AI.PROTECT
Attribute-based access control for SharePoint

Your information. Secured.

SharePoint is your productivity and collaboration platform. It helps your business thrive and your staff share information. But at the same time, you have a duty to protect your enterprise and its data.

With AI.PROTECT you can do both, without it being a burden. It’s collaborating on information – but within safe boundaries you have defined.

At a glance:

- Secure your data using rules you define providing Attribute-based access control for SharePoint.
- Protect sensitive data by combining the metadata associated with your content with Active Directory attributes.
- Define ethical walls, implement a deny permission, create jurisdictional boundaries and instantly lock down data at any time.

automated-intelligence.com
Information security is one of the most important risk factors for organisations to consider. Data needs to be protected to safeguard business interests, defend against external and internal threats, demonstrate good governance and ensure regulatory compliance.

But your data also needs to be accessible to the people who require it. If you put obstacles in their way – even for the best of reasons – you’ll restrict their ability to deliver results for your business.

What’s needed is a simple way of putting boundaries around data, which recognises the nature of its content, the clearance levels of those who need to access and the business rules defining its use.

With **AI.PROTECT** from Automated Intelligence, you can simultaneously maintain security and freedom of access in a way that’s simple and hassle-free for everyone.

Blanket rules don’t work. Sometimes the finance department really does need to see a sensitive document from a project. And sometimes a project document contains information that’s better not shared with everyone on the team.

With **AI.PROTECT** you can…

- **Use any metadata field to define a security policy** for an item in SharePoint – and that doesn’t just mean documents but sites, libraries and records too
- **Create positive or negative rules**, introducing a deny capability for SharePoint
- **Apply user attributes in Active Directory** that provide an access test for the item, whether that be:
  - a security classification (such as “secret” or “confidential”)  
  - something specific to a team or department, such as geographic location or team membership (HR, Finance or “Project X”)  

Direct access attempts are audited so you and your organisation can have confidence in, and full control of, your data at all times.

**Why AI.PROTECT?**

You get a flexible attribute-based security model that’s easy to set up, apply and maintain. Users with the necessary permissions can see and access the items they need, while those who don’t meet the criteria you define are blocked. What’s more, those without permission are not even made aware of the item’s existence; it won’t appear in the results of any search they do, nor when browsing within SharePoint.

You can focus on the productivity and competitiveness of your organisation in the knowledge your data is secure.

---

**Contact us to arrange a demonstration of our solution or a proof-of-concept proposal, and we’ll show you how you can protect your data without creating complications for yourself or your users.**

**Find out more**

T +44 (0)28 9099 6118 | E info@automated-intelligence.com | W automated-intelligence.com