proofpoint.

CUSTOMER STORY

Putting the Brakes on Insider Threats

CCC Information Services Uses Proofpoint Insider Threat Management (ITM) for Proactive Detection and Cultural Shifts

THE CHALLENGE

- Handle sensitive enterprise and consumer data
- Enable 1,700 employees and contractors to transact and work securely
- Monitor user and data activity and conduct rapid investigations

THE SOLUTION

- Proofpoint Insider Threat Management

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

Certified Collateral Corporation (CCC)

Founded in 1980, CCC is a leading software as a service (SaaS) provider to automotive-related industries. Through its CCC ONE™ platform, it provides companies with data, tools and solutions to do business. Some of CCC's clients include insurance providers, auto manufacturers, collision repairers, part suppliers and others. All of their clients trust the CCC with their sensitive information like data around car owners, rentals, auto claims and collisions.

The Challenge

In 2016, the company was faced with an insider threat. Upon resolving it, Daryl Brouwer, Chief Information Security Officer of CCC Information Services, knew he had to have a better system in place to respond to such incidents. He 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. He wanted 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.

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, it needed a tool that would support the security-conscious culture it was working to build at CCC.

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

> "ITM (formerly ObserveIT) has reduced the amount of time we spend on things dramatically. Something that would take six to seven 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

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.

CCC 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. Also, it needed a tool that would support the security-conscious culture it was working to build at CCC.

The Solution

CCC began using ITM in 2016. With ITM, 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 behaving in a way 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.

"ITM 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 ITM with people and process."

The Results

Hitting the gas on security

ITM has decreased the amount of time CCC's security team spends investigating insider threat incidents. Before using ITM, 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 ITM 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, ITM 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 **proofpoint.com**.