Une grande banque internationale assure la sécurité, la cyberrésilience et la conformité de ses systèmes.

Une grande banque canadienne s'appuie sur une suite intégrée de solutions Quest et sur son partenariat avec les meilleurs experts Active Directory du monde entier.

Pays : **Canada**

Effectif : **60 000 collaborateurs**

Secteur : **Finance**

Dans des domaines comme le secteur bancaire, la sécurité et la disponibilité d'Active Directory sont particulièrement importantes.

Aucune entreprise ne souhaite être victime d'une faille de sécurité ou d'un arrêt de service, mais pour des secteurs extrêmement réglementés et critiques comme la finance, de tels événements peuvent être particulièrement dévastateurs. C'est pourquoi depuis des années, cette grande banque canadienne présente en Amérique du Nord, dans les Caraïbes, en Europe et en Asie-Pacifique utilise une suite de solutions Quest pour sécuriser, surveiller et assurer la restauration rapide de son écosystème informatique hybride.

Cette banque dispose d'une seule forêt Active Directory (AD) de production avec sept domaines et un tenant Entra ID de production. Leur sécurité et leur disponibilité sont une priorité absolue. « Lorsque des boutiques en ligne, des médias sociaux et autres prestataires de services subissent une panne, les clients peuvent se fâcher et certains d'entre eux peuvent même se tourner vers un autre fournisseur », explique un ingénieur d'infrastructure senior de la banque. « Mais le secteur bancaire est particulièrement sensible, car c'est là que se trouve votre argent. Si nos opérations devaient être interrompues

Les enjeux

Une grande banque internationale doit assurer la sécurité et la cyberrésilience de son vaste écosystème informatique hybride. Elle doit aussi maintenir et prouver sa conformité à un ensemble croissant de réglementations de plus en plus strictes dans les nombreuses zones géographiques où elle propose ses services.

La solution

Depuis près de vingt ans, la banque s'appuie sur les solutions et l'expertise de Quest. Lorsqu'elle a effectué la migration des charges de travail vers le Cloud, Quest l'a accompagnée avec des solutions intégrées qui lui ont offert une visibilité et un contrôle unifiés sur l'ensemble de son environnement informatique. De plus, l'équipe Quest Professional Services fournit des conseils approfondis et un transfert de connaissances grâce auxquels la banque optimise de manière proactive la sécurité, la cyberrésilience et la conformité.

Les avantages

- Renforcement de la sécurité grâce à une solution robuste d'audit et de contrôle des modifications
- Amélioration de la cyberrésilience grâce à une sauvegarde fiable et une restauration rapide de l'environnement hybride
- Capacité à assurer et à prouver la conformité aux réglementations
- Tranquillité d'esprit procurée par la relation à long terme avec un partenaire et conseiller de confiance

pendant une période plus ou moins longue, il y aurait une perte de chiffre d'affaires, ainsi qu'un impact réglementaire, car nous devons nous conformer aux normes de plusieurs zones géographiques autres que le Canada, à savoir les États-Unis, l'Union européenne et bien d'autres. Mais le pire, c'est l'atteinte grave et durable à la réputation de la banque. Par conséquent, la sécurité et la cyberrésilience d'Active Directory sont essentielles pour notre entreprise ».

La banque utilise les solutions de sécurité et de restauration d'AD de Quest depuis près de 20 ans.

Elle travaille en partenariat avec Quest depuis près de vingt ans. « Nous avons commencé par la solution Recovery Manager for Active Directory, suivie d'InTrust et d'Active Roles, dont nous avons rapidement constaté la valeur ajoutée », explique l'ingénieur d'infrastructure senior. « Lorsque Change Auditor est apparu, nous en avons vu les avantages et nous l'avons donc adopté. Bien que nous suivions le marché de près depuis des années, nous n'avons jamais trouvé d'autre fournisseur proposant des produits avec une telle gamme de fonctionnalités, et qui coexistent et s'intègrent les uns aux autres, ce qui augmente considérablement la valeur ajoutée de l'ensemble de la solution. »

En outre, à mesure que les technologies progressent et que les réalités commerciales changent, la banque constate que les produits Quest ne cessent d'évoluer pour suivre le mouvement. « Presque toutes nos actions sur site sont étendues à l'espace Entra ID », ajoute-t-il. « Quest nous a proposé tout de suite des solutions SaaS qui nous donnent la visibilité et le contrôle nécessaires sur l'ensemble de l'environnement hybride. Ces outils ont rapidement rejoint notre portefeuille. Nous avons constaté que la valeur tirée de notre ensemble de solutions Quest est beaucoup plus intéressante pour nous que les autres outils du marché. »

Des fonctionnalités robustes d'audit et de gestion des modifications assurent une sécurité renforcée.

Aujourd'hui, les experts en cybersécurité recommandent aux organisations d'adopter une approche basée sur l'hypothèse d'une violation. Il est donc essentiel de mettre en œuvre une analyse et un audit complets de l'activité dans l'ensemble de l'environnement. Avec les solutions Quest, l'équipe informatique de la banque dispose de la visibilité et du contrôle nécessaires pour prévenir les violations et les arrêts de service coûteux.

« Nous avions l'habitude d'effectuer des audits avec des outils natifs. C'était un processus assez pénible, car il était difficile d'interpréter les logs complexes et d'identifier les menaces », se souvient l'ingénieur d'infrastructure senior de la banque. « Change Auditor fournit une fonctionnalité de log très enrichie qui nous est vraiment bénéfique. Nous avons facilement personnalisé certains des rapports intégrés, et maintenant nos équipes InfoSec peuvent repérer et enquêter avec précision sur les activités hors bande. Les rapports sont même générés automatiquement selon la planification choisie et envoyés à une boîte aux lettres désignée. »

L'équipe de la banque utilise également Change Auditor pour détecter les dérives dans les configurations d'Active Directory qui pourraient ouvrir des brèches de sécurité ou compromettre la disponibilité des services. « Au fil des ans, une instance Active Directory accumule généralement des droits d'accès excessifs, des identités périmées et d'autres problèmes, et la nôtre ne faisait pas exception à la règle », note l'ingénieur d'infrastructure senior. « Avec Change Auditor, nous avons pu collaborer avec l'équipe InfoSec et nettoyer l'annuaire pour le rendre plus sûr et plus facile à gérer. »

> **Bien que nous suivions le marché de près depuis des années, nous n'avons jamais trouvé d'autre fournisseur proposant des produits avec une telle gamme de fonctionnalités, qui coexistent et s'intègrent les uns aux autres pour permettre d'augmenter considérablement la valeur ajoutée de l'ensemble de la solution.**
>
> *Ingénieur d'infrastructure senior*
> *Grande banque internationale*

Un autre avantage de Change Auditor est sa capacité à bloquer les modifications apportées à des groupes de sécurité puissants, à des objets de stratégie de groupe critiques et à bien d'autres choses encore. « Grâce à Change Auditor, nous avons intégré de nombreux objets et attributs Active Directory dans des stratégies de protection, ce qui empêche leur modification, par accident ou par malveillance », explique l'ingénieur d'infrastructure senior. « Cette approche a résisté à des tests approfondis : nous effectuons régulièrement des exercices Red Team pour tenter d'ouvrir une brèche dans l'environnement, et Change Auditor est là pour nous en empêcher. »

De plus, grâce à son portefeuille Quest, la banque dispose de la visibilité et du contrôle nécessaires sur l'ensemble de l'environnement hybride. « Comme Change Auditor est intégré à On Demand Audit, nous disposons de rapports consolidés », explique l'ingénieur d'infrastructure senior. « Le fait de pouvoir suivre les modifications à la fois sur site et dans Entra ID représente une valeur ajoutée considérable pour nous. Par exemple, lorsqu'une équipe demande un accès à privilèges à certaines données ou applications, nous pouvons examiner en détail ses activités antérieures. Nous pouvons lui montrer les modifications qu'elle a apportées sur une longue période et lui démontrer qu'elle n'a pas besoin d'un accès à privilèges permanent. Nous pouvons ainsi réduire notre surface d'attaque. »

Une reprise d'activité rapide et fiable assure la cyberrésilience.

La banque reconnaît que même la stratégie la plus complète de détection et de réponse aux menaces d'identité ne peut prévenir tous les événements indésirables. C'est pourquoi elle a mis en place une solide stratégie de reprise d'activité utilisant Recovery Manager for Active Directory intégré dans On Demand Recovery.

En effet, les dirigeants de la banque comprennent à quel point les plateformes d'identité Active Directory et Entra ID sont essentielles à l'entreprise. L'ingénieur d'infrastructure senior se souvient qu'ils ont assisté à une présentation sur la tristement célèbre attaque NotPetya. Bien que la cible principale ait été l'Ukraine, des entreprises du monde entier ont subi des dommages considérables. Par exemple, le géant du transport maritime Maersk ne disposait d'aucune sauvegarde de son instance Active Directory. Il a donc dû faire péniblement la navette entre le Ghana et le Royaume-Uni pour restaurer un contrôleur de domaine qui, par chance, avait été mis hors ligne pendant l'attaque.

Selon les estimations de Maersk, cette restauration a coûté entre 250 et 300 millions de dollars, mais d'autres initiés pensent que le montant total était en réalité bien plus élevé. Le fait qu'il n'ait fallu que 45 secondes à NotPetya pour mettre à mal le réseau d'une grande banque a sans doute été encore plus marquant pour les dirigeants assistant à la présentation. « Nous n'avons pas eu à convaincre notre PDG de l'importance de nos plateformes d'identité », explique l'ingénieur d'infrastructure senior. « Il l'a compris très vite. La reprise d'activité d'AD et d'Entra ID était adaptée au risque connu par l'entreprise. »

Avec les solutions Quest, la banque a mis en place une stratégie complète de reprise d'activité qui comprend deux serveurs Recovery Manager synchronisés dans chaque datacenter. « Chaque serveur dispose d'une sauvegarde complète et immuable de l'ensemble de l'environnement. Nous n'avons donc pas besoin des quatre serveurs pour survivre à un sinistre, un seul nous suffit. En outre, nous disposons de deux serveurs Recovery Manager dans Azure avec leurs propres sauvegardes immuables, ce qui assure une redondance supplémentaire. »

> **Recovery Manager for Active Directory dépasse de loin tous les autres produits du marché. Mais vous ne pouvez pas planifier uniquement pour AD local ; vous devez également planifier pour Entra ID. Ensemble, Recovery Manager et On Demand Recovery permettent une restauration de bout en bout de l'ensemble de la plateforme d'identité, y compris la restauration d'objets spécifiques et la reprise d'activité.**
>
> *Ingénieur d'infrastructure senior*
> *Grande banque internationale*

La banque teste régulièrement son plan de reprise d'activité, et les résultats sont éloquents. « Si un incident de cybersécurité détruisait l'ensemble de notre forêt, nous pourrions restaurer la forêt en moins de quatre heures », explique l'ingénieur d'infrastructure senior. « Recovery Manager supprime les définitions des plus de 70 contrôleurs de domaine que nous avons en production et crée une nouvelle forêt intacte en utilisant l'une de nos sauvegardes immuables. De plus, grâce à l'intégration dans On Demand Recovery, nous pouvons restaurer non seulement AD, mais aussi Entra ID. »

La sécurité et la cyberrésilience sont essentielles pour assurer la conformité aux normes en vigueur.

Les institutions financières sont soumises à des exigences réglementaires et à une surveillance strictes, et les banques ayant une présence internationale doivent se conformer à des normes émanant de plusieurs juridictions. Les solutions Quest peuvent considérablement faciliter les tâches liées à la conformité.

« Change Auditor génère automatiquement les rapports dont nous avons besoin et les envoie aux équipes concernées », explique l'ingénieur d'infrastructure senior. « En même temps, Recovery Manager et On Demand Recovery nous permettent de respecter les exigences les plus strictes en matière de reprise d'activité. En fait, compte tenu de la précision des rapports et de la capacité des outils dont nous disposons, nous n'avons aucune difficulté à respecter les réglementations auxquelles nous sommes soumis. De plus, nous sommes bien positionnés pour répondre aux nouvelles exigences qui se présenteront. »

Une suite intégrée de solutions est essentielle pour les écosystèmes informatiques hybrides d'aujourd'hui.

Une collection de solutions ponctuelles disparates ne constitue pas une approche efficace en matière de cybersécurité et de cyberrésilience. Les entreprises ont besoin de solutions intégrées qui permettent une approche unifiée dans l'environnement hybride. En effet, l'ingénieur d'infrastructure senior de la banque indique qu'il s'agit là d'un critère déterminant de l'investissement dans les solutions Quest.

« La valeur ajoutée provient du vaste portefeuille des solutions Quest et dans la manière dont elles s'intègrent parfaitement les unes dans les autres et dont elles se complètent », ajoute-t-il. « Par exemple, Recovery Manager for Active Directory dépasse de loin tous les autres produits du marché. Mais vous ne pouvez pas planifier uniquement pour AD local ; vous devez également planifier pour Entra ID. Ensemble, Recovery Manager et On Demand Recovery permettent une restauration de bout en bout de l'ensemble de la plateforme d'identité, y compris la restauration d'objets spécifiques et la reprise d'activité. »

> **Très peu de fournisseurs présentent la maturité et les capacités de Quest. Nous apprécions particulièrement la solide expérience et les connaissances approfondies de Quest Professional Services. Nos équipes internes adoptent une approche très pratique et nous comptons sur les experts de Quest pour nous conseiller sur l'optimisation de nos processus. Ils nous aident à comprendre les bonnes pratiques et à utiliser les produits Quest le plus efficacement possible dans notre environnement.**
>
> *Ingénieur d'infrastructure senior*
> *Grande banque internationale*

Un partenaire expérimenté et fiable est aussi important qu'un logiciel.

Aussi précieuses que soient les solutions Quest utilisées par la banque, l'ingénieur d'infrastructure senior souligne sans hésiter que la relation avec le fournisseur est tout aussi cruciale. « Très peu de fournisseurs présentent la maturité et les capacités de Quest », note-t-il. « Nous apprécions particulièrement la solide expérience et les connaissances approfondies de Quest Professional Services. Nos équipes internes adoptent une approche très pratique et nous comptons sur les experts de Quest pour nous conseiller sur l'optimisation de nos processus. Ils nous aident à comprendre les bonnes pratiques et à utiliser les produits Quest le plus efficacement possible dans notre environnement. »

« Nous avions l'habitude d'effectuer des audits avec des outils natifs. C'était un processus assez pénible, car il était difficile d'interpréter les logs complexes et d'identifier les menaces. Change Auditor fournit une fonctionnalité de log très enrichie qui nous est vraiment bénéfique. Nous avons facilement personnalisé certains des rapports intégrés, et maintenant nos équipes InfoSec peuvent repérer et enquêter avec précision sur les activités hors bande. »

Ingénieur d'infrastructure senior
Grande banque internationale

L'équipe de support est tout aussi expérimentée et serviable. « En fait, nous n'avons pas eu beaucoup de demandes de support au fil des ans, car les solutions fonctionnent vraiment bien », remarque l'ingénieur d'infrastructure senior. « Mais lorsque nous la contactons, l'équipe de support est très réactive et résout généralement le problème rapidement. Et si nous découvrons un bogue, le problème est porté à la connaissance des responsables appropriés, ce que nous apprécions. »

En fait, la banque souhaite étoffer son portefeuille de solutions Quest. En particulier, elle cherche activement à protéger ses assets Tiers Zero avec Security Guardian et SpecterOps BloodHound Enterprise.

PRODUITS ET SERVICES

Produits

- Change Auditor
- Enterprise Reporter Suite
- GPOADmin
- InTrust
- On Demand Audit
- On Demand Migration
- On Demand Recovery
- 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-Anonymous-KA-FR-WL-90351