AI Data & Security Dashboard

AI & Data Security Posture Mangement

Billennium

Introducing our Data & AI Security Posture Management Solution

A unified platform that secures monitored AI estate and provides end-to-end visibility across security risks and controls.

What is a Data & AI Security Posture Management Solution?

A solution that leverages **Azure-native security and governance services**, along with established standards, to consolidate everything into a **single, clearly presented AI and data security dashboard.**

✓ Good news! AI and Data Security don't have to slow innovation. The **AI & Security Dashboard** gives your teams a clear, unified view of risk — so you can move faster with confidence and stay in control as AI scales.

Why teams choose us

☑ **Security posture–driven**

Built around continuous AI & data risk visibility, misconfiguration detection, exposure reduction across environments

☑ **Managed security**

ASSESS → PRIORITIZE → REMEDIATE → REPORT

Delivered as an ongoing service, not a one-time assessment

☑ **AI & data–centric by design**

Covers AI workloads, training data, data stores across cloud and hybrid environments

☑ **Compliance-ready by default**

Continuous control monitoring, audit-ready evidence and clear reporting without manual effort

☑ **Actionable risk prioritization**

Not just findings but clear priorities. Context-aware risk scoring, focus on what truly matters

Main challenges

Fragmented Visibility

AI projects, models and data are spread across multiple subscriptions, services and tools, with no single place that shows the full, end-to-end AI and data security posture.

Data Sprawl

Sensitive data is copied and replicated across clouds, SaaS, file shares and AI workloads without consistent classification, ownership or protection, making it difficult to know what data exists, where it resides and how it is used.

Shadow AI

Users experiment with Copilots, external LLMs and AI agents on their own, often with business-critical or sensitive data, outside central governance, DLP policies and monitoring.

Risky Misconfigurations

Open storage, over-permissive identities, weak network controls and poorly configured AI services create unintended exposure paths for sensitive data and AI workloads.

Compliance Gaps

There is no central view of how regulated or critical data is accessed and processed by AI services, which makes demonstrating controls, audit trails and compliance coverage extremely difficult.

Slow Response

Security signals are scattered across many tools, so detecting AI- and data-related incidents, triaging them and driving remediation is slow, manual and hard to track in a structured way.

How we solve these challenges - building solution

1. Scope & Environment Onboarding

AI workloads, data stores and subscriptions are scoped and onboarded into the existing Azure landing zone and Microsoft Defender for Cloud.

2. Cloud & Data Security Posture (Defender CSPM)

Security policies. Defender CSPM (including data security posture management) and Secure Score are configured to establish an initial cloud, data and AI security posture baseline.

3. Data Security Posture (Purview DSPM)

Microsoft Purview DSPM and DSPM for AI are enabled to complement Defender CSPM by discovering sensitive data. assessing cross-cloud data risks and mapping how data is used by AI workloads.

4. AI Workload Threat Protection

Data & AI security plans and AI threat protection capabilities are enabled in Defender for Cloud, with AI-related alerts integrated into Microsoft Defender XDR.

5. Centralized Telemetry in Sentinel

Log Analytics and Microsoft Sentinel are used to ingest and normalize telemetry and alerts from Defender, Purview and key Azure services into a single SIEM layer.

6. Analytics Rules & Automation

Analytics rules, incident types and playbooks are configured in Sentinel to detect AI- and data-related security incidents and to automate triage and response.

7. AI & Data Security Dashboard

A unified AI and data security dashboard is built using Defender, DSPM and Sentinel workbooks to present posture, risks. incidents and remediation status in one place.

8. Operating Model & KPIs

An operating model, governance routines and KPIs are defined so that AI and data security posture can be continuously monitored, reported and improved.

What we use ?

- Azure Landing Zone
- Azure Policy
- Microsoft Defender for Cloud (Defender for Storage, Defender for Databases)
- Microsoft Sentinel
- Microsoft Purview DSPM/ DSPM for AI

Make AI real—securely, governed and measurable

Gain visibility, reduce risk, strengthen your AI and data security posture

Secure your AI and data today