Popular International Home Improvement Chain Accelerates Digital Transformation and Automates Threat Detection and Response

10 million Customers
in the database protected

9,000 Connected
and secured mobile phones

250 Locations
with IT, IoT, and OT integrated into one secure platform

Industry

- Omnichannel retail

Environment

- 55,000 devices across IT, IoT, and OT environments
- 200 stores and approximately 45 warehouses
- 25,000 employees

Challenge

- Shadow IT
- Lack of visibility
- Protecting the personal information of over 10 million customers in the database
- Integrating a large ecosystem of devices and IT into one system
- High turnover of level-one cybersecurity staff

"With Forescout we can put cybersecurity control at the very beginning, not like the topping of ice cream at the end."

Gabriel Moliné
CISO, Leroy Merlin Spain

Overview

Leroy Merlin is an international home improvement retailer with a presence in Europe and Brazil. The company employs 25,000 people in Spain and has been a cornerstone of the country's economy for 40 years. The CISO for Leroy Merlin Spain, Gabriel Moliné, is taking the company through a digital transformation process in order to better serve its customers through a consistent omnichannel approach. In addition to 200 brick-and-mortar stores, the new integrated approach utilizes phone calls, in-store apps, and e-commerce to provide both goods and services to over 10 million clients in the company database.

Business Challenges

The organization's vast digital landscape includes IT, such as apps that help employees sell products and in-home services, IoT devices such as lighting and smart TVs on the sales floor, and OT that helps the stores and warehouses run, such as pistol scanners, paint-matching technology, and automated cash safes. The company also has more than 9,000 mobile phones on its network.

Shadow IT and a lack of visibility into the network were some of the company's main security challenges. On Moliné's first Friday on the job, the company was hit with a malware attack that forced the stores to close for an entire morning. Part of the problem, he recalled, was that "we didn't know what devices we had on our network, who had access to them, and what kind of access they had to communicate with the rest of the devices inside the store."

Moliné explained that, before Forescout, "We were spending a lot of money on data storage, staff, and training for a traditional security operations center (SOC) that helped with many tasks on a day-to-day basis but had a minimal impact on our level of security." He wanted to automate processes and improve accuracy in order to speed up response time in the event of a cybersecurity breach. This prompted the need for an automated detection and response solution.

Why Forescout?

Although the initial motivation for purchasing the Forescout platform had been to improve device visibility and compliance, Moliné realized the team could greatly expand on their initial use cases. Moliné had the strategic vision to step away from the traditional reactive cybersecurity approach that revolved around consolidating logs in a SIEM or utilizing a SOAR solution, where many alerts turned out to be false

The Forescout Platform

- Forescout TDR
- Forescout eyeSight
- Forescout eyeControl
- Forescout eyeSegment
- Forescout eyeExtend

Use Cases

- Threat detection and response
- Security automation
- Network access control
- IoT and OT security
- Network segmentation
- Device compliance

Results

- Created an integrated, more secure environment across IT, IoT, and OT
- Eliminated Shadow IT
- Protected customer data
- Increased use of automation to reduce time spent on routine cybersecurity tasks
- Lowered costs associated with its SOC
- Reduced level-one support tickets
- Improved retention of talent
- Provided more time for the core team to dedicate to the cloud transformation journey

positives. With Forescout TDR, automation streamlines the analyst function and process, so that only the most actionable, probable threats warranting analyst investigation are delivered in a consolidated dashboard. This greatly speeds up time to remediation.

Moliné takes a systematic, one-step-at-a-time approach to reducing cybersecurity risk. His goal is to avoid incidents happening inside the network in the first place so that limited security resources can be dedicated to increasing "security by default" within the system, and the team can be more "productive by design." With TDR, he noted, he was able to reduce risk associated with system vulnerabilities in his organization.

In a traditional SIEM process, he pointed out, "You spend a lot of time connecting stuff at the very beginning, instead of protecting and defending your infrastructure." Rather, he prefers to integrate solutions one at a time, analyze the results based on standard metrics, and then start the cycle again with new sources. Moliné considers this a key factor in the success they have had.

"Basically, this is a journey. Everybody wants to do automation faster, but many times when you try to go faster, you make mistakes, and this creates risk," he asserted.

Forescout fit the profile of what Moliné was looking for in a solution: it was quick to deploy, capable of integrating with multiple vendors in the organization's ecosystem, and supported his proactive and automated approach towards security without forcing him into one platform. "For me, TDR is something that has to be present in the entire network of devices; everything has to be connected to enable proactive response," asserted Moliné.

Business Impact

The overall impact Forescout has had on Leroy Martin is that it can now be more dedicated to its cloud journey and big picture strategic goals, such as building out its omnichannel capabilities.

"Thanks to Forescout, we can guarantee that Shadow IT is discovered," noted Moliné. This reduces the risk of a cyberattack on unmanaged devices and the operational impact of having to close the stores. It also protects the data of millions of customers.

By utilizing the automation capabilities of Forescout, the organization has reduced the number of level-one support tickets, and consequently reduced its reliance on high-turnover of level-one security talent. "The capability to use automation inside network access control (NAC) is something that brings a lot of value for me," said Moliné. Automation has also allowed the team to dedicate talent resources to more "elevated things," which has improved retention. The dedicated cybersecurity team has gained more time to put toward digital transformation.

Forescout has also given the team the power to resolve the problem of integrating such a large ecosystem of devices and IT into one secure cross-channel platform. Moliné remarked, "With Forescout, we can put cybersecurity control at the very beginning, not like the topping of ice cream at the end."

FORESCOUT®

Forescout Technologies, Inc.
Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591
Learn more at Forescout.com