NHS Trust

About the customer.

This NHS Trust is a large public healthcare organization in the United Kingdom. With thousands of users accessing critical systems and patient data across a distributed IT environment, the Trust needed to improve visibility into user activity, safeguard sensitive data, and meet stringent regulatory requirements under GDPR.

The challenge.

The Trust discovered a serious issue when files containing sensitive data were accidentally deleted. During the internal investigation, it became clear that the problem was rooted in excessive user permissions.

Their existing permissions structure had spiraled out of control. Users were unknowingly granted access to sensitive files via indirect group inheritance and nested permissions. The IT team had no efficient way to determine how or where these permissions were being applied, and more critically, no way to monitor the behavior of high-risk users with elevated privileges.

The organization recognized that without visibility into who had access to what—and what they were doing with that access—they faced a significant risk of data breaches and were falling short of GDPR compliance standards.

The solution.

The Trust evaluated several solutions and ultimately selected the Lepide Data Security Platform based on its strong combination of real-time visibility, privileged user monitoring, and competitive cost.

Lepide provided a single, unified console to audit changes across Active Directory, Group Policy, and File Servers. The platform delivered detailed insights into privileged user behavior, including real-time detection of anomalous or high-risk activity—enabling the IT team to take immediate action before a minor misstep could escalate into a breach.

Crucially, Lepide's permissions analysis engine helped the Trust identify users with excessive access and understand the inheritance paths that granted them. The team could now reverse unwanted permission changes quickly and restore least privilege across the environment.

Lepide also enabled the Trust to automate compliance reporting, giving internal stakeholders and external auditors accurate, up-to-date insight into data security posture and user activity.

Key security outcomes.

Benefit	Impact
Threat Detection and Response	Real-time insights into anomalous behavior from privileged users enabled faster containment and resolution.
Zero Trust Enablement	Identified and removed excessive permissions, supporting a least privilege model.
Improved Compliance	Delivered detailed, automated audit reports to support GDPR requirements.
Operational Efficiency	Reduced the manual effort needed to investigate incidents and manage access controls.

What the customer said.

"While price is always a factor, we ultimately chose Lepide as they were able to offer us compliance-related audit reports, and real time information on the state of our data security and what our users are doing."

IT Infrastructure Security Manager

Start your 20-day free trial today!