HashiCorp

ABN·AMRO | ÉTUDE DE CAS CLIENT

Pour la sécurité du cloud

Comment une institution financière de premier plan utilise HashiCorp Vault pour automatiser la gestion des secrets et générer des gains considérables pour son portefeuille de produits en pleine croissance

// L'infrastructure favorise l'innovation

À propos d'ABN AMRO

ABN AMRO Bank N.V. est la troisième plus grande banque des Pays-Bas, ayant son siège à Amsterdam. ABN AMRO propose une gamme complète de solutions et de produits financiers pour les clients dans les secteurs des services bancaires de détail, aux entreprises et privés. Son activité se concentre sur l'Europe du Nord-Ouest. La banque fournit ses services à environ 6 millions de clients et emploie un peu moins de 18 000 personnes. En 2008, ABN AMRO Bank a été nationalisée par le gouvernement néerlandais en compagnie de Fortis Bank Nederland. Elle est devenue une société cotée en bourse en 2015.

QUELQUES FAITS INTÉRESSANTS SUR ABN AMRO

Plus de 446 milliards de dollars d'actifs gérés

25 nouvelles plateformes implémentées

2 600 applications d'entreprise

25 000 associés

19 pays et territoires

Diminution significative du temps consacré à l'intégration des applications

Les secrets existants aujourd'hui disparaîtront demain

« Les secrets dynamiques et les capacités de chiffrement grâce à l'API de Vault, associés à son injecteur de secrets et à ses communications sécurisées, permettent d'intégrer en toute confiance des applications à notre plateforme de conteneurs en une fraction du temps et des efforts requis auparavant ».

TON VAN DIJK,
PRODUCT OWNER PRODUIT AGILE, ABN AMRO

Peu de secteurs exigent le même niveau de confidentialité et de sécurité que celui des services bancaires. Et peu de banques ont des exigences de sécurité aussi élevées qu'ABN AMRO.

La banque fournit une gamme complète de produits et de services à ses clients. Néanmoins sécuriser les systèmes, les applications et les données qui permettent ces services constitue une tâche ardue pour le Service de sécurité des systèmes d'information d'entreprise (Corporate Information Security Office, CISO) de 400 personnes.

« L'application de la gouvernance des accès et des identités à travers nos diverses applications commerciales client et back-end a été difficile mais gérable avec nos solutions de sécurité existantes, alors même que nous avons ajouté des milliers de nouveaux comptes et utilisateurs », déclare Ton van Dijk, Product owner produit agile de la banque dans l'espace identité et accès. « Cependant, notre système existant avait besoin d'un module supplémentaire et d'une surveillance pratique pour la gestion des secrets et des clés back-end éphémères dans nos applications internes et notre infrastructure, nous avons donc décidé de rechercher un moyen plus transparent et automatisé de traiter un élément aussi stratégique de nos activités ».

Empêcher un effet domino

Bien que le secteur des services financiers ait la réputation d'exiger des technologies éprouvées, ce qui rend souvent l'adoption précoce de la technologie difficile, ABN AMRO s'est engagé dans un processus de transformation numérique afin de moderniser et pérenniser ses activités. Pour autant, si la stratégie informatique multi-cloud et l'environnement de développement conteneurisé ont fourni des gains d'efficacité indispensables pour son portefeuille de produits en pleine croissance, cela a également créé un nouvel ensemble de complexités et de défis pour l'équipe CISO.

« La gestion des secrets constitue un élément critique de notre travail car si l'un des secrets est compromis, cela aura un énorme impact en aval », déclare Van Dijk. « Même un seul certificat de signature compromis peut mettre un système entier hors ligne, ce qui signifie potentiellement la perte de l'accès aux applications en ligne ou de les voir exposer au risque que quelqu'un y injecte malicieusement quelque chose. Et donc, le droit à l'erreur n'existe pas ».

La précédente solution de gestion des secrets de la banque comportait un certain nombre de connecteurs de systèmes prêts à l'emploi qui nécessitaient encore un travail important de programmation pour la configuration d'une nouvelle application. Pire encore, la plateforme autogérée ne s'intégrait pas correctement à l'instance Kubernetes de l'équipe, ce qui signifiait que l'un des ingénieurs de l'équipe devait créer un connecteur personnalisé pour les nouvelles applications ou nouveaux conteneurs, ce qui pouvait prendre plusieurs jours avant d'atteindre le stade de test.

De plus, ABN AMRO avait conscience que la diffusion des secrets devait être empêchée. Comme de nombreuses applications et plateformes sont fournies avec leurs propres moteurs de secrets, il est essentiel de disposer de cette surveillance centrale afin de pouvoir révoquer rapidement les secrets dans l'éventualité où un compromis sérieux se produirait. Lorsque les secrets sont transmis à travers une multitude de solutions, cela devient vite difficile à contrôler.

« L'ensemble du processus nous a révélé que s'appuyer sur un système de gestion des secrets sur site et autogéré nécessitant une assistance tierce pour tout type de changement s'avérait autant chronophage qu'inefficace concernant la gestion d'une composante cruciale de nos opérations », explique Van Dijk. Plus généralement, « il est devenu de plus en plus clair que nous avions besoin d'un environnement cloud natif qui prenait en charge le développement conteneurisé et mettait l'accent sur l'automatisation et cela sans avoir à entreprendre une refonte complète et coûteuse ou une actualisation de la technologie ».

Défis

Gestion sécurisée des secrets éphémères

Réduction de la dépendance envers les processus manuels de gestion des secrets

Intégration des applications consommateur et internes à un serveur de secrets

« La sécurité des données et des systèmes sous-tend chaque aspect de nos opérations. Avec Vault, nous avons l'agilité, la transparence et un support de classe mondiale pour élaborer en toute confiance des solutions répondant aux besoins actuels et futurs sans avoir à nous soucier constamment d'un secret mal géré mettant à mal l'ensemble de nos efforts ».

TON VAN DIJK,
PRODUCT OWNER PRODUIT AGILE, ABN AMRO

Gestion centrale et dynamique des secrets pour une entreprise en plein essor

Désireuse d'améliorer ses pratiques de gestion des secrets en éliminant les informations d'identification codées en dur des applications et des scripts développés en interne, l'équipe CISO d'ABN AMRO a adopté HashiCorp Vault après avoir effectué une démonstration de faisabilité impliquant les spécialistes en développement logiciel et sécurité de l'équipe.

Avec Vault, l'équipe CISO a implémenté un référentiel central de gestion des secrets, évitant ainsi le besoin d'opérateurs humains appliquant manuellement les politiques de secrets aux nouvelles applications et nouveaux hôtes. La plateforme « cloud-agnostic » simplifie considérablement la gestion des informations d'identification et des secrets partagés en automatisant nombre des processus les plus longs et les plus laborieux.

« Les secrets dynamiques et les capacités de chiffrement de l'API fournis par Vault, associés à son injecteur de secrets et à ses communications sécurisées, permettent d'intégrer en toute confiance des applications à notre plateforme de conteneurs en minimisant le temps et les efforts requis auparavant », déclare Van Dijk. « Nous sommes désormais en mesure de gérer les secrets éphémères dans AWS et Azure d'une manière impensable auparavant sans besoin d'ajouter du personnel, d'augmenter les coûts ou d'avoir des courbes d'apprentissage inutilement longues ».

Résultats

Suppression des modules de secrets éphémères coûteux aux fins de réduction des coûts et de la complexité

Les secrets dynamiques ont permis l'intégration de deux douzaines de nouvelles plateformes

Établissement des bases pour un modèle d'encryption-as-a-service

Solution

ABN AMRO utilise HashiCorp Vault pour créer un système de gestion des secrets centralisé couvrant ses applications dans AWS, Azure et d'autres applications internes qui automatise l'injection de secrets et le cryptage API pour une plus grande efficacité et un nombre moindre d'erreurs au niveau des secrets critiques.

À propos de Ton van Dijk

Ton van Dijk est le Product Owner produit agile pour ABN AMRO Bank. Ton est responsable de la gestion des secrets ainsi que des accès privilégiés. Ton est un vétéran de 30 ans du secteur des services financiers, ayant en pratique occupé l'ensemble de ces années un rôle en cybersécurité.

Stack technologique

- Infrastructure : Clouds Microsoft Azure, IBM et Cisco sur site, mainframe
- Plateforme : Windows Server, Linux, Z-OS
- Équilibreurs de charge : Windows
- API gateway : Apigee, APIM
- CA : service géré par CGI (certificats internes) plus quelques fournisseurs de certificats commerciaux
- IAM : Sailpoint, Ping Identity (IAM clients), Ping Federate (SSO)
- APM (gestion des performances applicatives) : Splunk, Tivoli (sur site), analyse des journaux (Azure)
- Provisionnement : ServiceNow, DevOps Azure
- Gestion de la sécurité : HashiCorp Vault


HashiCorp