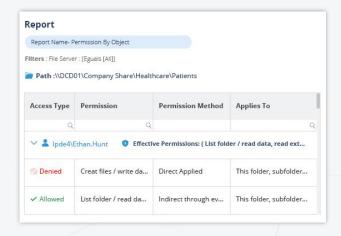
Lepide Trust

Get instant visibility over the changes being made to permissions and determine users with excessive permissions to implement a policy of least privilege.

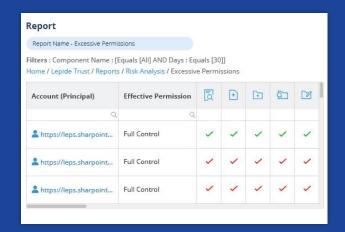


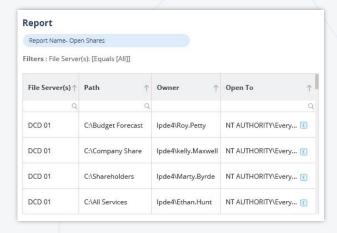
Analyze permissions.

Find out who has access to your sensitive data and how that access is being granted. Determine effective permissions by object, by user or by mailbox. Spot changes to permissions that create privileged users. Identify where they got these permissions from, and reverse the changes if required. Generate a list of your privileged users, and see where they are getting their permissions from.

Revoke excessive permissions.

Analyze the way that your employees are using their permissions to determine whether the permission is excessive. Lepide reports on users that have access to sensitive files or folders, but are not using that access, to give you a clear picture of where to start when revoking permissions to implement zero trust.





Spot data at risk.

Having sensitive data open to all users through open shares creates unnecessary risk. With Lepide, you can spot and react to this risk quickly. Auto share discovery enables you to spot new shares as they are created and determine whether the share is open – giving all users access to sensitive data.