



# Sainsbury's Case Study

Sainsbury's is one of the UK's leading retailers across food, clothing, general merchandise and financial services. Trading for 150 years, it is one of the best known and loved retail brands in the country.

Sainsbury's Tech Security team is responsible for defining and delivering the technology security strategy and roadmap across all of Sainsbury's brands and channels; including Argos, Tu clothing, Nectar loyalty, Habitat and Sainsbury's Bank, as well the core grocery business. The team works in partnership with the CTOs of all of Sainsbury's business areas to support the tooling, processes and resourcing across three outcome areas:

- Protecting data
- Protecting systems
- Meeting regulatory commitments

Mun Valiji is Chief Information Security Officer (CISO) at Sainsbury's and works at a peer level with the business CTOs, reporting directly to the Board.

"It is a complex role, as each business area has its own CTO, focused on driving their own products and processes. My team works in collaboration with each of them to enable innovation while ensuring compliance with industry and government regulation, as well our own policies."

The company has put trust at the heart of its proposition to customers, colleagues and the market, and for Mun's team this resonates strongly throughout their objectives.

## THE PROBLEM

To successfully fulfil its objectives, Sainsbury's Tech Security needs visibility into the distributed nature of projects and activity across the company. The 2,000-strong Tech team therefore has to work across an extremely heterogeneous and complex environment, often embedded into other teams to check that controls and measures are not a casualty to innovation.

Sainsbury's is a 'cloud first' organisation, a strategic IT decision to ensure the business can scale significantly at key times of the year. Mun comments: "At Sainsbury's we see big seasonal peaks so cloud is crucial to handling that scalability."

Achieving the necessary level of visibility across a complex web of cloud services (used both internally and with partners) requires that the team are equipped with the right tools that can give them detailed line of sight.

The Data Protection Officer role sits within Sainsbury's Data Governance team, another of the Security team's peer organisations. This team relies upon the insight and controls that the Security team owns.

# Sainsbury's

## PROFILE

### INDUSTRY

Retail, Finance

### REGION

United Kingdom

## CHALLENGES

- Incomplete visibility of cloud services
- Risk of sensitive data loss and non-compliance
- Restricted DLP capabilities
- Exposure to threats
- Lack of consistent policy enforcement

## BENEFITS

- Reduce risk of cloud threats
- Mitigate exposure of sensitive data
- Implement consistent policy enforcement
- Protect assets within cloud services
- Alignment of GDPR compliance

## SOLUTIONS

- Complete O365 protection
- Netskope SaaS protection with Cloud DLP
- Advanced Threat detection and remediation

# “It is imperative for me that we have complete line of sight—an end-to-end view of cloud implementation and services”

Mun Valiji | CISO at Sainsbury's

Mun: “It is imperative for me that we have complete line of sight—an end-to-end view of cloud implementation and services, including all egress and ingress points. Given our vision to be the most trusted retailer, knowing what is going on is the basic foundation to ensuring appropriate data governance.”

Across Sainsbury's the business handles a lot of data, governed by a range of regulations—both generalist (such as GDPR) and specialist (e.g. financial sector regulation for Sainsbury's Bank). With over 178,000 colleagues, Sainsbury's HR team is handling personally identifiable information on more colleagues than many organisations have to manage on all their customers. In addition to this, the Nectar business derives its core value from data, meaning that strict adherence to best practice for data governance is critical.

Mun continues; “I want us to be the first line of detection, response and management of our data, and if there is an issue we need to be able to quickly get to a position where we can take steps and measures.”

Taking action swiftly can itself be a challenge for such a large and busy organisation. The team needs a range of actions

available to it as overly heavy handed controls can easily disrupt another business process. For this reason, it is not enough to have a big red ‘block’ button; Mun works hard to ensure that his team has established engagement between business areas, and that the tools they use do not undermine that collaborative relationship.

## THE SOLUTION

Netskope was already installed at Sainsbury's before Mun's arrival two and a half years ago, but he notes that he went through a competitive RFP in his previous role at News Corp and selected Netskope.

Netskope maps billions of transactions, enabling Sainsbury's to understand user activity (e.g. upload, view, share, send, post) across tens of thousands of SaaS and IaaS services, and millions of websites. Importantly for Sainsbury's, Netskope gives line of sight into both sanctioned apps (such as Office365) and unsanctioned apps. This ensures Mun's team can identify shadow projects that may have accidentally overlooked integration with the security team—important in such a large organisation.



Netskope decodes these activities to reveal rich details about users, groups, locations, devices, and data. This enables Sainsbury's to go beyond seeing byte movement to gaining real insights and taking granular, policy-based action to mitigate cloud risks, protect sensitive data, and stop online threats. Netskope helps Mun's team answer questions and enforce policies such as: "Block users from Team-X from posting non-compliant messages on social media," and "Alert if any user uploads personally identifiable information (PII) to any big data app." Netskope is a single, cloud-native, platform that's built for integration, whether that's with new or existing security products.

## THE IMPLEMENTATION

While Netskope had been installed years earlier, Mun initiated a second wave implementation recently.

Mun: "I am always looking for absolute value from my tools, and encourage my team to ask themselves 'What happens if I switch it off?'. In the case of Netskope, I was aware that there was much more we could be doing with it. Maturing utilisation is a journey and in security we are adapting to a constantly changing risk outlook. There was a lot more that Netskope could do for us than the one or two use cases it was being tasked with."

The Sainsbury's and Netskope teams agreed to a committed 6 week re-implementation. Product, delivery and vendor teams all worked together, focusing on specific outcomes and fast integration of a minimum viable product.

Mun: "I always recommend starting with a small PoC in a high risk part of the business. Take on big projects in bitesize chunks so people can relate to a demonstrable value. For us the obvious PoC was OneDrive. I wanted to really focus on achieving in depth line-of-site, finding out what our data consists of, where it is stored, and how it is protected. As a 150 year old business you can imagine we have hundreds of millions of folders!"

Trying to implement and evaluate a system that sits inline has the potential to be disruptive to the business, and can be a

struggle in any organisation. For Sainsbury's the Netskope implementation had to work within a complex schedule of maintenance windows.

Mun explains the challenge; "I only choose vendors from the top right of Gartner's Magic Quadrant, but there is a risk in any software implementation that a new API will prove chattier than expected and hinder another process. For an implementation to go smoothly you need the best from your team, as well as from the vendor; judgement, drive and internal influence within both organisations. The worst case scenario is finding you have 'all the gear, and no idea'."

Key to the success of the implementation at Sainsbury's was Mun's work with the Operating Board; "In theory people are supportive of an implementation if it makes rational sense, but driving a programme of work to effect isn't easy. It requires the CISO to compete for capability, time and resources and there is a window to prove that value." Mun goes back to the Operating Board every quarter to report on the ROI and TCO of every project.

## THE RESULT

Six months on from the re-implementation of Netskope, Mun is very happy with the results that Sainsbury's is getting from the technology.

"The implementation was clean and stable, including a lot of support from Netskope. We are now operating across a range of use cases with a line-of-sight that we didn't have before, with access to more data points and telemetry than we have ever had."

Sainsbury's has defined appropriate use cases and policies across all cloud services—both sanctioned and unsanctioned. Starting with basic discovery to fully understand the organisation's cloud estate, Sainsbury's is now in a position to identify potential points of contagion or leakage—if any documents or data are sitting unprotected outside of the network.

Mun's team measures the effectiveness of Netskope by looking at the number of incidents and escalations they identify and

**"The implementation was clean and stable, including a lot of support from Netskope."**

Mun Valiji | CISO at Sainsbury's



handle. But Mun asserts these raw figures are only the start of the value Netskope provides; “For us, the data points are a bit like crime statistics for the police. They give us a snapshot of what has gone on, but more importantly they tell us the effectiveness of our tactics. Our strategy is constantly learning from those numbers. In the world of information security the world is changing daily, bringing new threats and risks. The data is telling us that we are doing the right things.”

With visibility into cloud security vulnerabilities, some of the most common tactics used by the team are relatively simple. The team has done a lot of work to identify and tune native controls within common apps such as OneDrive, where a new document is created with sharing as the default setting. They also work to educate colleagues to avoid oversharing of documents, using specific names instead.

The security team updates the data governance committee regularly. Mun; “We don’t want to be naysayers, but we do need to prescribe what colleagues can do within acceptable usage. We are ratcheting our implementation all the time because data protection is a clear and present challenge. If you get it wrong, GDPR fines can cost you up to 4% of your revenue—which for a business that does £28.5bn in retail sales is considerable.”

## FUTURE PLANS

Mun is fond of referring to his team’s role as being cultural. He believes that they are taking people on a journey and constantly fine tuning policy and process. With no shortage of support from the executive team he is also looking to the next steps, particularly working on a proposition to capitalise on automation opportunities.

Mun; “We are always looking to make the most of our assets. We have to continue to prove demonstrable value, doing things differently to get more from finite resources.”

The Sainsbury’s team is also aware that regulatory changes are a moving feast. While GDPR is unlikely to see many amendments in the near future, some parts of the Sainsbury’s business operate in markets that require considerable agility regarding compliance—such as Sainsbury’s Bank in the financial sector.

Mun concludes; “We would like to continue working closely with Netskope, getting access to alpha and beta modules so that we can always be at the leading edge, delivering against our objectives and identifying measurable outcomes.”



Netskope is the leader in cloud security. We help the world’s largest organizations take advantage of cloud and web without sacrificing security. Our patented Cloud XD technology targets and controls activities across any cloud service or website and customers get 360-degree data and threat protection that works everywhere. We call this smart cloud security. Visit [www.netskope.com](http://www.netskope.com) to learn more.