La banque d'investissement Greenhill & Co sécurise la pratique BYOD en protégeant les données hautement sensibles de ses clients accessibles sur les appareils de ses employés dans le monde entier

Le défi

Dan Dougherty, Responsable informatique de Greenhill & Co, est l'un des premiers à comprendre l'importance de la sécurité mobile. Il dirige alors, pendant le premier semestre 2016, le déploiement pilote de Mobile Threat Defense, un produit pas encore arrivé à maturité. Cependant, le déploiement ne s'est jamais terminé en raison du nombre élevé de faux positifs pour les attaques réseau et de la logique de « blackholing », qui consiste à faire disparaître le trafic entre les appareils des utilisateurs finaux et les serveurs du fournisseur, ce qui présentait un risque à la fois pour la confidentialité des utilisateurs finaux et les données hautement sensibles des clients.

Dan et son équipe internationale avaient besoin d'une solution pour relever les défis de Greenhill, à savoir sécuriser les données des clients et de l'entreprise accessibles aux employés depuis leurs appareils personnels, obtenir une visibilité sur les logiciels malveillants susceptibles de compromettre des données, comme les enregistreurs de frappe, et respecter les réglementations Sarbanes-Oxley en matière de protection des données sensibles.

Greenhill

Profil du client

Banque d'investissement indépendante implantée à New York, Greenhill est considérée comme l'une des sociétés les plus prestigieuses de Wall Street. L'entreprise compte 14 bureaux dans le monde et conseille des entreprises, des associations, des institutions et des gouvernements de premier plan dans le cadre de fusions-acquisitions, de restructurations, de financements et de levées de fonds.

Secteur d'activité : finance

Politique de mobilité : BYOD

Solution EMM : Citrix XenMobile

Défis de la sécurité

- Protéger les données financières des clients, notamment les informations importantes lors de fusions-acquisitions majeures
- Obtenir une visibilité détaillée sur les attaques de réseau et les logiciels malveillants entraînant des fuites de données, comme les enregistreurs de frappe
- Respecter les réglementations Sarbanes-Oxley en matière de protection des données sensibles

La solution

Greenhill a choisi Lookout Mobile Endpoint Security début 2017 pour remplacer son projet pilote et sécuriser les appareils mobiles de son programme BYOD après avoir constaté que la console d'administration de Lookout fournissait des alertes exploitables lors de la détection de risques mobiles et permettait d'identifier les événements à traiter en priorité.

L'équipe de Greenhill a parfaitement conscience que les logiciels malveillants mobiles sont de plus en plus répandus et sophistiqués. Elle est particulièrement préoccupée par les enregistreurs de frappe, étant donné la quantité d'informations client échangées par e-mail et souvent consultées sur des appareils mobiles personnels par les 82 Directeurs de l'entreprise. Voici l'avis de Dan : « Sans Lookout, un logiciel malveillant ou une application entraînant des fuites de données pourrait s'installer sur l'appareil d'un employé sans que nous nous doutions de rien. Un enregistreur de frappe pourrait notamment voler des informations à partir des notes ou des contacts qui se synchronisent sur le téléphone. »

> « Notre entreprise internationale conseille des clients dans le cadre de fusions et acquisitions qui représentent plusieurs milliards de dollars. Nous savons que nous sommes une cible potentielle et qu'une compromission des données serait lourde de conséquences. Nous faisons confiance à Lookout pour sécuriser les données sensibles auxquelles nos employés accèdent sur leurs appareils mobiles et envoyer des alertes exploitables à nos administrateurs. »
>
> **Dan Dougherty,** Responsable informatique, Greenhill & Co.

En outre, la méthode de correction des menaces pesant sur le réseau de Lookout a semblé plus efficace à Dan, car Lookout détecte les menaces réseau dès leur connexion et prévient les utilisateurs finaux afin qu'ils ne transmettent pas de données sensibles.

L'équipe de Greenhill cherche maintenant à tirer parti de l'intégration exclusive de Lookout et Microsoft Enterprise Mobility + Security pour activer des politiques d'accès conditionnel via Microsoft Intune et Office 365 qui permettraient de limiter l'accès aux données de l'entreprise pendant que Lookout vérifie l'absence de menaces mobiles sur un appareil.

Les résultats

Greenhill a terminé le déploiement de l'application Lookout sur les appareils mobiles de ses employés via son MDM Citrix XenMobile. Les employés de l'entreprise ont suivi une formation à la cybersécurité et sont davantage sensibilisés aux problèmes de sécurité. L'équipe de Greenhill s'attend donc à une réduction des risques initiés par les utilisateurs, comme les applications sideloadées ou les appareils jailbreakés, et à une augmentation des menaces ciblées, comme les logiciels malveillants.

Même si la sensibilisation des utilisateurs finaux à la sécurité est un avantage, Dan ne pense pas qu'il s'agisse d'un remède à tous les problèmes. En effet, les employés de Greenhill voyagent souvent pour le travail dans des pays où les risques peuvent être plus répandus et plus sophistiqués. Il aborde ces menaces potentielles avec pragmatisme : « Notre entreprise internationale conseille des clients dans le cadre de fusions-acquisitions qui représentent plusieurs milliards de dollars. Nous savons que nous sommes une cible potentielle et qu'une compromission des données serait lourde de conséquences. Nous faisons confiance à Lookout pour sécuriser les données sensibles auxquelles nos employés accèdent sur leurs appareils mobiles et envoyer des alertes exploitables à nos administrateurs. »