Phoenix, fournisseur de solutions informatiques et de services managés, fait confiance aux produits Quest qu'il commercialise.

Phoenix Software renforce sa sécurité et sa cyberrésilience grâce aux solutions Quest.

Pays : **Royaume-Uni**

Collaborateurs : **430**

Secteur : **solutions informatiques et fournisseur de services managés**

Site Internet : **www.phoenixs.co.uk**

Fournisseur primé de solutions informatiques et de services managés, Phoenix vérifie soigneusement les solutions qu'il propose.

Phoenix Software fournit des solutions informatiques et des services managés qui permettent aux entreprises britanniques de moderniser et de sécuriser leurs infrastructures et de protéger, visualiser et gérer leurs données. L'excellence de l'entreprise a fait l'objet de nombreuses récompenses, notamment les prix Microsoft du partenaire de l'année pour la gestion des terminaux modernes en 2023 et du partenaire de l'année au Royaume-Uni en 2021.

Les obligations et les engagements de Phoenix à l'égard des clients sont sa plus grande priorité. « Nous avons mis en place un processus d'intégration complet pour nos fournisseurs stratégiques », explique Laura Banks, spécialiste de la protection des données chez Phoenix.

Les enjeux

En tant que fournisseur primé de solutions informatiques et de services managés, Phoenix Software ne s'associe qu'avec des fournisseurs dont la qualité et la réputation sont irréprochables. En effet, chaque fois que cela est possible, les équipes informatiques de l'entreprise testent les solutions potentielles dans leur propre environnement avant de les proposer aux clients. Au cours de ce processus, quelques outils sélectionnés s'avèrent si précieux qu'ils intègrent la pile IT de l'entreprise.

La solution

Phoenix a appliqué son processus d'évaluation minutieux aux solutions Quest de sécurité et de cyberrésilience d'Active Directory. Elles ont passé ces tests haut la main. Par conséquent, les équipes informatiques internes s'appuient désormais sur ces outils pour toute une série de fonctions essentielles, de la détection et de la réponse aux cybermenaces jusqu'à la reprise d'activité.

Résultats ou avantages

- Bloque les menaces en empêchant les modifications des comptes stratégiques des administrateurs, des GPO et d'autres objets
- Renforce la sécurité d'AD grâce à une gouvernance efficace de la stratégie du groupe
- Garantit la cyberrésilience en réduisant le temps nécessaire à la reprise d'activité, de plusieurs jours à seulement une heure ou deux
- Facilite la conformité aux réglementations et aux contrats en automatisant les tâches de gestion des privilèges

« Si je vois une opportunité d'intégrer une nouvelle solution à notre pile technologique, elle sera soumise à notre équipe technique pour examen et test. Avant de la proposer à nos clients, nous attendons que nos techniciens nous confirment qu'il s'agit du meilleur produit disponible sur le marché. Nous n'intégrons que les meilleurs fournisseurs et les meilleures solutions. »

L'utilisation de ces solutions au sein de l'entreprise, lorsque cela est possible, présente de multiples avantages. « Nous avons à cœur d'utiliser les outils que nous vendons », souligne Shaun Tosler, responsable de l'infrastructure et de la sécurité chez Phoenix. « Il est évident que nous ne pouvons pas le faire avec tous les produits, mais quand nous vérifions qu'une solution fonctionne bien pour nous, nous pouvons être sûrs qu'elle satisfera aussi nos clients. De plus, cela permet à nos équipes d'acquérir de l'expérience avec les outils que nous vendons afin de mieux assister les clients qui les adoptent. »

En tant que Platinum Partner de Quest, Phoenix a eu l'opportunité de tester les solutions de sécurité et de récupération d'Active Directory. Ces solutions ont non seulement satisfait aux critères d'entrée dans la gamme des produits vendus par l'entreprise, mais elles se sont également révélées si précieuses qu'elles demeurent des composantes essentielles de son propre écosystème informatique. Ensemble, Change Auditor, GPOADmin et Recovery Manager, Active Directory Disaster Recovery Edition de Quest et One Identity Active Roles aident Phoenix à garantir une sécurité d'Active Directory et une cyberrésilience robustes.

Change Auditor offre une détection avancée des menaces et peut même neutraliser les attaquants.

Grâce à Change Auditor, Phoenix bénéficie d'une surveillance des menaces et d'un suivi de la sécurité en temps réel sur toutes les principales activités des utilisateurs et modifications apportées par les administrateurs. « Pour l'audit de sécurité, notre principal outil est Microsoft Sentinel », note M. Tosler. « Mais nous ne pensons pas qu'il soit judicieux de mettre tous nos œufs dans le même panier en n'ayant qu'un seul outil pour les fonctions critiques. Que se passe-t-il en cas d'erreur ou de compromission ? Change Auditor constitue une importante source d'information secondaire. En outre, en raison de sa position dans la structure technique d'AD, il fournit des informations enrichies que les logs natifs ne captent pas. »

Phoenix est encore plus enthousiaste quant à la capacité de Change Auditor à bloquer les modifications non désirées apportées aux objets critiques, tels que les comptes des administrateurs stratégiques et les principaux objets de stratégie de groupe (GPO). « Change Auditor arrêtera les hackers, quelles que soient les autorisations dont ils disposent, s'ils tentent de modifier des objets protégés », explique M. Tosler. « C'est notre filet de sécurité contre l'escalade des privilèges et les mauvaises configurations d'AD. Nous pouvons définir qu'un compte particulier ne peut pas être modifié du tout, ou qu'il ne peut être modifié qu'à partir d'une certaine plage d'adresses IP, etc. Par exemple, si chaque compte était accidentellement désigné comme administrateur de domaine, cela n'aurait pas d'importance, car Change Auditor ferait barrage pour refuser tout changement critique. »

En effet, avec Change Auditor, Phoenix est mieux positionné pour détecter et répondre rapidement aux menaces. « Avec Change Auditor, si un pirate s'introduit dans notre système AD, deux choses se produisent », explique M. Tosler. « Tout d'abord, l'attaque fera plus de bruit, ce qui signifie que nos autres outils de sécurité pourront plus facilement la repérer. Et même si l'attaquant réussit à déconnecter notre principale source de journalisation, Change Auditor continue de consigner les informations dans le log. En bref, nous avons plus de temps, la cyberattaque est moins discrète et nous bénéficions d'une meilleure protection à chaque étape. »

> **Recovery Manager est exceptionnel, c'est le seul outil qui automatise les tâches de restauration des contrôleurs de domaine après un sinistre. Tous les autres outils de sauvegarde se contentent de récupérer le fichier de base de données Active Directory et vous laissent faire le travail. Recovery Manager ne restaure pas simplement un fichier, il automatise l'ensemble du processus de récupération. En une heure ou deux, je peux rétablir l'environnement. Sans la solution, il nous faudrait des jours pour le reconstituer.**
>
> *Shaun Tosler, responsable de l'infrastructure et de la sécurité, Phoenix Software*

GPOADmin permet une gouvernance efficace de la stratégie de groupe.

La stratégie de groupe joue un rôle crucial dans la sécurité d'Active Directory et Phoenix utilise GPOADmin pour gérer ses GPO efficacement. « GPOAdmin nous permet de contrôler facilement le déploiement des GPO », explique M. Tosler. « Lorsque nous devons faire une mise à jour à une heure définie, nos ingénieurs n'ont pas à attendre jusqu'à une heure du matin pour déployer la modification afin qu'elle ait le moins d'impact possible sur les utilisateurs. Au lieu de cela, nous pouvons effectuer le changement, mettre en place les GPO et programmer le déploiement pour répondre à nos besoins. »

De plus, GPOADmin offre une gestion robuste des changements de GPO. « Le fait est que 99 % des failles de sécurité sont dues à l'absence d'une gestion appropriée des changements. Quelqu'un apporte simplement une modification sans avoir mis en place un processus adéquat », précise M. Tosler. « Nous utilisons la fonction d'approbation de GPOADmin pour nous assurer que si une personne effectue une modification, quelqu'un d'autre doit l'approuver, ce qui permet d'éviter les erreurs dues à la précipitation et les actes malveillants. De plus, GPOADmin suit chaque événement et fournit des détails clairs afin que nous puissions toujours savoir exactement ce qui a été modifié. »

Bien sûr, même avec les processus les plus rigoureux en place, des problèmes peuvent survenir. C'est pourquoi GPOADmin offre des capacités avancées de restauration. « Même avec les approbations et les tests les plus minutieux, il est possible qu'un GPO soit déployé et qu'un problème soit ensuite découvert », souligne M. Tosler. « Avec GPOADmin, nous pouvons rapidement et facilement restaurer les GPO à un état précédent afin de rétablir rapidement la sécurité d'Active Directory. Il est très rare qu'un outil tienne ses promesses en termes de contrôle et d'administration de la stratégie de groupe, mais c'est pourtant ce que fait GPOADmin, et il le fait très bien. »

Recovery Manager for Active Directory est « exceptionnel », et réduit le délai de restauration de plusieurs jours à quelques heures.

Pour garantir la cyberrésilience, Recovery Manager fournit des sauvegardes d'AD efficaces et fiables, en omettant des composants extérieurs et risqués tels que les fichiers de démarrage pour ne pas encombrer l'environnement. En effet, M. Tosler considère qu'il s'agit de « l'un des meilleurs outils du marché pour la sauvegarde d'AD. »

Toutefois, selon lui, c'est dans le domaine de la restauration que la solution est la plus efficace. « Recovery Manager est exceptionnel, c'est le seul outil qui automatise les tâches de restauration des contrôleurs de domaine après un sinistre », explique M. Tosler. « Tous les autres outils de sauvegarde se contentent de récupérer le fichier de base de données Active Directory et vous laissent faire le travail. Recovery Manager ne restaure pas simplement un fichier, il automatise l'ensemble du processus de récupération. En une heure ou deux, je peux rétablir l'environnement. Sans la solution, il nous faudrait des jours pour le reconstituer. De plus, il vous permet de restaurer des informations que vous ne pouvez tout simplement pas reconstituer, ce qui augmente considérablement sa valeur. »

> **« Nous avons mis en place un processus d'intégration complet pour nos fournisseurs stratégiques. Si je vois une opportunité d'intégrer une nouvelle solution à notre pile technologique, elle sera soumise à notre équipe technique pour examen et test. Avant de la proposer à nos clients, nous attendons que nos techniciens nous confirment qu'il s'agit du meilleur produit disponible sur le marché. Nous n'intégrons que les meilleurs fournisseurs et les meilleures solutions. »**
>
> *Laura Banks, spécialiste de la protection des données Phoenix*

Bien que Phoenix n'ait jamais eu à effectuer de reprise d'activité, savoir qu'elle peut compter sur de telles capacités de restauration lui procure une grande tranquillité d'esprit. « En cas de compromission d'un domaine, j'aurais 1 001 choses à penser, et le PDG ou le directeur de la technologie me demanderaient des comptes, car l'entreprise perdrait de l'argent à chaque seconde », explique M. Tosler. « Avec Recovery Manager, je sais que je n'ai qu'un seul bouton à presser pour lancer la récupération, restaurer nos identités et rétablir des services tels que la messagerie électronique. C'est véritablement inestimable. »

En effet, M. Tosler recommanderait Recovery Manager à toute entreprise dont l'Active Directory aurait été supprimé à cause d'un sinistre, et relève que la solution est susceptible d'offrir un retour sur investissement complet et immédiat. « Recovery Manager vous fournira une base solide pour entamer la restauration des systèmes », explique-t-il. « Imaginons que vous ayez des dizaines de milliers d'utilisateurs : la création manuelle de tous ces comptes pourrait prendre 10, 20 ou 30 heures. Recovery Manager supprime tout le travail et automatise la création de comptes. Les autres outils n'en sont pas capables. Le temps que vous gagnerez fera probablement plus qu'amortir le coût d'acquisition de la solution dans cette situation. »

Active Roles renforce la sécurité d'AD en simplifiant la gestion des identités.

Pour la sécurité des identités, Phoenix utilise Active Roles, qui permet de gérer et de déléguer précisément les privilèges entre les domaines Active Directory et les tenants Entra ID (anciennement Azure AD) à partir d'une console unique. En utilisant le contrôle d'accès granulaire basé sur les rôles (RBAC), Phoenix peut appliquer strictement le principe du moindre privilège.

« Active Roles fournit le niveau d'abstraction dont nous avons besoin pour la sécurité des identités », explique M. Tosler. « Par exemple, nous n'avons plus besoin de fournir des comptes d'administrateurs à nos techniciens du service d'assistance. Nous les dirigeons plutôt vers une interface web. Nous pouvons également déléguer des tâches telles que la gestion des groupes aux personnes disposant de l'expertise nécessaire, comme les développeurs d'applications personnalisées. De plus, seuls les comptes stratégiques peuvent effectuer des modifications directement dans AD. »

Active Roles aide également Phoenix à garantir la conformité avec les exigences en matière de souveraineté des données, aussi bien dans le cadre des contrats d'entreprise que de réglementations telles que le RGPD. « Nos collaborateurs ont besoin de partir en vacances et d'accéder à leurs e-mails, mais certains clients n'autorisent pas le traitement de leurs données en dehors du Royaume-Uni », explique M. Tosler. « Active Roles fournit l'automatisation dont nous avons besoin pour honorer ces contrats. Nous l'avons simplement configuré de manière à ce que l'utilisateur soit automatiquement retiré de certains groupes au début de ses vacances et qu'il y soit réintégré à son retour. Par conséquent, nous n'avons pas à nous soucier des utilisateurs qui conservent des droits d'accès qu'ils ne devraient pas avoir. »

Un ensemble de solutions qui fonctionnent ensemble

Aussi précieuse que soit chaque solution prise individuellement, Phoenix reconnaît qu'elles fonctionnent ensemble pour apporter encore plus de valeur. « Si vous adoptez Active Roles pour la gestion des identités, vous pouvez tout aussi bien faire appel à Change Auditor pour verrouiller AD », explique M. Tosler. « De même, Recovery Manager créera des sauvegardes et Change Auditor les surveillera et empêchera quiconque de les fausser. Avec ces types de contrôles en place, je peux être sûr que les données nécessaires à la remise en route du service seront là quand j'en aurai besoin. »

PRODUITS ET SERVICES

Produits

- Change Auditor
- GPOADmin
- Recovery Manager for Active Directory Disaster Recovery Edition
- One Identity Active Roles

Solutions

- Gestion des plateformes Microsoft

À propos de Quest

Quest crée des solutions logicielles qui exploitent les avantages des nouvelles technologies dans un paysage informatique toujours plus complexe. De la gestion des bases de données et des systèmes à la migration et à la gestion d'Active Directory et de Microsoft 365, en passant par la cyberrésilience, Quest aide ses clients à relever leurs prochains défis informatiques dès à présent. Quest Software. Où demain rencontre aujourd'hui.

CaseStudy-Phhoenix-KA-FR-WL-87341