GETVISIBILITY

How Getvisibility Helps Organisation to Maintain Active Directory Security

USE CASE

getvisibility.com

Organisation Challenge

Organisations are curating and creating more and more valuable data. This data is being created in unstructured formats, such as email, spreadsheets, and document and media files.

This data is very powerful, but it also represents a risk to organisations if it falls into the wrong hands. Data breaches cause reputational damage and commercial damage, and they can breach regulations causing large fines.

One of the key risk areas relates to who has access to sensitive data. Active directory weaknesses are often the primary targets for attackers who want to exfiltrate or infiltrate an organisation's data.

Organisations are under increasing pressure due to remote working and the number of new applications they need to support. Each new application and each new remote workstation is a new vulnerability.

Ensuring that each user has the most appropriate level of access to each file is a very large and complex problem. The wrong level of access can overly restrict your organisation's efficiency and the value it gets from its data.

Knowing your data is key—where your data is, what it is and how it's growing over time. To implement an effective, least-privilege model, you need to first understand your data.

Another big challenge is visibility into who has access to sensitive files and building suitable reporting that provides context and insight into the data and the extent of access to that data.

Solution

The Getvisibility solution gives oversight of your active directory risk and tracks how that risk changes over time.

The Getvisibility solution is designed to help your organisation maintain best practice for active directory security. The Getvisibility solution ensures that your organisation maintains focus on:

1. Visibility and documenting your organisation's active directory
2. Enforcing safe practices among users and with your AD administrators
3. Building security around the domain controller
4. Effectively applying the least-privilege model
5. Monitoring data and associated active directory for compromise

How the Getvisibility solution works for managing active directory risk:

- Automated Discovery - Finding all data on every file share and end point
- Classification- Accurately classifying all data, both NEW and LEGACY data
- Identify all the weak points in the active directory (AD)
- Build an inventory of all at-risk files and vulnerable files
- Rate the risk and measure the indicators
- Identify all sensitive data, whether it be compliance-related or commercially sensitive
- Determine who has access to what data
- Creates a risk rating based on stale passwords, passwords that never expire, level of admin access, admin accounts with SPN and accounts with no password policy
- Frequently scheduled reporting
- Dynamic altering on any active directory changes

Getvisibility is powered by advanced AI. Using advanced AI enables discovery and monitoring of active directory risk to a level where organisations can start to bring their risk under control. Advanced AI brings a level of automation, accuracy and throughput that would previously require massive amounts of human resources, money and time.