Case Study

QOSTODIAN PRIME™

# Desjardins Gets Even More Precise at Threat-Hunting

"Other tools follow the movement of files. With Prime, I can see the origin of a specific data element and see how it moved across people over time—without doing anything manually. **There's no one else on the market that works this way."**

Desjardins®

**Frederic Michaud,**

Principal Director, Evolution of Cybersecurity Threats

**Industry**

Financial Services, Banking

**Use Case**

Insider Breach Prevention

**Product**

QOSTODIAN PRIME™

**Desjardins Group is the leading cooperative financial group in Canada and the 5th largest in the world. Desjardins offers a full range of products and services to individuals and businesses through its extensive distribution network, online platforms and subsidiaries.**

## Pain

Ranked one of the safest banks in North America by Global Finance magazine, customer trust is the lifeblood of Desjardins Group. Powered by top-notch internal talent and leading cybersecurity solutions, Desjardins has excelled at meeting Canadian legislative and compliance regulations, which are generally considered to be the gold standard worldwide.

Over the last four years, and accelerated by the pandemic, Desjardins invested heavily in digitizing their product offerings. Simultaneously, Desjardin's security team ramped up a proactive strategy to safeguard sensitive data across all technology partners and platforms.

Frederic Michaud, Principal Director at Desjadins in the Cybersecurity Threats division, vets, implements, and manages tools, processes, and analytics to prevent insider threats and cyber fraud. According to Frederic, not all tools are created equal:

> **"The main problem with most software is that they focus on files, work stations, and servers. But, when you perform insider threat surveillance, you care about the users, about people's behavior."**

Working with other tools meant Frederic's team still needed to perform significant manual analysis. Through phone calls, office visits, and follow-ups, an internal team created their own triage framework and worked backwards to determine the flow of data across nearly 50,000 employees. In an organization as massive as Desjardins, tracking down this information and determining how data propagated was no easy feat.

**In addition to time-consuming investigations, Frederic and his team lacked clear indicators of risk levels for each item returned in scanning results. This made it even more difficult to quickly weed out false positives.**

## Solution

In an effort to expedite investigations, Frederic sought a solution that could help his security analysts:

- More precisely "threat hunt," reducing noise and triaging according to risk
- Track sensitive information across people
- See actionable results in an operational manner that saves time

## Qostodian Prime™ by the numbers

| | Desjardins' previous tool | Prime |
|---|---|---|
| **Risk** | Limited views of risk | Quantified risk levels<br>Monitoring of high risk employees |
| **Tracking** | Files | User behavior<br>Data elements |
| **Investigation** | Time consuming manual analysis | Automated view of data movement across people over time |

After evaluating multiple vendors, he noticed something remarkable: only one solution on the market–Qostodian Prime–tracked data elements. All competing solutions track files. Yet files, or the container for the data, change all of the time.

With Prime, Frederic now runs searches for data elements. He can see every employee in the organization who touched it and how it moved across people over time. Says Frederic:

> **"I can trace specific data elements back to the first person who made a mistake. I can see where it got out an environment, and how it moved across employees, without doing anything manually. Every time we find something, it's really easy to understand where it came from."**

When running keyword-specific searches, Frederic and his team leverage Prime's "hashing" feature, enabling them to search for sensitive information without storing it in a database.

Frederic also found that despite scanning massive documents across workstations, and all file types across workstations, email, One Drive, and more, Prime had the horsepower to get the job done 20x faster than competing technologies.

## Results

Prime provides Frederic and his team full contextualization of scanning results. Armed with reports that track sensitive information across people and contain clear next steps, the team reacts with speed and confidence. Manual time wasters have become a thing of the past.

Frederics's team of security analysts now threat-hunt more effectively, triaging with precision to address the biggest risks. He adds:

> **"I can figure out in a few seconds whether something is an issue or not. Prime empowers us to prioritize the most malicious threats to the least with confidence. We find that greater productivity and efficiency from my team equals better security."**

Prime's reports also help management keep an eye on the big picture. "In addition to the granular data, which allows us to monitor at-risk employees and ensure employees respect policies and procedures, I can also step back and evaluate the macro-level insights to manage risk effectively," says Frederic.