KKB

KKB (Bureau de crédit turc) classe ForeScout CounterACT® en première position en matière de sécurité des informations

SECTEUR

Finance

ENVIRONNEMENT

300 employés et 400 appareils dans un environnement très réglementé

DÉFI

- S'assurer que tous les ordinateurs et postes de travail connectés au réseau sont utilisés par des utilisateurs légitimes de l'entreprise
- Automatiser les contrôles de sécurité pour atténuer les risques et accélérer la réponse aux incidents de sécurité
- Éviter que la productivité de l'entreprise soit perturbée

SOLUTION

- Une solution sans agent, simple à utiliser, qui nécessite peu de tâches manuelles fastidieuses
- Installation rapide et non intrusive, intégration facile au réseau combiné de KKB qui comprend des points d'accès sans fil Aruba et des commutateurs Cisco®
- Intégration des plug-ins FireEye® et ArcSight™ à la plateforme ForeScout CounterACT, ce qui permet le partage des informations de sécurité et l'automatisation des actions de correction des points d'extrémité
- Solution de sécurité réseau très fiable ; l'image du trafic est dirigée vers CounterACT

RÉSULTATS

- Visibilité en temps réel et surveillance continue des points d'extrémité du réseau, ce qui réduit les risques de cyberattaques via des vulnérabilités connues
- Automatisation de la gestion du mot de passe d'administrateur local pour les appareils des travailleurs distants, ce qui permet d'économiser des semaines de main-d'œuvre par an
- Contrôle préventif des attaques de type « pass-the-hash »
- Meilleure conformité aux règlementations bancaires en matière de sécurité des informations

Présentation

Kredi Kayit Burosu (KKB), le premier et unique bureau de crédit de Turquie, a été créé par neuf grandes banques turques en 1995. L'activité de KKB consiste à réduire les risques financiers dans de nombreux secteurs, y compris dans le secteur bancaire, de la location automobile ou immobilière et des ménages. Un million de membres utilisent régulièrement son portail Internet. L'entreprise a traité 500 millions de requêtes en 2014.

Défi pour l'entreprise

La conformité et la cybersecurité des informations financières et personnelles sensibles sont fondamentales pour la réputation de KKB en tant que fournisseur de services fiable. Pour être en adéquation avec cette philosophie, KKB avait besoin d'une solution lui permettant de bénéficier d'une meilleure visibilité sur son réseau et d'un contrôle accru de ses 300 employés et 400 points d'extrémité.

Pourquoi ForeScout ?

Lorsqu'elle a commencé à rechercher une solution permettant d'améliorer la visibilité réseau et les contrôles de sécurité, la société KKB a contacté Symturk, son partenaire conseil en matière de sécurité des informations. Symturk a recommandé la solution ForeScout CounterACT® et a fourni une validation de principe sur site à Ali Kutluhan Aktaş, responsable de la sécurité du système d'information/gestion des risques chez KKB. Cisco ISE a aussi été envisagé.

Les critères d'évaluation étaient notamment les suivants : installation rapide, prise en charge d'une infrastructure informatique mixte (points d'accès sans fil Aruba et commutateurs Cisco), solution sans interruption destinée à garantir la continuité de l'activité, et d'avantage d'actions et de contrôles de conformité automatisés. KKB a pris sa décision après avoir comparé les fiches techniques et les références des deux produits.

« Nous avons choisi ForeScout et non la solution NAC Cisco en partie parce que nous disposons d'une infrastructure informatique mixte (et non juste Cisco), mais aussi parce que nous avions besoin d'une solution rapide et facile à installer », a commenté Aktaş. « ForeScout a donné de bons résultats dans ce domaine. En outre, CounterACT est une plateforme unique dotée de solides propriétés d'intégration. Le fait de pouvoir l'intégrer facilement à d'autres produits de sécurité, tels que FireEye, ArcSight et CyberArk®, a permis d'améliorer la visibilité et la protection de la cybersécurité au sein de KKB. En effet, nous sommes désormais en mesure d'accéder aux informations de sécurité combinées des produits et de les exploiter ».

Impact sur l'entreprise

Visibilité en temps réel sur les appareils et les vulnérabilités

Depuis le déploiement de ForeScout CounterACT, KKB bénéficie d'une bien meilleure visibilité sur les points d'extrémité de son réseau, et peut vérifier en permanence le niveau de sécurité de chaque appareil. « Auparavant, si une analyse des ports était en cours, et qu'il était possible qu'une activité malveillante se produise, nous pouvions l'identifier uniquement après qu'elle ait eu lieu », a indiqué Aktaş. « ForeScout permet de simultanément détecter, examiner et bloquer les menaces. En outre, CounterACT nous signale les failles de sécurité dès leur apparition, tout en nous permettant d'automatiser les actions de remédiation des points d'extrémité. Cela réduit le risque d'erreur humaine. »

« Nous avions besoin d'une solution NAC pouvant être déployée rapidement et sans risque d'interruption de l'activité. En outre, elle devait prendre en charge notre infrastructure informatique mixte Aruba et Cisco. ForeScout CounterACT nous a offert tout cela et bien plus encore, y compris des fonctionnalités impressionnantes d'intégration avec nos outils de sécurité existants FireEye et ArcSight. C'est pourquoi nous appelons CounterACT le « couteau suisse » de notre équipe de sécurité informatique, car il facilite et optimise les nombreux contrôles de sécurité et de conformité automatisés ».

- Ali Kutluhan Aktaş, Responsable de la sécurité du système d'information/ gestion des risques chez KKB

La différence ForeScout

Facteurs clés ayant contribué au succès global de KKB :

- Intégration du produit de sécurité via l'architecture ControlFabric
- Facilité de déploiement/ interopérabilité dans des environnements multifournisseurs
- Surveillance et atténuation continues des risques de sécurité et des cyberattaques
- Visibilité en temps réel sur tous les appareils du réseau
- Contrôles de sécurité et de conformité automatisés ; ce qui réduit les tâches manuelles fastidieuses

Pour en savoir plus, visitez le site **www.ForeScout.com**

Élaboration et mise en œuvre des politiques

Ali Kutluhan Aktaş nous décrit certaines des politiques de sécurité personnalisées créées par son entreprise à l'aide de CounterACT :

- « Nous avons intégré ForeScout-ArcSight-CyberArk de sorte que lorsqu'un ordinateur ou un ordinateur portable se connecte à notre réseau, ForeScout vérifie l'ancienneté de son administrateur local et, si celle-ci est supérieure à 45 jours, ForeScout envoie à ArcSight un message CEF indiquant le nom de l'appareil. ArcSight corrèle ce message avec notre règle personnalisée et exécute un script sur un agent installé sur le serveur CyberArk. Ce script permet à CyberArk de lancer le processus de modification de mot de passe, qui est changé avec succès. Cette mesure de sécurité est essentielle, en particulier pour les employés qui travaillent régulièrement hors site, loin des locaux de l'entreprise ».
- « À l'aide de ForeScout CounterACT, nous vérifions les hachages d'informations d'identification d'administrateur de domaine sur les ordinateurs clients et si nous détectons un hachage d'identifiant/ d'informations d'identification d'administrateur de domaine sur un poste de travail, nous isolons la machine du réseau. Cela garantit un contrôle préventif des attaques de type « pass-the-hash ». Nous vérifions également les privilèges d'administrateur local sur les postes de travail : Si le service d'assistance fournit un privilège d'administrateur local non approuvé à un membre du personnel, nous détectons et isolons ce point d'extrémité ».
- « Nous vérifions les services de prévention de perte de données via CounterACT et, s'ils ne sont pas exécutés, nous envoyons une commande pour qu'ils soient exécutés trois fois. S'ils ne s'exécutent toujours pas, ou sont totalement désinstallés, nous isolons l'appareil. Nous vérifions également des éléments, tels que le chiffrement de disque, les programmes P2P, les comportements suspects et la fréquence des analyses antivirus ».

Réduction des tâches manuelles fastidieuses

Un des critères de sélection de KKB concernait l'optimisation des contrôles de sécurité automatisés pour minimiser les tâches manuelles fastidieuses et les risques. « Avant ForeScout, nous devions modifier manuellement les mots de passe sur les ordinateurs et postes de travail, par exemple lorsqu'un employé quittait l'entreprise, ce qui prenait beaucoup de temps », a commenté Ali Kutluhan Aktaş « À l'aide de CounterACT, nous avons élaboré une politique personnalisée qui crée une liaison ForeScout-ArcSight-CyberArk, ce qui signifie que le processus est désormais automatisé. Cela nous permet de faire des économies, tout en garantissant une meilleure sécurité des informations. Selon mes estimations, nous économisons des semaines de travail par an grâce à notre proactivité et à l'automatisation de ce processus ».

Intégration du produit de sécurité

La technologie ControlFabric® de ForeScout permet à CounterACT et à d'autres systèmes informatiques d'échanger des informations et de corriger un large éventail de problèmes. KKB tire pleinement profit de ces opportunités en intégrant CounterACT avec ses solutions FireEye et ArcSight.

L'intégration de ForeScout à FireEye permet une surveillance en temps réel et l'atténuation des risques associés à des points d'extrémité non conformes ou compromis. Les menaces avancées persistantes, ordinateurs zombies et logiciels malveillants qui se propagent dans les environnements distribués et BYOD peuvent rapidement être identifiés, vérifiés et mis en quarantaine.

L'interopérabilité de ForeScout avec le système de gestion des événements et des informations de sécurité (SIEM) d'ArcSight fournit des informations détaillées sur le niveau de sécurité des points d'extrémité, permettant ainsi une meilleure prise de décisions en ce qui concerne les risques de sécurité liés aux points d'extrémité et aux violations de conformité.

ForeScout®

ForeScout Technologies, Inc.
900 E. Hamilton Avenue #300
Campbell, CA 95008 (États-Unis)

Numéro gratuit (depuis les États-Unis) 1-866-377-8771
Tél. (depuis les autres pays) +1-408-213-3191
Assistance technique 1-708-237-6591
Fax 1-408-371-2284

Copyright © 2016. Tous droits réservés. ForeScout Technologies, Inc. est une société privée basée dans l'État du Delaware. ForeScout, le logo ForeScout, ControlFabric, CounterACT Edge, ActiveResponse et CounterACT sont des marques commerciales ou des marques déposées de ForeScout. Les autres noms mentionnés sont des marques commerciales de leurs détenteurs respectifs. **Version 3_16**