KEYFACTOR

ÉTUDE DE CAS

Comment EQ Bank permet aux équipes de sécurité et aux équipes DevOps d'aller plus vite grâce à l'automatisation de la PKI et des certificats en tant que service.

L'entreprise

EQ Bank est la plateforme digitale de Equitable Bank, basée à Toronto. Fondée il y a plus de 50 ans, Equitable gère plus de 40 milliards de dollars d'actifs et s'est développée pour servir plus d'un quart de million de Canadiens. Lancée en 2016 en tant que première banque numérique née au Canada, EQ Bank a alimenté une croissance rapide en défiant les banques traditionnelles avec une expérience entièrement sans agence et des solutions bancaires plus intelligentes.

Les défis

En tant que leader dans le domaine des services bancaires numériques et première banque au Canada à héberger entièrement un système bancaire principal dans le nuage, la sécurité et la disponibilité sont primordiales pour EQ. Mais que se passe-t-il si un certificat expiré fait tomber l'infrastructure sous-jacente ou interrompt la productivité des équipes informatiques ? C'est exactement le défi que David Yu, vice-président de l'architecture de sécurité, devait résoudre face à la transformation numérique rapide et à la croissance de l'entreprise.

"Il y a deux ans, nous avons remarqué que nous utilisions beaucoup plus de certificats pour les applications que nous exécutons au sein de l'entreprise et les applications que nous développons en interne", explique David Yu. "Nous avions DigiCert pour les certificats de confiance publique, mais nous n'avions pas d'autorité de certification (CA) interne, et il n'y avait que des processus ad hoc pour que les propriétaires d'applications demandent et fournissent des certificats. Les équipes informatiques et d'infrastructure se contentaient d'émettre leurs propres certificats dans les environnements de développement et passaient à autre chose."

L'émission de certificats ad hoc rendait difficile le maintien d'une visibilité complète et la fourniture de rapports aux auditeurs internes. Sans processus définis, ils ne pouvaient pas suivre la manière dont les autres équipes de l'entreprise approvisionnaient les certificats. En conséquence, des certificats inconnus et non suivis arrivaient à expiration à leur insu, entraînant l'arrêt du fonctionnement des applications et détournant des ressources clés de leurs tâches quotidiennes pour remédier aux pannes.

Historiquement, l'équipe de sécurité a pu gérer manuellement quelques certificats dans des feuilles de calcul ; elle a également utilisé Active Directory Certificate Services (ADCS), parfois appelé Microsoft CA, pour émettre des certificats pour des cas d'utilisation interne limités. Cependant, l'équipe informatique est passée de 20 à plus de 150 personnes, un taux de croissance qu'il était impossible de supporter avec leur déploiement limité de Microsoft CA et leurs processus manuels de gestion des certificats.

Equitable Bank

INDUSTRIE

FServices financiers

LIEU

Toronto, Canada

DIFFICULTÉS

- Les anciens services de certification Active Directory (ADCS) ne pouvaient pas prendre en charge les cas d'utilisation DevOps et Cloud.
- Une mauvaise visibilité a conduit à des pannes inattendues causées par des certificats expirés et mal configurés.s
- Utilisation de certificats auto-signés qui ne répondaient pas aux normes de sécurité.

SOLUTION

EQ Bank utilise Keyfactor Command PKI as a Service (PKIaaS) et l'automatisation de la durée de vie des certificats pour éliminer les pannes et permettre aux équipes DevOps d'agir plus rapidement - sans le coût et la complexité de l'exécution de PKI sur site.

Un audit indépendant et une analyse des lacunes de la part d'un partenaire informatique de longue date ont confirmé qu'une solution de gestion des certificats était essentielle pour améliorer leur posture de sécurité et éviter de nouvelles pannes — un risque amplifié par l'utilisation généralisée des identités de machines dans leur infrastructure Azure et DevOps tentaculaire. C'est là que l'architecture de sécurité est intervenue dans le projet.

La solution

Avant tout, l'équipe chargée de l'infrastructure avait besoin d'une solution offrant les capacités d'émission de certificats d'une autorité de certification interne robuste, mais sans avoir à la construire et à la maintenir en interne. Yu explique qu'ils savaient dès le départ que les efforts et les dépenses liés à la mise en place d'une ICP seraient beaucoup trop lourds pour leurs équipes. Il aurait été très difficile de faire fonctionner une autorité de certification répondant à leurs normes de sécurité informatique en interne.

La solution devait également fournir une visibilité centralisée des certificats publics et privés pour que l'équipe de sécurité puisse superviser et gérer efficacement son parc informatique. Parallèlement, les administrateurs système et les développeurs avaient besoin d'un moyen facile de consommer les certificats et de les intégrer aux outils automatisés de leur environnement DevOps, notamment Azure Key Vault, Kubernetes et Istio service mesh.

Après avoir évalué plusieurs fournisseurs dans le cadre d'une validation de concept, l'équipe a choisi Keyfactor. La raison principale de leur décision est que Keyfactor était le seul fournisseur capable de fournir une autorité de certification entièrement gérée et hébergée aux côtés des capacités d'une solution complète d'automatisation du cycle de vie des certificats dans une seule plateforme cloud. Keyfactor offrait également l'ensemble le plus robuste d'API et d'intégrations que leur équipe DevOps pouvait commencer à utiliser immédiatement.

> "Les certificats expiraient, mais nous ne le savions pas avant que les systèmes ne tombent en panne. Depuis le déploiement de Keyfactor, nous avons entièrement éliminé ces incidents."
>
> **David Yu**
> VP, Security Architecture
> EQ Bank

RÉSULTATS

- Fourniture d'une infrastructure PKI en nuage robuste pour remplacer leur déploiement ADCS obsolète.
- Réduction de la charge de travail liée aux certificats de 2 équivalents temps plein (ETP).
- Protection des outils et de l'infrastructure DevOps alors que l'entreprise continue d'innover.

PRODUCTS

- Keyfactor Command
- Keyfactor PKI as a Service

L'impact sur le entreprise

Déplacement de la PKI vers le cloud

L'un des premiers objectifs d'EQ était de mettre en place et de faire fonctionner une nouvelle autorité de certification interne. En deux mois, la banque a migré de son autorité de certification Microsoft sur site vers la nouvelle PKI hébergée dans le cloud. La conformité à la norme SOC 2 de type II et une cérémonie complète de signature de la racine leur ont permis d'obtenir facilement les approbations de conformité et de sécurité dont ils avaient besoin pour le projet.

"Avec Keyfactor qui gère maintenant les aspects clés de notre infrastructure PKI, nous sommes en mesure de nous concentrer sur la proactivité dans les domaines de la sécurité, de la livraison de logiciels et de l'infrastructure", déclare Yu.

Keyfactor a également aidé l'équipe EQ à mettre en place des modèles de certificats, des flux de travail d'approbation, et des politiques pour aider à standardiser les processus d'émission et de provisionnement.

Désormais, les développeurs et les ingénieurs peuvent éviter les certificats auto-signés et obtenir des certificats auprès de DigiCert ou de leur PKI as a Service (PKIaaS) hébergé par Keyfactor, en utilisant les capacités de self-service de Keyfactor Command. En conséquence, le temps passé à demander et à fournir des certificats approuvés par la sécurité est passé de plusieurs heures à quelques minutes seulement.

O btenir une visibilité complète pour remédier aux risques

Keyfactor a également fourni une visibilité complète des certificats en balayant d'abord les bases de données des CA dans DigiCert CertCentral et leur implémentation ADCS existante sur site. Ensuite, ils ont travaillé avec l'équipe EQ pour permettre la découverte en réseau de tous les certificats internes et externes. Ce processus de découverte a fourni des informations exploitables pour identifier et corriger immédiatement les vulnérabilités, y compris les certificats auto-signés.

Grâce à un inventaire complet, les ingénieurs en sécurité n'ont plus à s'inquiéter des certificats inconnus, expirés ou faibles qui pourraient menacer la disponibilité et la sécurité des applications. Ils peuvent également répondre beaucoup plus rapidement aux demandes des auditeurs internes en utilisant des rapports programmés sur l'état et l'expiration des certificats.

Élimination des pannes grâce à l'automatisation

Depuis qu'elle utilise Keyfactor Command, EQ Bank n'a pas connu une seule interruption de service liée à la certification. En utilisant une combinaison d'alertes d'expiration et de flux de travail de renouvellement automatisé, l'équipe a effectivement éliminé les pannes et réduit considérablement le taux d'erreur humaine.

Yu explique que son service informatique a économisé deux équivalents temps plein (ETP) qui auraient auparavant été gaspillés sur des tâches manuelles liées aux certificats, notamment le dépannage des problèmes et la correction des pannes fréquentes.

L'un des premiers objectifs de l'équipe était d'automatiser les flux de travail de provisionnement et de renouvellement pour Azure Key Vault en utilisant des certificats provisionnés à partir de leur nouvelle PKI hébergée dans le cloud. En quelques jours seulement, Keyfactor a travaillé avec l'équipe EQ pour installer un Keyfactor Orchestrator et configurer l'intégration prête à l'emploi pour qu'elle fonctionne avec leur environnement Azure Key Vault. Désormais, chaque fois qu'un certificat arrive à expiration, Keyfactor automatise le processus de renouvellement et remplace automatiquement le certificat qui expire par un certificat de leur nouvelle PKI.

Approvisionnement en certificats intégrés aux flux de travail DevOps

Pour les entités axées sur le Cloud Computing comme EQ Bank, la confiance est primordiale. Chaque machine doit être authentifiée et vérifiée avec des identités basées sur des certificats pour garantir que les connexions sont fiables et sécurisées. Pour y parvenir, l'équipe DevOps utilise l'API complète de Keyfactor et les outils de référence pour s'intégrer à leurs outils et à leur infrastructure.

> "Nous voyons cela comme un mouvement trans-formationnel. Notre équipe DevOps n'a plus besoin de faire des pieds et des mains pour faire avancer les choses. Elle peut désormais agir beaucoup plus rapidement et faire tourner les certificats plus fréquemment, sans aucun temps d'arrêt."
>
> **David Yu**
>
> VP, Security Architecture
> EQ Bank

KEYFACTOR

Keyfactor est le leader des solutions PKI as-a-Service et de crypto-agilité. Notre plateforme de crypto-agilité permet aux équipes de sécurité d'orchestrer de manière transparente chaque clé et chaque certificat dans toute l'entreprise.

CONTACTEZ-NOUS

- www.keyfactor.com
- +1.216.785.2946

L'équipe DevOps a déjà utilisé Keyfactor pour automatiser l'émission et la rotation des certificats pour le chiffrement HTTPS et les points d'entrée à travers leurs conteneurs Docker, Azure Kubernetes Service (AKS) et les déploiements Services Mesh Istio.

"Nous considérons qu'il s'agit d'une transformation. Notre équipe DevOps n'a plus besoin de "sauter à travers des cerceaux" pour faire avancer les choses. Elle peut désormais agir plus rapidement et faire tourner les certificats plus fréquemment, sans aucune interruption de service", explique Yu.

Et ce n'est qu'un début. EQ Bank travaille à étendre l'automatisation et à intégrer davantage la plateforme Keyfactor Command dans ses processus DevOps. Yu a conclu que "Keyfactor a travaillé avec nous à chaque étape du processus, du lancement à la production, et ils ont été extrêmement proactifs. Leur expertise et leur soutien ont fait une différence incommensurable dans le succès de nos équipes."