HELPING SIRIUS XM PROTECT THEIR SALESFORCE CLOUD

Cloud Protection for Salesforce Case Study

F-Secure

Company name:
SiriusXM

Industry:
Entertainment

Country:
USA

Solutions from F-Secure:
F-Secure Cloud Protection
for Salesforce

About SiriusXM

SiriusXM is best known as one of America's most popular digital radio stations, with approximately 35 million subscribers. After its merger with the Pandora music streaming service in 2019, SiriusXM grew to be North America's largest audio entertainment company.

But what most fans don't realize is that behind the scenes, the company is also a leader in the connected car space. SiriusXM Connected Vehicle Services provides a range of digital services including entertainment and navigation, but its main value proposition is safety and security. The company assists car manufacturers with telematics and services such as car unlocking. Its RapidSOS emergency response platform for example automatically shares vehicle and crash data with 911 responders following a crash to support rescue and recovery efforts.

More than 12 million active vehicles currently use SiriusXM Connected Vehicle Services. The company was named 2020 Company of the Year in the Telematics Industry by Frost & Sullivan for its new CAN+ safety solution, which adds multiple new connected features.

Digitalizing to support the second-hand car market

One persistent challenge for SiriusXM was supporting the increasingly large American pre-owned vehicle market. Individuals purchasing used cars with connected capabilities would need to call their manufacturers to have them activated, and then be passed on to SiriusXM's contact center.

Naman Shah, Senior Director of Product Management at Sirius XM, comments: "The challenge was that everything around vehicles needs to have airtight security. If the process is too loose, someone could just go and pluck the vehicle registration number from the dashboard, call remote services, and have it remotely unlocked. So, it's essential to have strict systems around authentication."

"Unfortunately, our processes were also cumbersome and falling rapidly behind in a digital age. Customers needed to provide proof of ownership such as a title, but the only way to do this was to contact our call center, fax over the documents, then call back to confirm receipt and complete the enrolment. This was convoluted and frankly terrible from a customer experience perspective. We were certainly shedding potential customers each time. How many people even know where to find a fax machine?"

An unexpected vulnerability

To address this challenge, SiriusXM wanted to modernize the process and establish a streamlined service that enables second-hand vehicle customers to upload documents online quickly and easily.

In addition to improving customer acquisition and retention, a more efficient digital method would also free up call center agents to focus on more high-value interactions, rather than purely transactional processes. To accomplish this, SiriusXM created a new set-up that allowed customers to directly upload their documentation into the company's CRM system via Salesforce Service Cloud.

However, the plan hit a late-stage roadblock due to an unexpected security problem. Although every care was taken to properly secure customer details, the system itself introduced a potentially serious vulnerability.

"We had our security team as part of this project from day one to protect customer data," Naman explained. "But we didn't fully consider the security impact of the upload setup. Customers are uploading their documents directly into our Salesforce – but what happens if someone uploads a malicious file, either by accident or as an intentional cyber-attack? Someone could easily target our CRM directly with a ransomware attack; this is a very dangerous flaw and we couldn't proceed without a solution."

To solve this problem and get the project back on track, SiriusXM needed a security solution that rapidly and reliably scans documents submitted to Salesforce before they were uploaded into the system.

Crucially, this process could not disrupt the central goal of an efficient, streamlined experience for customers and contact center agents. With the project deadline in sight, it also had to be accomplished without months of development time and a large technical debt that would eat into the project's return on investment. SiriusXM's technical team didn't have the bandwidth to take on significant additional engineering work.

How F-Secure got things back on track

SiriusXM was introduced to F-Secure in January 2021 through its Salesforce account manager, who was helping the company implement the new Salesforce Service Cloud. They recommended F-Secure Cloud Protection for Salesforce (CPSF) because it is the only content security solution built in cooperation with Salesforce. After a demo, SiriusXM swiftly decided to go ahead with CPSF, and no other solutions were considered. F-Secure's reputation in the security industry and relationship with

Salesforce received immediate buy-in from SiriusXM's security team.

F-Secure met SiriusXM's core needs of a solution that could be implemented swiftly without incurring unnecessary expense. CPSF was implemented on a usage-based license covering up to 50,000 scans per year.

Naman commented: "It was a pleasant surprise to find there was no additional support needed after the initial implementation and configuration. F-Secure's reliable plug-and-play approach was exactly what we needed."

He added: "It was also a relief to know that F-Secure are specialists and would take care of any issues in getting it running smoothly, so our technical team could focus on the rest of the project."

With F-Secure in place, SiriusXM could safely proceed with launching its new process. CPSF scans all incoming documents for signs of malicious code or URLs, with F-Secure's threat intelligence ensuring that even the most recent threats will be caught and blocked.

Suspicious documents are quarantined and flagged for the SiriusXM team to assess. Agents can then reach out to customers and explain that there was an issue. Meanwhile, safe documents will rapidly pass through the system without delay.

"The upload issue only came to light at the 11th hour of the project, so speed was of the essence for us," Naman concluded. "But even if we had been aware of this issue from day one, F-Secure would still have been the ideal choice for us and we wouldn't do anything differently regardless of time or budget."

Scan all files, URLs and emails for malware
in Salesforce cloud environments.

Find out more

ABOUT F-SECURE

Nobody has better visibility into real-life cyber attacks than F-Secure. We're closing the gap between detection and response, utilizing the unmatched threat intelligence of hundreds of our industry's best technical consultants, millions of devices running our award-winning software, and ceaseless innovations in artificial intelligence. Top banks, airlines, and enterprises trust our commitment to beating the world's most potent threats.

Together with our network of the top channel partners and over 200 service providers, we're on a mission to make sure everyone has the enterprise-grade cyber security we all need. Founded in 1988, F-Secure is listed on the NASDAQ OMX Helsinki Ltd.

f-secure.com/business | twitter.com/fsecure | linkedin.com/f-secure

F-Secure