLP ne s'appliquent pas à toutes les solutions. Endpoint Protector a été créé non seulement pour protéger les données contre la perte et le vol, mais aussi pour prendre en considération les personnes qui utilisent les données :
Dès le début, nous avons organisé notre protection pour avoir un impact minimal sur l'efficacité des réseaux des entreprises ainsi que sur le travail quotidien des utilisateurs.