

# Putting the Brakes on Insider Threats

Automotive SaaS Provider CCC Information Services Uses ObserveIT for Proactive Detection and Cultural Shifts



## THE CHALLENGE

- Handles sensitive enterprise and consumer data
- Employs a 1,700 people plus many outside contractors, who must be able to transact and work securely
- Needs to be able to monitor user and data activity and conduct rapid investigations

## THE SOLUTION

- ObserveIT Insider Threat Management Platform

## THE RESULTS

- Responded and took proactive action against Insider Threats
- Supported investigations with a real-time record of user behavior
- Monitored patterns of behavior and identified potential risks
- Decreased time spent investigating Insider Threats
- Decreased mean time to detection

## The Company

Founded in 1980 as the Certified Collateral Corporation, the company now known as CCC is a leading software as a service (SaaS) provider to automotive-related industries. Through its CCC ONE™ platform, the company services insurance providers, auto manufacturers, collision repairers, part suppliers, and others with data, tools, and solutions to do business efficiently and to create a better experience for end-users. CCC's customers include brands like Nissan North America, BMW North America, and more.

CCC handles sensitive enterprise and consumer data around car owners, rentals, auto claims and collisions. They also employ almost 1,700 people and work with many outside companies, all of whom need to transact and work in a secure environment.

## The Challenge

In 2016, something strange happened... After the insider threat was resolved, Brouwer and his team were determined to not only understand how the incident occurred, but to put a system in place to better detect, investigate, and respond to similar incidents in the future.

To support future investigations and mitigate their insider threat risk, Brouwer began to look for solutions to monitor what was happening within CCC's firewalls and on their workstations and to gather as much context as possible in a timely manner when incident investigations are required.

Brouwer assessed other types of tools to address his challenges. However, these tools required significant administration and did not reach the level of accuracy CCC required.

"Security is not something we can do solely in a technological way. It's something that helps me grow my organization and change my organization." Daryl Brouwer, chief information security officer, CCC Information Services

The company required a solution that would monitor and record activity in a user's environment, send alerts for out-of-policy behavior, and integrate with other security measures already in place. But, perhaps most importantly, they needed a tool that would support the security-conscious culture they were working to build at CCC.

“ObserveIT has reduced the amount of time we spend on things dramatically. Something that would take 6-7 hours, we now do in 10-15 minutes. It’s a real advantage from a staffing and meantime-to-detection standpoint. It is key for investigations.”

**Daryl Brouwer**, Chief Information Security Officer, CCC Information Services

## The Solution

CCC began using ObserveIT in 2016. With ObserveIT, CCC is able to both respond to and take proactive action against insider threats. When an incident occurs, Brouwer’s team supports investigations with a real-time record of user behavior. On the proactive side, they are able to monitor patterns of behavior and curtail potential risks before an actual incident occurs.

In one case, Brouwer’s team discovered an employee engaging in behavior that was contrary to CCC’s security policies and culture; the company had a discussion with the employee, and the situation was rectified. CCC is also able to monitor potentially risky trends in user behavior, such as the use of USB keys or cloud solutions, and take corrective measures.

“ObserveIT has a unique perspective,” notes Brouwer. “The company looks at how it can become a part of my business, not just a technological tool. When looking at the future, it’s about how we integrate ObserveIT with people and process.”

## The Results

### Hitting the gas on security

ObserveIT has decreased the amount of time CCC’s security team spends investigating insider threat incidents. Before using ObserveIT, the team often spent six to seven hours researching whether a situation required further action.

That type of investigation now takes 10 to 15 minutes. In addition, the company has seen dramatically lower mean time to detection.

“It’s a real advantage from a staffing and mean time-to-detection standpoint,” says Brouwer. “It is key for us going forward as part of investigations.”

CCC is also able to use data from ObserveIT to enrich other network or systems data to develop a single source of truth and better understand the context around any incidents that arise.

### Driving cross-team collaboration

Beyond the security team’s concerns with preventing data loss and other insider threat risks, ObserveIT provides valuable and easy to decipher context for other functions within the company, including legal and HR.

“Every department has different requirements when it comes to either addressing problems or looking at security incidents,” Brouwer explains. “From a legal perspective, they want a certain level of evidence to support a legal case or criminal investigation. HR needs to satisfy employment law. On the security side, we’re always looking for data leak prevention, exfiltration of data, or things that will impact brand or reputation.”

## LEARN MORE

For more information, visit [observeit.com](https://observeit.com).

### ABOUT OBSERVEIT

ObserveIT, a division of Proofpoint, is the leading Insider Threat Management (ITM) solution with more than 1200 customers globally. ObserveIT helps organizations protect against data loss, malicious acts, and brand damage involving insiders acting maliciously, negligently, or unknowingly.

The ObserveIT platform correlates activity and data movement, empowering security teams to identify user risk, detect insider-led data breaches, and accelerate security incident response. Leveraging a powerful contextual intelligence engine and a library of over 400 threat templates drawn from customers and leading cybersecurity frameworks, ObserveIT delivers rapid time to value and proven capability to streamline insider threat programs.

©ObserveIT, Inc. ObserveIT is a trademark of Proofpoint, Inc. in the United States and other countries. All other trademarks contained herein are property of their respective owners.