Voici comment Varonis permet à HomeServe de sécuriser les données sensibles de millions de clients

« Varonis peut être considérée comme un moyen de gagner du temps, mais aussi de réduire les risques. Varonis permet de mettre en lumière des problèmes dont vous n'auriez même pas soupçonné l'existence auparavant. »

Matthew Mudry,
VICE-PRÉSIDENT ET RESPONSABLE MONDIAL DE LA CYBERSÉCURITÉ, HOMESERVE

ÉTUDE DE CAS

HomeServe

La mission de HomeServe est simple : libérer les gens des soucis et des désagréments liés aux réparations d'urgence à domicile. C'est leur activité principale depuis 2003.

EN BREF

LE PROBLÈME

- Faire face à une augmentation massive de l'utilisation du VPN pendant l'épidémie de COVID-19
- Garantir la sécurité des données sensibles des clients lorsque les employés travaillent à domicile
- Renforcer la surveillance du périmètre pour détecter les signes d'attaque sur le réseau, notamment le réseau VPN

LA SOLUTION

La plateforme de sécurité des données la plus complète :

- **DatAdvantage** pour vérifier chaque manipulation de fichier, sur site et dans Active Directory
- **Data Classification Engine** pour identifier les données sensibles
- **Data Classification Policy Pack** pour identifier et classifier les données sensibles relevant des réglementations sur la protection des données (RGPD/CCPA)
- **Data Transport Engine** pour automatiser la migration des données et appliquer les réglementations sur la confidentialité des données, notamment le RGPD ou le CCPA
- **DatAlert Suite** pour une détection rapide des menaces et une réponse adéquate face à celles-ci
- **Edge** pour surveiller et sécuriser la hausse très importante du nombre d'utilisateurs se connectant via le VPN

LES RÉSULTATS

- Protection des données de millions de clients
- Connaissances exploitables sur les domaines à risque pouvant être traités de manière proactive
- Visibilité sans précédent sur l'activité Active Directory et VPN

Le problème

Protection des données employés et clients en pleine épidémie

Comme de nombreuses entreprises, HomeServe a généralisé le télétravail par mesure de précaution face à l'épidémie de COVID-19. Avec plus de 2 000 employés en Amérique du Nord, cela a entraîné une hausse très importante de l'utilisation du VPN.

Selon Matthew Mudry, vice-président et responsable mondial de la cybersécurité, cela représentait un défi logistique : Comment protéger les données des employés et, par conséquent, des clients, alors que tant de personnes travaillent à distance ?

Il savait que cela serait impossible sans être en mesure de savoir qui se connectait au VPN et à partir de quel endroit en toute transparence. Une visibilité sur les données sensibles, où qu'elles se trouvent, était nécessaire.

> « En plus d'une visibilité sur les personnes qui se connectent à notre VPN et leur lieu de connexion, nous devons savoir où se trouvent nos données PCI et PII (ou sensibles) afin de les protéger, surtout lorsqu'elles apparaissent dans un emplacement inattendu », explique M. Mudry.

Heureusement, il avait une solution. Depuis 2019, Varonis fournit à HomeServe des alertes et une visibilité inégalées sur ses dépôts de données. Varonis permet à HomeServe de maintenir un modèle de moindre privilège et de rationaliser les besoins réglementaires de base, comme le maintien de la conformité PCI.

Aujourd'hui, Varonis va aider HomeServe à protéger son personnel à distance. Avec Edge, HomeServe bénéficie d'une visibilité en temps réel sur les principaux risques de travail à distance et même sur les signes d'actes malveillants les plus subtils.

> « Varonis nous permet d'avoir une activité VPN transparente. Grâce à eux, nous pouvons savoir qui se connecte ou tente de se connecter à notre réseau et à quel moment, et établir des relations entre ces informations et les événements qui se déroulent sur notre réseau », explique Matthew.

Déterminée à tout mettre en œuvre pour assurer la sécurité de ses réseaux et clients, l'entreprise HomeServe a également commencé à déployer **DatAdvantage for Directory Services**, afin d'obtenir une piste d'audit unique et unifiée dans Active Directory.

« En plus d'une visibilité sur les personnes qui se connectent à notre VPN et leur lieu de connexion, nous devons savoir où se trouvent nos données PCI et PII (ou sensibles) afin de les protéger, surtout si elles apparaissent dans un endroit inattendu. »

La solution

Varonis savait exactement comment résoudre le problème

Les premières solutions déployées par HomeServe avaient pour objectif d'améliorer le contrôle de ses environnements sur site.

DatAdvantage pour Windows lui permet de vérifier la moindre manipulation de fichier et de contrôler les droits d'accès. Cette solution permet également à HomeServe d'exécuter un calendrier de conservation en identifiant les données obsolètes qui ont dépassé depuis longtemps les exigences de conservation et qui peuvent être supprimées en toute sécurité.

> « Nous avons fait appel à Varonis afin d'être en mesure de savoir qui est la dernière personne à avoir manipulé des données. Ainsi, nous pouvons identifier les données qui peuvent réellement être supprimées sans que cela ne nuise à l'entreprise », ajoute Matthew.

Data Classification Engine examine le contenu des fichiers afin d'identifier les données sensibles présentant des risques. Avec **Data Classification Policy Pack**, Matthew est en mesure de découvrir et de sécuriser facilement les données CCPA ou RGPD à risque.

Si quelque chose ne va pas, **Data Transport Engine** archive, met en quarantaine ou supprime automatiquement les données en fonction de règles prédéfinies, sans compromettre les structures de droits d'accès existantes.

> « Varonis nous aide non seulement à identifier les données sensibles, mais va encore plus loin en nous indiquant où elles se trouvent et qui a accès à ces fichiers. À partir de là, nous pouvons facilement les isoler, les mettre en quarantaine ou simplement déclencher une alerte pour protéger les données », explique Matthew.

Lorsque Varonis détecte un problème potentiel, la suite DatAlert assure une détection avancée des menaces ainsi qu'une réponse avancée face à celles-ci afin que Matthew et son équipe puissent rapidement évaluer les problèmes éventuels et prendre des mesures correctives.

> « Nous avons récemment effectué un test de pénétration et l'alerte de Varonis s'est déclenchée en premier. Cette alerte en temps réel est essentielle », selon Matthew.

Ces solutions ont jeté les bases de la protection du personnel à distance récemment mobilisé par HomeServe. L'analyste de sécurité Jeremy Diaz a travaillé en étroite collaboration avec l'équipe de réponse aux incidents (IR) de Varonis pour mettre en place des alertes et les faire fonctionner avec **DatAdvantage for Directory Services** et **Edge**.

> « De mon point de vue, le fait d'être en mesure de recevoir des notifications d'alerte de sécurité concernant mes données en temps réel est une véritable bouée de sauvetage. Varonis est toujours là », précise Jeremy.

En rassemblant des connaissances sur Active Directory, l'activité du serveur de fichiers et la télémétrie du périmètre, Varonis peut détecter des menaces dans Active Directory avant qu'elles ne deviennent des fuites de données à part entière. C'est la clé de voûte, et le maintien de sa sécurité est primordial.

« Nous avons récemment effectué un test de pénétration et l'alerte de Varonis s'est déclenchée en premier. Ce système d'alerte en temps réel est essentiel. »

Les résultats

Protection des données de millions de clients

Varonis a permis à HomeServe de mobiliser son personnel à distance en toute confiance. La transparence d'Active Directory, la télémétrie avancée du périmètre et le système d'alerte mis en place sur le VPN de HomeServe permettent à Matthew d'avoir l'esprit tranquille, car le maximum est fait pour assurer la sécurité des données des employés et des clients.

Grâce à Varonis, il trouve toujours de petites choses à améliorer et des risques potentiels pour la sécurité à traiter. Mais il préfère disposer de toutes les connaissances nécessaires plutôt que d'être victime de malveillance.

Selon lui, « Varonis peut être considéré comme un moyen de gagner du temps, mais aussi de réduire les risques. Varonis permet de mettre en lumière des problèmes dont vous n'auriez même pas soupçonné l'existence auparavant. »

« Il est difficile d'assurer la protection des données à grande échelle, mais il est réconfortant de savoir où se situe un problème et que localiser celui-ci ne revient pas à rechercher une aiguille dans une botte de foin. Disposer de cette visibilité d'un simple clic est épatant », ajoute Jeremy.

DatAdvantage for Directory Services offre à Matthew et à son équipe une visibilité sur l'espace Active Directory. Cette visibilité leur permet de suivre l'activité VPN et de résoudre les problèmes avant qu'ils ne s'aggravent.

Selon Matthew : « Avant Varonis, nous utilisions un autre outil qui offrait une visibilité limitée sur notre environnement Active Directory. Nous disposons désormais d'informations intelligentes et exploitables qui nous permettent d'identifier et de répondre rapidement à des problèmes tels que des comptes de service mal utilisés, des comptes de domaine inactifs et des modifications apportées aux groupes sensibles et protégés d'Active Directory. »

Grâce à Varonis, Matthew peut exploiter une piste d'audit claire pour suivre et, si nécessaire, annuler les modifications apportées à Active Directory. Il peut voir qui se connecte au VPN et depuis quel endroit. Il s'est déjà servi de ces informations pour mieux protéger la sécurité des données de HomeServe contre les risques potentiels.

« Nous avons la possibilité de voir les milliers de personnes qui se connectent à notre VPN et d'identifier celles qui ne le font pas. C'est important car cela nous permet de comprendre pourquoi ces personnes ne sont pas connectées, de résoudre leur problème et de nous assurer qu'elles reçoivent les mises à jour et les correctifs nécessaires », explique-t-il.

« Il est réconfortant pour moi de savoir où se situe un problème et que localiser celui-ci ne revient pas à chercher une aiguille dans une botte de foin. Disposer de cette visibilité d'un simple clic est épatant. »

VARONIS

Votre façon de travailler évolue. La sécurité de vos données est-elle à la hauteur ?

Bénéficiez d'une protection des données, d'une détection des menaces et d'une conformité adaptées à votre façon de travailler.

DEMANDER UNE DÉMO