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.

Executive Summary.

Organizations rely heavily on Active Directory, file servers, and Microsoft 365 to manage access to critical data and systems. However, poor visibility into these environments often leaves security teams blind to risks such as excessive permissions, stale accounts, and undetected insider activity. The Lepide Risk Assessment provides a clear picture of these vulnerabilities by analyzing auditing reports across your environment.

During this assessment, Lepide identified a number of high-risk areas that could expose sensitive data or impact compliance readiness. Key findings included:

- **Overexposed data** through open shares and broad access permissions.
- **Inactive and stale user accounts** that remain enabled, creating potential entry points for attackers.
- **Unattended stale data** that increases storage costs and complicates data governance.
- **Excessive group membership and permission changes** that expand the attack surface and weaken least-privilege principles.
- **Risky user behaviors** such as large-scale file copies, multiple failed logons, and unauthorized file modifications, which may indicate insider threats or compromised accounts.

These findings highlight common gaps in identity hygiene, permissions management, and user activity monitoring that are frequently exploited in real-world breaches. Without continuous auditing and alerting, these risks persist unnoticed until they result in data loss, regulatory penalties, or reputational damage.

By surfacing these risks in a single, consolidated view, the Lepide Risk Assessment enables IT and security leaders to prioritize remediation efforts and build a stronger foundation for Zero Trust. The insights delivered are not only technical but also actionable, helping organizations reduce exposure, improve compliance alignment, and demonstrate measurable improvements in security posture.

Active Directory Security

Identity-based attacks now account for over **80% of all attacks** observed by Microsoft.

Microsoft's Digital Defense Report 2024

50% of on-premises identity infrastructure incidents involved **misconfigured or poorly managed AD environments**.

Microsoft's Digital Defense Report 2024

Your Active Directory Misconfigurations

Inactive Users

10,985

Inactive user accounts increase the attack surface by providing dormant entry points that attackers can exploit to gain unauthorized access without drawing immediate attention.

Users with Passwords That Never Expire

15,969

User accounts with passwords set to never expire create long-term security gaps, making them prime targets for brute-force attacks and credential theft.

Admin Users

164

Excessive admin users weaken the principle of least privilege, increasing the likelihood that a compromised account could lead to full domain or data compromise.

Empty Security Groups

784

Empty security groups create confusion in access management, often leading to misconfigurations, overlooked cleanup, and potential exploitation.

Not Configured:

LDAPS

Failing to configure LDAPS leaves Active Directory communications unencrypted, exposing sensitive credentials and queries to interception or manipulation.

Admin Users

164

Excessive admin users weaken the principle of least privilege, increasing the likelihood that a compromised account could lead to full domain or data compromise.

Active Directory Security (continued)

Identity-based attacks now account for over **80% of all attacks** observed by Microsoft.

Microsoft's Digital Defense Report 2024

50% of on-premises identity infrastructure incidents involved **misconfigured or poorly managed AD environments**.

Microsoft's Digital Defense Report 2024

AD Risks Identified Through Auditing

Permission Changes

10,985

Unauthorized or excessive permission changes can grant users broad access to sensitive resources, enabling privilege escalation and data exposure.

Security Group Modifications

15,969

Altering security groups can bypass least-privilege controls, allowing unintended or malicious access to critical assets.

Failed Logons

164

Multiple failed logon attempts may signal brute-force attacks, password spraying, or attempts to use stolen credentials to gain unauthorized access.

Trust Modifications

784

Changes to domain or forest trusts can open backdoors for lateral movement and persistent access across environments.

Event Log Clear Reports

45

Clearing security logs is a common attacker technique to erase evidence of compromise and hinder forensic investigations.

Other Notable Findings

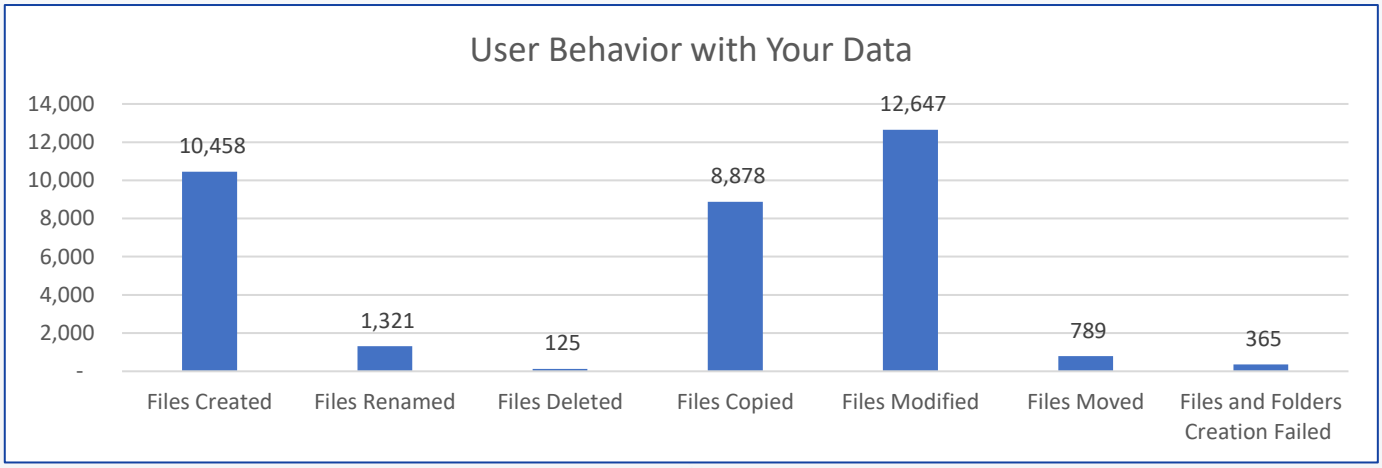
User Password Change Attempts - **14**
OU Modifications - **21**
Schema Modifications - **23**
DNS Zone Modifications- **74**
Sec Op Policy Modifications - **27**
Windows Setting Modifications- **54**
Admin Template Policy Modifications - **12**
Startup Script Modifications - **23**

Data Security

70% of breaches involve over-permissioned or unclassified data.

Gartner

Data-Related Risks Identified Through Auditing



User Behavior

Tracking user behavior around data is critical because it often reveals risks that permission audits alone cannot. Events like large-scale file copies, unusual modifications, or repeated failed logons are early indicators of insider threats or compromised accounts.

File copy activity is especially important, as attackers and malicious insiders typically exfiltrate data in bulk. Monitoring these behaviors in real time allows security teams to spot breaches in progress, limit damage, and maintain forensic evidence—turning static controls into a proactive defense against data loss.

Open Shares

7

Open file shares expose sensitive data to unauthorized users, creating a high risk of data leakage and insider abuse.

Stale Data

10,185

Unused or forgotten data increases the attack surface, drives up storage costs, and often contains sensitive information that remains unmonitored and unprotected.

Cost of Doing Nothing

Failing to address risks in Active Directory, file servers, and user activity monitoring does not simply maintain the status quo—it compounds exposure over time. Attackers increasingly exploit unmonitored accounts, excessive permissions, and weak auditing to move laterally, steal data, and erase traces of compromise. The financial, operational, and reputational costs of ignoring these risks are significant.

- **The average cost of a data breach in 2025 is $4.88 million, up from $4.45 million** in 2023 (IBM Cost of a Data Breach Report, 2025). This figure includes detection, escalation, notification, lost business, and post-breach response. Organizations that lack visibility into user activity and data access consistently face longer breach lifecycles and higher costs.

- Breaches involving **compromised credentials account for 71% of incidents**, making inactive accounts and weak identity hygiene one of the costliest oversights (Verizon Data Breach Investigations Report, 2024).

- **Stolen or misused privileged accounts** play a role in 74% of breaches, highlighting the importance of auditing group and permission changes on file servers and Active Directory (Forrester Research, 2024).

- Organizations that fail to detect and contain breaches quickly pay a premium: IBM found that breaches contained in under 200 days cost **$1.12 million less** than those discovered later (IBM Cost of a Data Breach Report, 2025).

- Beyond direct financial loss, **regulatory fines for non-compliance** are growing. GDPR fines alone surpassed €1.78 billion in 2023 (CMS Law, 2024), much of it tied to poor access controls and insufficient monitoring of personal data.

The cost of doing nothing is not measured only in breach expenses and fines—it also manifests in lost customer trust, stalled compliance certifications, and reduced competitive standing. Without proactive auditing of file servers, Active Directory, and user behavior, organizations are left reacting to incidents rather than preventing them. By contrast, those that invest in continuous monitoring and risk assessment consistently lower breach costs, improve compliance readiness, and demonstrate stronger data governance to stakeholders.

Your 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, removing passwords that never expire, and cleaning up inactive/disabled users and empty security groups.

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 surrounding 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 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