Customer Success

Specsavers upgrades identity security for unprecedented operational efficiency

Overview

Specsavers is the largest privately-owned optical company in the world, with 2,615 stores across eleven countries in three continents. It serves over 42.9 million customers with optics, audiology, and domiciliary services, and employs more than 41,500 people.

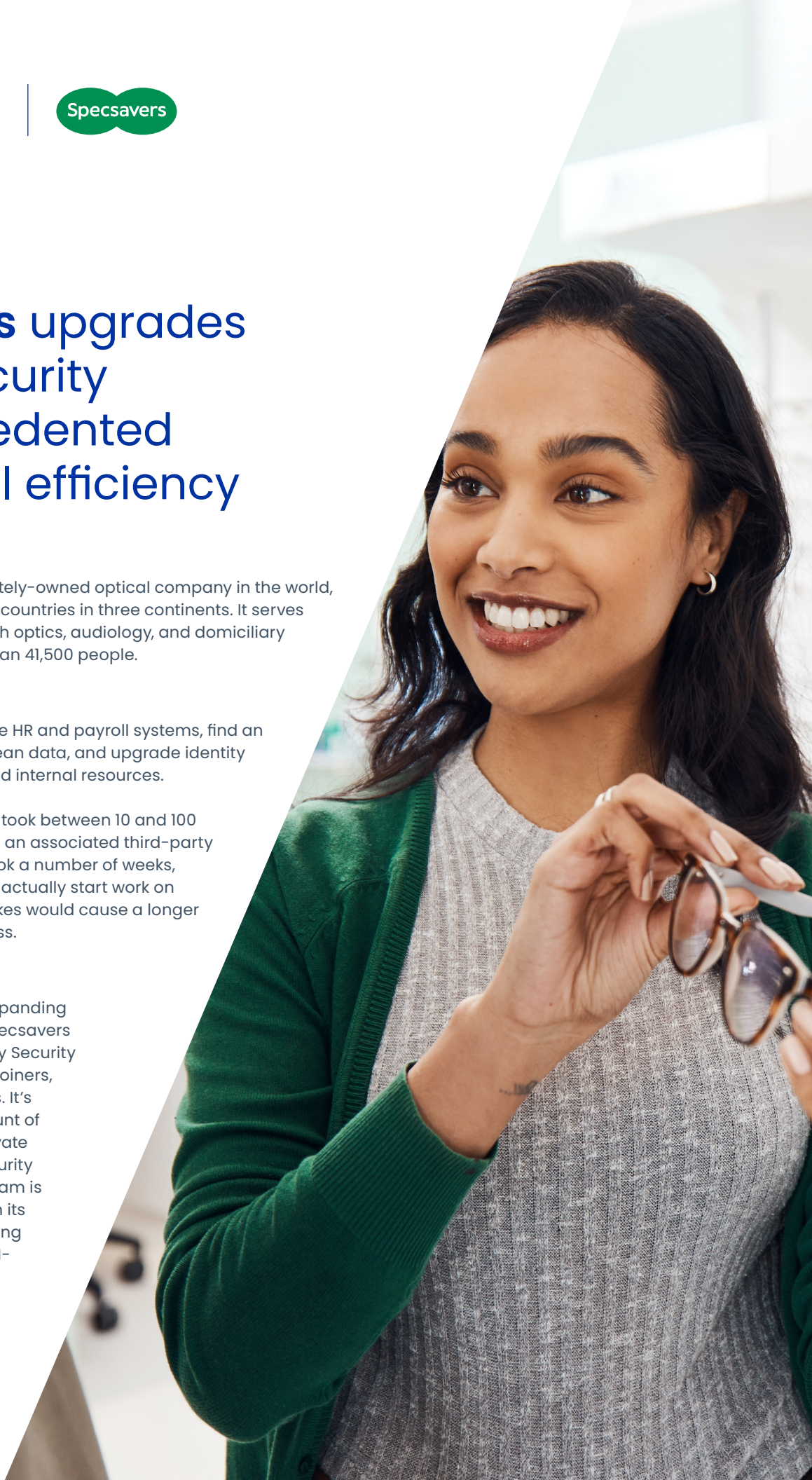
Challenge

Specsavers sought to centralize HR and payroll systems, find an efficient means to maintain clean data, and upgrade identity and access security with limited internal resources.

Giving each new joiner access took between 10 and 100 tickets, with each ticket adding an associated third-party cost. The process also often took a number of weeks, meaning a new joiner couldn't actually start work on their start date, and any mistakes would cause a longer delay in granting correct access.

Solution

Alongside hiring a CISO and expanding the identity and data team, Specsavers invested in the SailPoint Identity Security Cloud platform to manage its joiners, movers, and leavers processes. It's since automated a large amount of otherwise manual tasks to elevate operational efficiency and security to transformative levels. The team is now ready to go even further in its identity journey, by implementing advanced new tools such as AI-powered automation.



42.9M
customers worldwide

20K
Microsoft 365 licenses recovered

10X+
identities managed, from 4,000 users on old platform to 40,000 users on new SailPoint platform

As the UK's biggest optical and audiology provider, and the largest privately owned optical and audiology business in the world, Specsavers certainly has an eye for the extraordinary. Founded in 1984 by a husband-and-wife team in Guernsey, today the retail chain manages 2,615 stores across eleven countries in three continents – serving over 42.9 million customers and employing more than 41,500 workers.

Specsavers enjoys a strong brand identity, with its stores often the anchor tenant on many British high streets. Its slogan "Should've gone to Specsavers" is also one of the UK's most recognizable and beloved ad campaigns. Maintaining this customer trust is pivotal to Specsavers's success and core values. So, the company needed to build a more robust identity security program to improve internal stakeholders' productivity and promote even greater customer satisfaction. Fortunately, they were able to achieve success with SailPoint's solutions.

Initial identity and access management challenges

At the beginning of Specsavers's identity journey, all of its processes were manual. When the company onboarded a new employee, HR created a ServiceNow form, and then a corporate team member manually created an Active Directory and ServiceNow account and placed the new employee into relevant email distribution groups. It was an incredibly time-consuming process that sapped essential day-to-day resources.

To make things more complex, each country with a Specsavers presence used a different HR platform and payroll system. This lack of a centralized system meant line managers weren't connected and there were no links to an HR or payroll number. Employees just existed as names, with thousands of duplicates. Without a dedicated internal resource or owner, Specsavers's identity data often lacked organization. According to Adam Manning, Digital Identity and Automation Specialist at Specsavers, "If an employee left, it was simply down

to luck as to whether their account got closed based on whether a line manager remembered to raise a request."
A CISO soon joined the business and immediately recognized how time-consuming and risky its service issues were. The team put together a business plan recommending the company implement improved identity and access management.

Expansion and evolution of the issue

The Specsavers team began to research solutions and advocate them to the board. "When selling it to senior leadership, there are two main elements of value," said Danial O'Shea, Identity & Access Management Product Owner at Specsavers. "One is, how can we ensure the least privilege when leavers exit the organization and remove access in a timely manner? And then there's operational efficiency. How can we ensure that the right access is ready on day one for all our people when they're joining or moving within the organization? And how can we minimize the time the company spends on manually requesting access, approving access, or even certifying?"

During their research, the Specsavers team realized that SailPoint would be the ideal solution for their needs, especially when considering the unique set-up of the business. Specsavers operates a 'joint venture partnerships' model, in which every store is locally owned and led by its directors. Employees therefore often work in different branches, employed by different directors, making centralized identity management even more complex. So, the business would need an advanced software partner that could handle such intricacies.

Danial said, "We chose SailPoint because it's clearly a technology market leader in the identity space, with all the right technical capabilities and future road map. The tech capability coverage mirrored where we want to go on our identity journey, and we were looking for a strong vendor partnership – someone who listens to what we have to say and responds accordingly."

Switching to SailPoint

At the time, Specsavers's employees used a very customized version of SAP SuccessFactors. The company was managing about 3,000 corporate users and 1,000 third parties. However, the third parties weren't managed from an HR source, but from a series of ServiceNow forms that the managers filled in with start dates, current line manager, and end dates. Then, they had to send an email to the ServiceNow team if they wanted that end date extended. The key objective for the team was data integrity – making sure that all accounts in the system are genuine and in use.

The switch to SailPoint completely changed the landscape for Specsavers's identity and access management, because suddenly every employee in the UK and Ireland needed to have a managed identity. The company had to move from a platform

that was just managing 4,000 users to one that could manage ten times the number of identities, bringing in manufacturing, distribution and retail across 40,000 employees in the UK and Ireland. It would also have to be centralized. As a global program, eventually every single employee across retail, corporate and manufacturing distribution sites in the world would sit on this same platform, managed by SailPoint.

Transitioning to stronger identity and access management

Specsavers looked at the transition as four pillars: the strategy for identity, operating model, people and talent involved in the program, and the technical capabilities through the tool. The product owner also assessed Specsavers's current state, using consultants and vendor partnerships, such as SailPoint's business value assessment service.

"The way we approached our identity program was about assessment," Danial said. "We reviewed the organization and made plans to annually reassess where we're at and where we want to get to, because we knew the demands and the priorities of the organization would constantly change."

Upon the launch of the company's new people and payroll program, Specsavers hired a product manager and data analyst to cover the existing accounts that needed to grow into those identities. The company also brought in two digital identity specialists to be the eyes and ears and the technical control and governance of the platform. An immediate benefit of their presence was the recovery of 2,000 Microsoft 365 licenses that were either duplicates or leavers that had never been cleared out of the system.

"One of the first changes the team communicated to stakeholders was around the operating model and ownership

> **"Because of identity security, we've been able to automate a large number of manual tasks, reduce our risk, and improve our information security posture. We can now ensure role-based access control so that people have the least privileges to fulfill their role, helping to ensure watertight organizational security.**
>
> **Danial O'Shea**
> Identity & Access Management Product Owner
> Specsavers

of identity, and the value it will bring to the company," said Danial. "They built a business case for future investment, be that in people, change to the operating model, change of ownership of processes, and whether they wanted to bring them in or move them out."

"If Specsavers had experienced a data breach as a result of identity mismanagement, then it would have cost a lot of money, and certainly a lot of reputation," added Adam. "The new CISO campaigned for a move from central delivery into a foundation technology. They also hired a product owner, whose primary job function was to review identity capabilities, the Target Operating Model, strategy, people, and tech capabilities."

Achieving dramatic identity improvements

Specsavers finally had all its provisioning and deprovisioning managed with SailPoint. But there was little structure around how the team managed demand for identities, such as an influx of new joiners. When faced with a demand or a request, there wasn't a process or a methodology for prioritizing it. The team needed a system to make sure that it was adding or providing the most business value first, at the right points.

Specsavers invested significant time and effort into creating more efficient ways of working and has seen huge improvements. Its recruitment drive enabled technical team members to focus on delivery and take privileged access management under their remit.

By the end of the year, Specsavers had dramatically improved from an identity management perspective, a Target Operating Model in terms of clarity of ownership, and a clearer, more easily communicated strategy. This year, the team decided to upgrade to the full SailPoint Identity Security Cloud Business Suite Plus. They carried out a mapping exercise to chart the technical capabilities within SailPoint and other identity tooling to those regulatory compliance points, which helped them get across the line with their business case.

Looking to the future

Today, Specsavers uses SailPoint's platform to comprehensively manage its joiners, movers and leavers. "Within an organization the size of ours – in the region of 45,000 employees – the ability to automate at a global scale has been really beneficial," said Danial. "Then, in terms of tech capabilities, access certifications, information security, and our regulatory and contractual compliance obligations are now defined as essential. SailPoint provides us with the capability to address those challenges." Thanks to the certification capabilities within SailPoint, it has become far easier for Specsavers to ensure regulatory compliance.

Meanwhile, one of Specsavers's biggest future priorities is role mining. Specsavers has over 2,500 businesses that all run

in their own slightly unique way and, for retail employees in particular, there isn't a standard role or access profile that can be applied because everyone might be working slightly differently. Unique role mining creation wouldn't have been possible without SailPoint's AI capabilities, and Specsavers can now begin to automatically identify, group, and administer all users. This will help to accelerate application onboarding and make a dramatic change to its risk profile specs.

New developments, such as the automation of role-based access and deprovisioning, also eliminate the need for managers to request access or approve access all the time through ServiceNow tickets. This will enable Specsavers to accelerate returns on investment. It's still in the early stages of its data journey, but SailPoint has helped the company to lay the groundwork for even faster, more effective transformation. Specsavers is now better equipped than ever to boost its internal productivity, which in turn is set to improve external branch services and customer satisfaction.

"In terms of how far we've come – everything being manual versus today – we've really come a long way," said Danial. "Because of identity security, we've been able to automate a large amount of otherwise manual tasks within the organization to improve operational efficiency. And we've been able to reduce our risk and improve our information security posture. We can now ensure and work towards role-based access control, so that people just have the least privileges to fulfill their role, rather than the historical scenario in which people accrued access over time – which obviously left the organization open to more risk."

"We're really excited about the next 12, 24, and 36 months to see how far we can go, especially with some of the automation AI capability with SailPoint and how that can help us accelerate our journey," said Adam. "We've still got a massive learning curve to go on, but we've got the right people and talent, and now we've got the right tech capabilities."

About SailPoint

SailPoint equips the modern enterprise to seamlessly manage and secure access to applications and data through the lens of identity – at speed and scale. As a category leader, we continuously reinvent identity security as the foundation of the secure enterprise. SailPoint delivers a unified, intelligent, extensible platform built to defend against today's dynamic, identity-centric cyber threats while enhancing productivity and efficiency. SailPoint helps many of the world's most complex, sophisticated enterprises create a secure technology ecosystem that fuels business transformation.

sailpoint.com

CU2574-2412