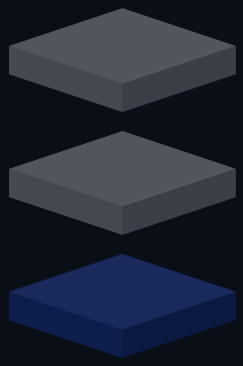
Ariavor



Governed reporting across a production network

An industrial manufacturer whose 25 sites each reported on their own terms. One governed model now serves the network, and every viewer sees only their own numbers.

SECTOR
Industrial manufacturing

PERIOD
7 months

PATH
Foundation to Acceleration

NETWORK
25 sites

OCTOBER 2026

AT A GLANCE

25 site reports, replaced by one network report

Every site could report on itself and none could be compared with another, because the numbers that make a network comparable are also the numbers a site manager should not see for a neighbouring site. One governed model with the access rules inside it solved both.

25
production sites, reporting on one layer

800+
BI consumers, each seeing only their own numbers

3
domain semantic models: Operations, Controlling, Executive

7
months from the first review to group-wide reporting

Anonymised by sector and size, because the confidentiality that protects this client would protect you too. Sector and outcomes are real; identifying detail is not.

Before and after

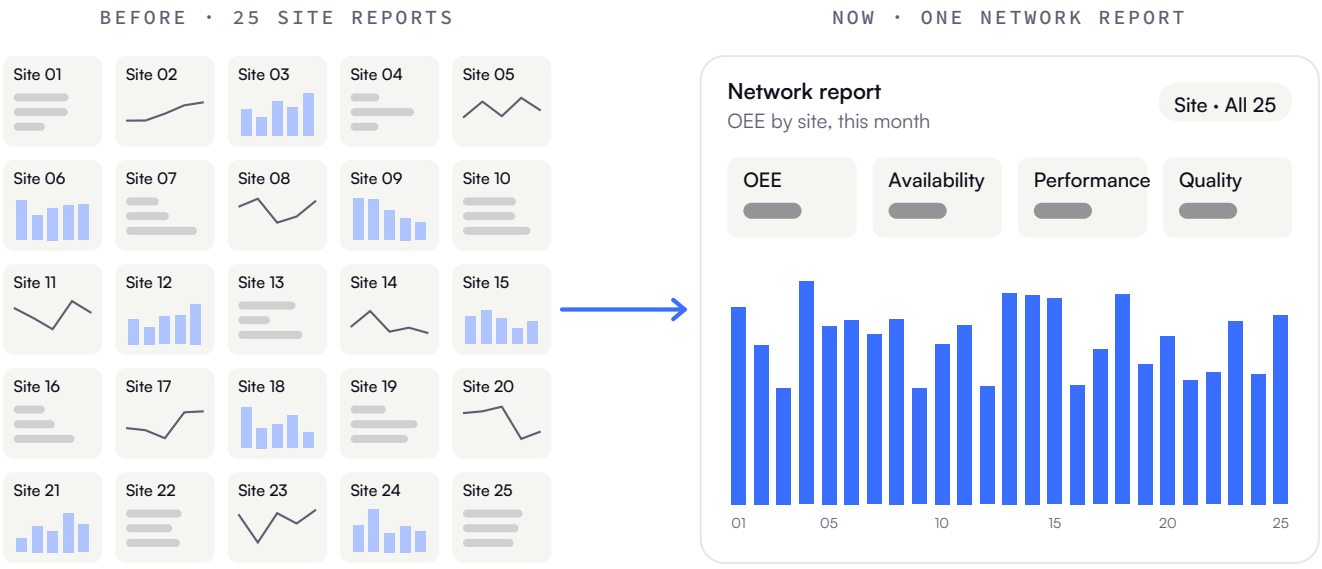


Figure 1 · Before, every site reported on its own terms and in its own layout. Now one network report reads one governed model. Illustrative: no client figures are shown.

Before and after (cont.)

CLIENT

A manufacturer of 1,000 to 5,000 people with 25 production sites, each reporting on its own terms and largely in Excel.

MANDATE

Introduce Microsoft Fabric from scratch and move the group from site-level reporting to one group-wide reporting platform, without opening each site's numbers to the others.

One report, a different view for each viewer

The obvious fix, putting every site in one place, was the thing nobody could sign off. So the access rules sit inside the model rather than around it: the same report shows a site manager their own site, shows group operations all 25 side by side, and the assistant answers within the same rules.

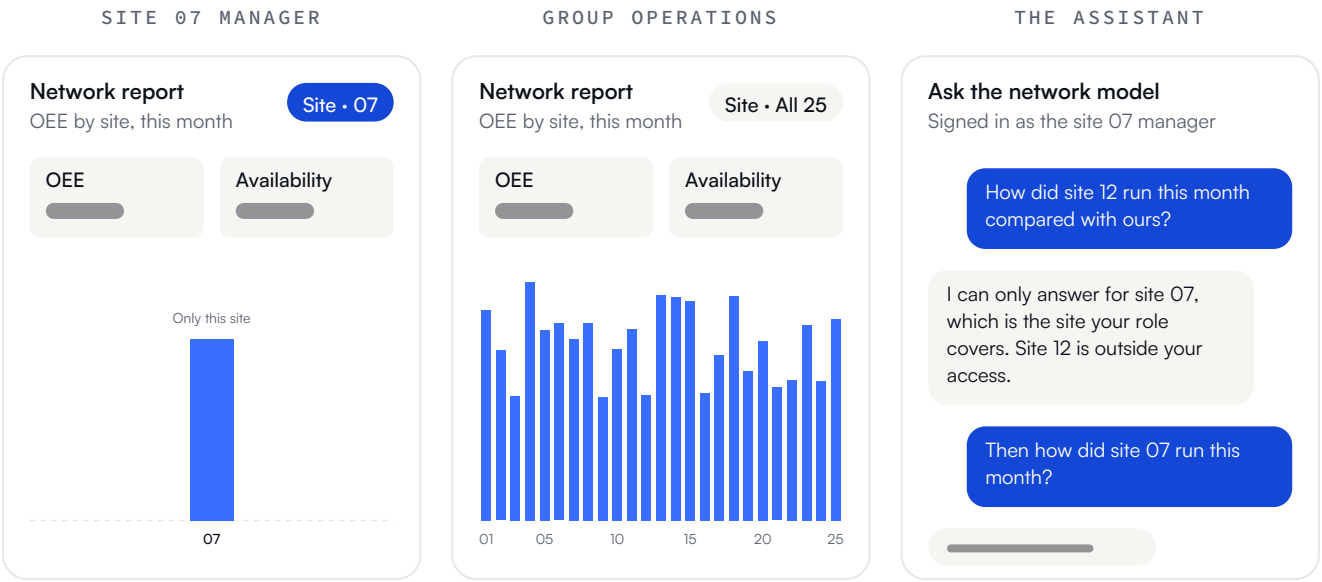


Figure 2 · One report, three viewers. Row-level security decides what each one sees, and the assistant answers inside the same rules. Illustrative: no client figures are shown.

- ✓ One reporting layer across the production network, not one per site.
- ✓ Every stakeholder sees exactly their own numbers, and only those.

One report, a different view for each viewer (cont.)

- ✓ The access rules carried by the model rather than by who has the file.
- ✓ AI answering within the same rules, with no second way into a neighbouring site's numbers.

The architecture

Every site keeps its own systems. What was missing was the layer above them: shopfloor, production and ERP data conformed into one site and asset model, read by 3 domain models over Direct Lake.

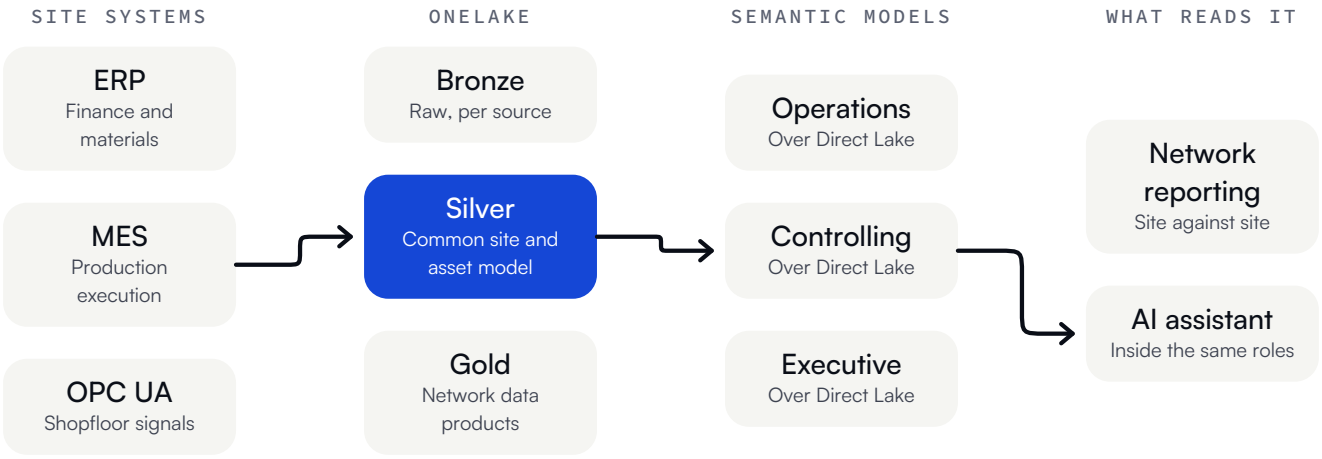


Figure 3 • Site systems into a medallion lakehouse, conformed into one site and asset model, and read by 3 domain models. Reports and the assistant read under the same security.

The access rules sit in the model, not around it. The alternative was a report or a workspace per site, which multiplies the model by the network and puts the comparison back out of reach.

One model for the network, not one per site. A model per site is easy to secure and impossible to compare across, and comparing the sites was the reason the network needed reporting at all.

AI inside the same row-level security. An assistant on a governed model inherits the model's security, or it becomes the second way in that the first one was built to prevent.

How access is enforced

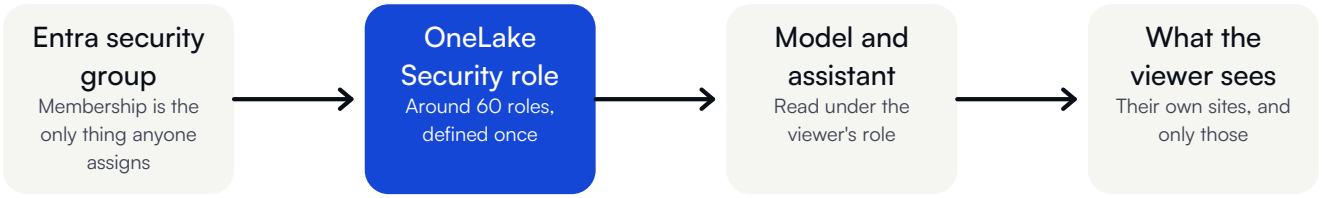


Figure 4 · Roles are driven entirely by Entra security groups, so access changes without anyone touching the model.

- Private Link and managed private endpoints, so data moves on the private network.
- Customer-managed keys for the data at rest.
- Purview sensitivity labels, with dynamic data masking on the columns that need it.

Workspace topology

	DEV	TEST	PROD
Bronze raw, per source	Sites isolated by role	Sites isolated by role	Sites isolated by role
Silver site and asset model	Sites isolated by role	Sites isolated by role	Sites isolated by role
Gold network data products	Sites isolated by role	Sites isolated by role	Sites isolated by role

Figure 5 · Bronze, Silver and Gold across DEV, TEST and PROD. Sites are separated by roles rather than by separate systems, so the topology does not grow with the network.

What the client has today

- ✓ One screen for the group-wide OEE comparison across all 25 sites.
- ✓ Month-end closed on the cockpit rather than from site workbooks.
- ✓ Every viewer sees exactly their own sites, through around 60 roles driven by Entra security groups.
- ✓ A new plant onboarded as standard work rather than as a project.

What the client has today (cont.)

- ✓ Production capacity sized from measured load rather than from an estimate.
- ✓ AI answering inside the same security the reports run on.

WHERE IT LEFT THEM

One reporting layer for a network that had been reporting in pieces, with the security model doing the work that used to be done by not sharing the file.

STACK

Microsoft Fabric · OneLake · OneLake Security · Direct Lake · Spark · MES · OPC UA · Power BI · DAX · Azure Key Vault · Purview · Azure DevOps

Niklas Hoeppener • Founder • info@ariavor.com • ariavor.com