

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.

This Risk Assessment is a sample and contains sample data only.

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 It may not be published or redistributed without the prior written consent of both Lepide and the recipient.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



3	Identity Security
4	Threat Surface Area
5	Data Security
6	Recommendations
8	About us

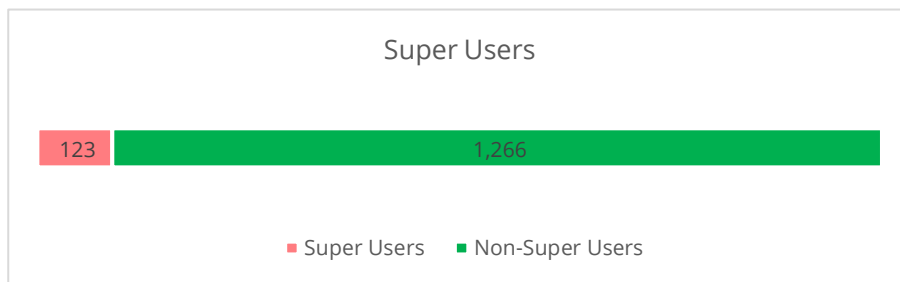
IDENTITY SECURITY

Your employees are one of the major risks to the security of your data and infrastructure. Making sure you have assigned permissions properly, and knowing how they are using those permissions will limit the potential damage that a rogue insider or compromised account could have.

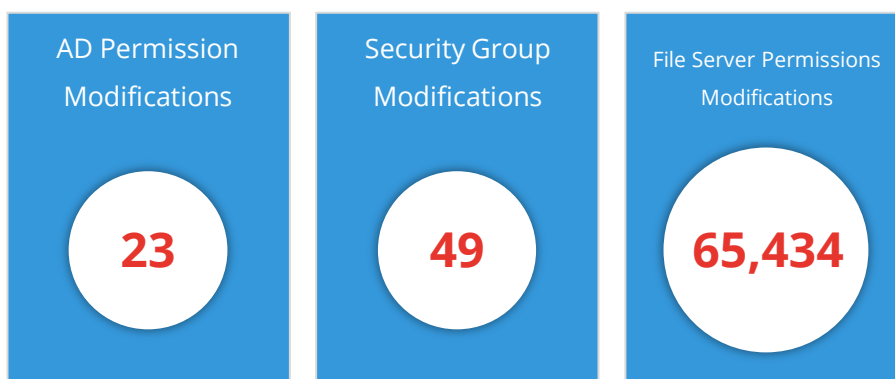
1,765,654

Failed Logons

A very high number of failed logons could indicate either a brute force attack, or misconfigurations in Active Directory.



Having a large proportion of administrative or "super" users creates a large threat surface area. If attackers were to compromise these accounts, they would gain access to everything.



Modifications that result in permissions being escalated may lead to unwanted access to sensitive data. To remain compliant, with a zero trust model, you need to ensure that modifications to permissions do not result in users with excessive privileges.

THREAT SURFACE

Reducing the potential threat surface area that you have is one of the most important parts of identity and data security. Often, misconfigurations or a “messy” Active Directory can lead to inadvertent data loss, or provide an avenue for attackers to gain access.

74

Users with Administrative Privileges

Lepide suggests you have 74 users with administrative permissions. It’s possible that these permissions may be excessive.

17 employees have passwords set to never expire. If an attacker gained access to these accounts, they would have that access indefinitely. Open shares often lead to unnecessary or unwanted access to sensitive data. Most of the time, open shares can be significantly cleaned up. Large volumes of stale data are potentially a breach of compliance laws, and present a larger risk in terms of data loss or exfiltration.

Non-Compliant Passwords

23

Open Shares

49

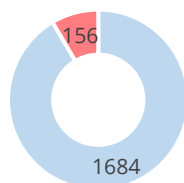
Stale Data

65,434

Empty Groups/OUs/GPOs

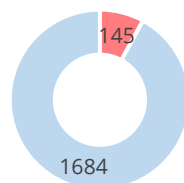
49

Inactive Users



Active Users Inactive Users

Disabled Users

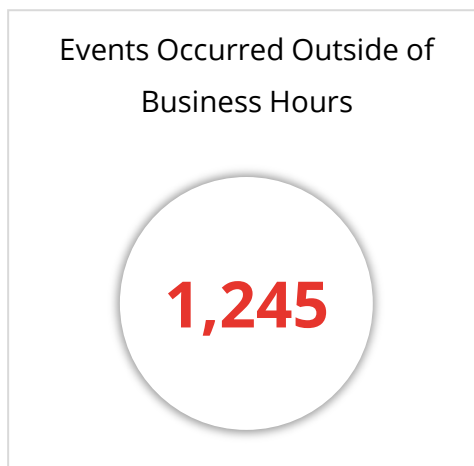
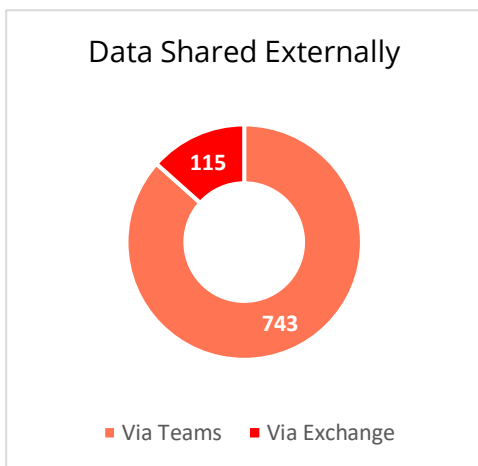
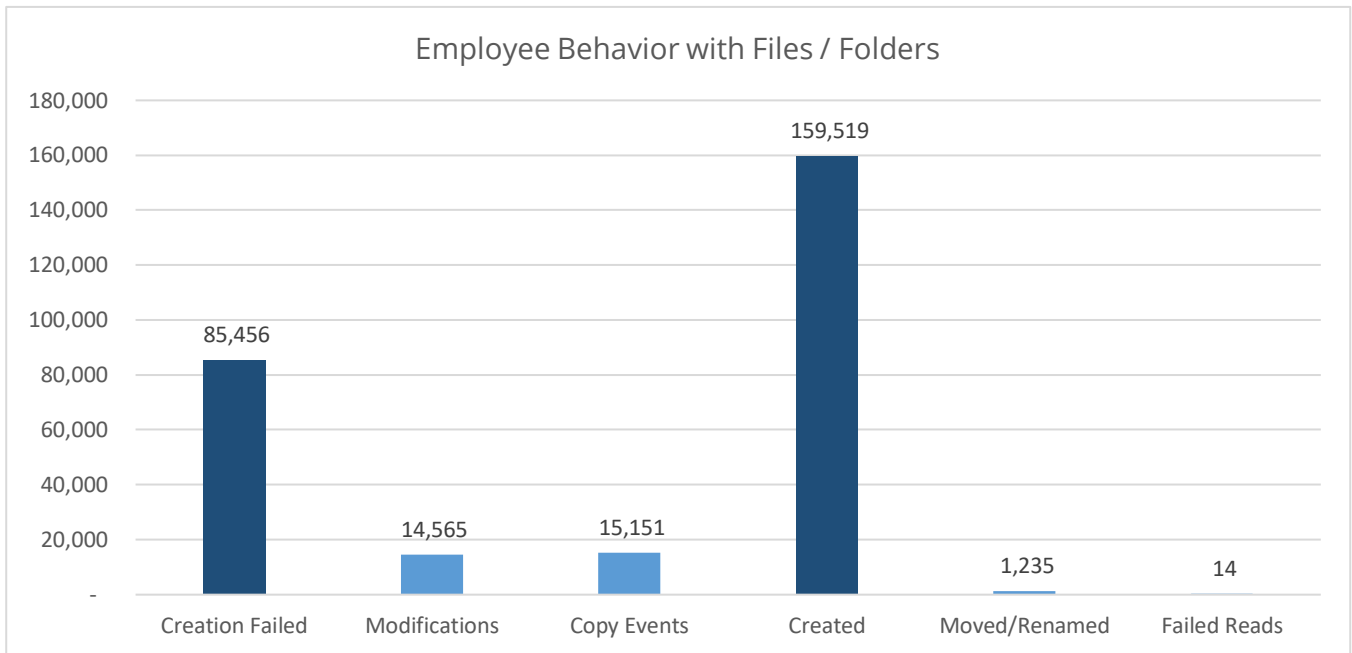


Disabled Users Enabled Users

Inactive/disabled users create a larger threat surface area, particularly when those users still have permissions to data. Attackers may target these accounts.

DATA SECURITY

Protecting sensitive data involves knowing where sensitive data is located, identifying which users have access to it, and monitoring user interactions with it. Users copying, moving, modifying and accessing sensitive data need to be monitored closely. Utilizing the anomaly spotting technology in Lepide will enable you to determine baselines for “normal” activity, and receive alerts when anomalies are spotted.



Data being shared externally is potentially a breach or data leakage, particularly if that data is sensitive. Carefully monitoring how users are using MS Teams and Exchange can help to mitigate this. Likewise, when users are accessing data outside of business hours, it could be an indication of an insider threat. This is especially true if our anomaly spotting technology deems it be “abnormal” behavior for the user.

RECOMMENDATIONS

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

Reduce your potential attack surface and the chance of privilege abuse by auditing policy and group modifications, implementing stricter password security, and removing passwords that never expire, open shares, empty groups, empty OUs, and empty GPOs. You should also clean up inactive and disabled users and reducing the number of administrative users where possible.

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.

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 Data-Centric Audit & Protection (DCAP) and Data Loss Prevention (DLP) as an example.

STEP 4

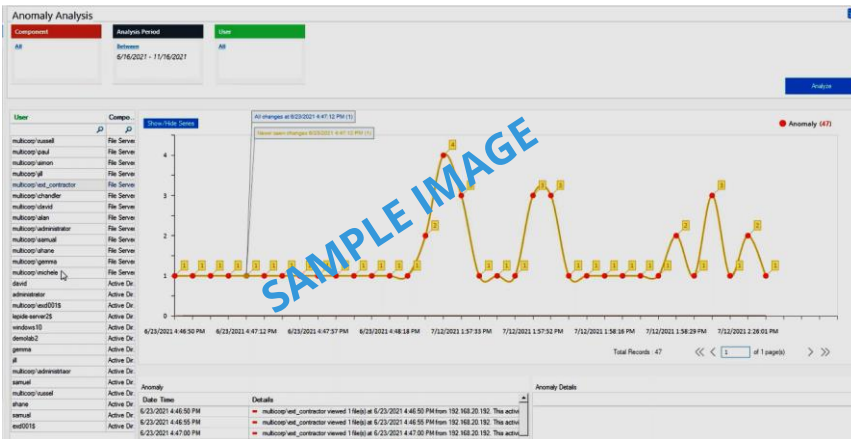
Where applicable, look for native security controls and log sources that can be leverage and integrated with DCAP specific security solutions. Understand the shortcomings between the different types of security solutions available and through continuously monitoring and reviewing any existing security 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 surrounding the data.

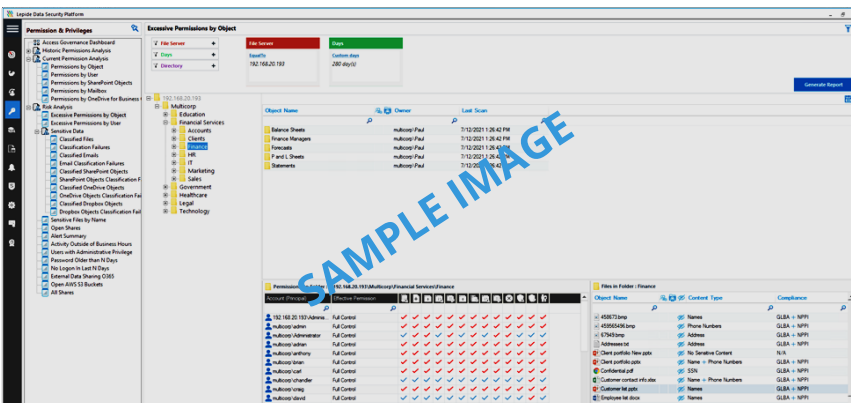
RECOMMENDATIONS

We recommend that you deploy the Lepide Data Security Platform and make use of Lepide Detect. The Lepide anomaly spotting technology will enable you to determine what “normal” behavior looks like when we’re talking about modifications to files, permissions and more. Without the context of knowing what’s “normal” for specific users, being able to detect potential threats becomes very difficult.

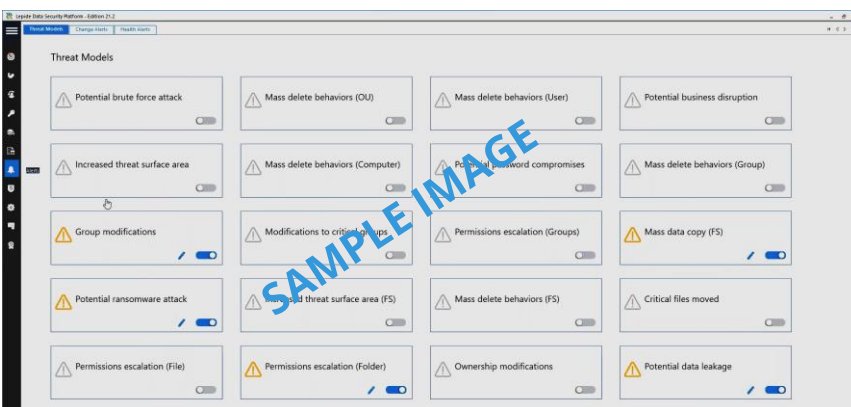


A longer learning period will enable our anomaly spotting technology to improve in accuracy.

Similarly, after a learning period, we recommend reviewing the excessive permissions reports to determine whether you have users with excessive permissions to sensitive data. Lepide suggests which users might have permissions that can be revoked to enable zero trust.



We also recommend, based on your risk assessment results, that you enable a number of the threat models below to help you identify and react to a potential threat quickly. Enabling the data-related threat models, coupled with anomaly spotting, should help dramatically reduce the risk of a breach or attack going unnoticed.



ABOUT LEPIDE

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

Protecting the Data of Thousands of Organizations Worldwide



HOGGE · FENTON



FUJITSU

NHS

Deloitte

