AQ SECURE

Secure Implementation and Use of AI Solutions

INTRODUCTION

The Power and Promise of Generative AI

AQ SECURE

Artificial Intelligence has become an integral part of modern data-driven business processes, significantly contributing to innovation and efficiency. However, AI deployment carries substantial risks for data protection, compliance, and intellectual property that require robust security measures and clear governance frameworks.

Generative AI technologies including Large Language Models (LLMs) for text, diffusion models for images, and generators for audio, video, and multimodal content open diverse opportunities for companies to foster creativity and productivity.

AI supports automation, improves decision-making, and optimizes operational processes across industries.

SECURITY LANDSCAPE

AQ SECURE

The Critical Security Landscape

77%

Data Leaks

Of data breaches occur through inserting data into generative AI solutions

9/10

Companies Affected

German companies report data theft incidents

€289B

Economic Damage

Cost to German economy from industrial espionage in 2025

AI solutions often process highly sensitive information that must be comprehensively protected. The risk of unwanted internal access to confidential data through AI solutions like Microsoft Copilot or ChatGPT, combined with the threat of confidential company information being shared with external AI platforms, creates an urgent need for robust security measures.

KEY CHALLENGES

AQ SECURE

The Implementation Challenge

The deployment of generative AI solutions has rapidly transformed the data security landscape in companies, driven by several critical challenges:

Infrastructure Overload

Isolated data security solutions have led to inefficiencies and significantly strained company resources

Data Fragmentation

Data is distributed across endpoints, SaaS applications, email, internet, and generative AI solutions

Escalating AI Risks

Companies use 20-90 different AI applications weekly, amplifying insider threats

Regulatory Pressure

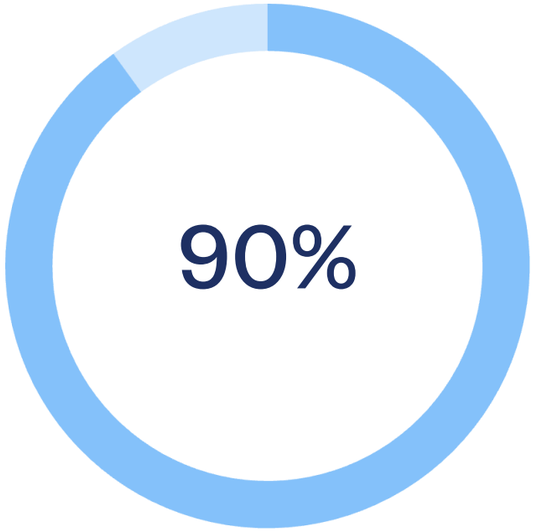
Evolving regulations (GDPR, NIS2, DORA, EU AI Act) require proactive data governance

SHADOW AI

AQ SECURE

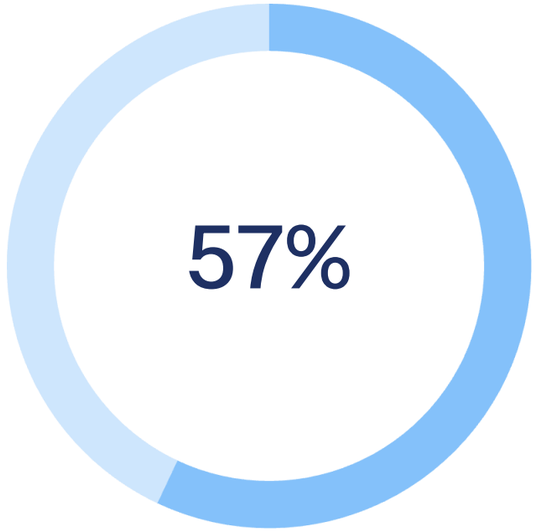
Shadow AI: The Hidden Threat

Shadow AI represents the uncontrolled use of generative AI solutions by employees or teams without IT approval or security oversight a rapidly growing threat posing immense security challenges.



Unauthorized Usage

Employees use public AI solutions like ChatGPT via private accounts



Data Exposure

Respondents admitted entering confidential company information into AI solutions

AQ SECURE

Critical Risks of Shadow AI

Data at Risk

- Intellectual property (source code, designs)
- Customer data
- Financial information
- Meeting notes
- Internal strategy papers

Once uploaded, data can end up in AI providers' training datasets or be stored long term. Many AI providers reserve the right to reuse entered data to improve their models, leading to uncontrollable data leaks or loss of control over intellectual property.

AQ SECURE

Consequences of Uncontrolled AI Use

Loss of Control

IT departments cannot monitor data flow or enforce security policies

GDPR Violations

Potential breaches of data protection regulations

Information Exposure

Sensitive information may fall into wrong hands

AI provider privacy policies are often unclear and complex, particularly regarding GDPR and industry-specific requirements, creating high-risk scenarios for companies without proper oversight.

AQ SECURE

SECURITY STRATEGY

Comprehensive Strategies for Securing AI

To safely and controllably leverage the productivity and efficiency of generative AI solutions without compromising overall cybersecurity and data security, comprehensive strategies are required. This begins with assessing AI readiness and developing a strategic roadmap for secure and effective AI implementation.

AQ SECURE

Key Security Strategies

1

Secure Development & Deployment

Implementation and integration of AI solutions into existing infrastructure while adhering to best practices and compliance regulations

2

AI Solution Protection

Protecting AI solutions from attacks and manipulation AI faces new attack vectors beyond traditional IT security

3

Data Classification & Risk Assessment

Identifying vulnerabilities and hidden AI cybersecurity risks through DSPM solutions

4

Compliance & Regulatory Requirements

Ensuring adherence to GDPR, ISO 27001, ISO 42001, BSI-Grundschutz, and EU AI Act

5

Monitoring & Transparency

Creating visibility into who uses AI, what prompts are submitted, which files are uploaded, and associated risks

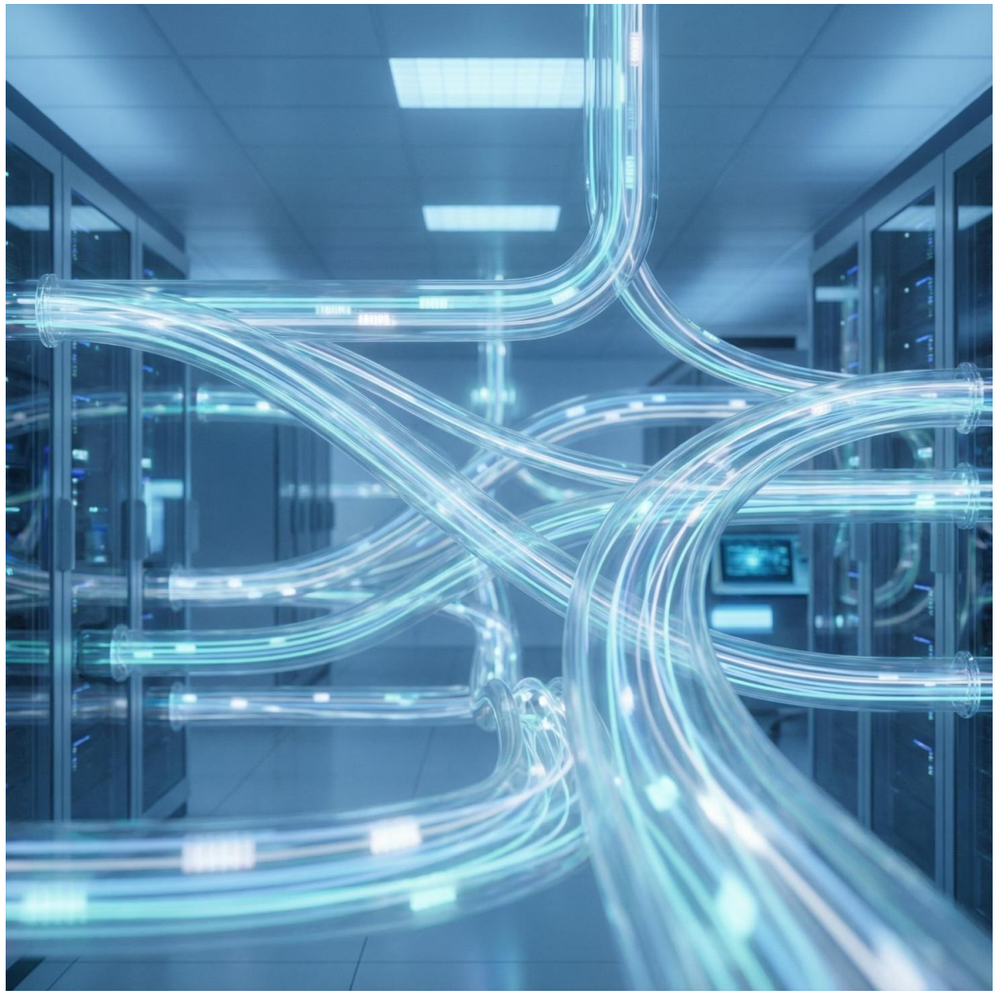
Data Transparency Challenge

AQ SECURE

Data is no longer in one location but moves and is distributed across endpoints, SaaS applications, email, the internet, and generative AI solutions.

A significant problem is transparency: 85% of companies don't know where their sensitive data is stored.

Data Security Posture Management (DSPM) solutions help identify and classify sensitive and confidential data within companies, addressing risks early before protective measures block unauthorized data sharing.



DSPM SOLUTIONS

AQ SECURE

Data Security Posture Management (DSPM)

Component	Function	Example
DSPM Scanner	Identification of sensitive data inventories	Scan of storage paths, cloud buckets
Risk Analysis Dashboard	Visualization of vulnerabilities	Detection of misconfigured storage
Policy Recommendations	Derivation of protection rules	Definition of sensitive data categories

Distributed Storage Landscapes

Hybrid and multi-cloud environments

Data Protection & Compliance

Ensuring regulatory adherence

Access Governance

Enforcement of data access policies

DLP Preparation

Foundation for prevention rules

AQ SECURE

DLP SOLUTIONS

Data Loss Prevention (DLP)

To protect sensitive data from unauthorized access, theft, or loss, prevent data breaches, comply with regulations, and minimize financial and reputational damage, companies should implement DLP solutions alongside DSPM.

DLP deployment offers a comprehensive approach to protecting sensitive data based on the combination of technical solutions, policies, and employee awareness.

AQ SECURE

DLP Architecture and Modules

Module	Function	Example
Core DLP Engine	Rule-based classification & control	Blocking confidential files
Endpoint DLP Agent	Protection on endpoints (USB, clipboard, etc.)	Screenshot lock, USB control
Email/Web/Cloud DLP	Control of communication and upload channels	Warning for sensitive email attachments
Risk-Adaptive Protection	Dynamic response to user behavior	Escalation for anomalies

Risks Without DLP: Loss or misuse of sensitive data, data leakage via USB, email, or Shadow AI, and data abuse by over-privileged users

BROWSER SECURITY

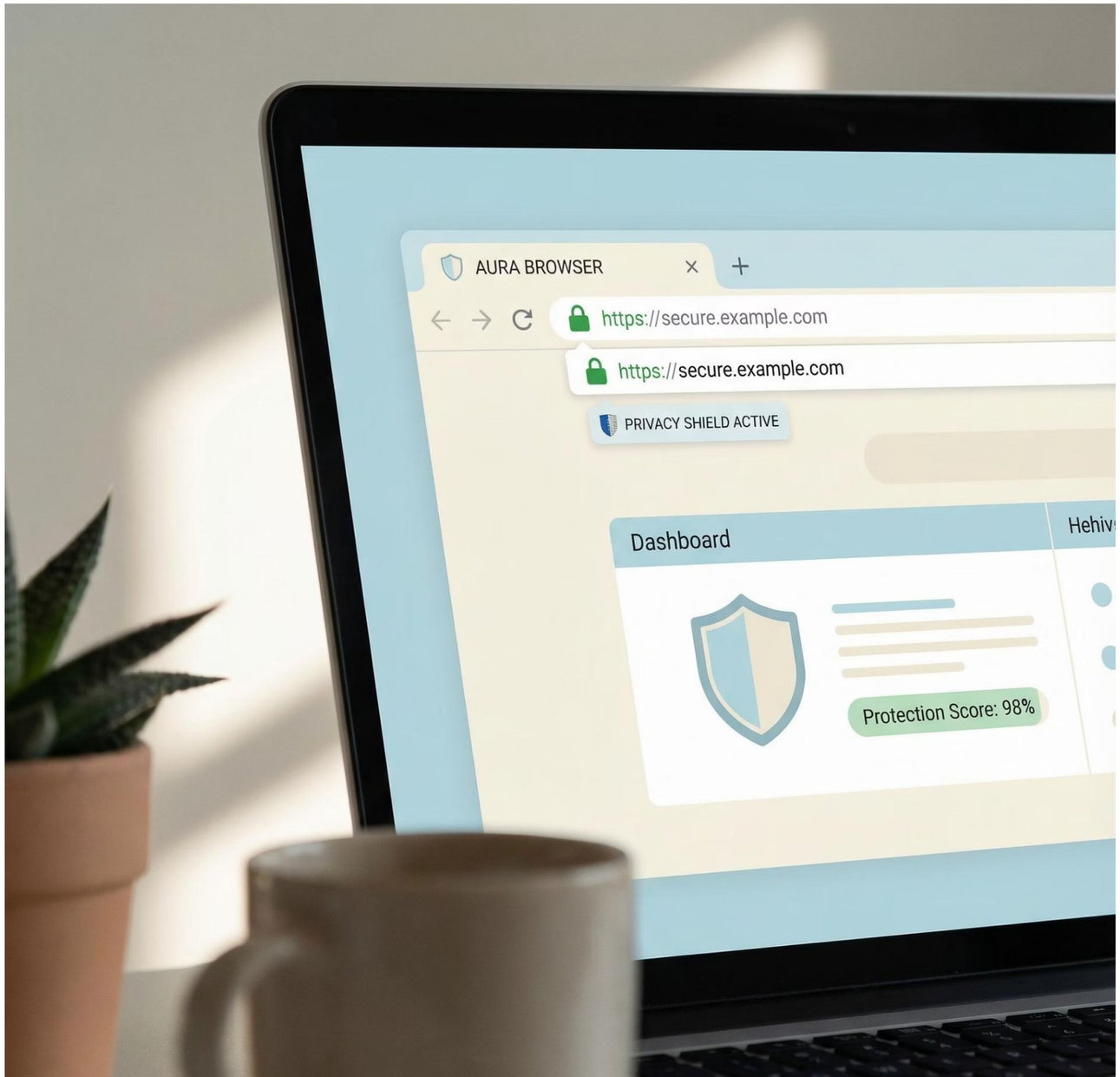
AQ SECURE

Web Browser Security with Integrated DLP

The strategic pillar for managing Shadow AI risks and protecting generative AI solutions is web browser security with integrated DLP.

Since employees typically access generative AI solutions through web browsers, they can share confidential company data with external AI solutions.

Modern web browser security solutions with integrated DLP functionality offer advanced protection mechanisms to specifically counter these risks, enabling secure use of generative AI solutions even in Bring Your Own AI (BYOAI) scenarios or open SaaS environments.



AQ SECURE

Browser Security Benefits

IT Transparency

Visibility into actual AI solution usage and whether sensitive data is involved

Controlled Access

Safe use of AI solutions while maintaining security standards

Compliance Assurance

Protection against misuse while ensuring regulatory compliance

BUSINESS GOALS

Achieving Strategic Objectives

AQ SECURE

Through implementation of proposed data security solutions and strategies, companies can achieve the following business goals and design their AI initiatives securely and successfully:

Minimize Data Risks

Detection and classification of data, remediation of excessive access (Least Privilege), and continuous search for publicly shared files

Deploy AI Securely

Unlock AI productivity without risk through Shadow AI management, policy enforcement via user coaching, and safeguards preventing unauthorized disclosure

Ensure Compliance

Strengthen regulatory adherence through more precise policy implementation across various channels, avoiding legal violations

Boost Productivity

Leverage generative AI capabilities safely and controllably to increase productivity without compromising overall cybersecurity posture

HUMAN FACTOR

The Human Factor: Security Culture

Beyond technical safeguards, a strong IT security culture and awareness are crucial. Regular training must sensitize employees to AI risks.

Clear Communication

Which AI solutions are approved and which data must never be entered into external AI solutions or AI-supported applications

Risk Awareness

Understanding the consequences of data exposure and unauthorized AI usage

Continuous Education

Regular updates on evolving threats and best practices

Only through a multi-layered AI security approach that combines technical solutions with governance and employee awareness can AI solution usage be successfully ensured.

AI SECURITY FRAMEWORK

AQ SECURE

The AI Security Framework

Assessment

Evaluate AI readiness and identify vulnerabilities

Strategy

Develop comprehensive security roadmap

Optimization

Refine policies and adapt to threats

Implementation

Deploy DSPM, DLP, and browser security

Training

Build security culture and awareness

Monitoring

Continuous oversight and risk detection

AQ SECURE

Your Partner for Secure AI Implementation

At AQ SECURE, we understand the specific challenges small and medium-sized enterprises face when introducing AI. We accompany you with a pragmatic, targeted, and technology-open approach on the path to secure implementation and use of AI solutions.

Our cybersecurity experts support you in successfully and securely designing your AI initiatives with comprehensive guidance tailored to your business needs.

AQ SECURE

NEXT STEPS

Take the Next Step

If you want to learn how we can help you to securely introduce and use AI solutions in your company, schedule a consultation with our cybersecurity experts today.

> We support you in successfully and securely designing your AI initiatives.

Through targeted deployment of AI, data, and browser security solutions, you can safely and productively leverage AI's full potential while ensuring compliance and protecting against misuse.