Customer Success

Currys

Reduces its risk profile and automates identity security with SailPoint

Overview

Currys is a leading technology products and services retailer based in London with over 800 stores across eight countries, including the United Kingdom, Ireland, Greece, and the Nordic countries. In addition, the company is a mobile virtual network operator (MVNO) of the iD Mobile cell phone network.

Challenge

Like many retailers, Currys has a constantly changing pool of employees that tends to increase around major holidays such as Christmas. As a result, the organization was challenged to efficiently grant, manage, and revoke identity security for its ever-changing group of employees. The company also needed to automate its manual access management processes and ensure that access wasn't overprovisioned.

Solution

Currys partnered with SailPoint to automate identity security processes in its United Kingdom locations. The solution not only saved significant time that was previously consumed by manual access control management, but it also automatically provides a complete audit trail for changes, reducing compliance challenges. In addition, Currys can now run automated recertification campaigns to verify access rights. It has integrated easily across multiple internal systems, including Microsoft Active Directory, ServiceNow, and SAP SuccessFactors.

>3x
risk reduction with total user risks not executed reduced from over 8,700 to under 2,800

>210hrs
of manual effort saved over the course of a year based on just four applications

24K
identities managed

Retail technologies move fast, and so does Currys. The London-based electronics and services retailer offers everything from washing machines to laptops to phones and cell service across more than 800 stores in eight countries.

A crucial part of Currys' business is its associates, who help consumers make informed decisions and wise choices from an array of technology options. Their goal is to guide customers to the right technologies at prices they can afford so they can enjoy the benefits. To help customers and do the best job possible, Currys' employees need access to various systems and applications.

But managing that access and ensuring that employees have access to only what they need, and not to resources they don't, can be complex and time-consuming. Currys knew that it needed effective and efficient identity and access management for its more than 28,000 employees.

"What drove our need for identity security was the need to ensure that the right people have access to the right systems at the right time while fundamentally ensuring that our data and systems are secure," said Nicholas Rossiter, Head of Technology Risk, Currys. "As a company, it's impossible to keep data secure unless you know exactly what people have access to."

The challenge of securing and auditing access without tool

Since Currys is a major retailer with hundreds of stores, its retail employee population grows and shrinks as seasonal adjustments are made. Those changes require the company to add, remove, and change access for those employees depending on their employment status and roles. For Currys, it ended up being a time-consuming manual process.

"Our biggest challenge was the process for provisioning, de-provisioning, and managing movers. It was all very manual and based on Excel files," said Rossiter. "It was a slow and clunky process, and we didn't always get it right the first time."

Currys had a team that manually created new accounts based on a daily report from its HR system, so the response time was at least a day. To complicate matters, once a new employee was added, multiple teams had to be contacted to add access to the different systems needed, adding complexity and increasing the potential for problems.

There was also no good template for creating new user accounts. Administrators often duplicated an existing account in the same department, risking overprovisioning new users. In addition, the manual process for adding, changing, or deleting access made it difficult to provide complete audit reports for access changes.
Last, but not least, given the compartmentalized and manual processes, the organization didn't have an efficient way to fully calculate access risk or do an effective access risk analysis.

Solving identity governance issues with SailPoint

After undertaking an RFP process to evaluate possible options, Currys selected SailPoint to solve its access and identity security challenges. Currys deployed SailPoint Access Risk Management to provide effective and efficient access risk analysis and give the company granular visibility and improved compliance.

"SailPoint's Access Risk Management tool does everything we need it to do," said Rossiter. "It comes with a rulebook and connects nicely to the SAP S4 and ECC systems. We've gotten some rapid and easy wins from it."

An essential consideration for Currys in selecting SailPoint was the product's integration capabilities. Currys used SailPoint's integrations to connect to SAP ECC and S4 seamlessly. "SailPoint's connectors and integrations worked well for us," said Rossiter. "They've been one of the success factors for our deployment. We've even used API calls to automate integrations with some of our legacy systems, and it's worked quite nicely."
In addition to using SailPoint's Provisioning capabilities, Currys is also leveraging SailPoint's Separation of Duties and Access Certification functionality.

> **"SailPoint's Access Risk Management tool does everything we need it to do. It comes with a rulebook and connects nicely to the SAP S4 and ECC systems. We've gotten some rapid and easy wins from it.**
>
> **Nicholas Rossiter**
> Head of Technology Risk
> Currys

The business benefits of automated access management

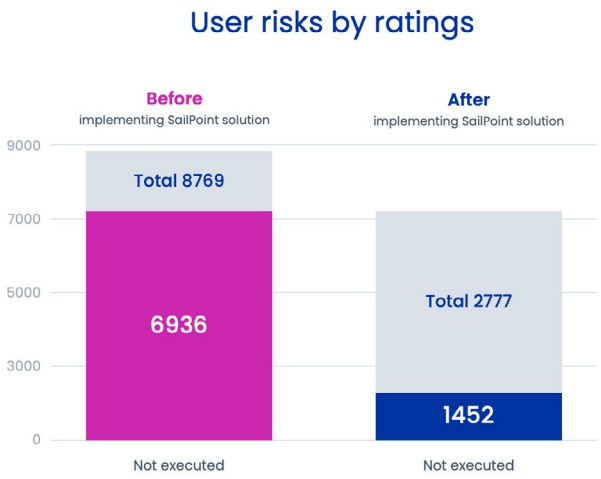
A significant benefit to the SailPoint solution is that user access can be granted instantaneously versus the previous manual solution when employees didn't always get access on time.

"SailPoint has helped us reduce the time to provision, de-provision, and make changes. Now we can do it in minutes with no errors," said Rossiter. "SailPoint has really helped eliminate all the manual access management changes we previously had to make. Now, with SailPoint, it's a seamless process that's integrated with our other systems."

Another positive impact for Currys of deploying SailPoint has been on the completeness of its auditing reports. Audit reports are now available almost immediately and from one source instead of having to be pieced together from multiple disparate tools and platforms.

"By integrating IdentityNow with ServiceNow, every provisioning, de-provisioning, or change is tracked in an audit trail, and we can validate the complete flow. That's helped massively," said Rossiter. "It's all in one place now." Overall, the automated solution has also resulted in time savings. Rossiter estimates that the company is saving 210 hours of manual effort annually, and that's based on the results from only four applications.

Risk reduction has also been another important benefit of deploying SailPoint. With the solution, Currys has been able to sharply reduce the non-executed



permissions that its users have. Its finance support team has seen big payback from the SailPoint deployment because now it has a tool that gives them a complete view of everyone's access privileges and what they're doing and executing.

"With SailPoint, we've made progress very quickly in removing excess access that some of our users had," said Rossiter. "In just a short time, we reduced not executed risks by over 78%. It's a huge benefit."

Another way that Currys eliminates access risk is by having SailPoint automatically initiate a recertification campaign whenever a user moves or their birth access gets changed. The new manager can approve or adjust the user's historical access as needed while the system provides suggested templated access for different roles.

The role-based templates can also be used for new employees and have helped reduce the previous overprovisioning of access from simply duplicating existing accounts for new users.

"Being able to select specific roles in a role-based access model is huge for us from a compliance and audit perspective," said Rossiter. "And being able to group access based on roles and automate it so that it takes minutes rather than having an administrator manually add everyone is huge."

This also results in time savings for managers since they can select the roles for their employees, and access is granted within minutes versus the manual processes that used to take one or two days.

A bright future for further identity management automation

While the SailPoint deployment has already significantly impacted Currys' risk reduction and efficiency, the company isn't stopping. So far, Currys has focused on using SailPoint with its SAP systems in the United Kingdom, integrating over fifty systems, including Microsoft Active Directory, ServiceNow, and SAP SuccessFactors. Its plans for SailPoint include rolling the solution out to additional systems and locations.

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.