Comment Varonis protège un promoteur immobilier d'une cybermenace difficile à détecter

ÉTUDE DE CAS

« Varonis Edge a été la **seule solution** capable de détecter les menaces de tunneling DNS. **Aucun autre produit n'a su y parvenir.** »

Tony Hamil,
ingénieur en cybersécurité

À PROPOS DE CETTE ÉTUDE DE CAS :

Notre client est une société de promotion immobilière respectée. À sa demande, nous ne mentionnons pas son nom dans cette étude et omettons toute information sensible.

EN BREF

LES PROBLÈMES

- Contrôle de l'intégrité des fichiers durant leur migration vers un nouveau logiciel de partage de fichiers basé sur le cloud
- Protection des informations sensibles sur site et dans le cloud
- Détection des cyberattaques et des fuites de données potentiellement destructives au moyen du tunneling DNS et d'autres méthodes

LA SOLUTION

La plateforme de sécurité des données la plus solide :

- **DatAdvantage** intégré avec Windows et Exchange Online
- **Data Classification Engine** pour Windows et SharePoint
- **DataPrivilege** pour aider à assurer la conformité et faciliter la gouvernance de l'accès aux données
- **DatAlert** pour détecter les malwares ou les fuites de données internes potentiels
- **Edge** pour repérer les signes d'attaque subtils depuis le périmètre du réseau

LES RÉSULTATS

Plus de confiance et de tranquillité d'esprit grâce aux atouts suivants :

- Une solution pouvant détecter de manière fiable les attaques de tunneling DNS
- Une interface utilisateur simple et intuitive qui rationalise la détection et la prévention des menaces
- Une assistance client de premier ordre
- Des mises à jour et un lancement de modules complémentaires en continu pour garantir la protection des clients et de leurs données

Les problèmes

Protection des fichiers sur site et dans le cloud

Tony Hamil est l'ingénieur en cybersécurité principal d'un grand promoteur immobilier en Amérique du Nord. Il est notamment chargé de protéger l'entreprise contre les pirates informatiques, d'améliorer continuellement ses capacités de détection et de réponse face aux menaces, et de gérer les applications de sécurité comme Varonis.

Son entreprise a adopté Varonis en 2015. Elle venait juste d'implémenter Box, un logiciel de partage de fichiers basé sur le cloud, et avait besoin de verrouiller les autorisations et d'obtenir une meilleure visibilité sur son stockage de données sur site et dans le cloud.

> M. Hamil explique : « Au départ, nous avons choisi Varonis pour trois raisons : DatAdvantage, qui nous a permis de cartographier l'accès aux données, Data Classification Engine, qui nous a montré quelles données sensibles étaient vulnérables, et DataPrivilege, qui nous a aidé à gérer la propriété de nos données les plus importantes.
>
> En matière de contrôle d'intégrité des fichiers, il était évident que nous devions opter pour Varonis. Les autres fournisseurs étaient dépassés, présentaient des performances inférieures ou impactaient négativement nos activités. »

Les cybermenaces devenant plus sophistiquées, l'entreprise a continué d'ajouter des solutions Varonis, telles que DatAlert, pour s'adapter à cette croissance et renforcer ses défenses de cybersécurité.

« DatAlert m'envoie une notification lorsqu'un élément requiert mon attention. Les alertes peuvent indiquer la présence d'outils d'intrusion, de fichiers chiffrés par un virus cryptolocker, ou encore d'un utilisateur chargeant une quantité inhabituelle de données », explique-t-il.

« En matière de contrôle d'intégrité des fichiers, il était évident que nous devions opter pour Varonis. Les autres fournisseurs étaient dépassés, présentaient des performances inférieures ou impactaient négativement nos activités. »

Le problème

Se prémunir contre les cybermenaces qui échappent aux défenses traditionnelles

Qu'en est-il des menaces qui sont notoirement difficiles à détecter ? Le tunneling DNS est une méthode qu'utilisent les pirates pour éviter d'être repérés en déguisant l'exfiltration de données en trafic Web habituel.

Les menaces de ce type échappent souvent à la détection car elles sont difficiles à déceler ; mais les ignorer a déjà coûté plusieurs millions de dollars à des entreprises du monde entier.

À titre d'exemple, en 2016, une attaque DNS a compromis toute l'infrastructure DNS d'une grande banque brésilienne, notamment la messagerie d'entreprise et l'ensemble de ses 36 domaines.

Les pirates ont pu tout intercepter, des opérations de banque en ligne à la totalité des transactions mobiles, dans les points de vente, aux DAB et liées aux investissements. L'attaque a fait des milliers, voire des millions, de victimes parmi les clients de la banque.

Et cette banque n'était que l'une des dix institutions touchées par les mêmes cybercriminels au moyen du tunneling DNS.

Tony Hamil a réalisé à quel point le risque était important pour son entreprise.

> « Chaque entreprise qui possède un domaine a des serveurs DNS, et ces serveurs ont des DNS ouverts sur le monde. Normalement, vous ne pouvez pas utiliser le port 53 de votre système vers l'extérieur, mais si vous passez par les serveurs DNS, cela ressemble à une activité légitime », explique-t-il.

Il ne souhaitait confier à Varonis la protection des données vulnérables de son entreprise qu'à condition que la plateforme puisse contrer cette menace, et prouver sa capacité à l'aider à détecter les attaques les plus discrètes et à s'en prémunir.

La solution

La solution d'audit et de protection centrée sur les données la plus solide contre les menaces presque indétectables

Edge est l'un des derniers produits de Varonis. En analysant les métadonnées de télémétrie du périmètre (DNS, VPN et proxy Web) et les activités d'accès aux données, il vous aide à détecter et à bloquer même les plus furtifs des malwares, intrusions APT et tentatives d'exfiltration de données.

M. Hamil a passé au crible la version de démonstration d'Edge. Il a effectué un exercice de Red Teaming avec exfiltration DNS, en simulant une attaque de tunneling DNS et en y opposant toutes les solutions proposées.

> « J'ai utilisé un outil appelé DNScat2 pour simuler une attaque de tunneling DNS à la fois via nos serveurs DNS publics et nos serveurs DNS internes, pour montrer à quel point c'est dangereux.
>
> **Varonis Edge a été la seule solution capable de détecter les menaces de tunneling DNS. Aucun autre produit n'a su y parvenir.** Certains d'entre eux pouvaient collecter des événements DNS, mais sans m'offrir une vision d'ensemble sur la situation comme Varonis le fait », ajoute-t-il.

Bien que l'entreprise ait investi des millions dans la cybersécurité, Varonis Edge a été le seul produit à déceler l'attaque de tunneling DNS. La réussite du test a permis de convaincre facilement les parties prenantes de sa nécessité.

M. Hamil est heureux d'avoir eu la possibilité d'essayer Edge avant de l'acheter, et ce niveau de service représente pour lui l'un des principaux avantages de sa collaboration avec Varonis.

> Il rapporte : « Chaque fois que j'ai besoin de résoudre un problème ou que je souhaite tester un nouveau produit, son service client est toujours excellent.
>
> Lorsqu'un incident s'est produit il y a trois ans, la réponse de Varonis a été immédiate. Un membre de l'équipe Varonis a travaillé 10 heures par jour jusqu'à ce que le problème soit résolu. Je ne connais aucune autre entreprise qui propose une assistance et un service client de ce niveau. »

Certes, Varonis n'est pas la seule entreprise à proposer la classification des données et le contrôle de l'intégrité des fichiers, mais Tony Hamil ne voit pas d'autre solution offrant des rapports aussi détaillés ou une protection aussi complète à son organisation et à ses utilisateurs.

D'après lui, « Varonis ne se contente pas de contrôler l'intégrité des fichiers. La plupart des plateformes peuvent vous indiquer l'emplacement d'un événement. Mais seul Varonis offre une corrélation complète des données et une piste d'audit unifiée des événements qui montre exactement ce qui se passe et chaque fichier qui a été touché, y compris dans le cloud. »

« Varonis Edge a été la seule solution capable de détecter les menaces de tunneling DNS. Aucun autre produit n'a su y parvenir. »

Les résultats

Gain de temps, tranquillité d'esprit et confiance dans le fait que l'entreprise dispose de la plateforme de sécurité des données la plus fiable

M. Hamil a beaucoup d'expérience dans le domaine de la cybersécurité, et il utilise les solutions Varonis depuis des années. Il a pu constater à quel point Varonis a évolué pendant cette période.

« En 2015, Varonis faisait déjà ce que nous en attendions, mais la prise en main était compliquée. Ils se sont incroyablement améliorés sur ce point. La solution est intuitive, beaucoup plus simple à utiliser, et elle présente les données en temps réel. »

> « En moins d'une minute, je peux cliquer sur une alerte et examiner les analyses. Je peux voir tous les fichiers auxquels une personne a accédé, tant au niveau du serveur que du cloud. Je peux voir ce qui s'est passé pendant les pauses, si la personne était censée avoir accès à ce fichier, si elle a chargé quelque chose de suspect, ou s'il s'est produit d'autres anomalies.
>
> Si j'essayais de faire tout cela avec plusieurs outils, il faudrait bien plus de temps pour trouver tous les journaux d'événement, les assembler, corréler toutes les données et m'assurer que tout est en ordre. Avec Varonis, j'effectue ces opérations rapidement sur une plateforme centralisée. Cela nous a permis d'économiser au moins un ETP (équivalent à temps plein). »

Les améliorations techniques et les fonctionnalités supplémentaires introduites par Varonis au fil des ans ont simplifié son utilisation et accru sa capacité à protéger les données sensibles. Même les menaces les plus difficiles à détecter, comme les attaques DNS, ne peuvent échapper à Varonis et Edge.

C'est pour cela que la solution de cybersécurité Varonis s'est imposée à Tony Hamil en 2015, et qu'elle reste son choix préféré aujourd'hui.

> « En termes d'utilisation, de classification de données, de contrôle des fichiers et des autorisations, ou de corrélation de toutes ces données, aucune autre solution n'arrive à la cheville de Varonis.
>
> Je connais tous les grands fournisseurs, et aucun autre n'offre le même niveau de détail, les mêmes performances ou la même étendue de connaissances », conclut-il.

Ne laissez aucune menace de sécurité passer inaperçue.

Varonis vous aide à sécuriser vos données, à rester en conformité et à détecter les menaces potentielles avant qu'elles ne se transforment en problèmes majeurs.

DEMANDER UNE DÉMO