



AI Trust Supported by Governance

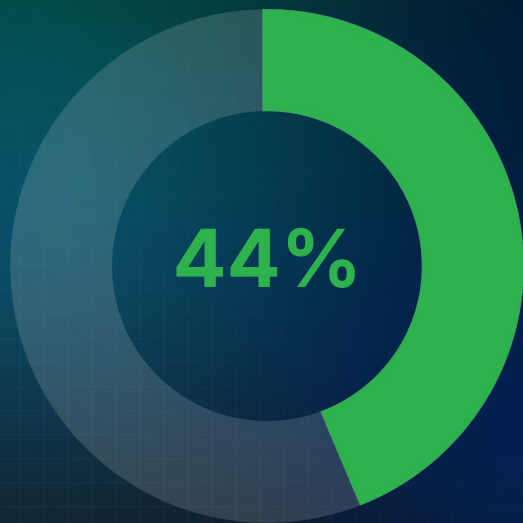
Bringing Together Data Quality, Privacy, and
Security for AI Trust

James M Barker, Data Strategy Principal

May 7, 2026



Data Quality concerns have quickly become the biggest barrier for AI adoption in 2025 for AI Leaders



BARC

2025 REPORT

Lessons From the Leading Edge

Up from 19% in 2024



The **AI Trust** Chasm: Current Tools are Failing

Where Enterprise AI Stands Today

AI project abandonment jumped from 17% to 42% YoY ([S&P Global](#))

"The Gap"

Low quality data

Data leakage

Poor governance

Lack of compliance and risk controls

Data lineage

Result: Focus on low-value low-risk use cases that can't scale

The Promise of AI

KPMG projects AI will add \$2.84T to US GDP by 2030

AI Trust - Common Myths

Data Quality

Bad Data Generates Bad AI

- Get the data right
- Use the right data
- Increase confidence in AI

“

Data quality is subjective, we are ok with what is generated. Trust well, I don't know?

Data Sensitivity

Using Sensitive Data in AI - Show Stopper

- What data can be used in AI
- What data is PCI, PII, PHI
- Tracking & Control of Data for AI

“

Sensitivity isn't a problem for us the CISO makes sure we only use data available for use. We trust the data we use is ok, I don't care?

Data Security

CISO Teams can do so much for AI Safety

- Partitioning of Data Helps
- Controlling Access Helps More
- Renegade AI Solutions are the issue

“

We don't have AI data use problems, our CISO makes sure the right data is being used in AI. If we are using the wrong data, it's the CISO's fault

Common Myths

AI turns a small data problem into
an enterprise crisis

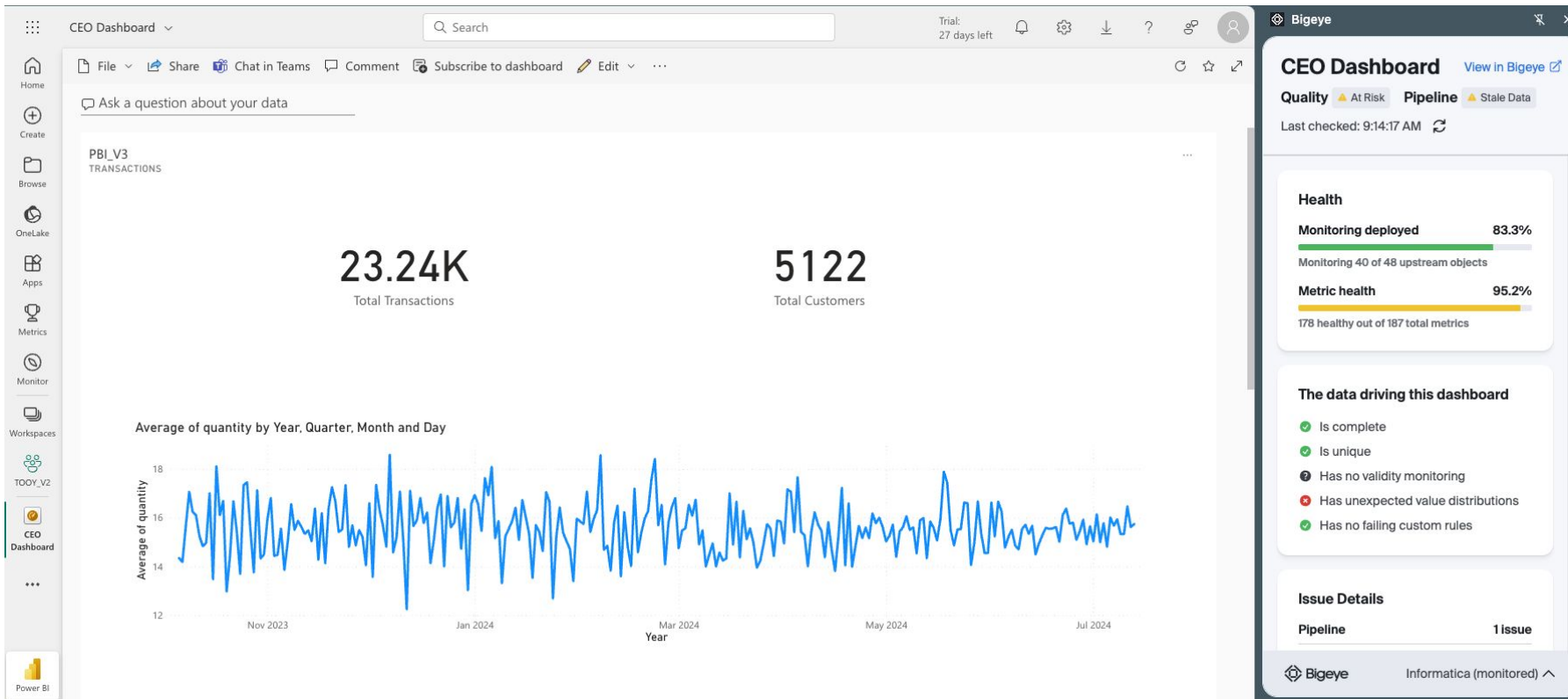


AI is only as
good as the
data it runs on

Data Quality



End User - Can I Trust this Report?





AI is only one
strike away
from being
shut down

Data Sensitivity



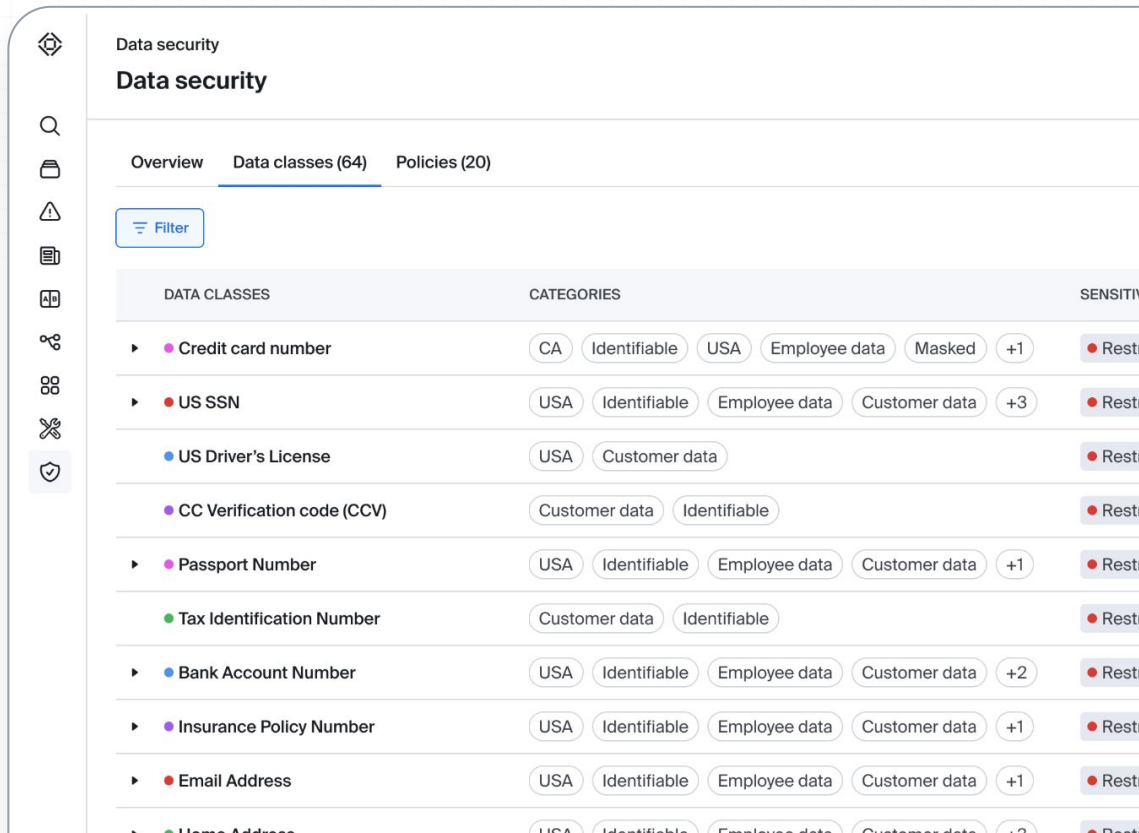
Capability Example

Sensitive Data Scanning

Automate discovery, classification, and reporting of sensitive data across your data landscape.

Get started quickly with built-in sensitive data classifiers, or modify them to meet your organization's unique classification needs.

Set sensitivity levels for enforcement and reporting, and visualize findings in the context of your lineage graph.



The screenshot displays the 'Data security' section of the Bigeye interface. It features a sidebar with navigation icons and a main content area with tabs for 'Overview', 'Data classes (64)', and 'Policies (20)'. A 'Filter' button is present. The main area shows a table of data classes with their categories and sensitivity levels.

DATA CLASSES	CATEGORIES	SENSITIVITY
▶ Credit card number	CA, Identifiable, USA, Employee data, Masked, +1	Rest
▶ US SSN	USA, Identifiable, Employee data, Customer data, +3	Rest
• US Driver's License	USA, Customer data	Rest
• CC Verification code (CCV)	Customer data, Identifiable	Rest
▶ Passport Number	USA, Identifiable, Employee data, Customer data, +1	Rest
• Tax Identification Number	Customer data, Identifiable	Rest
▶ Bank Account Number	USA, Identifiable, Employee data, Customer data, +2	Rest
▶ Insurance Policy Number	USA, Identifiable, Employee data, Customer data, +1	Rest
▶ Email Address	USA, Identifiable, Employee data, Customer data, +1	Rest
▶ Home Address	USA, Identifiable, Employee data, Customer data, +2	Rest



RBAC can only
do so much

Data Security





AI Guardian

AI Guardian synthesizes signals across the AI Trust Platform to provide visibility into the context, data, and files your AI applications consume.

With these insights, teams can deploy AI agents faster while maintaining stronger governance, trust, and security.

UNIQUE TO BIGEYE

The only AI Guardian vendor focused on the quality and sensitivity of data being accessed, not just security, governance, etc with runtime protection.

Weyland Copilot Conversation - jeremy.bear@weylandbank.com

Prompt: What credit card should I recommend to Emily Thompson?

Dec 18, 2025, 1:48 PM

Chat conversation

Chat lineage

Conversation History

Access Details

USER PROMPT • DEC 18, 2025, 1:48 PM

What credit card should I recommend to Emily Thompson?

AGENT RESPONSE

- 🧠 Analyzing request...
- 📊 Querying Snowflake for customer data... ✓ Retrieved customer profile and account balances
- 💳 Fetching credit card products... ✓ Loaded 10 available card products
- ⚙️ Running eligibility analysis... ✓ Recommendation generated

Based on **Emily Thompson's** excellent financial profile, I recommend the **Wondrous Elite**.

Emily's Financial Status:

- Account Balance: \$329,500
- Credit Score: 795
- Outstanding Loans: \$12,000

🔍 weyland_bank_demo

⚠️ Warning Policies evaluated: PII Pr

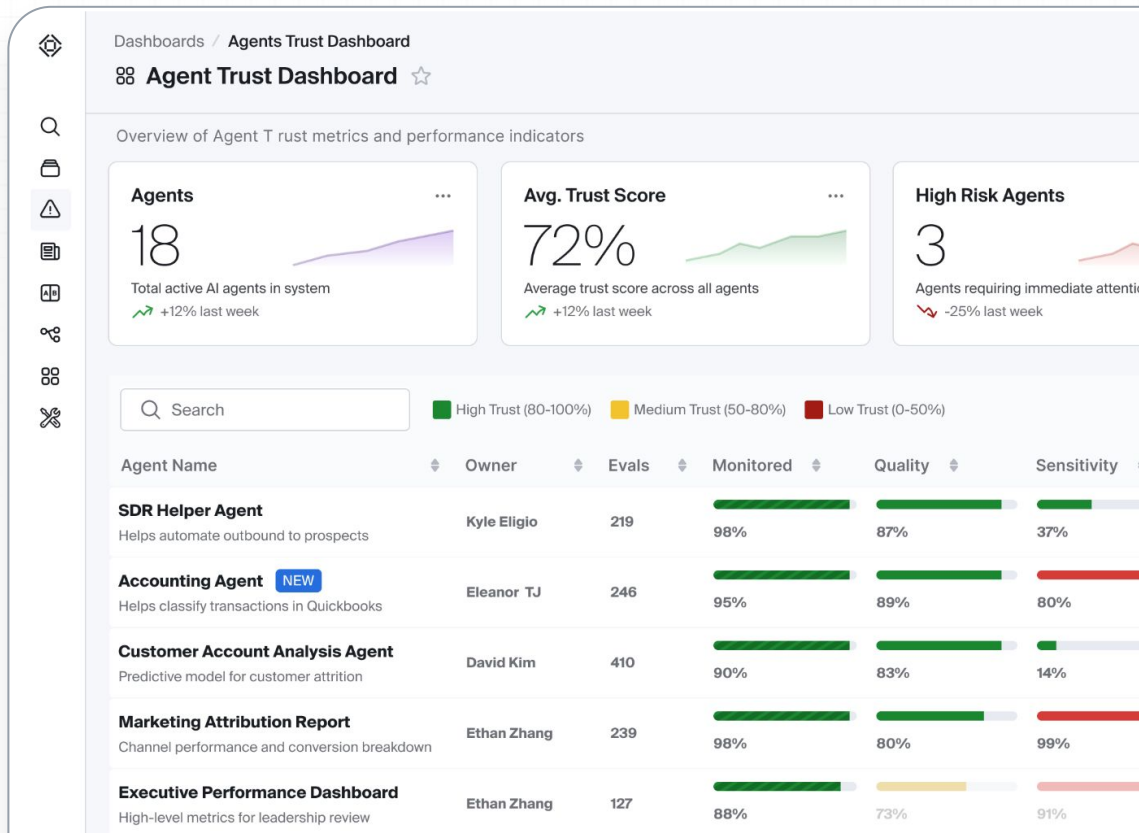
Tables accessed: ✓ weyland_bank,
⚠️ weyland_bank,
✓ weyland_bank,
✓ weyland_bank,

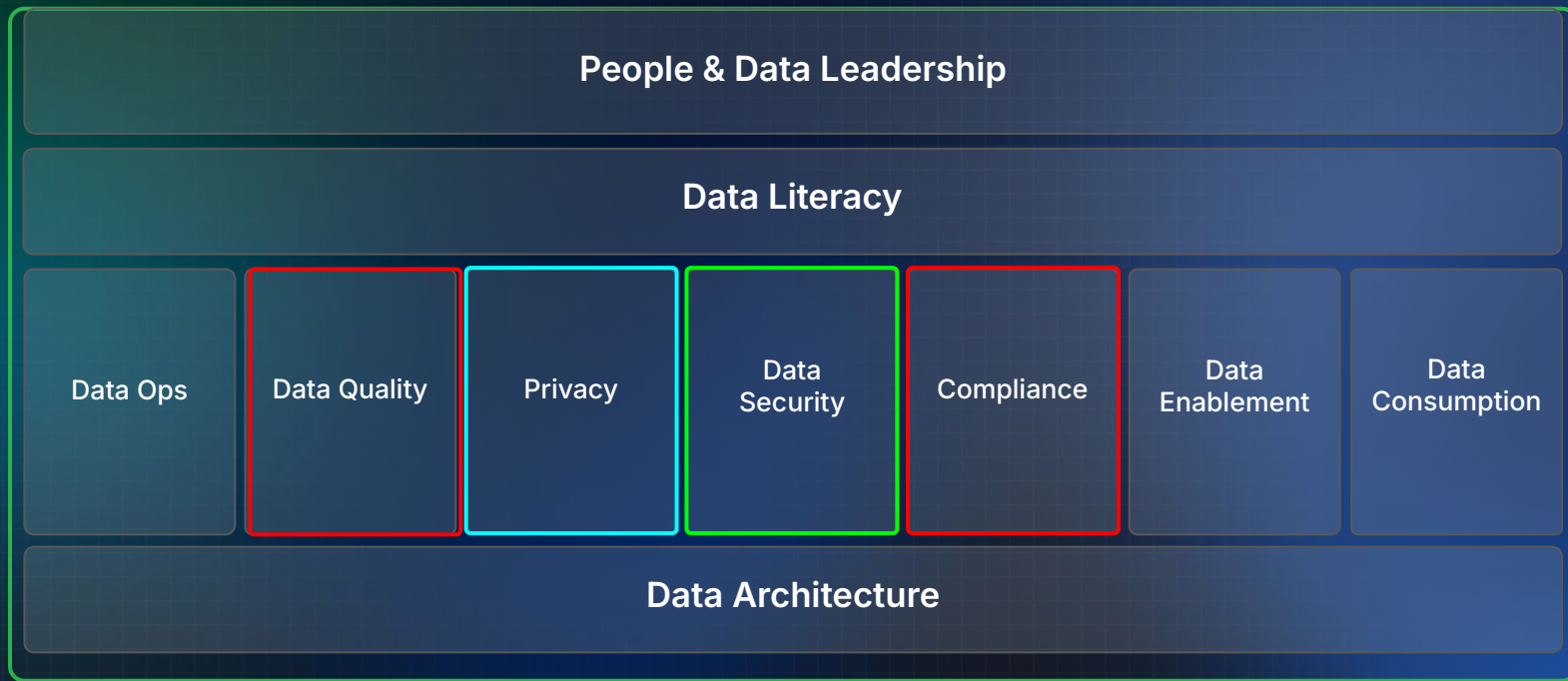
Feature Preview

AI Guardian

Increase adoption of agentic AI by ensuring data used by agents meets your quality, sensitivity, and certification policies.

Bigeye automatically tracks structured and unstructured data accessed by agents and gives you a single pane of glass for quantifying agent trustworthiness.







AI Guardian

Data Access Gateway + Policy Engine



Data Observability

Monitoring + Rules + Alerting



Data Sensitivity

Scanning + Classification



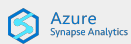
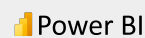
Data Governance

Certification + Ownership + Glossary



Metadata Platform

Data Catalog + Data Profiling + Data Lineage



AI Trust - Common Myths

Data Quality

Bad Data Generates Bad AI

- Get the data right
- Use the right data
- Increase confidence in AI

“

Focus on Foundations - get the data right and keep it there:i.e. meet “Business Fit”

Data Sensitivity

Using Sensitive Data in AI - Show Stopper

- What data can be used in AI
- What data is PCI, PII, PHI
- Tracking & Control of Data for AI

“

Identify what data can be shared, used, or is privacy sensitive (PCI, PII, PHI) and make sure it is used in AI solutions appropriately

Data Security

CISO Teams can do so much for AI Safety

- Partitioning of Data Helps
- Controlling Access Helps More
- Renegade AI Solutions are the issue

“

Use CISO capabilities as much as possible, but don't feel resolved that this is 'Their' problem. Expect the unexpected

Getting it Right



***Download Our
Research Report***



Next Steps for AI Success

Get your Data AI Ready

Invest in data lineage and observability solutions

Read the full BARC Research

Benchmark where you are against other AI leaders

Join our Design Partner Program

Help shape what trusted enterprise AI looks like in practice.

Let's Connect! <https://www.linkedin.com/in/jim-barker/>