

How Varonis Simplifies Data Subject Access Requests and Secures Sensitive Data for NFT Distribution

The Customer

Location: UK

Industry: Distribution, Warehousing and Logistics

Products: DatAdvantage for Windows, GDPR Patterns, Data Classification

Engine for Windows and SharePoint, and Data Transport Engine



Delivering Food Fuelling the UK

NFT Distribution is the UK's leading provider of time-critical food distribution, delivering chilled, ambient, and frozen food and drink products from the production line to retailer distribution centres. Its national network of depots, warehouses, and large vehicle fleet deliver around 130,000 pallets of food and drink products to UK grocery retailers each week.

The Challenge

With 1,500 employees and 15 sites across the UK, it is essential for the company to maintain control over where its sensitive data is stored and make sure that only the right people have access.



As Jo-Anne Winfrow, IT Service Delivery Manager at NFT comments, “We’re a relatively small IT team and must manage a substantial volume of data on legacy IT systems that have evolved over the years to support our company growth. Our challenges included managing permissions and controlling our sensitive data – this could be everything from operational data, internal information such as timesheets or phone lists, to higher-level management information, including employee or financial data.”

NFT sought a solution that would help achieve GDPR compliance, show clients that its infrastructure is secure when tendering new contracts, and demonstrate that it is actively protecting data for customer audits.

Security was another priority. NFT had previously been targeted by ransomware, which served as a stark warning that the organization’s data was a target. Although NFT successfully contained the attack and no data was compromised, the company wanted an extra layer of security in place to mitigate any risks.

“Varonis was the only place to look based on its features and performance.”

Solution

Winfrow had seen a demonstration of the Varonis Data Security Platform and recognized that its capabilities would exactly match their requirements. “For us, Varonis was the only place to look based on its features and performance,” says Winfrow.

Following an initial proof of concept, NFT deployed Varonis DataAdvantage -- which maps who can access data, who does access data, and where users have too much access -- across its servers. NFT also began using Varonis’s Data Classification Engine and GDPR Patterns to easily identify and lock down sensitive data in line with compliance requirements.



Expediting Data Subject Access Requests

During the early stages of its deployment, Varonis quickly proved its worth by streamlining processes around Subject Access Requests (SARs), which is a crucial part of the GDPR. Under the GDPR, individuals have new rights to request and access data which must be provided “*without undue delay and in any event within one month of receipt of the request.*” Fulfilling these requests manually can be a complex and time-consuming process.

Before NFT deployed Varonis, the team had to rely on manual data checks. With data located over different file servers, the process could take days to complete. Now staff can enter details – from payroll number or names -- and conduct a fully automated search to identify relevant information quickly. With Data Transport Engine they can seamlessly move files from one location to another that match their own search parameters.

“Using Varonis, not only are we assured of the accuracy of searches, we also save a considerable number of manhours that we would otherwise have to devote to manual data searches,” says Winfrow.

Securing Access to Sensitive Data

The team also needed a more structured process for ensuring that the right people have access only to the data that they needed to do their jobs and that when they left the organization there were robust processes for closing off accounts and access to data.

Winfrow continues, “In the past, when a new user joined, permissions would often be copied over from an existing user, or, if staff were moved to a different role, their existing permissions would be carried over with them.”



With Varonis, NFT gained full visibility into which users are accessing files and folders. The company also locates sensitive information and moves, quarantines or deletes it automatically based on preset rules.

“Varonis has given us complete visibility over just how much sensitive data we have and provided a structured process from which we can manage permissions for permanent and agency staff,” says Winfrow.

Using Varonis, the team has identified anomalous file behavior that could point to suspicious activity requiring further investigation. Winfrow comments: “On one occasion, we received an email alert which highlighted that an employee had started accessing more idle data than they needed to do their job. We were quickly able to take action, which, without Varonis, we would have had no other way of identifying.”

Support for the Future

With Varonis, the NFT meets their immediate data protection requirements and is better prepared to streamline and archive data in the future.

The company is currently looking to manage and remove stale data, including planning information and historical trends for Christmas distribution that may still hold business value to staff. NFT plans to use Varonis to help them locate and archive only relevant data to ensure the business continues to operate smoothly.

NFT also values the support from the Varonis team. As Winfrow concludes, “Varonis has been invaluable in advising us and are always available to offer any help that's needed. We simply can't compromise on security and with Varonis, we have a team – and solution – that has given us full control over our data.”