LEPIDE

LEPIDE
DEEP DIVE

SECURE ACTIVE DIRECTORY

THE COMPLETE GUIDE

Active Directory (AD) is central to IT, managing user authentication, access, and resources. Its critical role makes it a prime target for cybercriminals who exploit misconfigurations and poor security, leading to breaches, ransomware, and data theft.

www.lepide.com

Introduction

Active Directory (AD) lies at the heart of most organizations' IT environments, serving as the backbone for user authentication, access management, and resource allocation. Its integral role in ensuring smooth operations and secure access makes it an attractive target for cybercriminals. Threat actors are increasingly exploiting misconfigurations, outdated practices, and poor security hygiene within AD environments, leading to devastating breaches, ransomware attacks, and data theft.

Recent statistics reveal that over 70% of ransomware attacks target Active Directory in some capacity, highlighting the critical need to prioritize its security. For organizations striving to protect their sensitive data and maintain operational resilience, securing AD isn't just an IT requirement—it's a business imperative.

This whitepaper provides a comprehensive guide to implementing 10 best practices for Active Directory security. Whether you're looking to proactively fortify your AD environment or address vulnerabilities after a security assessment, these actionable recommendations will help you mitigate risks, prevent unauthorized access, and maintain the integrity of your systems.

By following these best practices, you can create a robust foundation that minimizes your organization's exposure to internal and external threats, while supporting compliance with modern security frameworks like Zero Trust. Let's get started with the strategies you need to ensure your Active Directory remains secure, resilient, and ready for the evolving cyber threat landscape

Implement Strong Password Policies

Passwords remain a critical line of defense in securing Active Directory, but weak or compromised passwords are among the most common ways attackers gain unauthorized access. To mitigate this risk, organizations must enforce strong password policies that balance security with usability.

Key Recommendations:

Enforce Password Complexity and Length Requirements:

- Require passwords to include a mix of uppercase and lowercase letters, numbers, and special characters.
- Set a minimum length of at least 12 characters but encourage passphrases for added security and memorability.

Enable Password Expiration and History Settings:

- Configure policies to require periodic password changes (e.g., every 60 90 days).
- Maintain a password history to prevent users from reusing recent passwords.

Adopt Multi-Factor Authentication (MFA):

- Implement Supplement passwords with additional authentication factors, such as a mobile app, hardware token, or biometric verification.
- FA especially for privileged accounts, remote access, and sensitive systems.

Monitor and Prevent Common Password Use:

- Use tools that compare user passwords against known breached or commonly used password databases.
- Enforce restrictions on weak patterns (e.g., “Password123” or “CompanyName2024”).

Educate Users on Best Practices:

- Train employees to create strong, unique passwords and recognize phishing attempts designed to steal credentials.
- Promote the use of password managers to reduce password reuse and simplify complexity.

Why does this matter?
Weak passwords = easy attacks (credential stuffing, brute force → network movement). Strong policies + MFA = block access, better security (all attacks). Securing accounts = stronger, protected organization.

Enforce the Principle of Least Privilege (PoLP)

The Principle of Least Privilege (PoLP) is a cornerstone of effective Active Directory (AD) security. It ensures that users, applications, and systems are granted only the minimum level of access necessary to perform their tasks. By limiting permissions, PoLP reduces the attack surface and helps prevent the misuse of privileges during a breach.

Key Recommendations:

Limit Administrative Privileges:

- Restrict domain administrator privileges to a small, trusted group of personnel.
- Use dedicated admin accounts that are separate from everyday user accounts.

Create Tiered Administration Models:

- Implement a Tiered Access Model, where accounts are grouped into levels (e.g., Tier 0 for domain controllers, Tier 1 for servers, and Tier 2 for end-user devices).
- Ensure that credentials from lower tiers cannot access higher tiers, mitigating lateral movement during an attack.

Remove Unnecessary Permissions:

- Regularly review and revoke permissions that are no longer required.
- Eliminate shared accounts, generic accounts, and accounts with "stale" privileges.

Restrict Privileged Group Membership:

- Closely monitor sensitive groups like "Domain Admins," "Enterprise Admins," and "Schema Admins."
- Use temporary membership or just in-time access for tasks requiring elevated privileges.

Segment Access to Resources:

- Use Role-Based Access Control (RBAC) to ensure users can only access the data and systems relevant to their roles.
- Apply network segmentation and enforce permissions at both the file and folder levels.

Advanced PoLP Measures:

Implement Privileged Access Management: Use PAM solutions to secure, monitor, and control privileged accounts. This includes features like password vaulting and session monitoring. Enable User Account Control: Prevent unauthorized applications from running by requiring administrative approval for elevated actions.

Why This Matters?

Excessive permissions are a leading cause of privilege escalation and lateral movement within compromised environments. Attackers who gain access to a standard account often look to elevate privileges to access sensitive systems, such as domain controllers. By enforcing PoLP, you make it significantly harder for adversaries to exploit privileges, contain breaches more effectively, and maintain tighter control over your AD environment. Incorporating PoLP as a continuous practice, rather than a one-time setup, is essential to building a resilient and secure Active Directory.

Regularly Monitor and Audit AD Changes

Active Directory (AD) is a dynamic system that evolves as users are added, roles are updated, and policies are modified. While this flexibility is necessary for organizational operations, it also introduces opportunities for unauthorized changes and potential breaches. Regularly monitoring and auditing AD changes is essential to detect suspicious activities, enforce accountability, and ensure compliance with security and regulatory requirements.

Key Recommendations:

Enable Native Auditing Features:

- Activate Advanced Security Auditing in Windows Server to track key events, such as logons, account modifications, and access attempts.
- Focus on auditing high-value activities, like changes to privileged groups, Group Policy, and access permissions.

Leverage Centralized Loggins Solutions:

- Use Security Information and Event Management (SIEM) systems to collect, analyze, and correlate logs across your AD environment.
- Ensure logs are tamper-proof and stored securely for forensic analysis.

Track Privileged Account Activities:

- Continuously monitor the actions of accounts privileges. with administrative
- Look for unusual behaviors, such as access to unauthorized systems, logins from unfamiliar locations, or excessive failed login attempts

Monitor Group Membership Changes:

- Keep an eye on sensitive groups, such as "Domain Admins" or "Enterprise Admins," for unexpected additions or removals.
- Configure real-time alerts for changes to high-privilege groups.

Audit Access Permissions Regularly:

- Review file, folder, and resource permissions to identify over provisioned access.
- Detect and resolve any anomalies, such as permissions granted to inactive or service accounts.

Detect Anomalous Login Patterns:

- Set up alerts for unusual login activity, such as multiple failed attempts, logins during non business hours, or logins from unrecognized IP addresses.
- Implement geofencing policies to block logins from high-risk regions.

Advanced Auditing Practices:

Integrate AI and Machine Learning: Use advanced analytics tools to detect patterns indicative of insider threats or external attacks, such as privilege escalation or lateral movement. Automate Reporting: Automate audit reports to save time and maintain compliance with frameworks like GDPR, HIPAA, and PCI DSS.

Why This Matters:

Without consistent monitoring and auditing, unauthorized changes in AD can go unnoticed, leaving your organization vulnerable to breaches, ransomware, or data exfiltration. Attackers often exploit the lack of visibility into AD activity to establish persistence or elevate privileges. Proactive monitoring and auditing not only mitigate these risks but also enhance your organization's ability to respond quickly to security incidents.

By incorporating a robust monitoring and auditing strategy, you can strengthen your Active Directory's security posture and ensure a well-maintained, resilient IT environment.

Secure Domain Controllers

Domain Controllers (DCs) are the backbone of an Active Directory (AD) environment, managing authentication, access control, and directory services. Given their critical role, they are a prime target for attackers looking to compromise an organization's IT infrastructure. Securing these systems is paramount to protecting your AD environment and minimizing the risk of a complete domain takeover.

To begin with, it is crucial to restrict both physical and network access to your Domain Controllers. Physically, they should be housed in secure locations with limited access to authorized personnel only. On the network side, DCs should be isolated through segmentation, allowing communication only with trusted systems and limiting exposure to potential threats. Implementing strong firewall rules further reduces the risk of unauthorized connections.

Keeping your Domain Controllers updated is another essential practice. Regularly applying patches for Windows Server and associated services ensures that known vulnerabilities are addressed. Many attacks exploit outdated systems, making timely updates a straightforward yet powerful security measure. Staying subscribed to vendor notifications for critical updates can help organizations act swiftly in response to emerging threats.

Authentication to DCs must also be robust. Multi-factor authentication (MFA) should be mandatory for administrators, adding an extra layer of protection against compromised credentials. To further enhance security, administritive tasks should only be performed using Secure Admin Workstations (SAWs), which are isolated from regular network traffic and protected against malware.

System-level security is equally important. Enable Secure Boot to guard against unauthorized firmware changes and rootkits, and encrypt DC disks with BitLocker to ensure that sensitive data remains protected in case of physical theft. In addition, disable unnecessary services, features, and protocols to minimize the attack surface. Non-essential ports should also be closed to reduce opportunities for exploitation.

Access to Domain Controllers should be tightly controlled. Only trusted and well-trained personnel should be permitted to manage or access these systems. Non-administrative accounts must not have interactive logon privileges, even indirectly, to prevent accidental or malicious misuse. Furthermore, routine backups of Active Directory and related configurations are essential. These backups should be stored offline or in isolated environments to protect them from ransomware attacks and ensure rapid recovery in the event of a breach.

Monitoring Domain Controllers for suspicious activity is vital. All logins, Group Policy changes, and system modifications should be audited regularly. Advanced monitoring tools can help detect abnormal behavior, such as unexpected replication changes or unauthorized access attempts, providing early warning of potential compromises.

In environments requiring additional security, consider deploying Read-Only Domain Controllers (RODCs) in branch offices or less secure locations. These provide authentication services without exposing writable AD databases, reducing the risk of tampering. Additionally, implementing a Tiered Access Model—isolating Tier 0 systems like Domain Controllers from lower-tier environments— ensures tighter control and limits the potential for lateral movement.

Securing Domain Controllers is not just about protecting a single system—it's about safeguarding the entire Active Directory infrastructure. A well-protected DC provides resilience against advanced threats, ensures business continuity, and reinforces the integrity of your IT environment. By adopting these practices, organizations can significantly reduce their risk exposure and strengthen their overall security posture

Limit Service Accounts and Protect Their Credentials

Service accounts are essential for running applications, services, and automated processes within an Active Directory (AD) environment. However, their elevated privileges and often weak security configurations make them a common target for attackers. Compromising a service account can provide an attacker with persistent access and the ability to escalate privileges, making it critical to limit their usage and secure their credentials.

The first step in managing service accounts is to minimize their use wherever possible. Organizations should assess whether a service truly requires a dedicated account or if a more secure alternative, such as a managed service account (MSA), can be used instead. MSAs are specifically designed for services and applications, offering automatic password management and simplified administration, reducing the risk of credential misuse.

For service accounts that must remain in use, privileges should be carefully restricted following the Principle of Least Privilege (PoLP). These accounts should have only the permissions necessary to perform their specific tasks and nothing more. Avoid assigning service accounts to high-privilege groups like "Domain Admins," as this creates a significant risk if the account is compromised. Regularly reviewing and updating service account permissions ensures they remain appropriate as needs evolve.

Password management for service accounts is another critical area. Strong, complex passwords should always be enforced, with a length of at least 25 characters to make brute force attacks impractical. Passwords should be changed regularly, particularly for accounts that do not support automated password rotation. Avoid reusing passwords across multiple service accounts, as this can create a single point of failure.

Organizations should also take steps to limit the exposure of service account credentials. Avoid hardcoding passwords in scripts, applications, or configuration files, as these can easily be extracted by attackers. Instead, use secure storage solutions such as password vaults or storage solutions such as password vaults or secret management tools to store and retrieve credentials when needed.

Monitoring and auditing service account activity is essential for detecting misuse. Track login activity, changes to the account, and unexpected behavior, such as logins from unusual locations or attempts to access unauthorized resources. Implementing alerts for suspicious activity provides an additional layer of protection, enabling a swift response to potential threats.

To further reduce the attack surface, organizations should disable interactive logon for service accounts. Service accounts should never be used as regular user accounts or for administrative purposes. By enforcing this separation, you reduce the likelihood of an attacker exploiting these accounts for lateral movement within the network.

Securing service accounts is a continuous process that requires regular reviews and adjustments. By limiting their usage, restricting privileges, enforcing strong password policies, and monitoring activity, organizations can significantly reduce the risk associated with these accounts. When properly managed, service accounts cease to be a vulnerability and instead serve their intended purpose securely, supporting the stability and functionality of your Active Directory environment.

Patch and Update Regularly

Keeping your Active Directory (AD) environment secure requires more than just configuring access controls and permissions; it also requires a proactive approach to patching and updating. Cybercriminals frequently target vulnerabilities in outdated software and systems, with many successful attacks exploiting known flaws that could have been prevented with timely updates. Regular patching is one of the most effective ways to protect your AD infrastructure and minimize the risk of compromise.

To ensure a robust patch management strategy, it is essential to stay on top of updates for all components of your AD environment, including Windows Server, AD-related services, and third party software. Many attacks, including those targeting AD itself, leverage vulnerabilities in outdated operating systems or unpatched applications. Regularly applying security patches and updates ensures that your systems are fortified against known threats and vulnerabilities.

A key aspect of patching is the timely application of critical updates. It's important to review vendor patch notifications and apply emergency security fixes as soon as they are released, particularly when they address zero-day vulnerabilities or active exploits. Delaying these updates increases the window of opportunity for attackers to exploit the vulnerability.

While critical patches should be prioritized, it's also important to maintain a regular update schedule for less urgent fixes. Establishing a monthly or quarterly patch cycle, depending on the criticality of the updates, ensures that your systems are consistently kept up to date. Additionally, it's essential to patch not just your domain controllers but also any servers, workstations, and network devices that interact with your AD infrastructure, as vulnerabilities in these systems can affect the entire network.

Before applying patches in a production environment, it is prudent to test them in a staging environment. This helps ensure compatibility with your existing systems and applications and minimizes the risk of operational disruptions. A staging environment acts as a buffer to detect potential issues before rolling out patches to live systems.

Automating the patching process where possible can further streamline this critical task. Many organizations implement automated patch management tools to help identify missing patches and deploy them across their systems. These tools can also generate reports and logs, helping you track which patches have been applied and identify any systems that may require attention.

In addition to patching operating systems and applications, consider regular firmware and hardware updates, especially for devices like routers, f irewalls, infrastructure that and other network interact with AD. Vulnerabilities in these devices can also pose a significant risk to your AD environment if left unpatched.

Regular patching not only protects against cyberattacks but also helps ensure compliance with industry regulations and standards, such as GDPR, HIPAA, and PCI-DSS, which often require maintaining updated systems.

By implementing a rigorous patch management strategy, you can significantly reduce the likelihood of a successful attack on your Active Directory infrastructure. Promptly applying updates, testing them thoroughly, and automating where possible helps maintain a secure environment that is resilient to the evolving threat landscape. Regular patching may seem like a routine task, but it is one of the most crucial components of a strong and secure AD security posture.

Protect Against Kerberos Attacks

Kerberos authentication is a critical component of Active Directory (AD), enabling secure communication and authentication between clients and servers in a network. However, because it plays such a pivotal role in the security of AD, it is often targeted by attackers seeking to exploit vulnerabilities for privilege escalation, lateral movement, and network persistence. Protecting against Kerberos attacks is essential for maintaining the integrity and security of your AD environment.

One of the most effective ways to protect against Kerberos attacks is by ensuring that Kerberos tickets (TGTs—Ticket Granting Tickets) and service tickets are encrypted using strong encryption algorithms. By default, Kerberos tickets use RC4-HMAC encryption, which is vulnerable to brute force attacks. To mitigate this risk, organizations should configure AD to use stronger encryption protocols, such as AES 128 or AES-256. These algorithms significantly increase the difficulty of cracking Kerberos tickets, making attacks like pass-the-ticket (PTT) or ticket renewal attacks much harder to execute.

Another critical aspect of defending against Kerberos attacks is protecting Service Principal Names (SPNs), which identify services running on networked computers. Attackers often abuse SPNs to escalate privileges through attacks like Kerberos ticket forging or Golden Ticket attacks. To minimize this risk, ensure that SPNs are registered only for legitimate service accounts and closely monitor for unauthorized SPN registrations. Regularly auditing and verifying SPNs can help identify potential misuse and reduce the chances of attackers manipulating these entries to gain elevated privileges.

In addition to monitoring SPNs, it's essential to limit ticket lifetimes and renewal periods. By default, Kerberos tickets are valid for extended periods (typically 10 hours or more), which gives attackers more time to exploit compromised credentials. Reducing ticket lifetimes and enabling more frequent ticket renewals can help limit the window of opportunity for attackers. However, this approach should be balanced against operational needs, as excessively short ticket lifetimes can negatively impact user experience and increase administrative overhead.

To further strengthen Kerberos security, consider implementing Protected Users groups within AD. These groups restrict the ability of certain accounts, particularly high-privilege certain accounts, particularly high-privilege accounts, to request tickets using older or weaker encryption methods. Additionally, enabling Kerberos Armoring (or Fast User Switching) can prevent attackers from manipulating tickets during transit, adding an extra layer of protection against Man-in-the Middle (MITM) attacks.

Regular auditing and monitoring of Kerberos activity is critical for detecting potential attacks early. Look for abnormal behaviors such as the creation of unusually large numbers of service tickets, unauthorized ticket requests, or any failed ticket validation attempts. Suspicious Kerberos activity can be an indication of an ongoing attack, such as pass-the-ticket or golden ticket attacks, that requires immediate investigation. Implementing real-time alerts for these anomalies can help you identify and respond to threats quickly.

Furthermore, organizations should enforce the Principle of Least Privilege (PoLP) for user accounts and service accounts. Limiting access to only the necessary resources reduces the attack surface, ensuring that even if an attacker is able to obtain a Kerberos ticket, their ability to escalate privileges or move laterally within the network is constrained.

Protecting against Kerberos attacks requires a multi-layered approach that includes strong encryption, careful monitoring of SPNs and ticket lifetimes, regular auditing, and the application of least privilege principles. By taking these steps, organizations can significantly reduce the risk of a successful Kerberos attack and ensure the continued security of their Active Directory environment.

Use Group Policy to Enforce Security Settings

Group Policy is a powerful tool for managing and enforcing security settings across an Active Directory (AD) environment. By configuring Group Policy Objects (GPOs), organizations can standardize security measures, reduce misconfigurations, and ensure consistent application of best practices throughout their network.

One of the most critical uses of Group Policy is to enforce password and account lockout policies. By setting requirements for password complexity, expiration, and minimum length, you can reduce the risk of compromised credentials. Account lockout policies can further protect against brute-force attacks by locking accounts after a set number of failed login attempts.

Group Policy also helps manage administrative privileges and access control. You can restrict local administrator accounts, enforce the Principle of Least Privilege (PoLP), and prevent the use of shared or generic administrative accounts. GPOs can be used to define which users can log on locally or remotely, minimizing unnecessary access points.

Another essential application is hardening system settings. GPOs allow you to disable outdated or insecure protocols, enforce encryption standards, and restrict the use of removable media. You can also configure logging and auditing policies to ensure visibility into critical system events and potential security threats.

Regularly reviewing and updating GPOs is critical to maintaining security. As threats evolve, policies must adapt to address new vulnerabilities and compliance requirements. By leveraging Group Policy effectively, you can create a secure, well-managed AD environment that reduces risks and enhances operational consistency.

Implement Zero Trust Principles

Zero Trust is a security framework that assumes no user or system should be trusted by default, regardless of whether they are inside or outside the network perimeter. In an Active Directory (AD) environment, this approach minimizes risks by limiting access and continuously verifying user and device identities.

To adopt Zero Trust, start by segmenting your network and applying strict access controls. Users should only have access to the resources they need, with all other access denied by default. Multi-factor authentication (MFA) is essential to verify user identities, particularly for accessing sensitive systems like domain controllers or administrative tools.

Continuous monitoring is another key aspect of Zero Trust. Implement tools to analyze user behavior and detect anomalies, such as unusual login patterns or unauthorized access attempts. Additionally, enforce strong authentication and authorization policies across devices and applications to ensure all access is validated in real time.

By implementing Zero Trust principles, The Lepide Data Security Platform The easiest way to secure your Active Directory with continuous auditing, threat detection and user behavior analytics. Explore In-Browser Demo Explore In-Browser Demo organizations can greatly reduce the likelihood of unauthorized access or lateral movement within the network, strengthening AD security against both internal and external threats.

Backup and Disaster Recovery Planning

Backup and disaster recovery planning are essential for protecting Active Directory (AD) from catastrophic failures, ransomware attacks, or data corruption. Without a reliable recovery plan, an AD breach or outage can lead to prolonged downtime and significant operational disruptions.

Regularly back up all critical AD components, including domain controllers, system state, and Group Policy Objects. Ensure backups are stored securely in isolated environments, such as offline or immutable storage, to protect them from ransomware or tampering. Test these backups frequently to verify that data can be restored quickly and accurately.

Disaster recovery plans should include detailed procedures for restoring AD in various scenarios, such as hardware failures, accidental deletions, or cyberattacks. Clearly define roles and responsibilities for IT staff and maintain updated documentation to guide recovery efforts.

A robust backup and disaster recovery strategy not only ensures business continuity but also enhances resilience against evolving threats, allowing organizations to restore operations swiftly and securely when incidents occur.

With a UBA profile in hand, the DSP can then decide whether a sudden flurry of permission updates or file queries and that correlates with the same user making an unusual number of AD lookups is normal — which might be the case say for a sys admin conducting system maintenances — or unusual and possibly the indication of a ransomware attack if the activities are associated with an ordinary employee in, say, the accounting or marketing department.

A security operations center that relies on a DSP can then, after perhaps verifying against manual checks of the system logs, confidently proceed in a response: stopping processes involved in the ransomware encryption, disabling user accounts that have been taken over by hackers, removing unusual registry entries, and then begin the file recovery process and notifying appropriate privacy and legal departments.

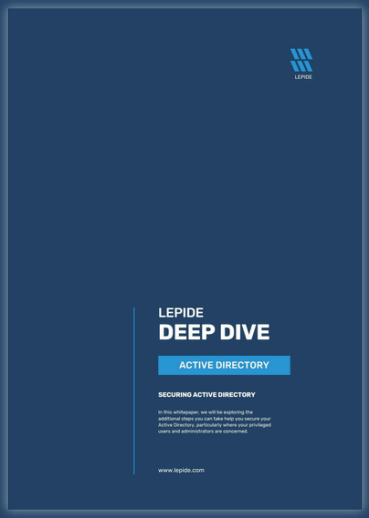
An added benefit to the DSP is that besides being able to detect threat an attack in progress, they can also automate some of the security protections we mention early.

Their auditing capabilities allow the DSP to understand user access patterns and therefore help derive folder permissions that reflect those employees that need access as part of their jobs. The DSP can also scan folders, AD, and Microsoft Exchange email accounts to discover sensitive data — PII, passwords, and confidential data — that either should be better protected with more restrictive permission, or perhaps in the case of plaintext passwords, just completely removed. Some DSPs can even automate a permissions approval process when an employee requests access to a project folder, routing it to the appropriate manager.

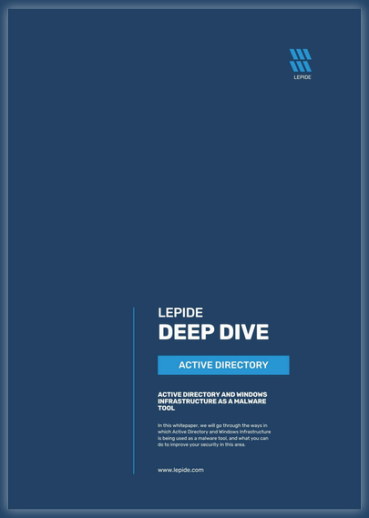
While it may be impossible in all cases to prevent ransomware from entering a system — particularly as new zero-days are discovered — it is possible with DSPs to make these occurrences a rarity, and to stop this malware in an early phase of its encryption process, long before it causes significant disruption..

Discover More Lepide Content

Read More



Read More



Read More

About Lepide

Mission

Our mission is to break the mold by delivering simple auditing and security solutions that enable organizations to protect their data and user directories, minimize their risks, and thrive.

Who we are

At Lepide, we believe that managing and securing your data shouldn't be complicated. Since 2005, we've empowered thousands of companies to protect and manage their unstructured data effectively. Lepide audits and protects files and folders, and the systems that govern access to them, without requiring a massive IT security team to manage it.

Why we exist

52% of organizations do not have the tools to confidently handle insider threats. 63% of companies admit that sensitive files are accessible to all employees. Companies simply don't have the visibility to detect threats and lack the speed to respond. Most enterprise-grade solutions that try to address these problems come with high costs and steep learning curves. Not Lepide.

What we do

- Lepide audits and protects files, folders, and access control systems.
- We offer this protection without requiring a large IT security team.
- Lepide unifies data security and Active Directory (AD) auditing across on-premises and cloud platforms.
- We provide enterprise-grade security at a non-enterprise cost.
- Lepide emphasizes faster reporting.
- The platform is designed for ease of use.
- Lepide is competitively priced.

Lepide in Numbers

Customers

1,000+

AND CLIMBING

Employees

100+

AND CLIMBING

Global Offices

3

AND CLIMBLING!

Solutions up close

Lepide Auditor

Find out more

Change Auditing and Reporting Solution

Audit and report on changes taking place to your key systems and data to help reduce your threat surface area, detect threats and meet compliance demands.

Lepide Trust

Find out more

Permissions Analysis Solution

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

Lepide Detect

Find out more

Real Time Threat Detection and Response Solution

Pre-defined threat models, and automated threat response, mean you can detect the signs of a compromise or security incident, and react in real time before it causes significant damage.

Lepide Identify

Find out more

Data Discovery and Classification Solution

Persistent data classification adds context to your security efforts. E-Discovery helps to speed up privacy and data subject access requests.

Lepide Protect

Find out more

Permissions Management Software

Easily define, monitor, and adjust permissions across your environments to prevent unauthorized access to sensitive information by ensuring that only authorized personnel have access to critical data.

Lepide IQ

Find out more

Our AI helper

Lepide IQ, ensures that organizations stay agile by interrogating data faster to provide essential information on demand and in turn saving valuable time in decision-making processes.