



AGENTIC AI CONTROL

idgard—the secure gatekeeper for
your data in the AI era.

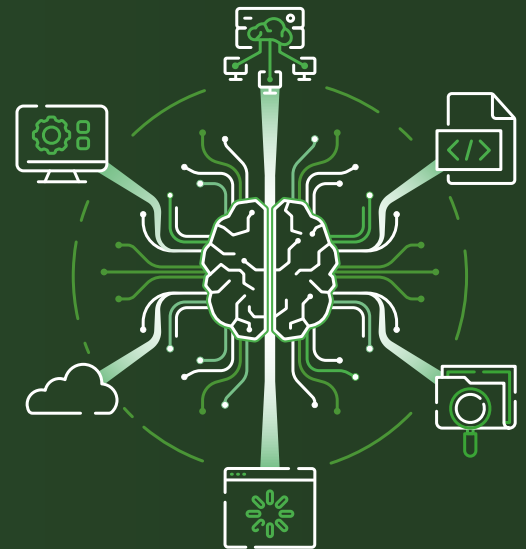


When AI agents access your data

Autonomous AI agents are changing the way data is used—but also how it is at risk.

Invisible risks

AI agents generally access all data sources available to them. This becomes particularly critical for data stored locally on end devices, as it is easily accessible to the AI. Without targeted protective measures, this means that all locally stored information can be fully viewed and used by AI agents.



Why this is problematic

AI agents do not always act in a controlled manner:

- › due to flawed decisions
- › due to manipulated or misleading information on the internet
- › due to a lack of security mechanisms
- › or simply due to unintentional errors

Consequences for your company

- › Data leaks to external AI services
- › Loss of confidential information through its use in training data
- › Unnoticed data changes—intentional or accidental

In short:

*Where data is available
unprotected, it is also available
to AI agents.*

idgard: Secure access instead of uncontrolled AI

idgard consistently protects your data—even from autonomous AI agents.

Your security advantages

- › No local data storage by default
- › No access by AI agents without authorization
- › Full control over data access

When AI is used strategically

You consciously decide when and how AI is allowed to access data:

- › Granular access control (ERM)
- › AI sees only data that has been explicitly approved
- › Complete traceability
- › Access and changes can be audited at any time
- › Cryptographically secured

Two **secure** use cases

1. AI agent with controlled access

- › Dedicated user account for the agent
- › Access via API—no additional system required
- › Fully controllable & traceable

Ideal for:
automation, analysis, secure AI integration

2. AI agent with local access

- › Only specifically downloaded data is used
- › No access to other content
- › Full control remains with the user

Ideal for:
individual tasks, maximum data security

Real-world example

Without idgard:

The AI processes local files, which can result in confidential documents being unintentionally transmitted. As a result, this data may end up in the training systems of external AI services. Additionally, there is a risk that manipulated content could be incorporated into the processing, leading to distorted or incorrect results.

With idgard:

Only the data that is actually needed is shared, preventing unauthorized access. At the same time, every activity remains transparent, as changes can be traced at any time. In this way, confidential content remains protected at all times.

Conclusion

Autonomous AI requires oversight. idgard is your shield:

- › You decide what AI is allowed to see
- › You reliably prevent data leaks
- › You remain in control at all times



We create trust through security.

idgard GmbH
Landsberger Str. 396
81241 Munich

+49 (0)89-444 435 140
contact@idgard.com
www.idgard.com

idgard combines highly secure data exchange and virtual data rooms in a single product—for efficient and legally compliant digital collaboration. The highest security and compliance requirements are met, ensuring GDPR-compliant processing of sensitive data.

More than 1,200 companies already rely on idgard, including IT and communications providers, management consultancies, financial service providers, government agencies, and operators of critical infrastructure.

