Lepide Case Study

Preventing permissions sprawl and implementing zero trust.

About the customer.

This U.S.-based financial services company employs around 1,500 staff and manages highly sensitive customer and transaction data across hybrid environments. Its IT operations are overseen by a small but experienced security and infrastructure team, reporting directly to the CIO. Protecting sensitive data, ensuring compliance, and strengthening defenses against insider threats and ransomware were identified as critical priorities.

The challenge.

The company's Active Directory and File Server environments had grown organically over many years. As a result, permissions sprawl had become a serious risk. Employees often retained access to systems and files long after changing roles, and over-permissioned accounts were widespread.
This situation created three major issues:

- **Excessive access to sensitive data**: Many users had more permissions than required, violating the principle of least privilege.
- **Audit fatigue**: Internal audit teams spent weeks trying to reconcile permissions and prove compliance with financial regulations.
- **Slow detection of threats**: Security teams lacked visibility into who was accessing critical systems and files, making it difficult to spot malicious activity or insider threats in real time.

The organization recognized that continuing without addressing these gaps would leave it exposed to both compliance penalties and data breaches. They wanted to move toward a **zero-trust model** where no user was trusted by default and access was tightly controlled and continuously validated.

The solution.

The company selected Lepide after evaluating several alternatives, choosing it for three key reasons:

- **Permissions Intelligence**: Automated discovery of over-permissioned accounts, excessive group memberships, and open shares across both AD and File Servers.
- **Zero Trust Enablement**: The ability to enforce least-privilege policies by right-sizing permissions and monitoring for drift in real time.
- **Unified Visibility**: A centralized view of all user activities, file access attempts, and permission changes across on-premises and cloud resources.

Implementation was completed in under two weeks. The IT team:

- Deployed Lepide's **permissions analysis** to map access across thousands of sensitive folders and AD groups.
- Established automated policies to **detect and remediate** risky permission changes.
- Configured continuous monitoring for anomalous logon behavior, lateral movement attempts, and suspicious access to regulated data.
- Leveraged reporting templates to demonstrate compliance with SOX, GLBA, and other financial industry regulations.

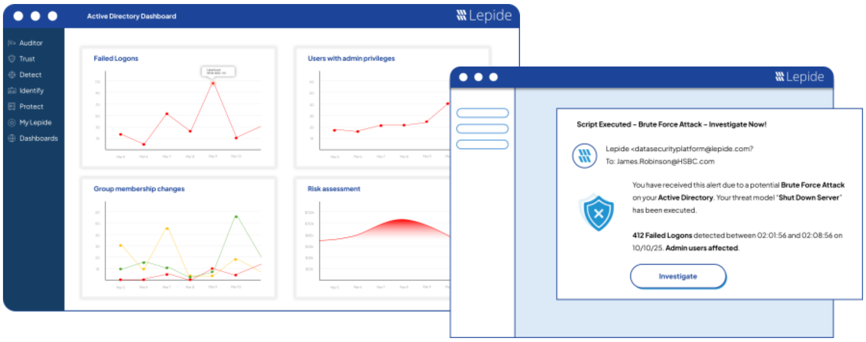
Key security outcomes.

Benefit	Impact
Reduced Permissions Sprawl	Automated identification and remediation of excessive privileges cut down high-risk accounts by 63%.
Zero Trust Implementation	Continuous monitoring and least-privilege enforcement laid the foundation for a zero-trust model.
Faster Compliance Audits	Reporting time for access reviews and regulatory audits was reduced from weeks to hours.
Proactive Threat Detection	Real-time alerts on suspicious logons and unauthorized file access enabled faster incident response.
Improved Security Posture	The organization transitioned from reactive clean-up to proactive, policy-driven data security.

What the customer said.

"Lepide gave us the visibility we needed to finally get permissions under control. We now have confidence that our users only have access to what they need, nothing more. It's a huge step forward toward zero trust."

Director of IT Security, Anonymous Financial Services Company



Script Executed – Brute Force Attack – Investigate Now!

Lepide <datasecurityplatform@lepide.com?
To: James.Robinson@HSBC.com

You have received this alert due to a potential **Brute Force Attack** on your **Active Directory**. Your threat model "**Shut Down Server**" has been executed.

412 Failed Logons detected between 02:01:56 and 02:08:56 on 10/10/25. **Admin users affected**.

Start your 20-day free trial today!