Schneider Electric sécurise 50 000 terminaux mobiles avec Lookout

Le défi

Schneider Electric est à la pointe de la transformation digitale en matière de gestion énergétique et d'automatisation dans les maisons, les bâtiments, les centres de données et les infrastructures de tous les secteurs. L'entreprise adopte une approche moderne et axée sur la technologie dans le cadre de sa mission visant à développer les meilleurs systèmes de gestion énergétique et d'automatisation pour ses clients. Elle est consciente que pour continuer à proposer des solutions énergétiques sécurisées, fiables, efficaces et durables au fil de son évolution, elle doit déployer un solide effectif mobile dans le monde entier, qui pourra s'appuyer sur des appareils et des applications mobiles afin de mener à bien ses projets et de renforcer sa productivité sur le terrain.

Alors que Schneider a pris de l'ampleur pour atteindre plus de 170 000 employés répartis sur plus de 100 pays, la sécurité est devenue sa priorité. Pour gérer les appareils mobiles, Schneider utilise un système EMM afin de contrôler l'accès aux ressources d'entreprise telles que les e-mails et les applications internes, un système SIEM pour regrouper des données relatives à la sécurité, une authentification unique pour un accès simplifié, ainsi que d'autres mesures de sécurité traditionnelles qui visent à protéger les ressources d'entreprise. Avec tout cela, il ne restait plus qu'un élément à couvrir : la sécurisation des terminaux mobiles.

Ce projet a été mené par Simon Hardy, responsable mondial des services Office 365 et de la mobilité d'entreprise chez Schneider. Simon savait qu'une solution de Mobile Threat Defense (MTD) était essentielle à la mise en place d'une flotte mobile sécurisée, mais il lui fallait trouver une solution pouvant être mise en œuvre facilement dans l'infrastructure existante, sur un parc important d'appareils mobiles. Il était essentiel que cette solution MTD soit capable de s'intégrer facilement avec les solutions EMM et SIEM de Schneider afin de générer une valeur immédiate en identifiant les menaces et en permettant à Schneider de s'aligner avec les exigences de conformité rigoureuses liées aux utilisateurs et au reporting interne

Schneider Electric

Profil du client

En tant que leader de la gestion énergétique et de l'automatisation avec une présence dans plus de 100 pays, Schneider Electric a pour ambition d'aider ses clients à atteindre plus d'objectifs avec moins de ressources, dans ce monde davantage connecté, réparti et intelligent, où le besoin en énergie ne cesse de croître. Schneider Electric s'efforce d'aider ses clients à exploiter les ressources, les actifs, les processus et les infrastructures le plus efficacement et durablement possible au moyen de solutions et de services technologiques innovants.

Secteur d'activité : Services d'utilité publique/ Services gérés

La solution

Lookout Mobile Endpoint Security

Les résultats

- Sécurisation de 50 000 terminaux Android et iOS à travers le monde
- Intégration fluide avec des plates-formes SIEM, SSO et EMM existantes
- Déploiement à travers l'ensemble du parc global via Microsoft Intune
- Conception d'un plan pour une politique de mobilité BYOD en utilisant Lookout comme solution MTD par défaut pour ces appareils

Défis de la sécurité

- Mettre en œuvre un outil de cybersécurité capable de protéger les utilisateurs mobiles d'Office 365 qui accèdent aux données d'entreprise.
- Démontrer aux auditeurs la capacité de l'outil à maîtriser les menaces de cybersécurité à l'encontre des terminaux mobiles, ainsi que la visibilité détaillée de l'utilisation des terminaux par les employés.
- Sécuriser une flotte mobile en rapide évolution à l'échelle internationale tout en adoptant deux politiques de mobilité différentes.

La stratégie de sécurité de Schneider est fondée sur l'accès aux applications et aux appareils actuels eux-mêmes plutôt que sur leur sécurisation. La société a également mis en place des mesures visant à garantir la sécurisation des connexions qui permettent d'accéder aux ressources d'entreprise. Simon a toutefois reconnu qu'un renforcement de la sécurité de l'ensemble des endpoints était nécessaire et la société a placé les terminaux mobiles en haut de la liste des éléments à améliorer, en plus des mesures déjà utilisées.

Critères de la solution

- S'intégrer aux solutions actuelles d'EMM, d'authentification unique et de SIEM, ainsi qu'aux autres outils de sécurité existants
- Protéger la propriété intellectuelle et veiller au respect des diverses normes et réglementations de conformité
- Être facile à mettre en œuvre, à maintenir et à gérer tout en éduquant le personnel sur les menaces mobiles
- Assurer une détection efficace des menaces en se fondant sur un vaste ensemble de données avec un minimum de faux positifs

La solution

En choisissant Lookout Mobile Endpoint Security, Schneider a bénéficié d'une visibilité immédiate sur les attaques mobiles et sur la posture à adopter en matière de protection des mobiles. Sachant qu'un déploiement considérable attendait son équipe, Simon a décidé de procéder à un déploiement étape par étape en commençant par sécuriser un petit nombre d'utilisateurs clés afin de vérifier que la solution répondait bien aux exigences et aux attentes de l'entreprise. Après avoir utilisé Lookout pendant six mois et constaté que la solution dépassait ses attentes, Schneider a multiplié par 20 le nombre de déploiements, puis au bout d'un an, a étendu la couverture à l'ensemble du parc de 50 000 appareils.

« Très connue dans le domaine de la sécurité mobile, l'entreprise Lookout a déjà analysé plus de 170 millions d'appareils. Dans le cadre de notre évaluation globale, nous avons également trouvé qu'il s'agissait de la solution la plus mature. Ainsi, nous nous sommes sentis confiants vis-à-vis de notre décision d'opter pour le leader du marché. »

En plus de renforcer les outils de sécurité actuels, Lookout a également comblé un vide au niveau de la posture de sécurité de Schneider. Associer Lookout à un EMM signifie que les terminaux sont soumis à une vérification continue de leur état de santé lorsqu'ils accèdent à des ressources d'entreprise. Cela permet de garantir que seuls des appareils sains accèdent aux données professionnelles, sans mettre en danger l'ensemble de l'entreprise. En intégrant Lookout aux terminaux des employés dotés d'une solution EMM et en tirant parti de l'activation en un clic, Schneider a pu étendre la couverture à un vaste effectif mobile en toute simplicité.

Les résultats

Avec 50 000 appareils Android et iOS désormais sécurisés par Lookout, Schneider s'aligne parfaitement avec les exigences de sécurité internes et externes, tout en bénéficiant d'une visibilité inégalée sur le risque mobile. Le processus de déploiement, simplifié pour les administrateurs de la solution comme pour les utilisateurs finaux, a permis d'assurer une couverture totale à chaque étape du processus de déploiement, en toute simplicité.

En tant qu'organisation internationale, Schneider se doit de protéger constamment ses employés contre les attaques sur le terrain. C'est d'ailleurs ce qu'elle a pu faire au moyen d'une détection pointue et précise des attaques de type man-in-the-middle, avec un taux de faux positifs extrêmement faible. Elle doit également respecter les lois de sécurité et de confidentialité de plus de 100 pays, ce qu'elle peut faire pour les appareils mobiles en créant des politiques personnalisées depuis la plate-forme Lookout.

Maintenant que l'entreprise Schneider a terminé le déploiement de Lookout pour 50 000 appareils COPE, elle a hâte de commencer un programme BYOD pour les employés et d'utiliser Lookout pour sécuriser 25 000 appareils supplémentaires. Après avoir prouvé la simplicité du processus de déploiement et la valeur immédiate de la solution et de la détection faite par l'IA des applications malveillantes et des terminaux compromis, Schneider a confiance en son objectif de faire de Lookout une partie intégrante du développement de son programme de mobilité à travers le monde.

Lookout a permis à Schneider de bâtir une stratégie complète de sécurité mobile en adoptant un programme de mobilité plus complexe, fondé sur un déploiement simple et une visibilité immédiate des risques, ainsi que sur le respect des politiques de sécurité internes et externes du monde entier.