

# Lepide

# Risk Assessment Report


The Lepide Risk Assessment Report is a detailed summary of the potential security threats in your organisation right now. It is based on data collected over 15 days from a sample of your live environment and is designed to highlight security vulnerabilities and recommend remediation.

## DISCLAIMER

The information contained in these documents is confidential, privileged and intended only for the recipient. It may not be published or redistributed without the prior written consent of both Lepide and the recipient.



# Contents Summary



1	Permissions and Privileges
2	User and Entity Behavior Analytics
3	Environment States and Changes
4	Risk Summaries
5	Recommendations















# Risk Summaries

---

## LOW RISK

0 AD Permission Modifications  
0 Mailbox Database Modifications  
0 Policy Modifications  
0 Admin Template Policy Modifications  
0 Startup Script Modifications  
0 Security Options Policy Modifications  
0 Trust Modifications  
0 Schema Modifications  
0 DNS Zone Modifications

### Recommendation

Continuous and proactive scanning of your IT environment is required to ensure that no states or changes pose risk to your data. Continually monitor activity to spot any anomalous user and entity behavior.

---

## MEDIUM RISK

29 Exchange Server Permission Changes  
779 Mailbox Modifications  
33 File Server Permission Changes  
35 AD Group Modifications  
425 Inactive Users  
44,355 Files Created/Moved/Modified

### Recommendation

There is a large attack surface that needs to be addressed. Clean up inactive users and audit file creations/modifications to address this problem. Determine which users are trying to access files they don't have permission to and monitor them closely.

---

## HIGH RISK

5,073 Failed Logons  
3 Open Shares  
10,535 Files Copied  
24,867 Failed File Reads

### Recommendation

You need to determine why you are seeing so many failed logons. Is there a brute force attack underway? Ensure that you remove all open shares to reduce your potential attack surface and the chance of privilege abuse. Audit file copy events and failed file reads to determine whether sensitive data is at risk.



# Recommendations and Summary

Based on our 15 day analysis of your environment, we have determined the following next steps we believe that you should take to immediately increase your data security.

## STEP 1

You need to determine why you are seeing so many failed logons. Is there a brute force attack underway? Ensure that you remove all open shares to reduce your potential attack surface and the chance of privilege abuse. Audit file copy events and failed file reads to determine whether sensitive data is at risk.

## STEP 2

Upon identifying sensitive data and potential risks and threats that could lead to a security or data breach, ensure there are adequate and efficient security controls in place to effectively mitigate the risk. This could include alerting, monitoring, auditing and a periodic review process which should not be limited to a single team. Encourage effective data owners, department managers and all other personnel responsible for sensitive data to manage these security controls implemented by the DCAP solutions.

## STEP 3

Categorize, in order of importance, the highest areas of risk surrounding the silos that require adequate protection starting with the data at most risk first. Also, identify if applicable where there could be a crossover between solution specific functionality based upon storage type but also upon the different security controls required such as DCAP and DLP as an example.

## STEP 4

Where applicable, look for native security controls and log sources that can be leveraged and integrated with DCAP specific security solutions. Understand the shortcomings between the different types of security solutions available and through continuously monitoring and reviewing any existing security controls, perform a gap analysis in the existing security strategy and plan for appropriate measure to fill those gaps.

## STEP 5

Identify how data is being transferred between data silos and the user interactions surrounding the data. Understand the permissions and privileges being granted to both users and applications/systems and where appropriate, revoke any unnecessary permissions to adopt a least privilege model surround the data.

## ABOUT LEPIDE

Lepide are the fastest growing provider of data-centric audit and protection solutions to enterprises all over the world. The award-winning LepideAuditor enables you to put data at the heart of your security strategy; mitigating the risks of data breaches and helping to meet compliance requirements.



Discovery &  
Classification



Permissions &  
Privileges



User & Entity  
Behavior



Environment  
States & Changes



Data Risk Assessment