Weltweit tätige Bank sorgt für Sicherheit, Cyber Resilience und Compliance

Die in Kanada ansässige Bank setzt auf eine integrierte Suite von Quest Lösungen – und auf die Partnerschaft mit den weltweit führenden Experten für Active Directory.

Land: **Kanada**

Mitarbeiter: **60.000**

Branche: **Finanzen**

In Branchen wie dem Bankwesen ist die Sicherheit und Verfügbarkeit von Active Directory besonders wichtig.

Kein Unternehmen möchte eine Sicherheitsverletzung oder einen Serviceausfall erleiden, doch für stark regulierte und kritische Sektoren wie den Finanzsektor können solche Ereignisse besonders verheerend sein. Aus diesem Grund verlässt sich eine große kanadische Bank mit Niederlassungen in Nordamerika, der Karibik, Europa und dem Asien-Pazifik-Raum seit Langem auf eine Reihe von Lösungen von Quest, um ihr hybrides IT-Ökosystem zu sichern, zu überwachen und eine schnelle Wiederherstellung zu gewährleisten.

Die Bank verfügt über eine einzige Active Directory (AD)-Produktionsstruktur mit sieben Domänen und einem Entra ID-Produktions-Tenant. Sie sicher und verfügbar zu halten, hat höchste Priorität. „Wenn bei Einzelhändlern, Social-Media-Unternehmen und vielen anderen Dienstanbietern ein Ausfall auftritt, sind die Kunden verärgert und einige von ihnen wechseln vielleicht sogar zu einem anderen Anbieter“, erklärt ein leitender Infrastrukturingenieur der Bank. „Aber das Bankwesen ist noch sensibler, denn dort befindet sich Ihr Geld. Sollte unser Betrieb für längere Zeit ausfallen, würde dies zu

Herausforderungen

Eine große internationale Bank muss die Sicherheit und Cyber Resilience ihres großen hybriden IT-Ökosystems gewährleisten. Dabei muss sie auch die Compliance mit der wachsenden Zahl immer strengerer Vorschriften in den zahlreichen Regionen, in denen sie tätig ist, sicherstellen und nachweisen.

Lösung

Seit fast zwei Jahrzehnten verlässt sich die Bank auf die Lösungen und das Know-how von Quest. Bei der Migration von Workloads in die Cloud konnte Quest integrierte Lösungen bieten, die für einheitliche Transparenz und Kontrolle über die gesamte IT-Umgebung hinweg sorgen. Darüber hinaus bietet das Quest Professional Services-Team fundierte Beratung und Wissenstransfer, um die Bank in die Lage zu versetzen, Sicherheit, Cyber Resilience und Compliance proaktiv zu optimieren.

Vorteile

- Stärkere Sicherheit durch robuste Audits und Änderungskontrolle
- Verbesserte Cyber Resilience mit zuverlässiger Sicherung und schneller Wiederherstellung der Hybrid-Umgebung
- Fähigkeit, Compliance zu gewährleisten und nachzuweisen
- Sorglosigkeit, die sich aus einer langfristigen Beziehung mit einem vertrauenswürdigen Partner und Berater ergibt

Umsatzeinbußen führen und hätte auch regulatorische Auswirkungen, da wir Auflagen aus mehreren Regionen erfüllen müssen, darunter nicht nur Kanada, sondern auch die USA, die EU und andere. Aber noch wichtiger wäre der schwere und dauerhafte Schaden für den Ruf der Bank. Daher sind Active Directory-Sicherheit und Cyber Resilience von entscheidender Bedeutung für unser Unternehmen."

Die Bank verlässt sich seit fast zwei Jahrzehnten auf die AD-Sicherheits- und Wiederherstellungslösungen von Quest.

Die Bank arbeitet bereits seit fast zwei Jahrzehnten mit Quest zusammen. „Wir haben mit Recovery Manager for Active Directory begonnen, gefolgt von InTrust und Active Roles, und den Mehrwert schnell erkannt", sagt der Senior Infrastructure Engineer. „Als Change Auditor auf den Markt kam, erkannten wir die Vorteile sofort und haben es eingeführt. Obwohl wir den Markt über die Jahre hinweg genau beobachtet haben, haben wir keinen anderen Anbieter gefunden, der Produkte mit einer so großen Bandbreite an Funktionen anbietet – welche auch noch ergänzend integrierbar sind, was den Mehrwert der gesamten Lösung erheblich steigert."

Darüber hinaus stellte die Bank fest, dass die Quest Produkte im Zuge des technologischen Fortschritts und des Wandels der geschäftlichen Gegebenheiten ständig weiterentwickelt wurden, um stets auf dem neuesten Stand zu bleiben. „Fast alles, was wir vor Ort machen, wird auf den Entra ID-Bereich ausgeweitet", fügt er hinzu. „Quest hat uns SaaS-Lösungen zur Verfügung gestellt, die uns Transparenz und Kontrolle über die gesamte Hybrid-Umgebung hinweg bieten, und diese Tools haben sich schnell in unser Portfolio eingefügt. Wir haben festgestellt, dass der Mehrwert, den wir aus dem Quest Lösungspaket ziehen, für uns im Vergleich zu anderen Tools auf dem Markt viel attraktiver ist."

Robuste Audits und Änderungsmanagement sorgen für hohe Sicherheit.

Cybersecurity-Experten empfehlen Unternehmen heute, stets davon auszugehen, dass Sicherheitsverletzungen vorkommen können. Daher ist es wichtig, eine umfassende Prüfung und Analyse der Aktivitäten in der gesamten Umgebung durchzuführen. Mit den Lösungen von Quest verfügt das IT-Team der Bank über die nötige Transparenz und Kontrolle, um kostspielige Sicherheitsverletzungen und Ausfallzeiten zu verhindern.

„Früher haben wir Audits mit nativen Tools durchgeführt und fanden das ziemlich mühsam. Es war schwierig, die kryptischen Protokolle zu interpretieren und Bedrohungen zu identifizieren", erinnert sich der Senior Infrastructure Engineer. „Change Auditor bietet uns eine hochgradig angereicherte Protokollierung, die für uns wirklich von Nutzen ist. Wir haben einige der integrierten Berichte problemlos angepasst und unsere InfoSec-Teams können nun Aktivitäten außerhalb des Netzwerks genau erkennen und untersuchen. Wir lassen die Berichte sogar automatisch nach dem von uns gewählten Zeitplan erstellen und an ein bestimmtes Postfach senden."

Das Bankteam nutzt ebenfalls Change Auditor, um Abweichungen in den Active Directory-Konfigurationen zu erkennen, die Sicherheitslücken öffnen oder die Verfügbarkeit von Diensten gefährden könnten. „Im Laufe der Jahre neigt jedes Active Directory dazu, überschüssige Zugriffsrechte, veraltete Identitäten und andere Probleme anzusammeln, und unseres war da keine Ausnahme", bemerkt der Senior Infrastructure Engineer. „Dank Change Auditor konnten wir gemeinsam mit dem InfoSec-Team das Verzeichnis bereinigen, um es sicherer und einfacher verwaltbar zu machen."

> **Obwohl wir den Markt über die Jahre hinweg genau beobachtet haben, haben wir keinen anderen Anbieter gefunden, der Produkte mit einer so großen Bandbreite an Funktionen anbietet – und die auch noch nebeneinander bestehen und untereinander integriert sind, was den Mehrwert der gesamten Lösung erheblich steigert.**
>
> *Senior Infrastructure Engineer*
> *Große internationale Bank*

Ein weiterer Vorteil von Change Auditor ist die Möglichkeit, Änderungen an leistungsstarken Sicherheitsgruppen, kritischen Gruppenrichtlinienobjekten und mehr zu blockieren. „Mit Change Auditor haben wir viele Active Directory-Objekte und -Attribute in Schutzrichtlinien aufgenommen, die verhindern, dass sie versehentlich oder böswillig geändert werden“, erklärt der Senior Infrastructure Engineer. „Dieser Ansatz hat umfangreichen Tests standgehalten: Wir führen regelmäßig Red-Team-Übungen durch, bei denen versucht wird, in die Umgebung einzudringen, und Change Auditor war zur Stelle, um den Einbruch zu verhindern.“

Darüber hinaus bietet das Quest Portfolio der Bank Transparenz und Kontrolle über die gesamte Hybrid-Umgebung hinweg. „Da Change Auditor in On Demand Audit integriert ist, verfügen wir über ein konsolidiertes Berichtswesen“, sagt der Senior Infrastructure Engineer. „Die Möglichkeit, Änderungen sowohl vor Ort als auch in Entra ID zu verfolgen, ist für uns ein enormer Mehrwert. Wenn zum Beispiel ein Team privilegierten Zugriff auf bestimmte Daten oder Anwendungen beantragt, können wir seine früheren Aktivitäten gründlich überprüfen. Wir können ihnen zeigen, welche Änderungen sie über einen langen Zeitraum hinweg vorgenommen haben, und beweisen, dass sie eigentlich keinen ständigen privilegierten Zugriff benötigen. So können wir unsere Angriffsfläche minimieren.“

Schnelle und zuverlässige Disaster Recovery sorgt für Cyber Resilience.

Die Bank ist sich bewusst, dass selbst die umfassendste Strategie zur Erkennung von und Reaktion auf Identitätsbedrohungen nicht alle negativen Ereignisse verhindern kann. Dementsprechend hat sie eine robuste Disaster Recovery-Strategie entwickelt, die Recovery Manager for Active Directory integriert mit On Demand Recovery verwendet.

Die Führungsspitze der Bank weiß, wie wichtig die Identitätsplattformen Active Directory und Entra ID für das Unternehmen sind. Der Senior Infrastructure Engineer erinnert sich an einen Vortrag über den berüchtigten NotPetya-Angriff. Das Hauptziel war zwar die Ukraine, aber Unternehmen auf der ganzen Welt erlitten enorme Schäden. Der Schifffahrtsriese Maersk verfügte beispielsweise über keine Sicherungen seines Active Directory und musste daher einen Domänencontroller, der glücklicherweise während des Angriffs offline war, mühsam von Ghana nach Großbritannien shutteln. Maersk schätzt, dass die Wiederherstellung 250 bis 300 Millionen US-Dollar gekostet hat, obwohl Insider vermuten, dass die Summe in Wirklichkeit viel höher war. Noch überzeugender für die Führungskräfte bei dem Vortag mag die Tatsache gewesen sein, dass es nur 45 Sekunden dauerte, bis NotPetya das Netzwerk einer großen Bank zum Absturz brachte. „Wir mussten unserem CEO nicht erklären, wie wichtig unsere Identitätsplattformen sind“, sagt der Senior Infrastructure Engineer. „Er war bereits im Bilde. Die Disaster Recovery von AD und Entra ID wurde auf das dem Unternehmen bekannte Risiko abgestimmt.“

Mit den Lösungen von Quest hat die Bank eine umfassende Strategie zur Notfallwiederherstellung implementiert, die ein Paar synchronisierte Recovery Manager-Server in jedem Rechenzentrum umfasst. „Jeder Server verfügt über eine vollständige, unveränderliche Sicherung der gesamten Umgebung. Wir brauchen also nicht alle vier Server, um eine Katastrophe zu überleben, sondern nur einen. Außerdem haben wir zwei Recovery Manager-Server in Azure mit eigenen unveränderlichen Sicherungen, was zusätzliche Redundanz bietet.“

> **Recovery Manager for Active Directory ist jedem anderen Produkt auf dem Markt haushoch überlegen. Aber Sie dürfen nicht nur für Ihr lokales AD planen, sondern müssen auch Entra ID einbeziehen. Zusammen bieten Recovery Manager und On Demand Recovery eine End-to-End-Wiederherstellung der gesamten Identitätsplattform, einschließlich Wiederherstellung bestimmter Objekte und Notfallwiederherstellung.**
>
> *Senior Infrastructure Engineer*
> *Große internationale Bank*

Die Bank testet ihren Notfallwiederherstellungsplan regelmäßig, und die Ergebnisse sprechen für sich. „Bei einem Cybersecurity-Vorfall, der unsere Gesamtstruktur zerstört, wissen wir, dass wir diese innerhalb von vier Stunden wiederherstellen können“, berichtet der Senior Infrastructure Engineer. „Recovery Manager entfernt die Definitionen der mehr als 70 Domänencontroller in unserer Produktionsumgebung und erstellt mit einer unserer unveränderlichen Sicherungen eine unberührte neue Gesamtstruktur. Und dank der Integration mit On Demand Recovery können wir nicht nur AD, sondern auch Entra ID wiederherstellen.“

Sicherheit und Cyber Resilience sind unerlässliche Voraussetzungen für Compliance.

Finanzinstitute unterliegen hohen regulatorischen Anforderungen und einer strengen Aufsicht, und Banken mit internationaler Präsenz müssen Vorschriften aus mehreren Rechtsordnungen einhalten. Die Lösungen von Quest können diesen Compliance-Aufwand drastisch verringern.

„Change Auditor erstellt automatisch die Berichte, die wir brauchen, und sendet sie an die entsprechenden Teams“, erklärt der Senior Infrastructure Engineer. „Gleichzeitig können wir mit Recovery Manager und On Demand Recovery die strengsten Anforderungen an Disaster Recovery erfüllen. In der Tat haben wir angesichts der Tiefe der Berichterstattung und der Leistungsfähigkeit der Werkzeuge keinerlei Probleme, die Vorschriften zu erfüllen, denen wir unterliegen. Außerdem sind wir gut aufgestellt, um alle neuen Anforderungen, die auf uns zukommen, zu erfüllen.“

Eine integrierte Suite von Lösungen ist für die heutigen hybriden IT-Ökosysteme von entscheidender Bedeutung.

Eine Sammlung unterschiedlicher Einzellösungen ist heute kein effektiver Ansatz für Cybersicherheit und Cyber Resilience mehr. Unternehmen benötigen integrierte Lösungen, die einen einheitlichen Ansatz für die gesamte hybride Umgebung ermöglichen. Der Senior Infrastructure Engineer argumentiert, dass dies ein entscheidender Vorteil der Investition der Bank in Quest Lösungen ist.

„Wenn Sie sich das umfangreiche Portfolio der Quest Lösungen ansehen und verstehen, wie sie nahtlos ineinander übergehen und sich gegenseitig ergänzen, erkennen Sie ihren Mehrwert“, sagt er. „Recovery Manager for Active Directory zum Beispiel ist jedem anderen Produkt auf dem Markt haushoch überlegen. Aber Sie dürfen nicht nur für Ihr lokales AD planen, sondern müssen auch Entra ID einbeziehen. Zusammen bieten Recovery Manager und On Demand Recovery eine End-to-End-Wiederherstellung der gesamten Identitätsplattform, einschließlich Wiederherstellung bestimmter Objekte und Notfallwiederherstellung.“

> **Es gibt nur sehr wenige Anbieter, die so ausgereift und leistungsfähig sind wie Quest. Wir schätzen besonders die umfassende Erfahrung und das Wissen von Quest Professional Services. Unsere internen Teams sind sehr praxisorientiert und wir verlassen uns auf die Experten von Quest, die uns bei der Optimierung unserer Prozesse beraten. Sie helfen uns, die besten Praktiken zu verstehen und die Quest Produkte in unserer Umgebung möglichst effektiv einzusetzen.**
>
> *Senior Infrastructure Engineer*
> *Große internationale Bank*

Ein erfahrener und vertrauenswürdiger Partner ist genauso wichtig wie ein gutes Softwareprodukt.

So sehr die Bank die Lösungen von Quest auch schätzt, die sie einsetzt, der Senior Infrastructure Engineer betont, dass die Beziehung zum Anbieter ebenso wichtig ist. „Es gibt nur sehr wenige Anbieter, die so ausgereift und leistungsfähig sind wie Quest“, stellt er fest. „Wir schätzen besonders die umfassende Erfahrung und das Wissen von Quest Professional Services. Unsere internen Teams sind sehr praxisorientiert und wir verlassen uns auf die Experten von Quest, die uns bei der Optimierung unserer Prozesse beraten. Sie helfen uns, die besten Praktiken zu verstehen und die Quest Produkte in unserer Umgebung möglichst effektiv einzusetzen.“

> Früher haben wir Audits mit nativen Tools durchgeführt und fanden das ziemlich mühsam, weil es schwierig war, die kryptischen Protokolle zu interpretieren und Bedrohungen zu identifizieren. Change Auditor bietet uns eine hochgradig angereicherte Protokollierung, die für uns wirklich von Nutzen ist. Wir haben einige der integrierten Berichte problemlos angepasst und unsere InfoSec-Teams können nun Aktivitäten außerhalb des Netzwerks genau erkennen und untersuchen.

Senior Infrastructure Engineer
Große internationale Bank

Das Support-Team ist ebenso erfahren und hilfsbereit. „Wir hatten im Laufe der Jahre eigentlich nicht viele Support-Einsätze, weil die Lösungen so gut funktionieren“, bemerkt der Senior Infrastructure Engineer. „Aber wenn wir uns an das Support-Team wenden, erhalten wir schon nach kurzer Zeit eine Antwort und das Problem ist meist schnell gelöst. Und wenn wir auf einen Produktfehler stoßen, wird das Problem an die zuständigen Führungskräfte weitergeleitet, was wir sehr schätzen.“

In der Tat ist die Bank daran interessiert, ihr Portfolio an Quest Lösungen zu erweitern. Insbesondere sucht sie aktiv nach Möglichkeiten, ihre Tier-Zero-Assets mit Security Guardian und SpecterOps BloodHound Enterprise zu schützen.

PRODUKTE UND SERVICES

Produkte

- 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

Lösungen

- Verwaltung von Microsoft-Plattformen

Über Quest

Quest stellt Softwarelösungen bereit, mit denen das volle Potenzial neuer Technologien in einer zunehmend komplexen IT-Landschaft ausgeschöpft werden kann. Von der Datenbank- und Systemverwaltung über die Migration zu und Verwaltung von Active Directory und Microsoft 365 bis hin zur Cyber Resilience: Quest hilft Kunden, bereits heute ihre IT-Herausforderungen von morgen zu bewältigen. Quest Software. Where Next Meets Now.

CaseStudy-Anonymous-KA-DE-WL-90351