0

T

The Trusted Advisor

ADVISORY

FABRIC COMMUNITY MEETUP · ONLINE · 13 OCT 2026

Fabric Governance – Domains, Workspaces & Lineage

Matthias Falland

THE TRUSTED ADVISOR

ABOUT ME

Matthias Falland

The Trusted Advisor · Microsoft Data Platform MVP since 2018

- **Microsoft MVP** Data Platform, since 2018
- **Fabric Friday** weekly on YouTube, one Fabric element per episode
- **Fabric Architecture Podcast** weekly, with an AI co-host
- **Fabric Periodic Table** fabricperiodictable.com, all 57 elements
- **Meetups** Zurich, Hamburg, Basel: over 5,000 members

TONIGHT

Questions carry the evening

Teams Q&A is open now – ask any time.

Workspace · Domain · Capacity · a look at Lineage

Everything from tonight:
links, handout
the-trusted-advisor.com/events/…

37

WS

Workspace

GOVERN

Workspace

NO. 37 · WS · GOVERN

> A container for items that divides OneLake into separately secured parts.

What a workspace is

37

WS

Workspace

GOVERN

What it is A container for items, such as lakehouses, notebooks and reports. It divides OneLake into separately secured parts.

What it is for The one place to hang security, cost, region and lifecycle.

Assigned to A capacity: it pays the compute and sets the region. Pro and PPU workspaces sit on shared capacity.

Normal use One workspace per team and stage, such as Dev, Test and Prod, connected to Git.

Limit 1,000 items per workspace, parent and child items counted.

FILM «FOUR BOUNDARIES IN ONE OBJECT», SCENE 3

Four workspace roles

Admin Everything, plus delete the workspace, add admins, connect to Git.

Member Add members and lower roles, allow resharing, create and edit items.

Contributor Create and edit items, run notebooks and pipelines, read all data.

Viewer See items and output, read through SQL (ReadData), no Spark read.

Changes A role change applies at the user's next sign-in.

37

WS

Workspace

GOVERN

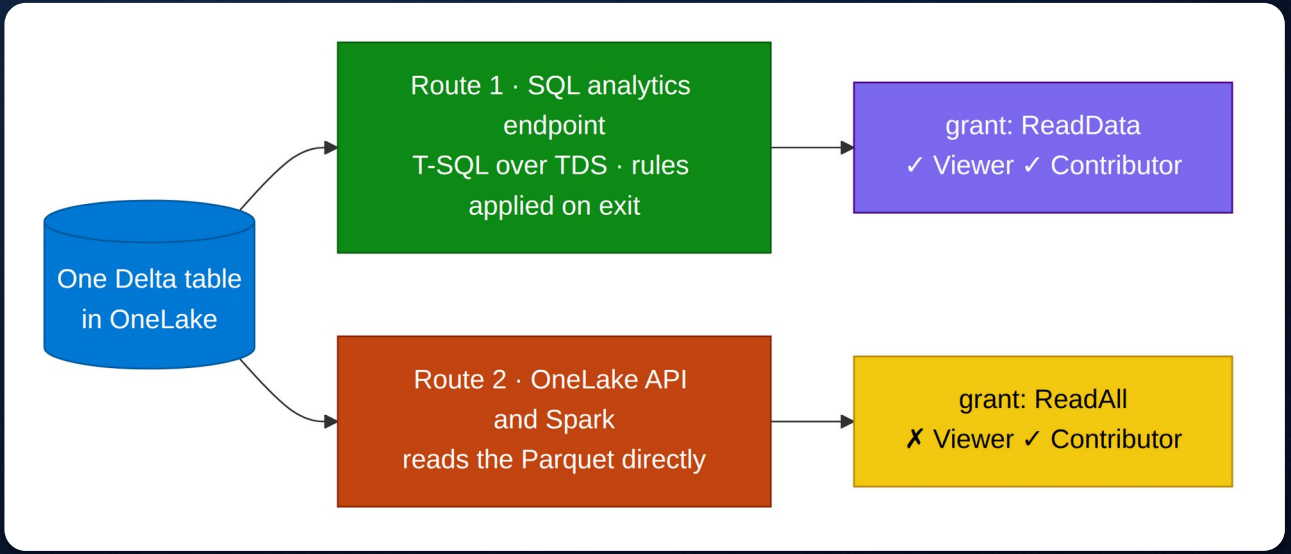


DIAGRAM 2 OF THE EPISODE'S ARCHITECTURE – THE VIEWER LINE: ONE TABLE, TWO ROUTES

37
WS
Workspace
GOVERN

Contributor plus a OneLake security rule around HR – who can still read the HR folder?

ANSWER IN THE CHAT

02 The cut carries everything

one object, four jobs

1 · SECURITY

Who reads what's inside?

Workspace role

2 · COST

What does the compute cost?

Capacity

Workspace

3 · REGION

Which datacentre is it in?

Datacentre

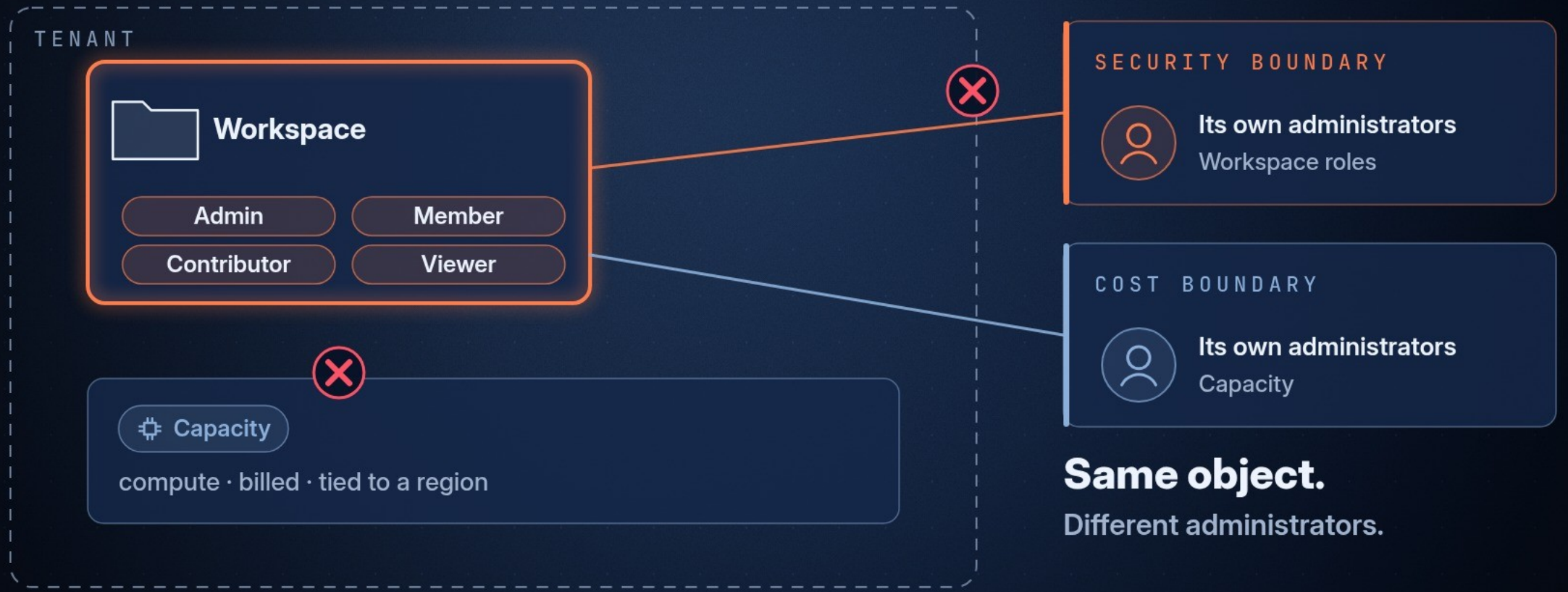
4 · LIFECYCLE

Which branch does it ship from?

Git integration

04 Same object, different owners

roles stop at the workspace edge



Same object.

Different administrators.

05 The asymmetry of attention

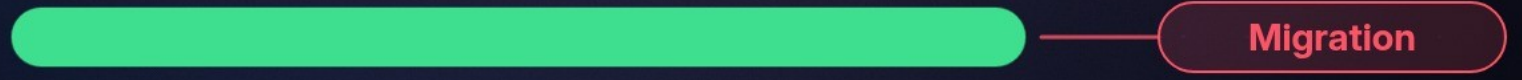
what gets configured, and when

1 **Security**

2 **Cost**

3 **Region**

4 **Lifecycle**



37
WS
Workspace
GOVERN

Create and Inspect a Workspace

WHAT YOU WILL SEE

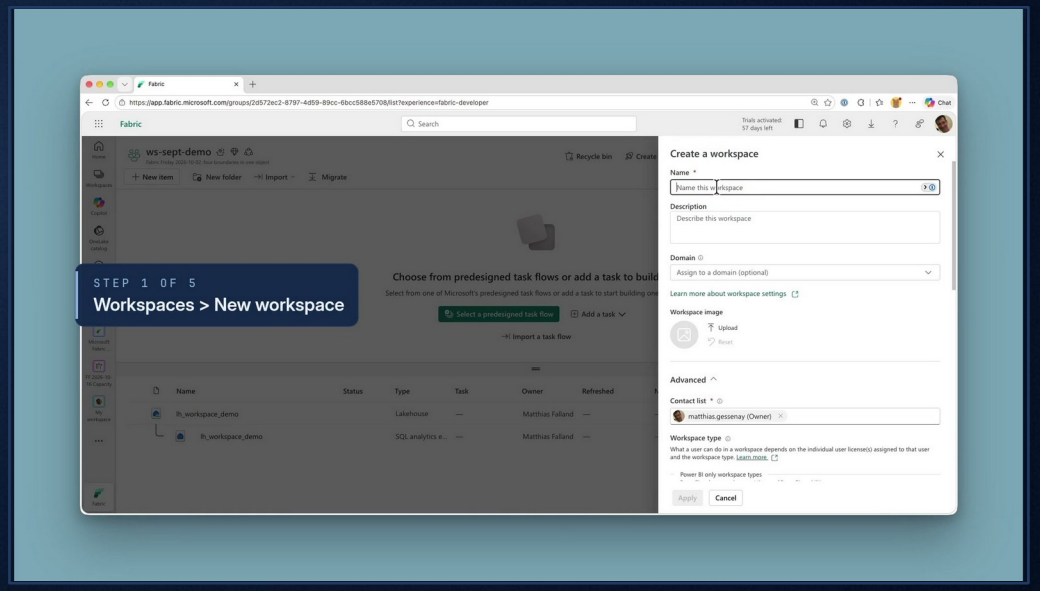
A new workspace from scratch, then where each of its four boundaries sits in the settings.

WHO DOES IT

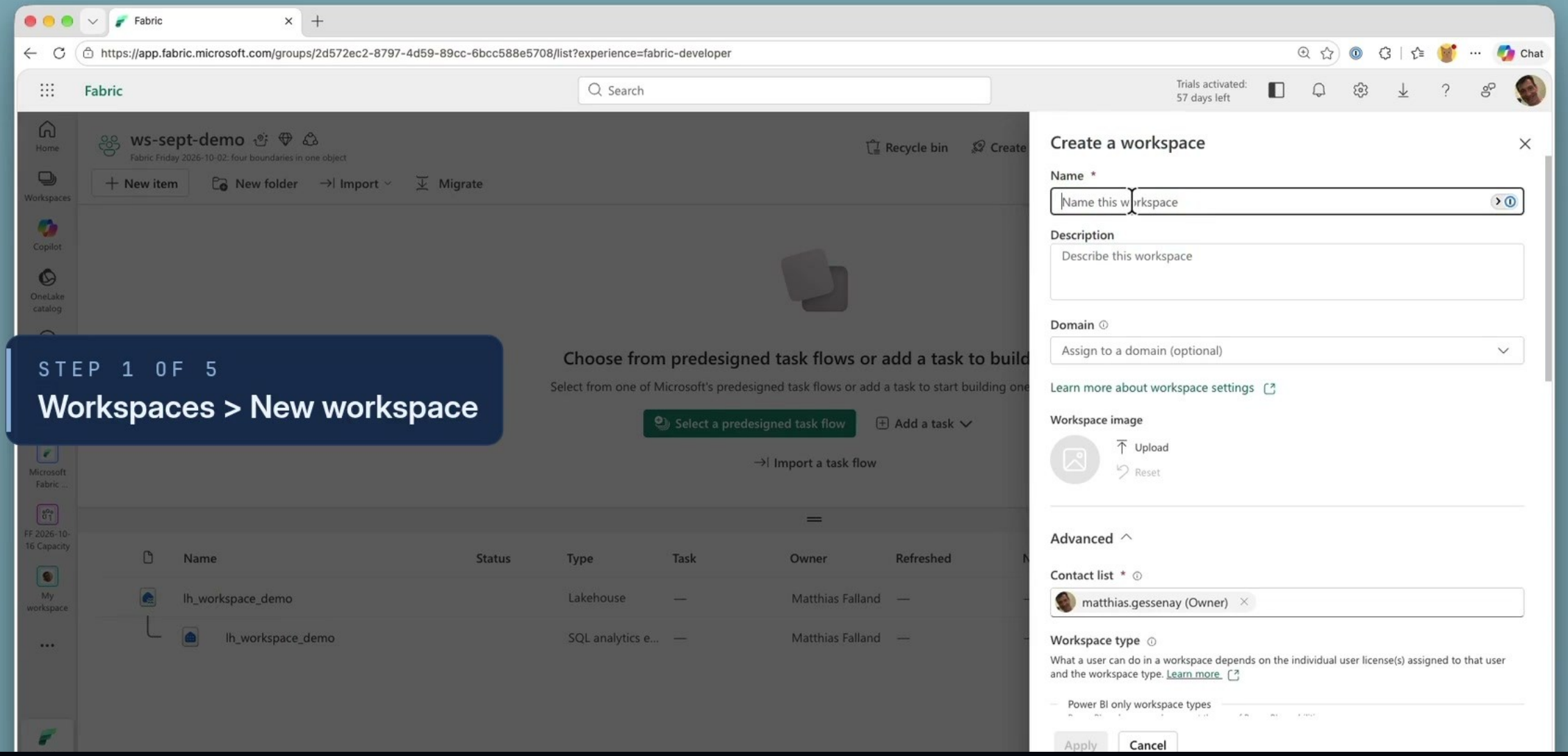
Me, as workspace Admin, on a Fabric Trial capacity.

WATCH FOR

Git integration is an Admin action. Only 7 item types move to another region.

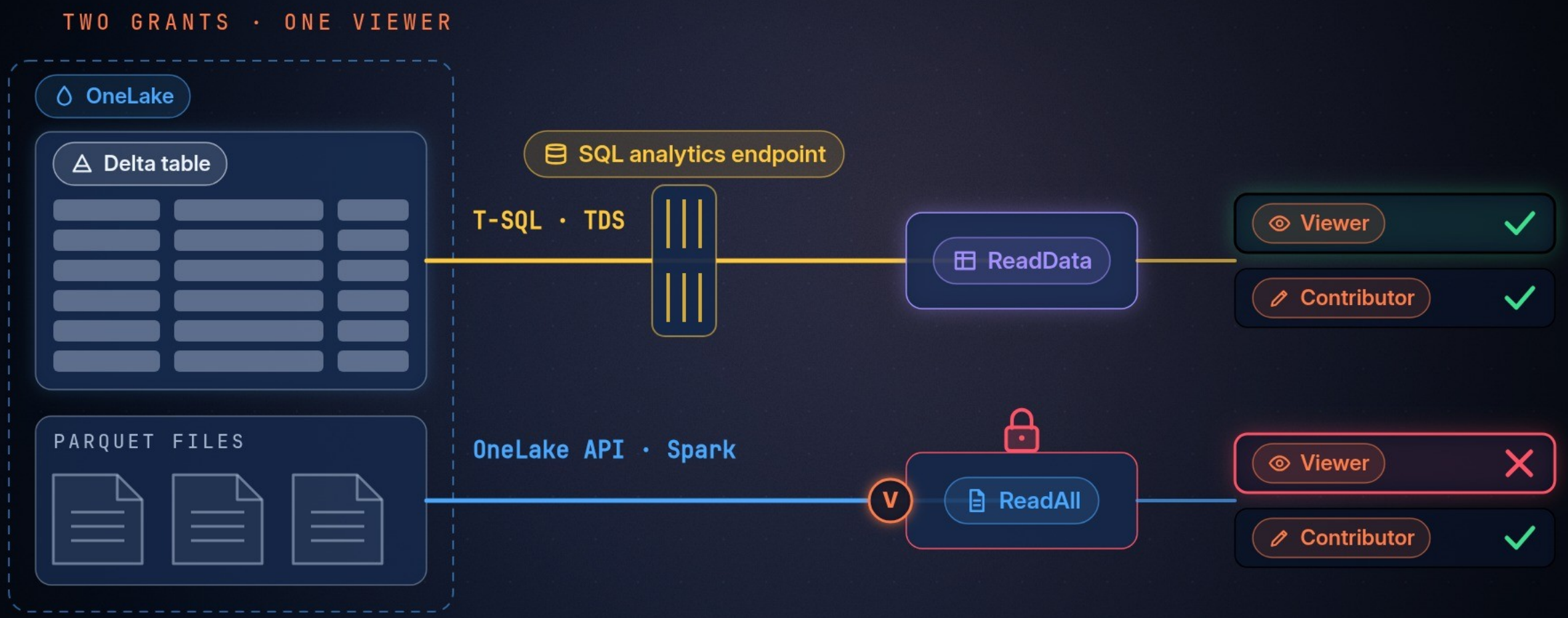


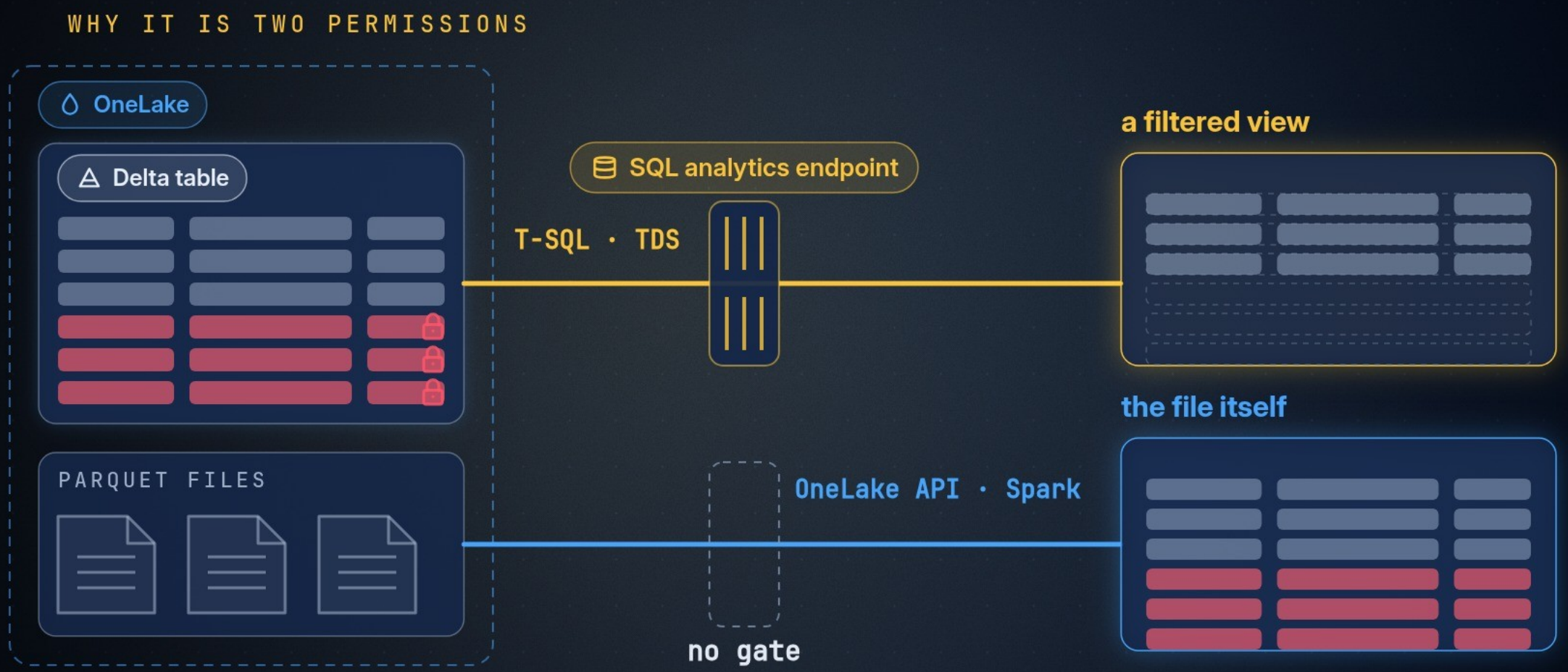
▶ 92 S · PLAYS WITHOUT VOICE



▸ DEMO · CREATE AND INSPECT A WORKSPACE

Watch it in the episode: https://youtu.be/tpePwivxtzk?t=170


TWO GRANTS · ONE VIEWER
OneLake
Delta table
PARQUET FILES
SQL analytics endpoint
T-SQL · TDS
OneLake API · Spark
ReadData
ReadAll
Viewer
Contributor
Viewer
Contributor


WHY IT IS TWO PERMISSIONS
OneLake
Delta table
PARQUET FILES
SQL analytics endpoint
T-SQL · TDS
OneLake API · Spark
no gate
a filtered view
the file itself

THE DESIGN CONSEQUENCE

37
WS
Workspace
GOVERN

Same Table, Two Routes

WHAT YOU WILL SEE

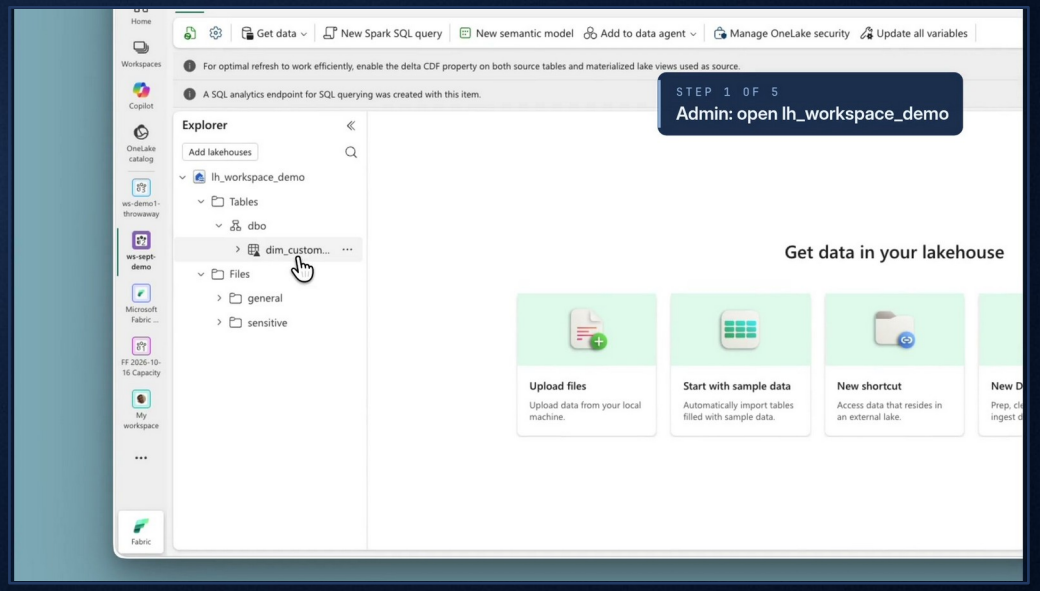
One Delta table, read twice – through the SQL analytics endpoint, then through Spark in a notebook.

WHO DOES IT

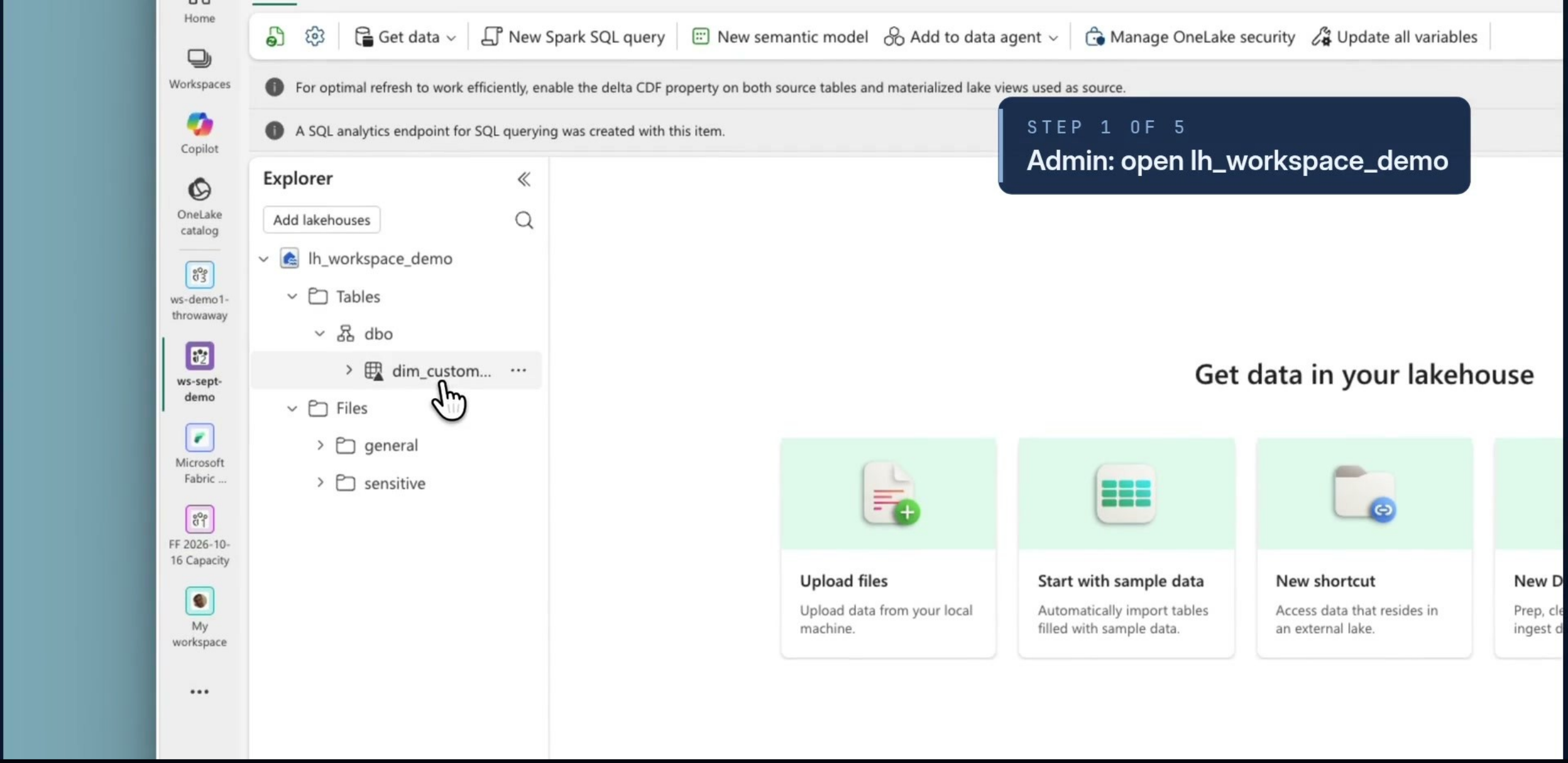
Me as Admin first, then a demo identity as Viewer in a second browser, then moved to Contributor.

WATCH FOR

The Viewer's Spark read fails with 403. ReadData is not ReadAll.



▶ 209 S · PLAYS WITHOUT VOICE



▸ DEMO · SAME TABLE, TWO ROUTES

Watch it in the episode: https://youtu.be/tpePwivxtzk?t=388

VIEWER · DARK UNTIL A ROLE GRANTS

Viewer

folders visible

2 / 3

role · Sales

role · Marketing

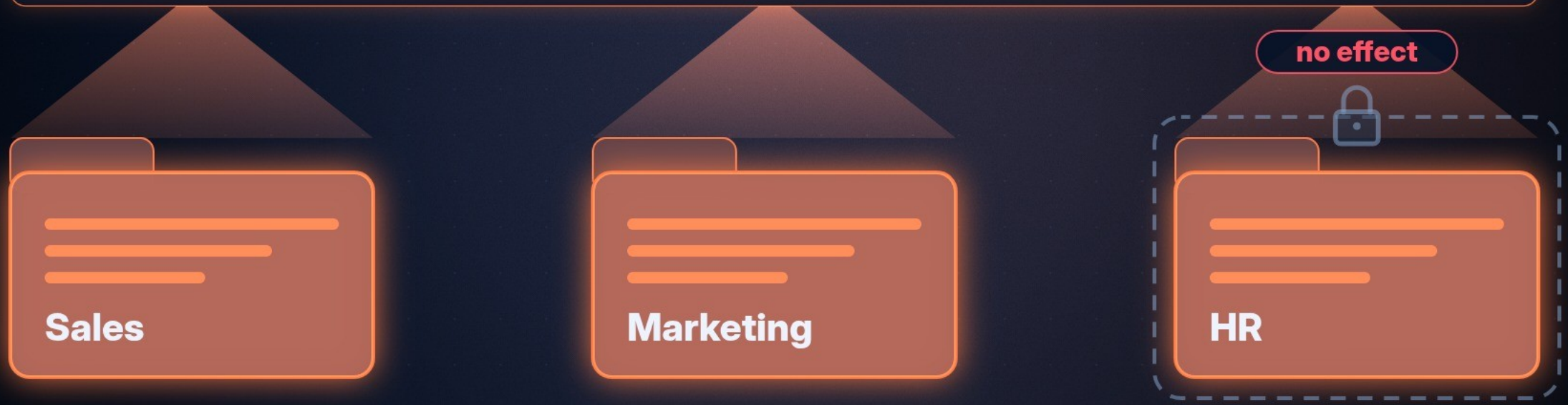
no role

CONTRIBUTOR · READ + WRITE

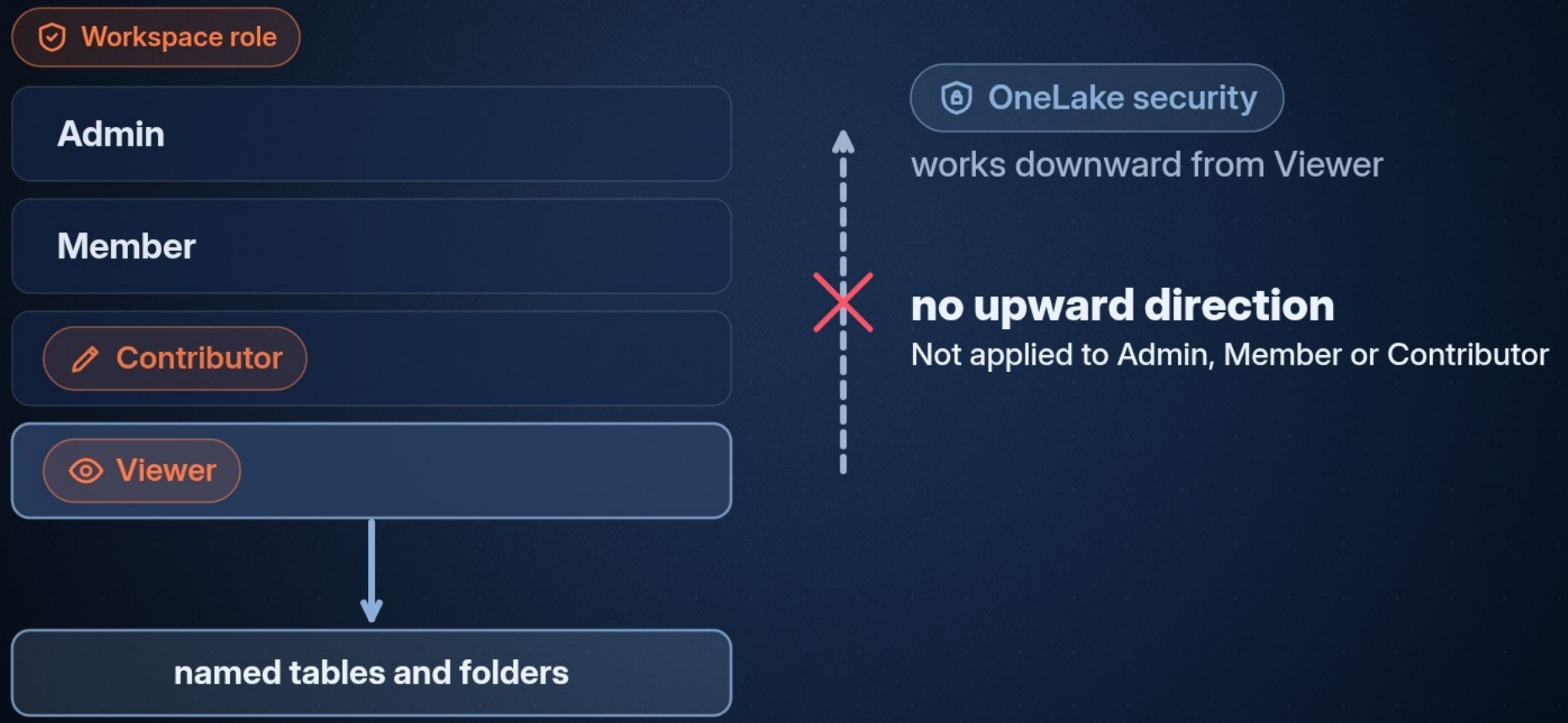
Contributor

never in the dark

Read + Write on all the data in the workspace



THE WHY


Workspace role
Admin
Member
Contributor
Viewer
named tables and folders
OneLake security
works downward from Viewer
no upward direction
Not applied to Admin, Member or Contributor

THE EXPENSIVE CONSEQUENCE

Row-level security

Contributor

8 of 8 rows

the filter no longer applies

ROLE CHANGE

Viewer → Contributor

reason: fix a report

security review

37
WS
Workspace
GOVERN

Watch the Override

WHAT YOU WILL SEE

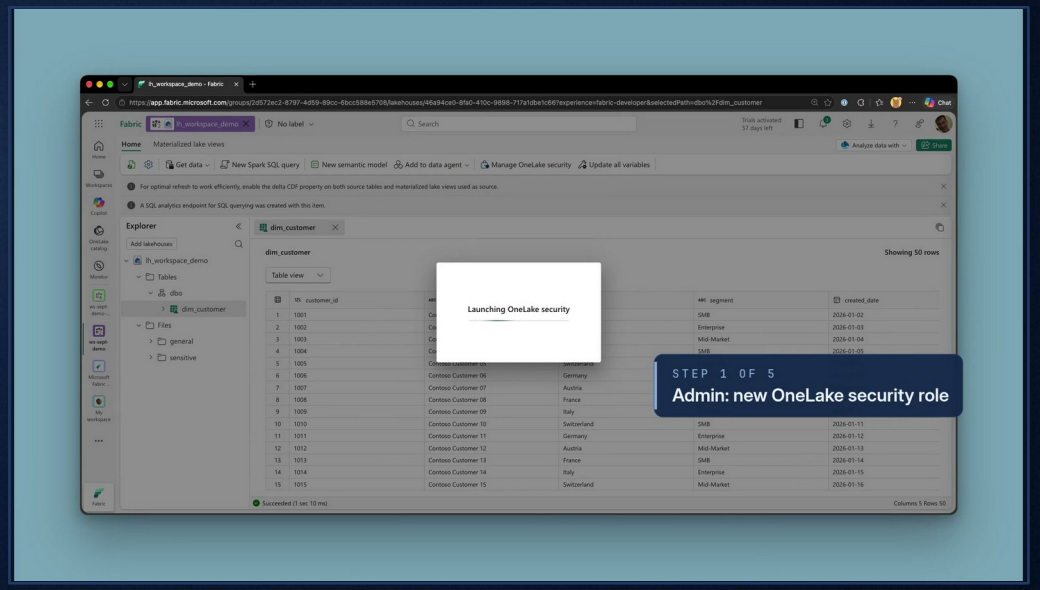
A OneLake security role that grants only Files/general, tested on one identity in two workspace roles.

WHO DOES IT

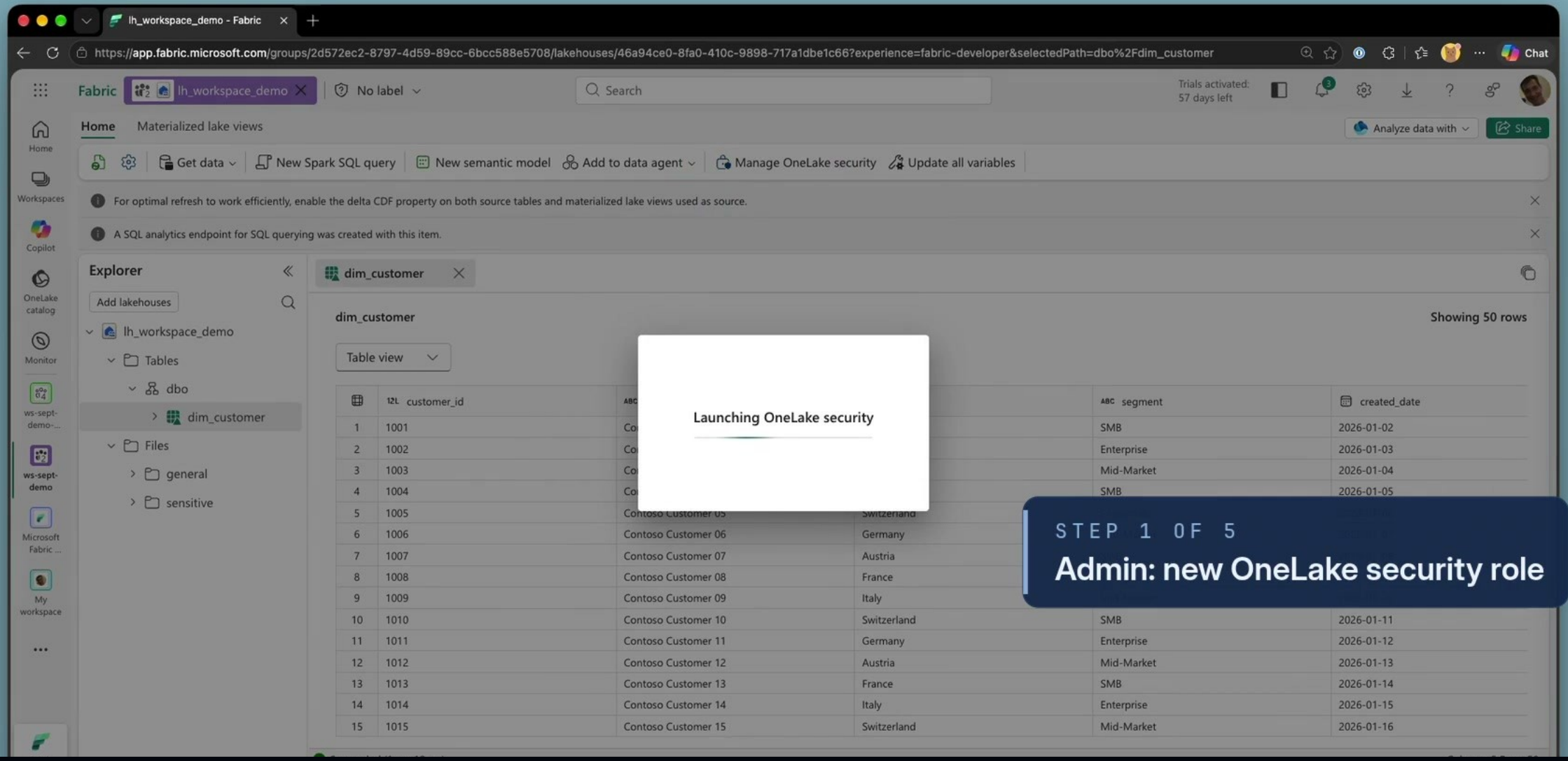
Me as Admin builds the role; the demo identity tests it, first as Contributor, then as Viewer.

WATCH FOR

As Contributor the identity still lists sensitive. As Viewer only general opens.



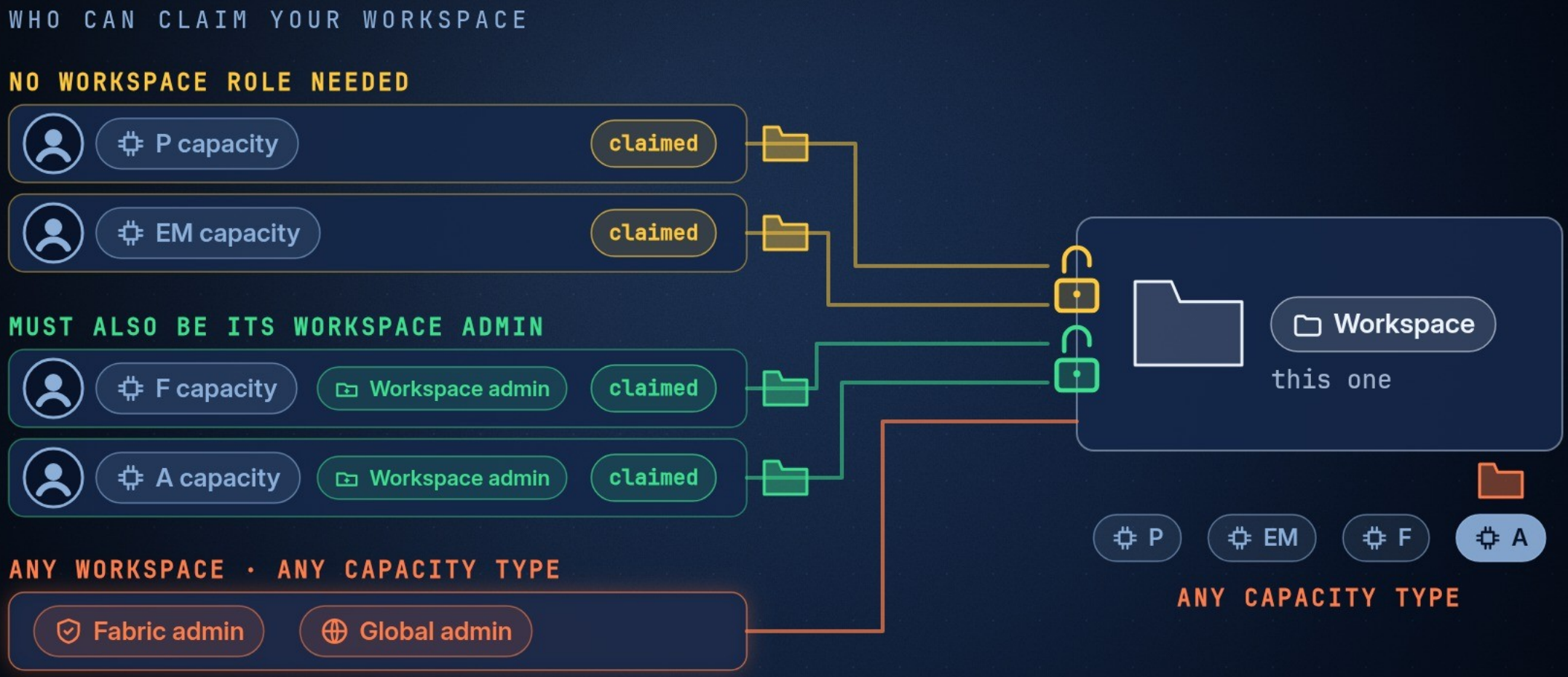
▶ 124 S · PLAYS WITHOUT VOICE



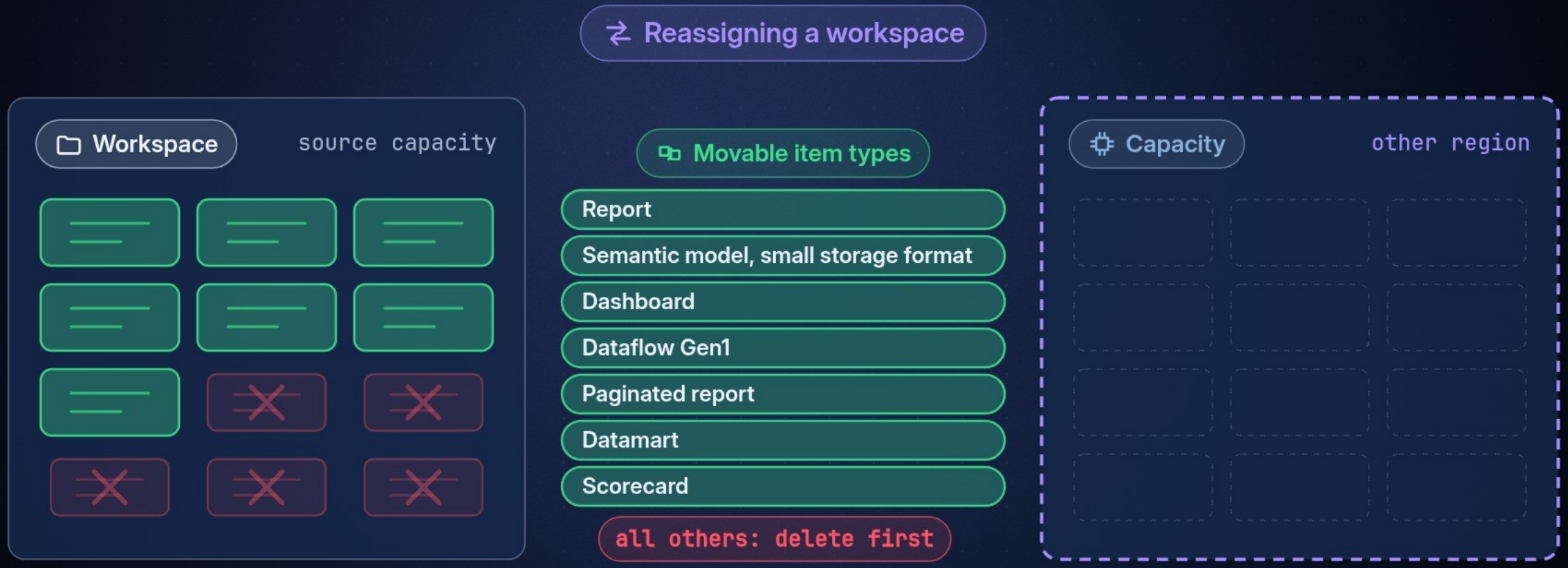
	customer_id		segment	created_date
1	1001		SMB	2026-01-02
2	1002		Enterprise	2026-01-03
3	1003		Mid-Market	2026-01-04
4	1004		SMB	2026-01-05
5	1005	Contoso Customer 05	Switzerland	
6	1006	Contoso Customer 06	Germany	
7	1007	Contoso Customer 07	Austria	
8	1008	Contoso Customer 08	France	
9	1009	Contoso Customer 09	Italy	
10	1010	Contoso Customer 10	Switzerland	SMB	2026-01-11
11	1011	Contoso Customer 11	Germany	Enterprise	2026-01-12
12	1012	Contoso Customer 12	Austria	Mid-Market	2026-01-13
13	1013	Contoso Customer 13	France	SMB	2026-01-14
14	1014	Contoso Customer 14	Italy	Enterprise	2026-01-15
15	1015	Contoso Customer 15	Switzerland	Mid-Market	2026-01-16

▸ DEMO · WATCH THE OVERRIDE

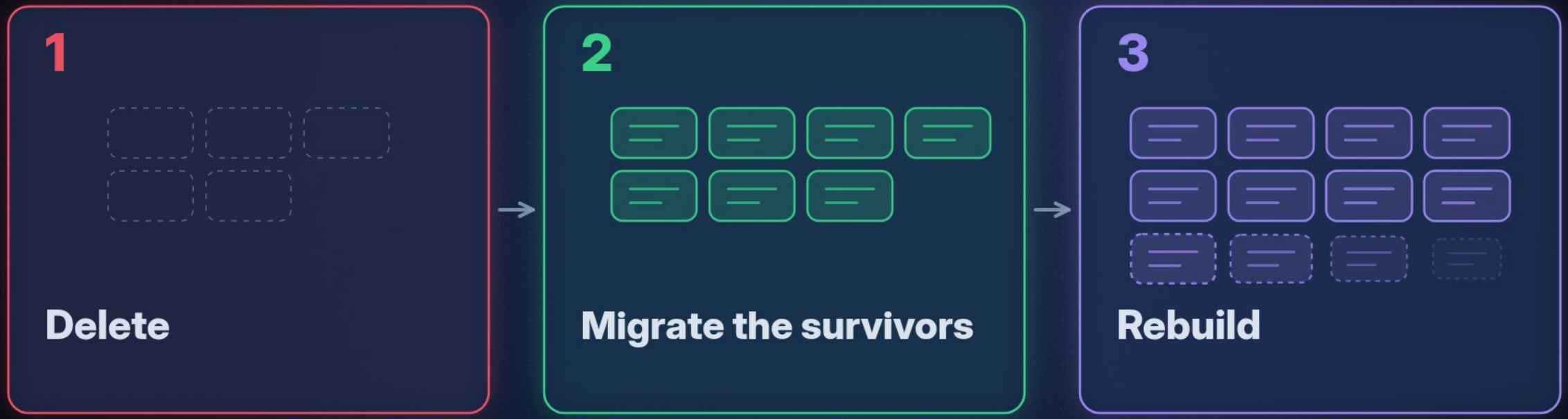
Watch it in the episode: https://youtu.be/tpePwivxtzk?t=751


WHO CAN CLAIM YOUR WORKSPACE
NO WORKSPACE ROLE NEEDED
P capacity
claimed
EM capacity
claimed
MUST ALSO BE ITS WORKSPACE ADMIN
F capacity
Workspace admin
claimed
A capacity
Workspace admin
claimed
ANY WORKSPACE · ANY CAPACITY TYPE
Fabric admin
Global admin
Workspace
this one
P
EM
F
A
ANY CAPACITY TYPE

WHAT A MOVE COSTS



A CROSS-REGION MOVE



37
WS
Workspace
GOVERN

A workspace is not a folder. It is a cut through OneLake – and the cut has to carry everything.

Security, cost, region, lifecycle. Three of the four stay invisible until they are expensive.

DECISION RULES

- Split on a boundary you need: audience, capacity, region, release cadence.
- Start at Viewer, grant upward with OneLake security.
- A region change is a migration project: delete, migrate, rebuild.

Traps

37
WS
Workspace
GOVERN

TRAP	FIX
Viewer cannot read via Spark	OneLake security grant, not a role bump
OneLake rule ignored for Contributor	Viewer plus explicit grants
RLS silently stops applying	Enforced only in the Viewer role
Git connect grayed out	Admin only, not Member
Revoke did not take effect	Applies at next sign-in
Items gone after a region move	Only 7 item types cross regions

39

DOM

Domain

GOVERN

Domain

NO. 39 · DOM · GOVERN

> A grouping of workspaces by business area: whose data is this, not who may see it.

What a domain is

39

DOM

Domain

GOVERN

What it is A grouping above workspaces, usually by business area, such as Finance or Sales.

What it gives A domain attribute on every item, a OneLake catalog filter, delegated tenant settings, a business owner.

The rule One workspace belongs to at most one domain. Subdomains go one level down.

Not a boundary Access stays with workspace roles and item permissions.

Visible Every user in the tenant sees every domain name.

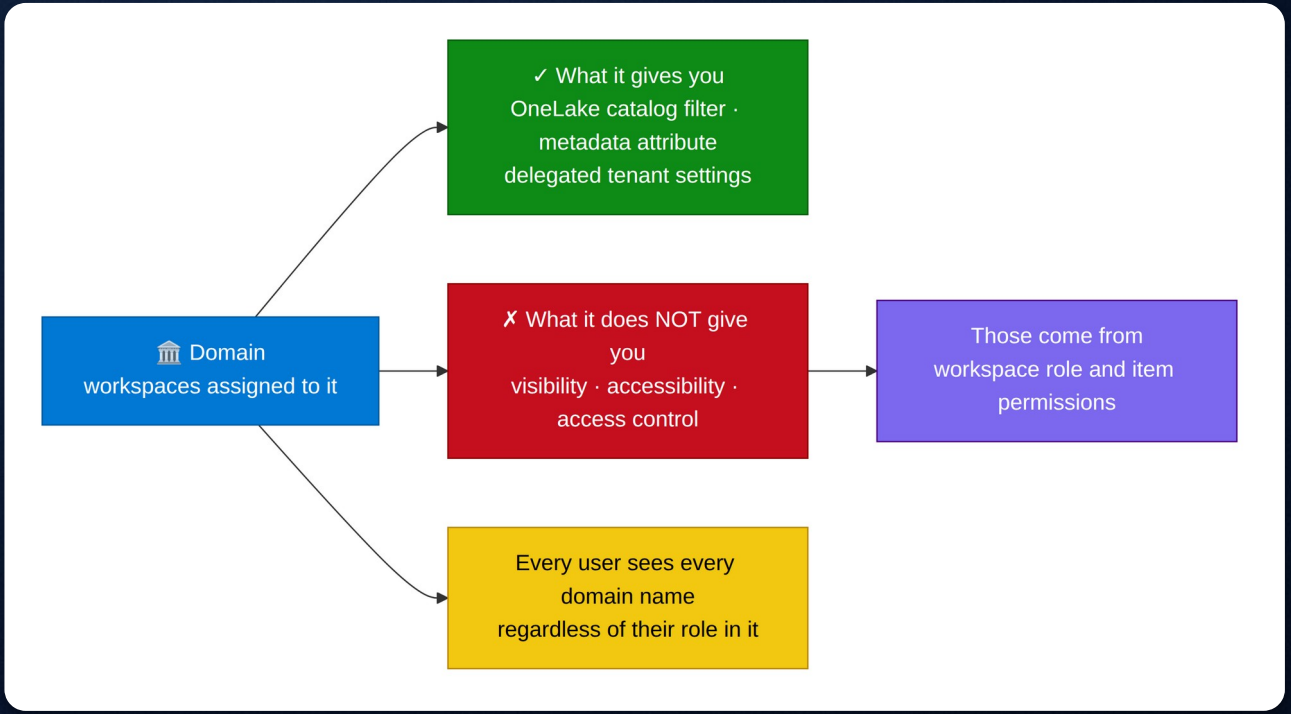


DIAGRAM 1 OF THE EPISODE'S ARCHITECTURE – WHAT A DOMAIN DOES, AND WHAT IT DOES NOT

Who runs a domain

39

DOM

Domain

GOVERN

Fabric admin Creates, renames and deletes domains, adds domain admins.

Domain admin Edits the description, defines contributors, assigns workspaces, delegated settings.

Domain contributor Assigns own workspaces to the domain, and must already be workspace Admin.

Subdomains Name and description only. Their admins are the parent's admins.

Default domain New workspaces of listed users or groups land there automatically.

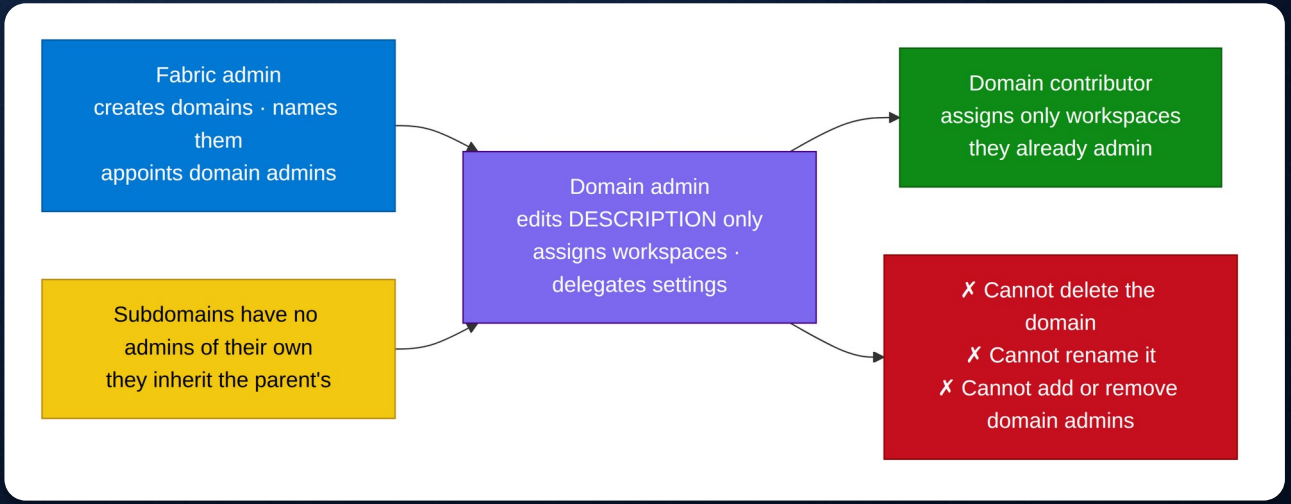


DIAGRAM 2 OF THE EPISODE'S ARCHITECTURE – THREE ROLES, AND THE FOUR THINGS AN ADMIN CANNOT DO

39

DOM

Domain

GOVERN

You moved the sensitive workspaces into their own domain. Are they protected now?

ANSWER IN THE CHAT

01 The sentence

straight from Microsoft Learn

Domain assignment doesn’t affect item visibility or accessibility for tenant users.

MICROSOFT LEARN · FABRIC DOMAINS

DISCOVERY · VISIBILITY · ACCESS DEPEND ON

DEPENDS ON

Workspace role

Admin, Member, Contributor or Viewer: the role that decides what someone can do in a workspace.

Microsoft Learn · Permission model

DEPENDS ON

Item permissions

Permissions on one item, such as Read or Write; they can give access to a single item in a workspace.

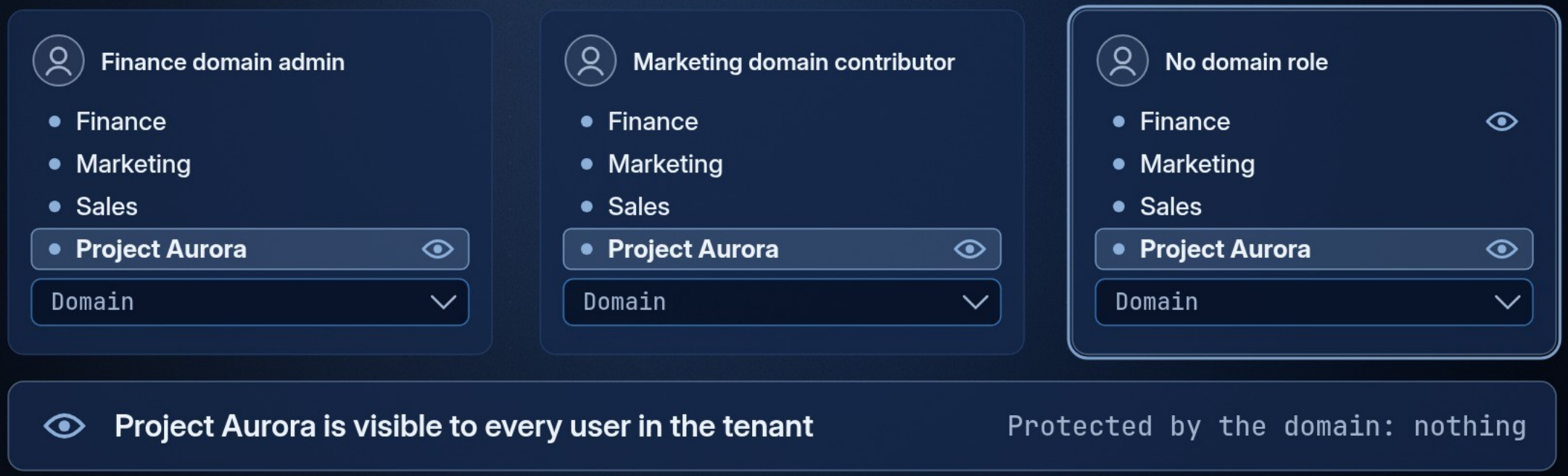
Microsoft Learn · Permission model

03 # Names are public

every user sees every domain

What does your domain name give away?

DOMAIN NAMES HERE ARE ILLUSTRATIVE

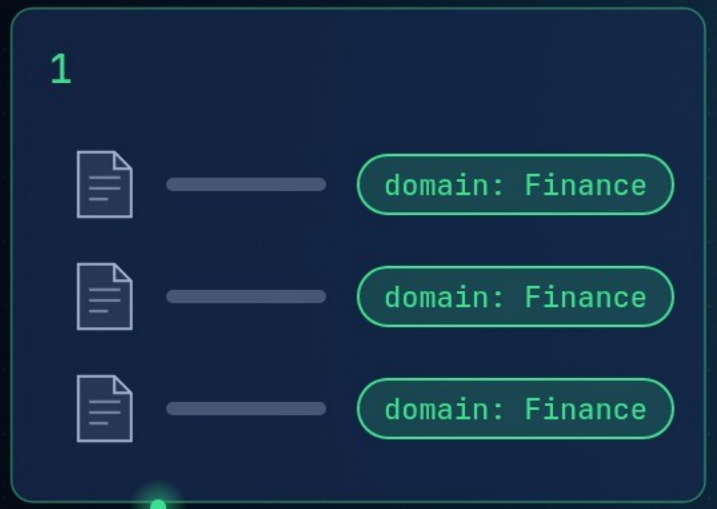


Project Aurora is visible to every user in the tenant

Protected by the domain: nothing

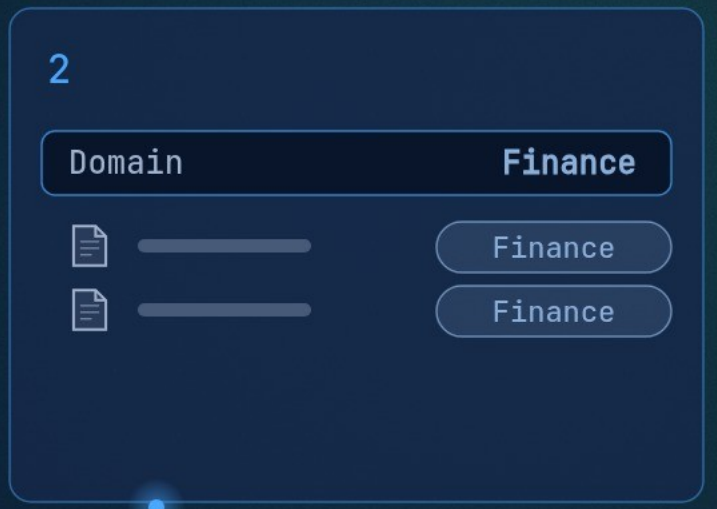
04 What you do get

three real things



Domain attribute

An item's metadata field naming its domain; every item in an assigned workspace gets it.



OneLake catalog

Where you find and explore Fabric items; its domain selector shows one domain's items.

Delegated settings

Tenant settings handed down to a domain, so its business unit can set its own rules.

05

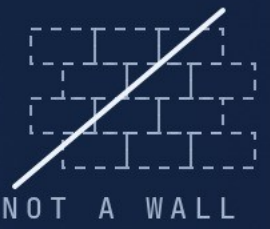
The sentence to keep

two questions, two layers

DOMAIN LAYER

Whose data is this?

Domain attribute · OneLake catalog · Delegated settings



ONE LAYER DOWN

ACCESS LAYER

Who may see it?

Workspace role · Item permissions

02 · DOMAIN · DEMO 1/3 · UP NEXT

The Filter That Is Not a Fence

39

DOM

Domain

GOVERN

WHAT YOU WILL SEE

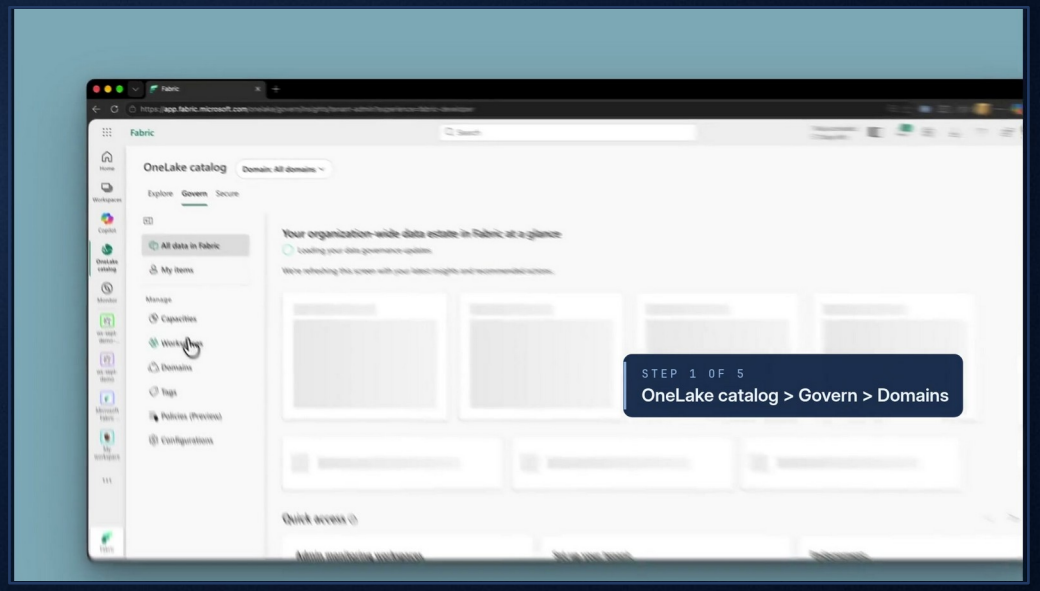
Two domains in the OneLake catalog, the domain filter, then the same catalog as another person.

WHO DOES IT

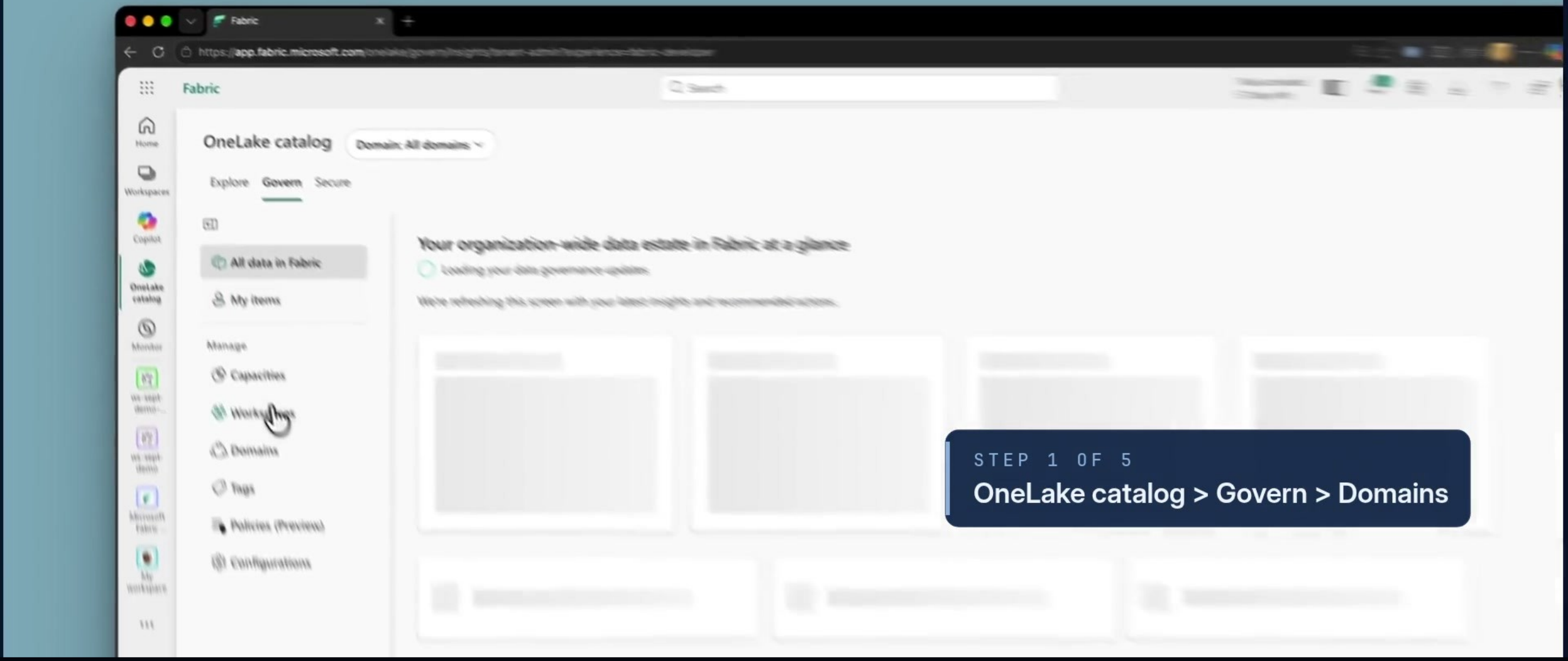
Me as admin, then a demo identity with no role in either domain.

WATCH FOR

The filter narrows what you find. The workspace role alone decides what opens.



▶ 129 S · PLAYS WITHOUT VOICE

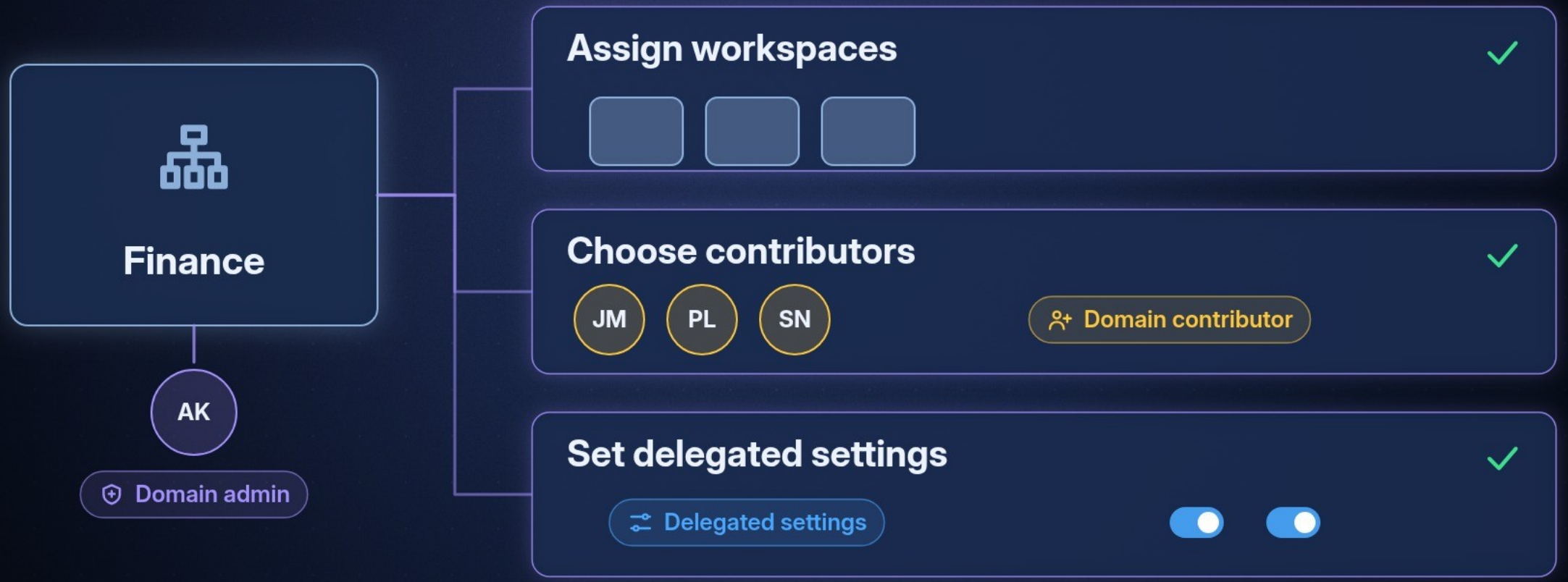


▸ DEMO · THE FILTER THAT IS NOT A FENCE

Watch it in the episode: https://youtu.be/8wRSvnF_CtQ?t=198

Fabric admin — Domain admin — Domain contributor

DOMAIN ADMIN · WHAT THE ROLE DOES



Fabric admin ------- Domain admin ------- Domain contributor

DOMAIN ADMIN · GENERAL SETTINGS

DOMAIN SETTINGS

Name

Finance

Description

Owned by the finance business unit

Domain admins

AK JM + Add admin × Remove admin

Delete domain

NOT THE DOMAIN ADMIN

1 Rename the domain

2 Delete the domain

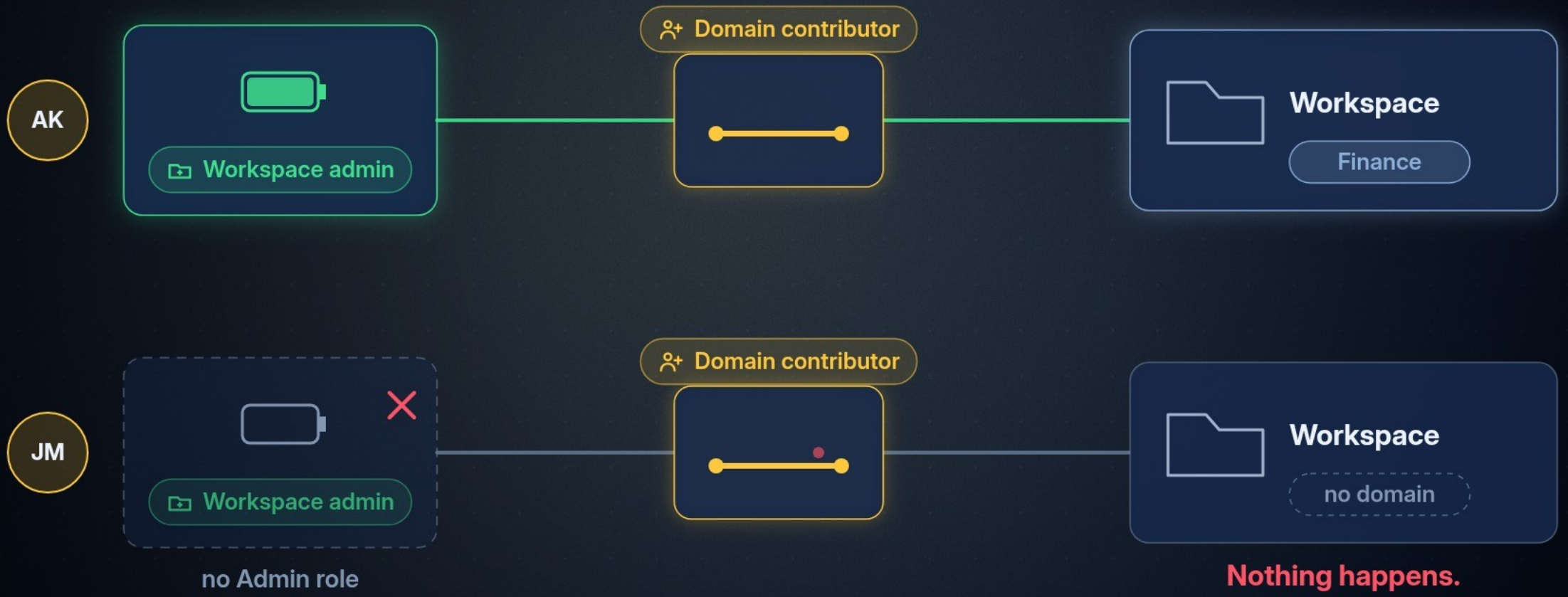
3 Add a domain admin

4 Remove a domain admin

Fabric admin

Fabric admin ------- Domain admin ------- Domain contributor

DOMAIN CONTRIBUTOR · ASSIGN A WORKSPACE



Fabric admin

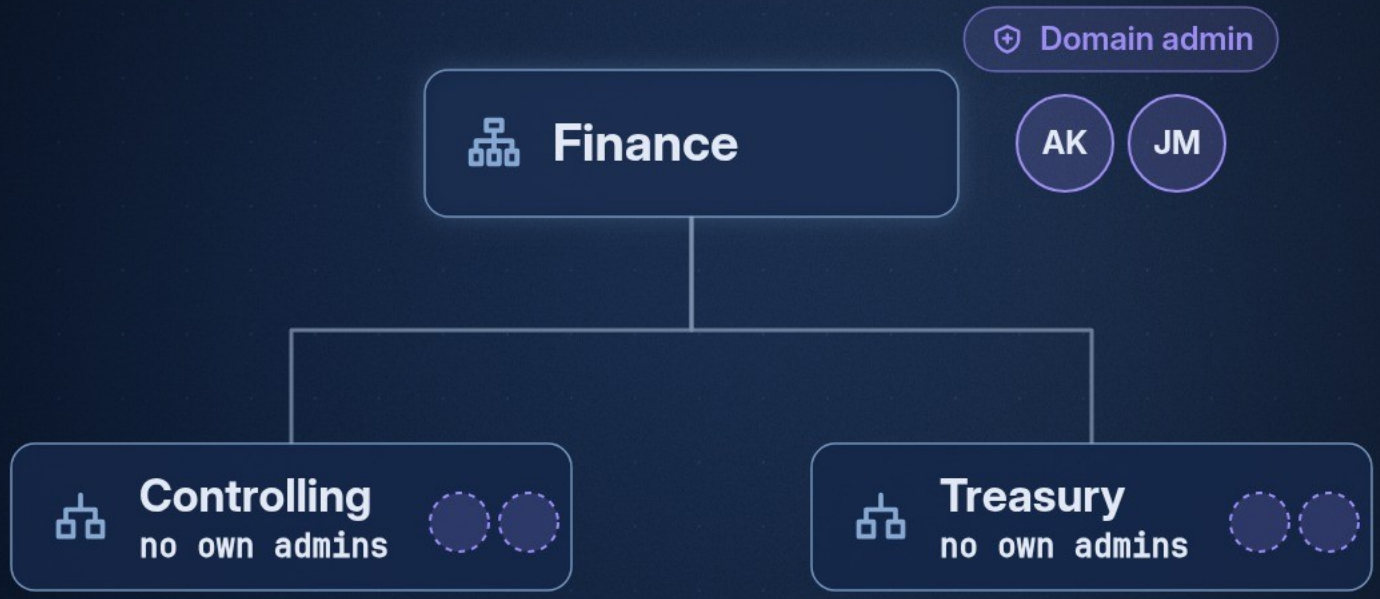
Domain admin

Domain contributor

SUBDOMAINS

HIERARCHY

2 levels



ADMINISTRATION

1 level

the shallower one

The Contributor Who Cannot Contribute

39
DOM
Domain
GOVERN

WHAT YOU WILL SEE

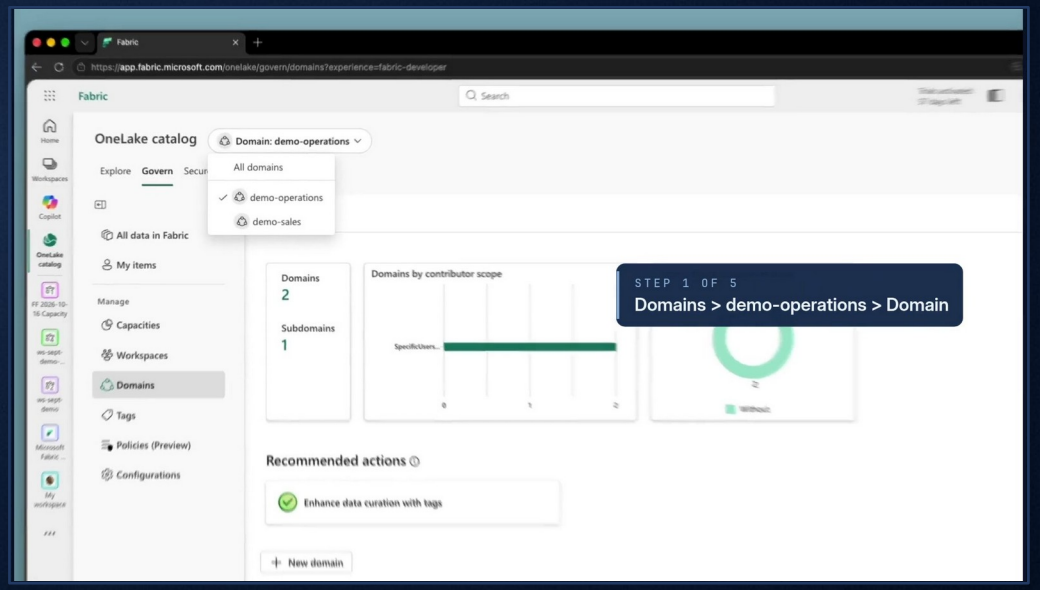
A demo identity becomes domain contributor and tries to assign a workspace to the domain.

WHO DOES IT

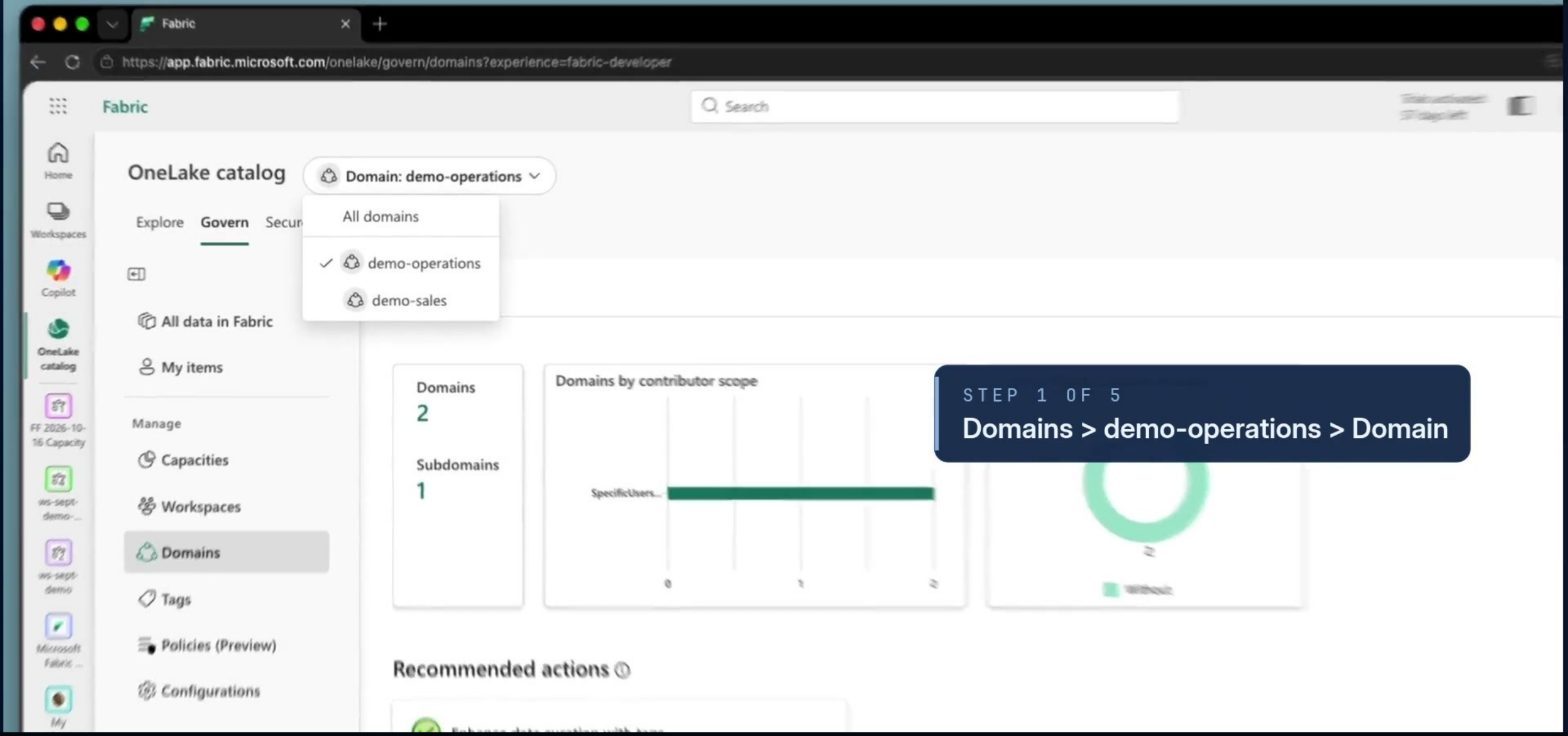
Me as admin sets the roles; the demo identity, first Viewer of the workspace, then its Admin.

WATCH FOR

The Domain field stays grayed out until the identity is workspace Admin.



▶ 136 S · PLAYS WITHOUT VOICE



▸ DEMO · THE CONTRIBUTOR WHO CANNOT CONTRIBUTE

Watch it in the episode: https://youtu.be/8wRSvnF_CtQ?t=469

02 **The rule**

default domain · one scan

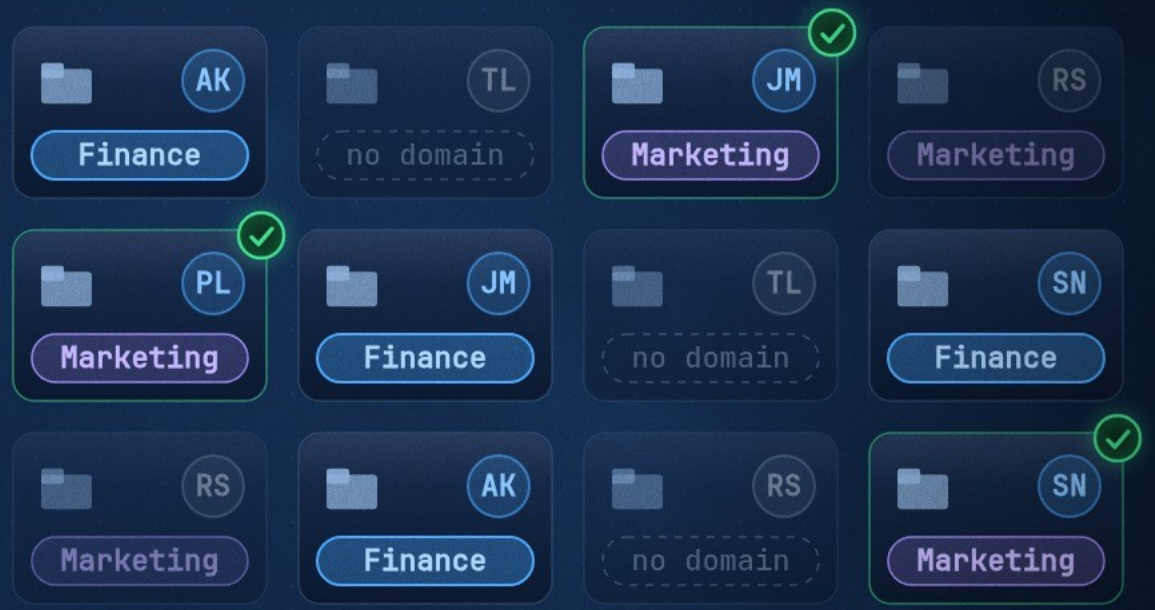
Default domain Finance

APPLIES TO

AK a named user

Finance analysts
SECURITY GROUP

JM PL SN



assigned ✓ preserved admin not on the list: left alone

03 **The price**

a role as a side effect

assigned by the default domain

Domain contributor

generally

may assign the workspaces they admin to a domain, or change the current assignment.

Microsoft Learn · Fabric domains · Domain roles

You configured: a convenience

You handed out: a role

03 **The price**

manual can override, automatic cannot

Manual assignment

BY NAME · BY ADMIN · BY CAPACITY

Allow tenant and domain admins to override workspace assignments (preview)

on by default

Default domain

AUTOMATIC

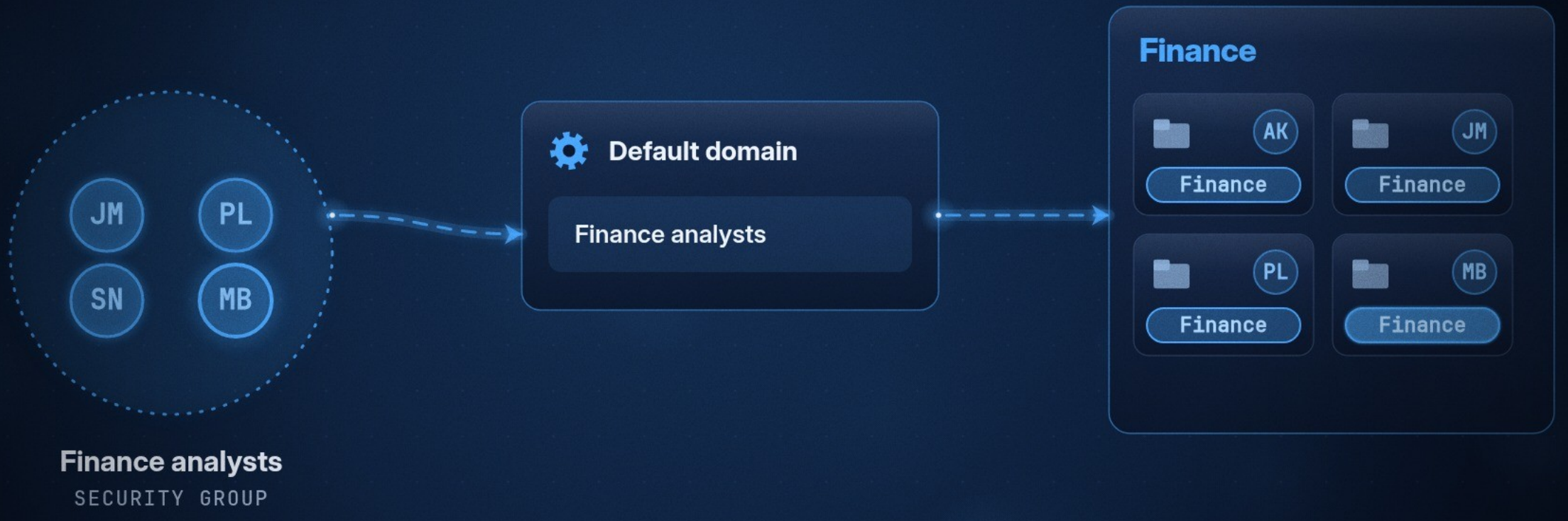
never overrides

the existing assignment stays

The convenient one is the cautious one.

03 **The price**

the group is the topology



39

DOM

Domain

GOVERN

An Assignment Nobody Made

WHAT YOU WILL SEE

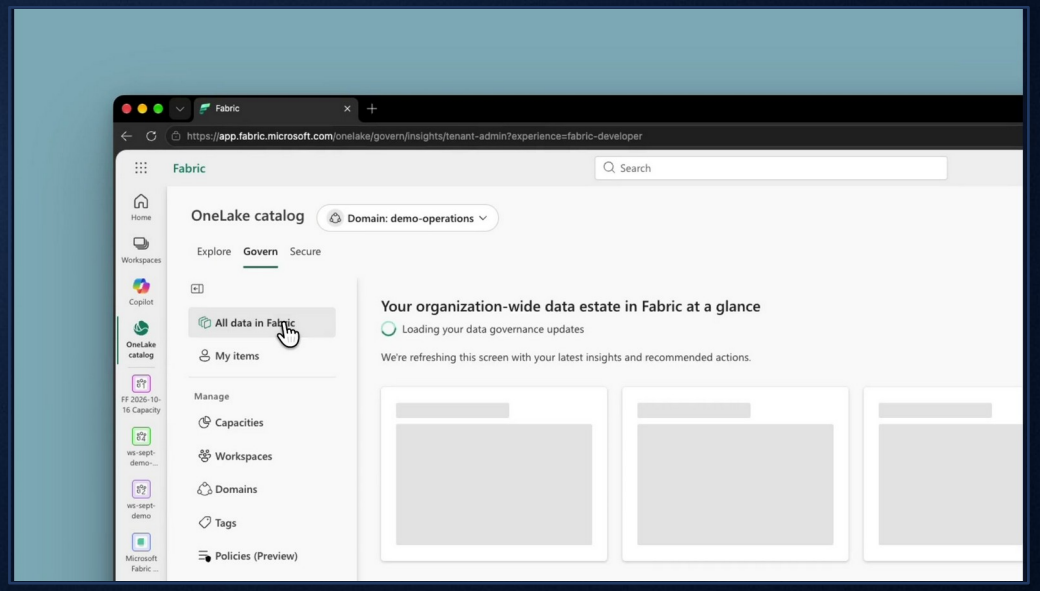
The default domain setting, then a new workspace created by a listed identity.

WHO DOES IT

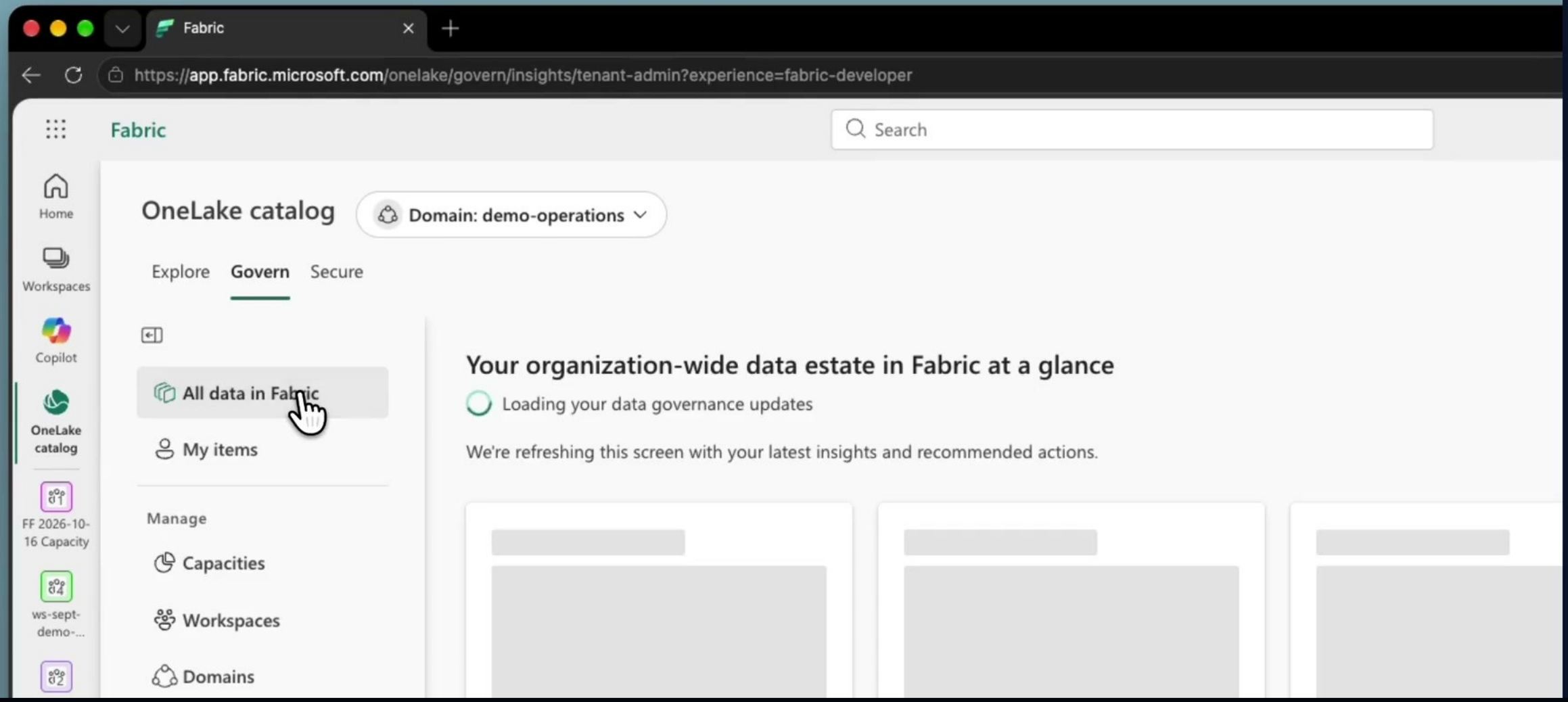
Me as admin adds the identity to the default domain list; the identity creates the workspace.

WATCH FOR

The Domain field is empty at first. Reopened, it reads demo-sales: nobody picked it.



▶ 108 S · PLAYS WITHOUT VOICE



▸ DEMO · AN ASSIGNMENT NOBODY MADE

Watch it in the episode: https://youtu.be/8wRSvnF_CtQ?t=774

03 A hand-applied label wins

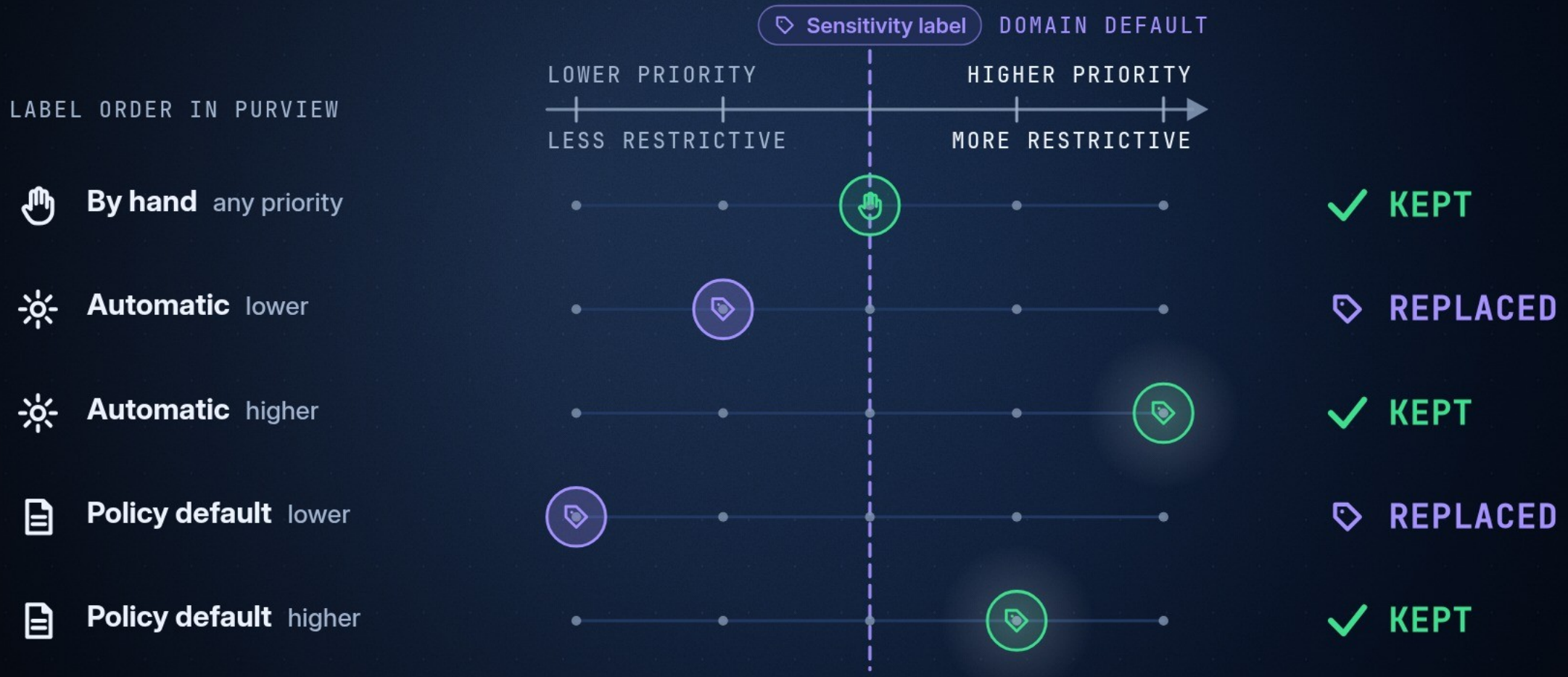
the one rule to remember

✓KEPT

never overridden, at any priority

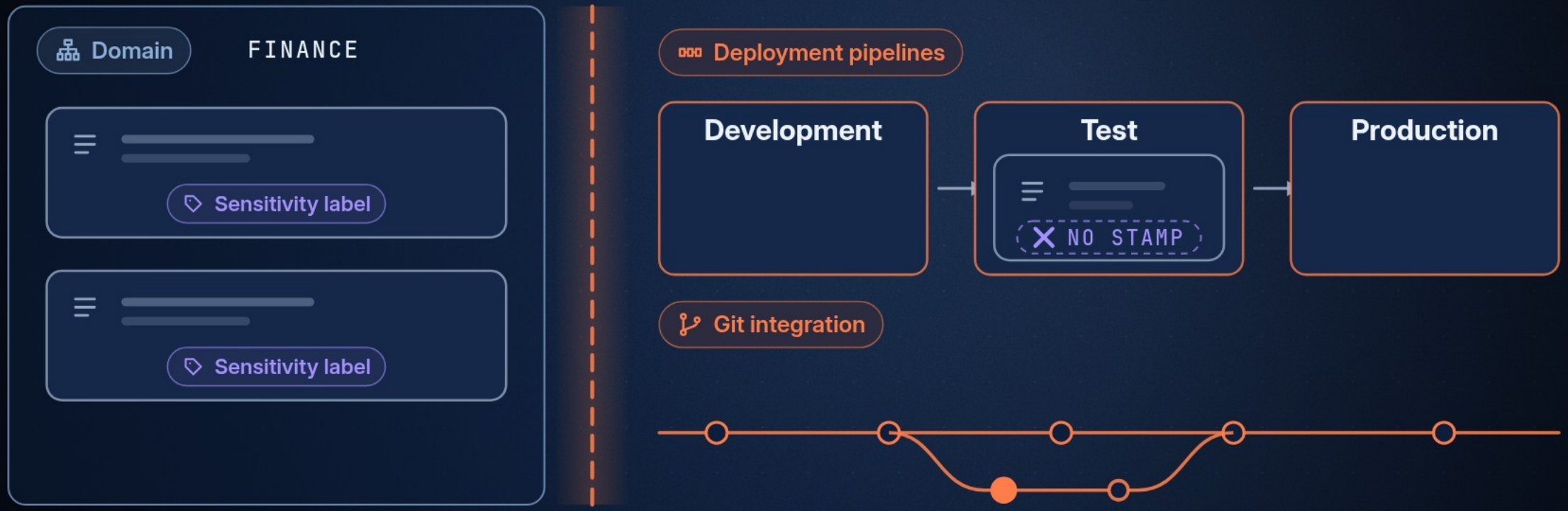
04 Everything else is a comparison

the label already there, against the domain default



05 Where the stamp stops

the limitation, read as written



Deployment pipelines and Git integration are currently not supported.

39

DOM

Domain

GOVERN

A domain answers "whose data is this?" – not "who may see it?"

Discovery, metadata and delegated settings. All three are real. None is a boundary.

DECISION RULES

- Access lives one layer down – workspace roles and item permissions.
- Every user sees every domain name. Never encode a secret in one.
- Default domain: name groups you maintain, review regularly.

Traps

39

DOM

Domain

GOVERN

TRAP	FIX
Domain used as a security boundary	Workspace roles + item permissions
Confidential unit named as a domain	Every user sees every domain name
Domain contributor can do nothing	Must also be workspace Admin
Workspace needed in two domains	One workspace, one domain
Workspaces appear in a domain unbidden	A default domain is running
Labels stop at the pipeline	Pipelines and Git not supported

38

CAP

Capacity

GOVERN

Capacity

NO. 38 · CAP · GOVERN

> A pool of compute in capacity units, shared by every workspace assigned to it.

What a capacity is

38
CAP
Capacity
GOVERN

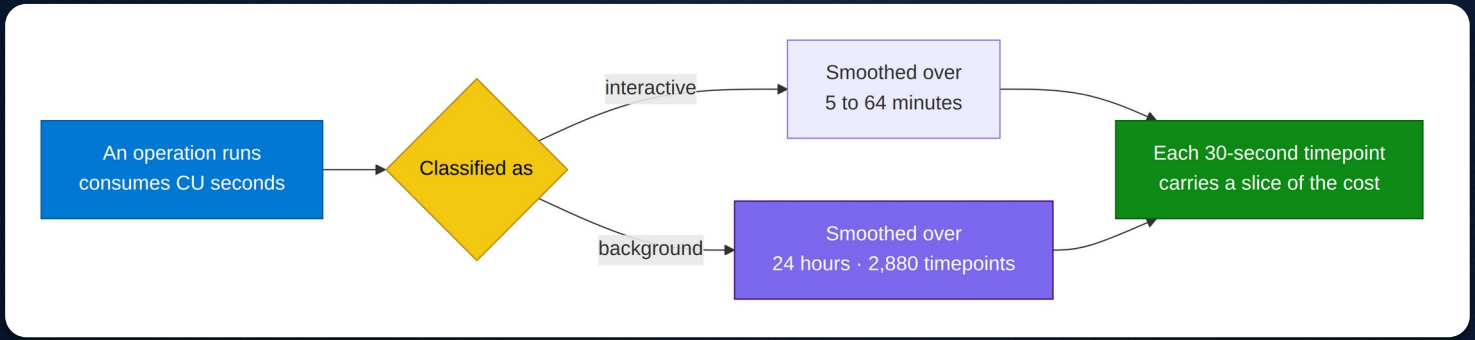


DIAGRAM 1 OF THE EPISODE'S ARCHITECTURE – WHERE A CU SECOND ACTUALLY LANDS

What it is	A pool of compute, measured in capacity units (CU). An F2 has 2 CU, an F64 has 64.
Who shares it	Every workspace assigned to it draws from the same pool.
Region	The capacity's region is where its workspaces keep their data.
Normal use	Size the SKU, assign workspaces, read the Metrics app, scale by SKU.
Shared capacity	My workspaces and Pro or PPU workspaces run on the tenant's shared capacity.

How usage is counted

38

CAP

Capacity

GOVERN

Timepoint 30 seconds, 2,880 per day. An F2 holds 60 CU seconds per timepoint.

Bursting Work may use more CU than the SKU allots, for a while.

Smoothing The cost is spread forward: interactive over 5 to 64 minutes, background over 24 hours.

Throttling Only when future timepoints fill up: first delays, then rejections.

Metrics app Read the smoothed line over 24 hours, not the spike.

FILM «WHERE A CU SECOND ACTUALLY LANDS», SCENE 6

38
CAP
Capacity
GOVERN

The red spike on your capacity chart – a forecast, or a receipt?

ANSWER IN THE CHAT

01

The unit nobody names

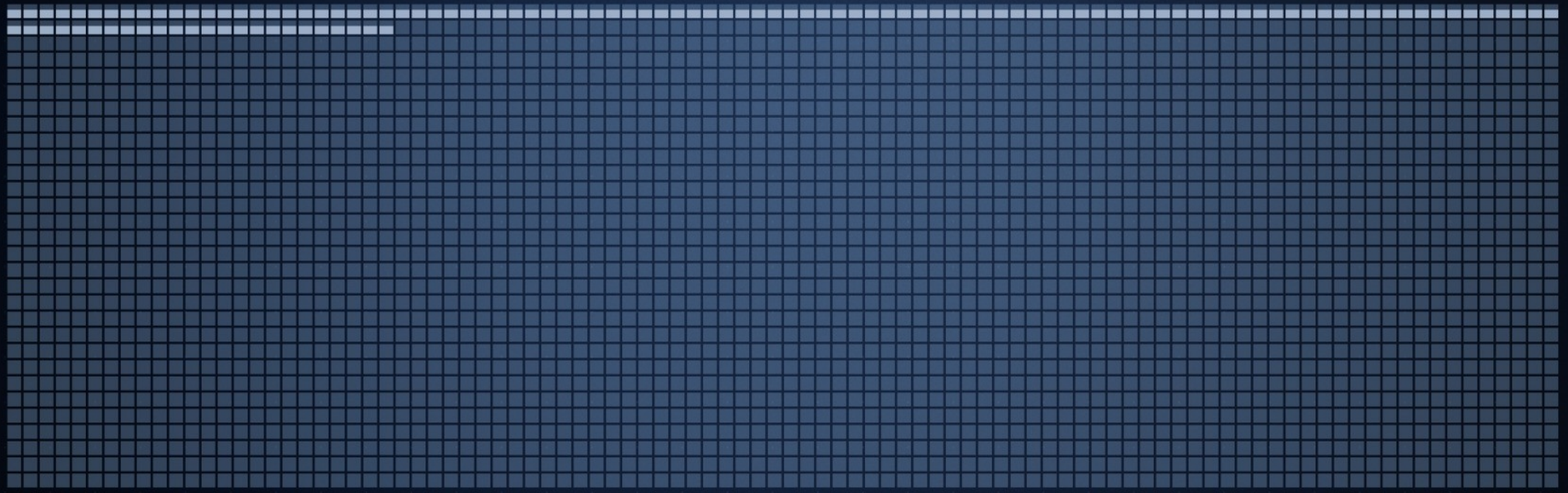
the timepoint

2,880

timepoints in 24 hours

30 SECONDS EACH

NOW



96 SLOTS A ROW · 30 ROWS · READ LIKE TEXT

24 HOURS LATER

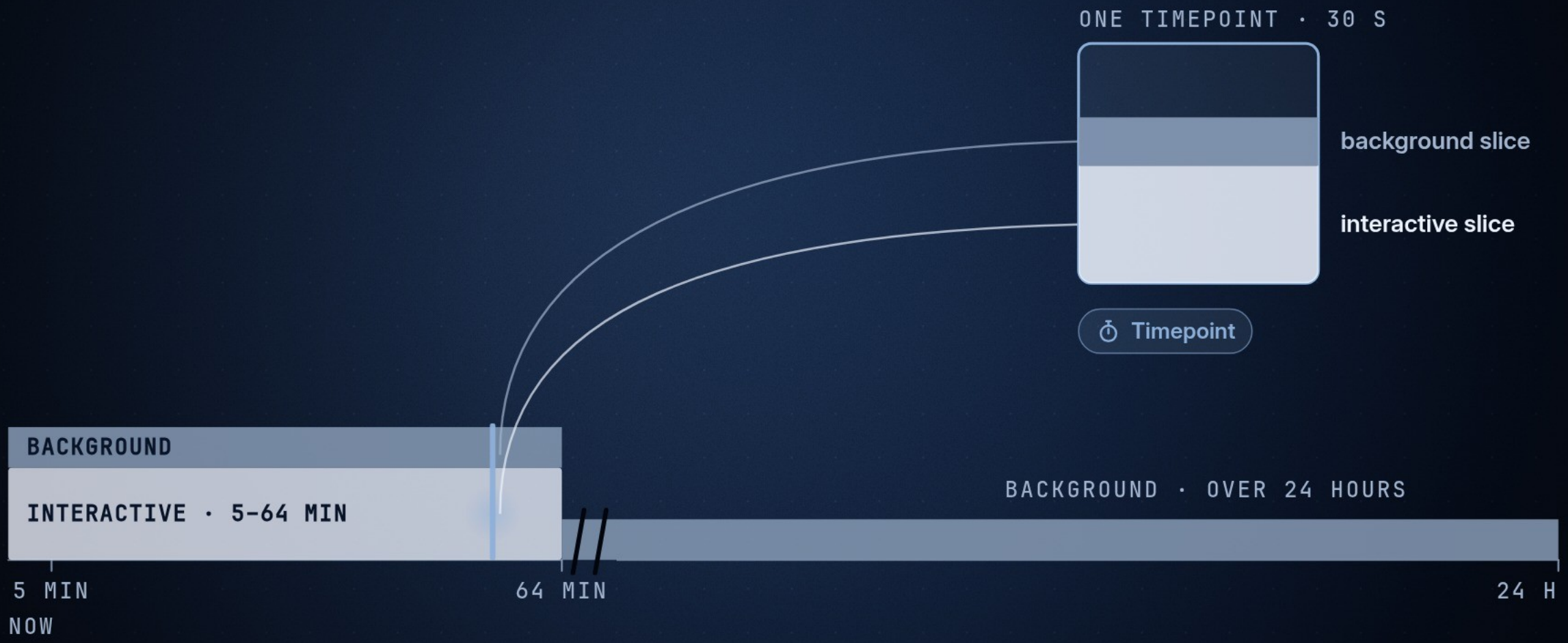
02 Why smoothing exists

sizing on the average, not the peak

A cost feature first, a performance feature never.

04 Two windows, one slot

interactive work spreads short, background work spreads long



05

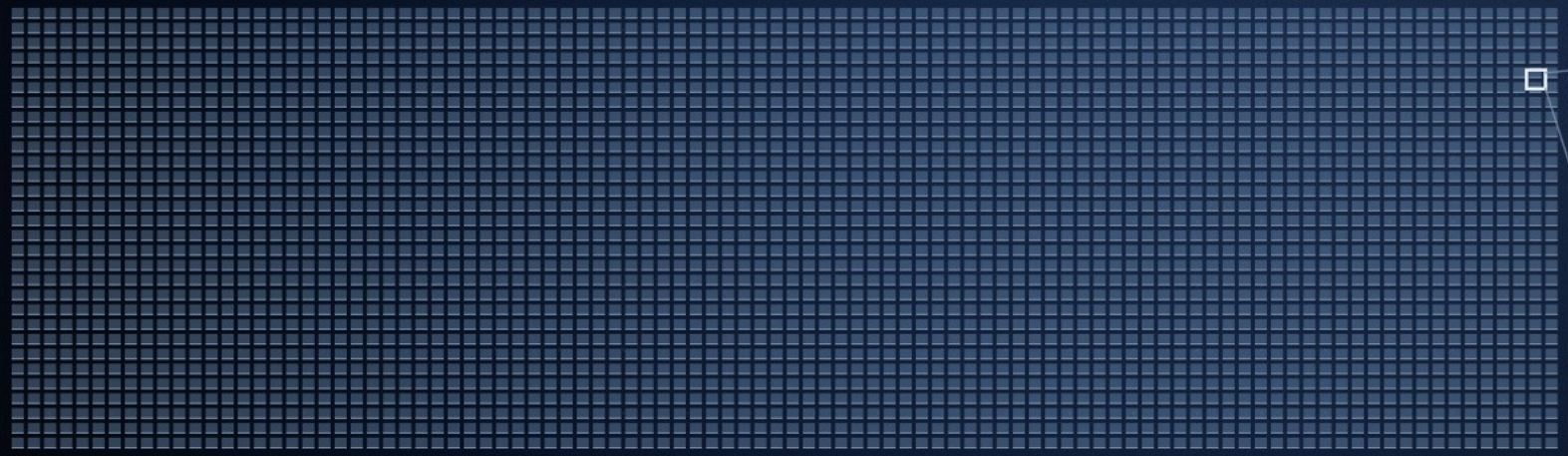
The documented example

one F2, one background job, one CU hour

An F2 provides 2 CU

3,600 CU seconds
÷ 2,880 slots
= 1.25 CU seconds

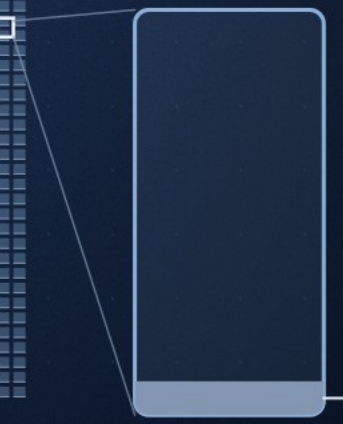
2,880 TIMEPOINTS · ONE DAY



Throttling

not triggered ✓

ONE F2 SLOT



60 CU seconds
= 100 % of a slot
(2 CU × 30 s)

≈ 2.1 %

1.25 CU seconds

SLIVER DRAWN 4× LARGER

SOURCE · MICROSOFT LEARN · FABRIC CAPACITY THROTTLING POLICY

38
CAP
Capacity
GOVERN

Read the Metrics App

WHAT YOU WILL SEE

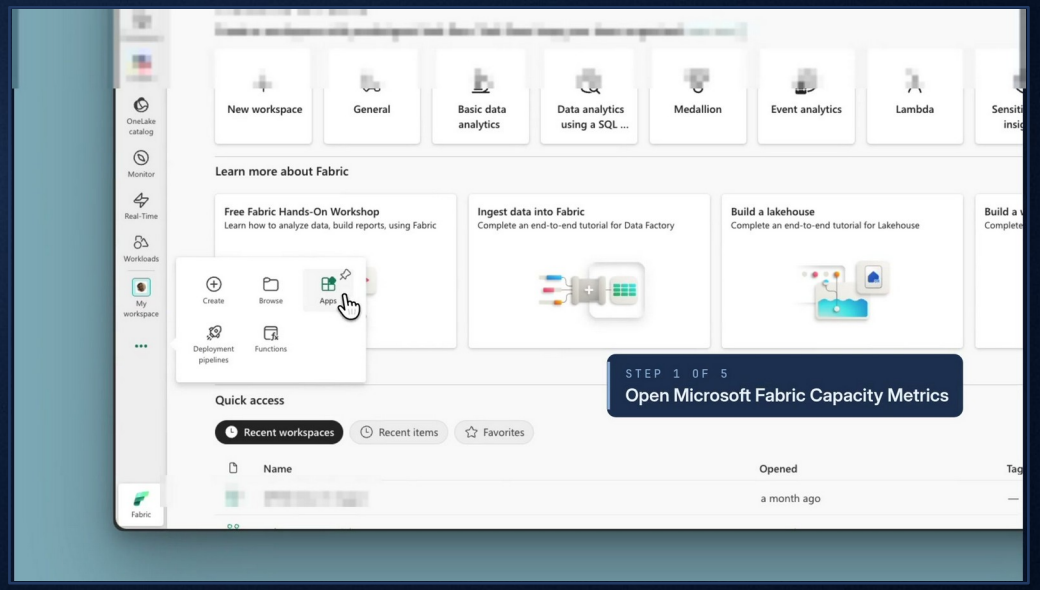
The Capacity Metrics app: the Compute page, one timepoint, interactive and background operations.

WHO DOES IT

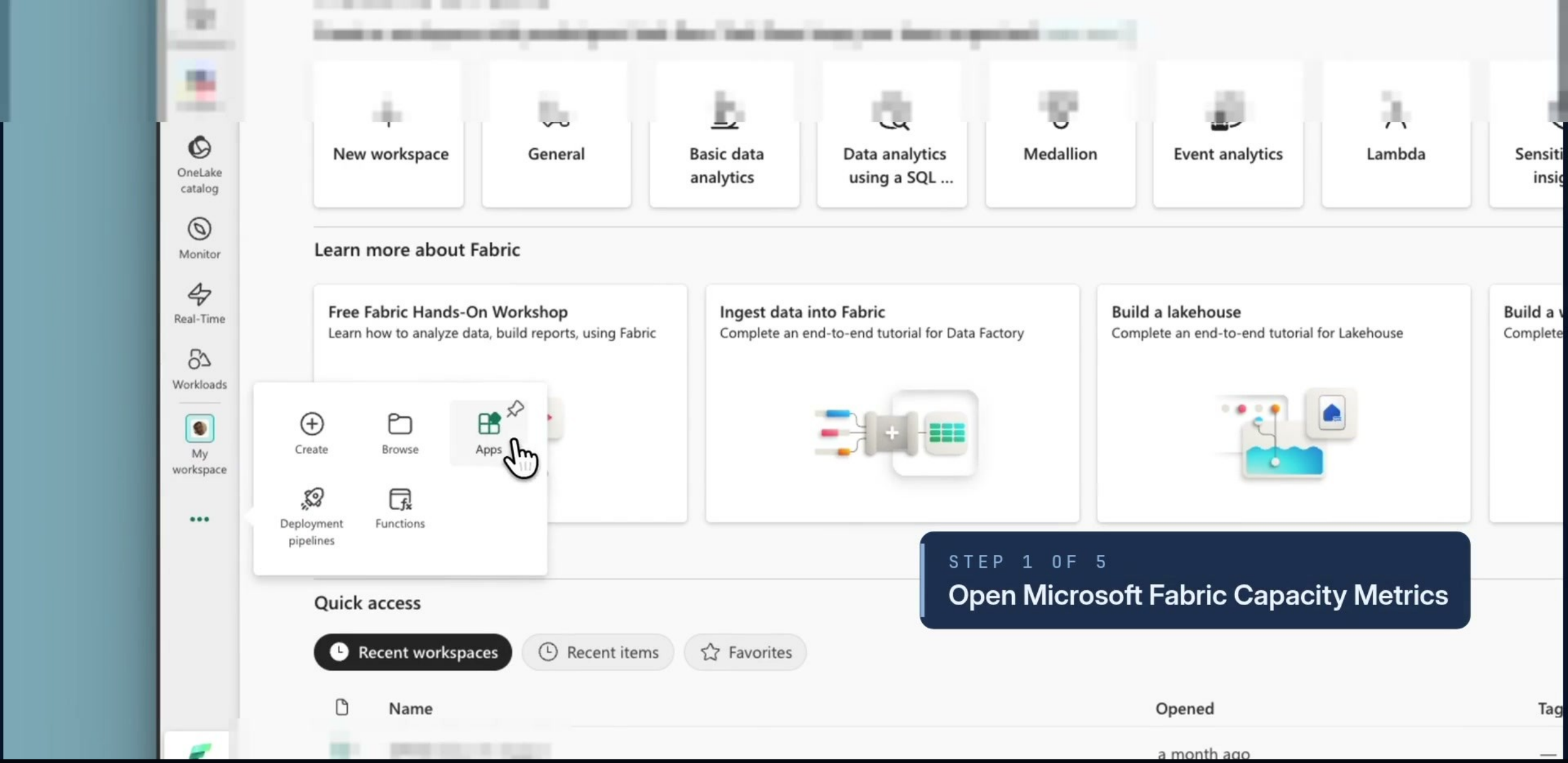
Me as capacity admin, in the Microsoft Fabric Capacity Metrics app.

WATCH FOR

A timepoint is 30 seconds. An afternoon notebook still pays into the evening's window.



▶ 156 S · PLAYS WITHOUT VOICE

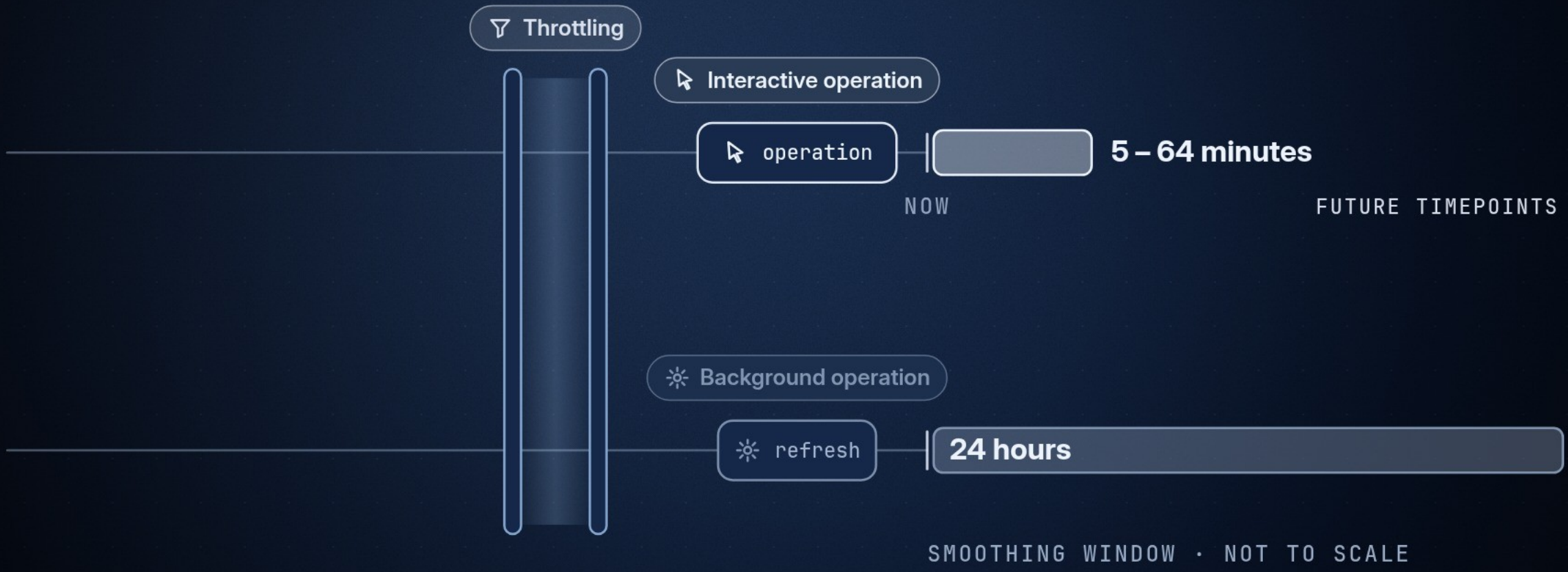


▸ DEMO · READ THE METRICS APP

Watch it in the episode (online Fri 16 Oct): https://youtu.be/iE-jdcseCaY?t=173

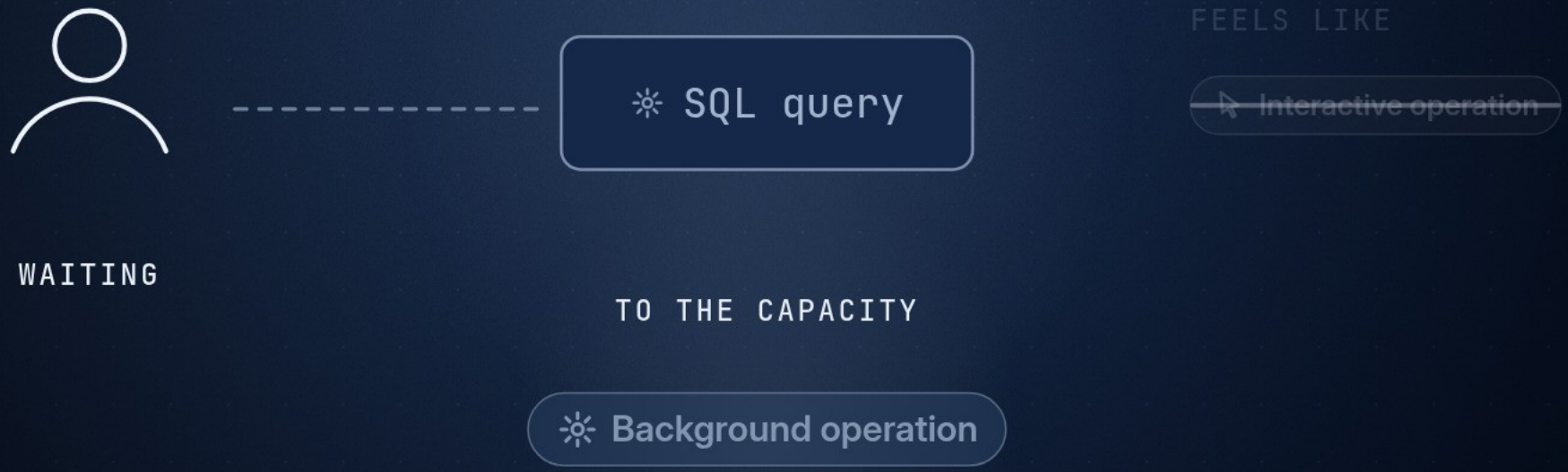
02 One stamp, two windows

it follows the operation, not the person



04 Warehouse

almost every operation is reported as background



05 One stamp, two directions

the same classification, seen from both sides

38

CAP

Capacity

GOVERN

Watch One Job Spread

WHAT YOU WILL SEE

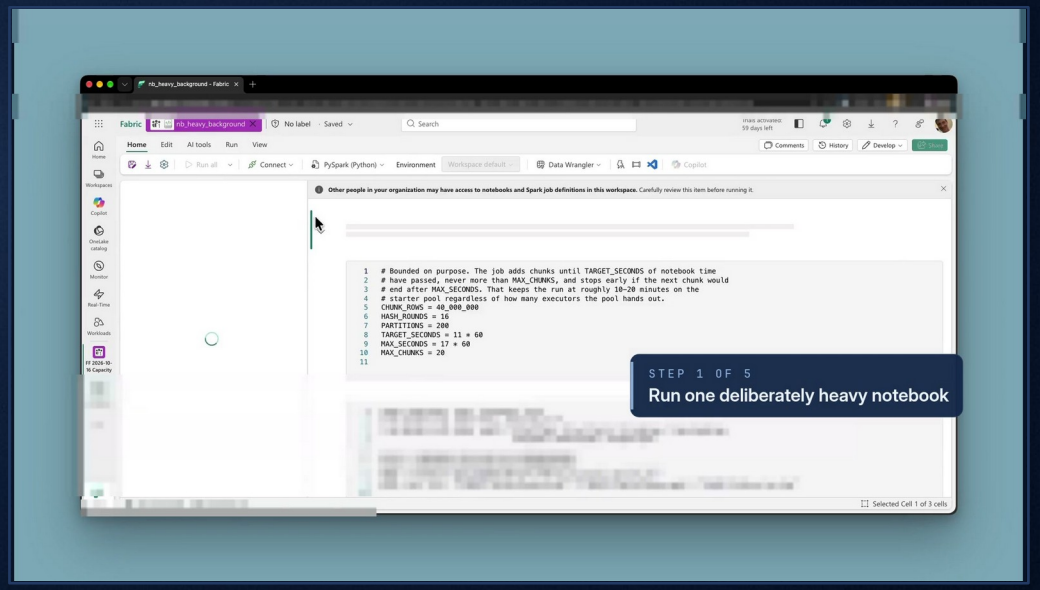
One deliberately heavy background notebook, then its cost in a single timepoint, hours later.

WHO DOES IT

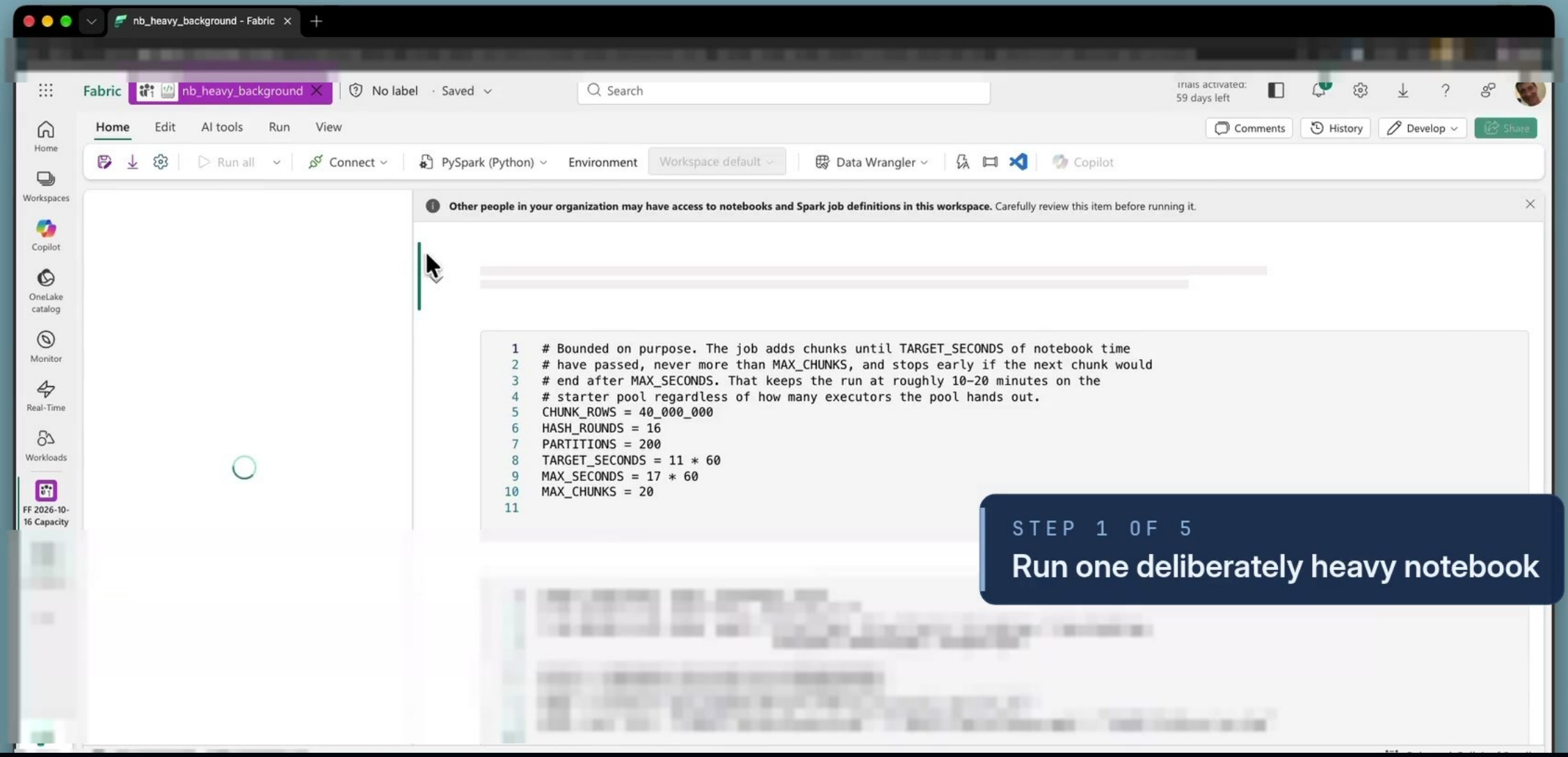
Me as capacity admin – run the notebook, then read the Metrics app.

WATCH FOR

Total CU divided by 2,880 gives the timepoint CU. Smoothing is a division.



▶ 126 S · PLAYS WITHOUT VOICE

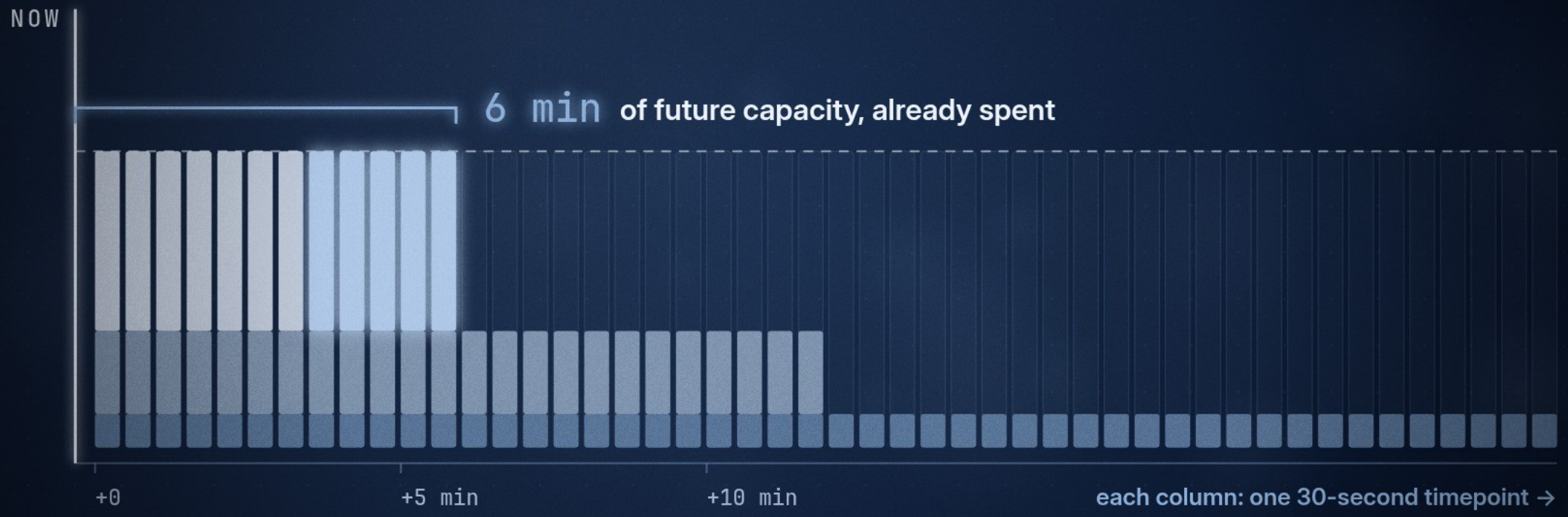


▸ DEMO · WATCH ONE JOB SPREAD

Watch it in the episode (online Fri 16 Oct): https://youtu.be/iE-jdcseCaY?t=465

01 The meter

minutes of future capacity already spent



02 The staircase

step 3 · everything new rejected

NEW REQUESTS

Interactive · report query — rejected

Background · refresh — rejected

Already running · in flight — never cut off

FUTURE CAPACITY ALREADY SPENT

0 — 10 min — 60 min — 6 h — 24 h

SPENT

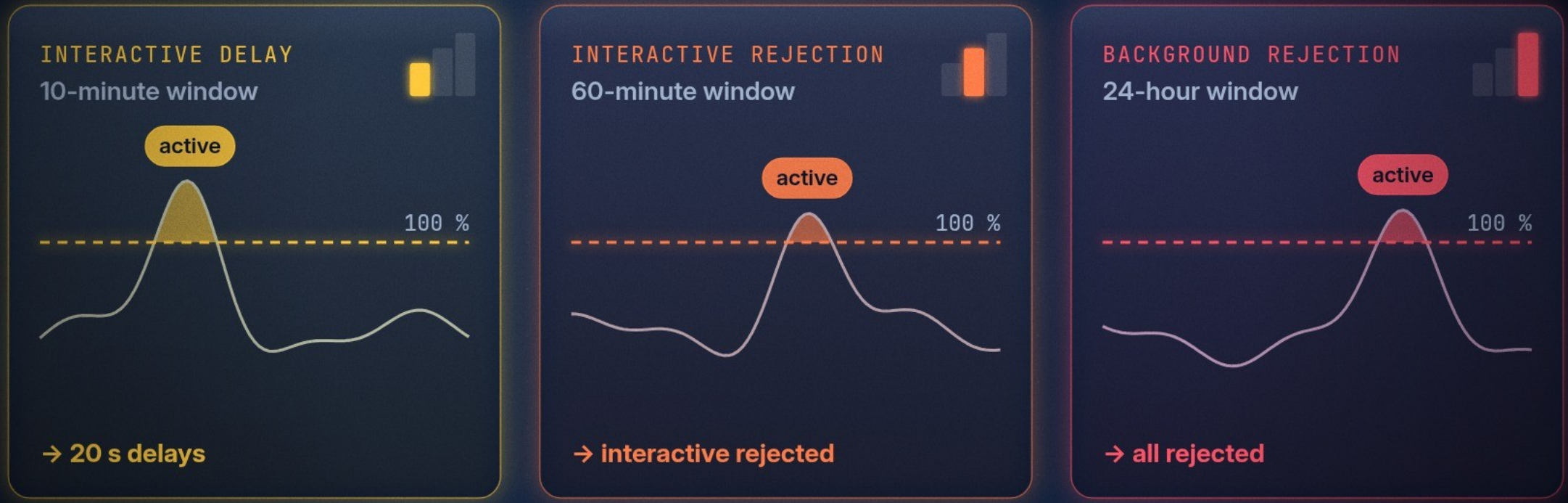
26 h

STEP 3

04

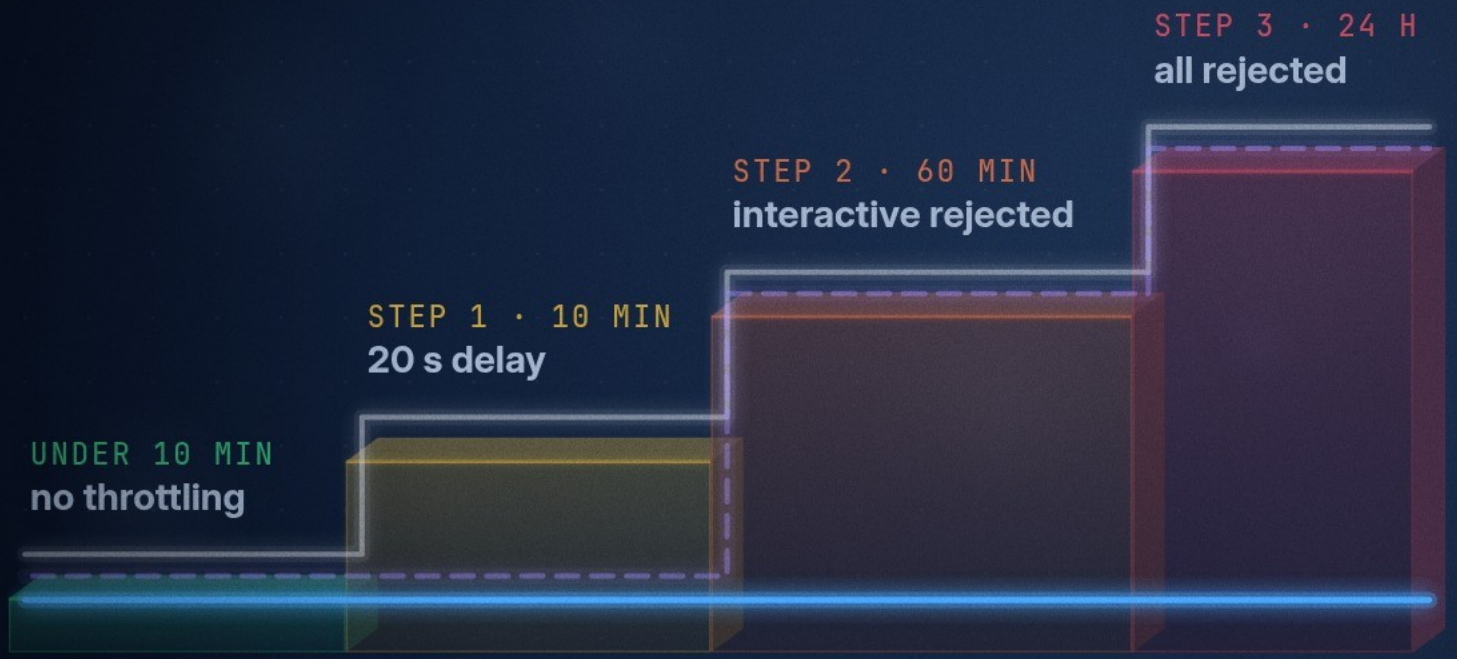
Where you see it

Capacity Metrics app · Compute page · Throttling



05 **The trade-off**

a policy per workload



Most workloads
delayed, then rejected

Real-Time Intelligence
no delay step, rejected at 60 min

Eventstreams
never throttled, starved of CU

The quietest failure: a stream that falls behind.

01 Sizing from the peak

the spike you remember is a receipt, not a forecast

02 Halve the SKU, double the percentage

the same smoothed work in a smaller box

> 100 %

Smoothing USAGE OF F64

headroom left: 0

Throttling **not yet**

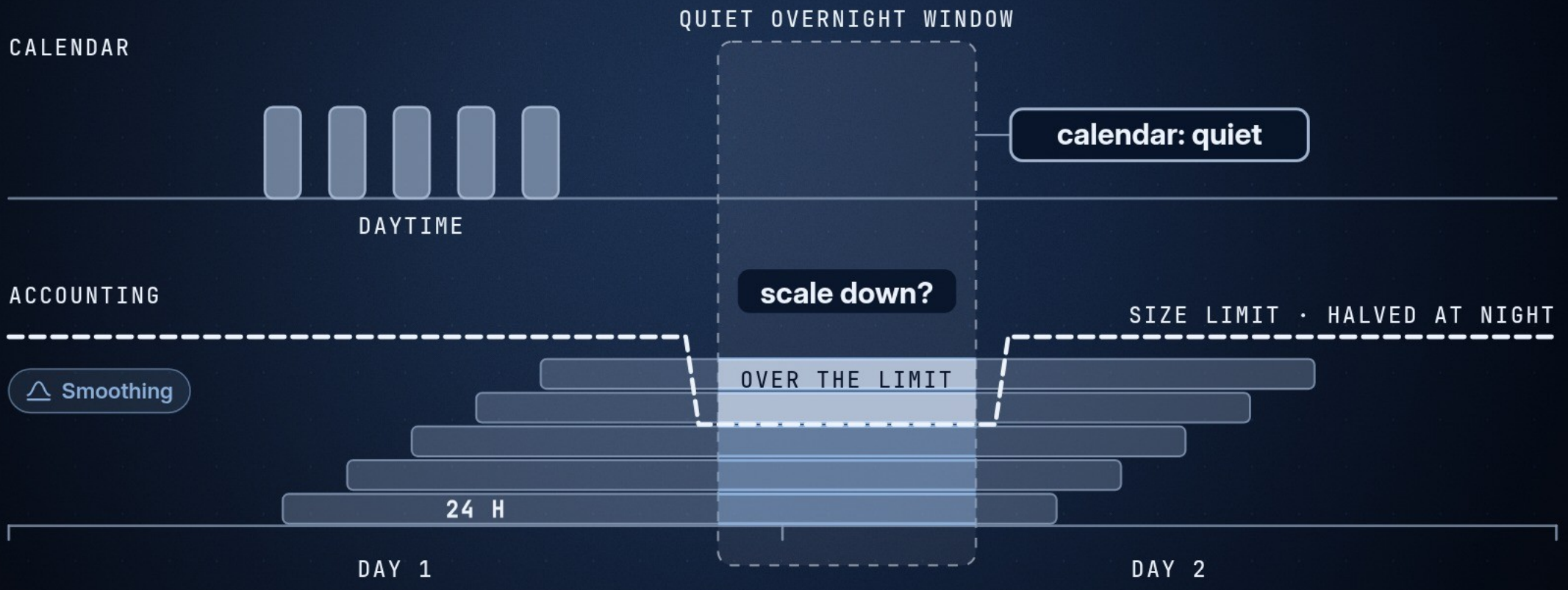
10 MINUTES OF FUTURE CAPACITY

Overage protection

Up to 10 minutes of future capacity can be consumed without any throttling.

03 No quiet period in the accounting

yesterday's daytime work is still on the ledger at night



04 Surge protection, honestly

it is not a sizing fix, and it has a price

38
CAP
Capacity
GOVERN

Fabric does not charge you when work happens. It spreads the cost forward.

Interactive pays over 5 to 64 minutes, background over 24 hours. Last night's refresh still pays into this afternoon.

DECISION RULES

- Size from the smoothed line, never from the spike.
- Halve the SKU, double the percentage: F128 under 40 % before F64.
- Surge protection is a trade, not a sizing fix.

38

CAP

Capacity

GOVERN

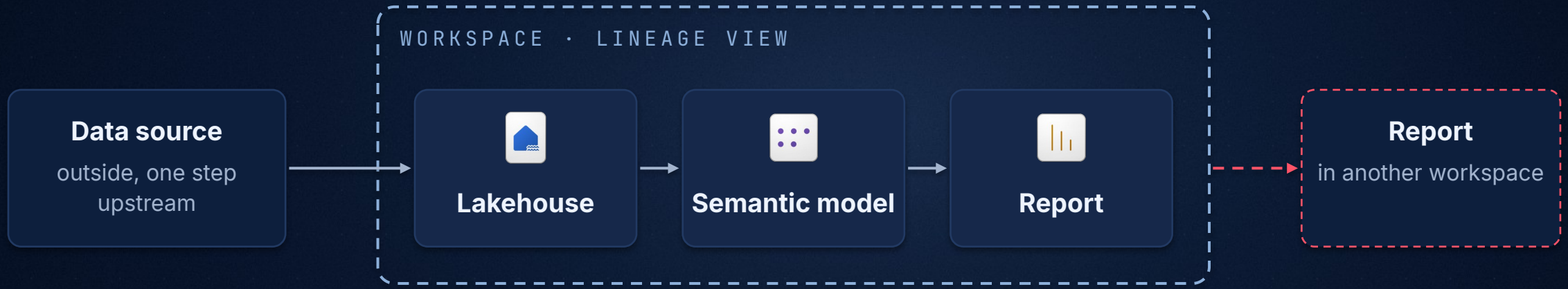
The staircase

FUTURE CAPACITY SPENT	WHAT HAPPENS
Up to 10 min	Nothing – overage protection
Past 10 min	New interactive waits 20 s
Past 60 min	Interactive rejected, background runs
Past 24 h	All new requests rejected
Real-Time Intelligence	Skips the 20 s step
Eventstreams	Never throttled – starved of CU

COMING UP ON FABRIC FRIDAY

Lineage – who breaks when this changes?

42
LIN
Data Lineage
GOVERN



Lineage view: every item in the workspace, plus one step upstream.

Not shown. Use impact analysis.

> **Lineage goes deeper on Fabric Friday, 6 Nov (Purview). Bring your question.**

QUESTIONS FROM THE COMMUNITY · 1/5 · WORKSPACE

Asked in public by people who aren't in the room tonight

> **"Two users can see all data, rather than being restricted by the configured security rules."**

Row-level security filters Viewers only. Contributor, Member and Admin bypass it.

Microsoft Q&A · 21 Aug 2026 · RLS Issue in PowerBI

"Does Domain permissions grant workspace roles?"

No. Domain = governance scope. Workspace roles = access.

Fabric Community forum · 16 Nov 2025 · Domain permissions & workspace roles

> **"If I have only one workspace can I add that workspace to multiple different domains?"**

No. One workspace belongs to at most one domain – choose, or split the workspace.

Fabric Community forum · 5 Jul 2026 · Workspaces and Domains Vs Workspaces and Capacities

> **"The throttling counter is increasing the day long for no reason."**

Background work is smoothed over 24 hours. Yesterday's jobs still pay into today.

Fabric Community forum · 16 Jun 2024 · Why is there CU usage while no activity running?

> **"At 01:00 AM, the capacity should automatically downscale (for example from F64 → F32) since usage is low."**

The night still carries smoothed daytime work. Halving the SKU doubles the percentage.

Fabric Community forum · 12 Mar 2026 · Support for Time-Based Auto Scaling of Microsoft Fabric Capacity

NEXT MEETUP

DevOps for Fabric – Git & Deployment Pipelines

Tuesday 10 November 2026 · 18:30 CET · Online

- Git integration and deployment pipelines, Dev to Test to Prod
- Variable libraries, sensitivity labels and Purview

Register on meetup.com

meetup.com/ai-and-intelligent-cloud

Q & A

Your questions

1. Open Q&A in the Teams meeting bar
2. Ask, or upvote a question already there

Written answers to everyone first. A public LinkedIn post a week later.

All links and the handout
the-trusted-advisor.com/events/…

RESOURCES

Keep going

START HERE · ALL LINKS AND THE HANDOUT

the-trusted-advisor.com/events/...

Handout PDF · every episode, Short, film and podcast from tonight

WORKSPACE

Episode on YouTube
Fabric Friday, 2 Oct

YouTube Short

Podcast episode

Fabric Periodic Table
fabricperiodictable.com

DOMAIN

Episode on YouTube
Fabric Friday, 9 Oct

YouTube Short

Podcast episode

LinkedIn – questions by DM
linkedin.com/in/matthias-falland

CAPACITY

Episode on YouTube (online Fri 16 Oct)
Fabric Friday, 09:00

YouTube Short (online Sun 18 Oct)

Podcast episode (online Fri 16 Oct)

The podcast
Fabric Architecture Podcast

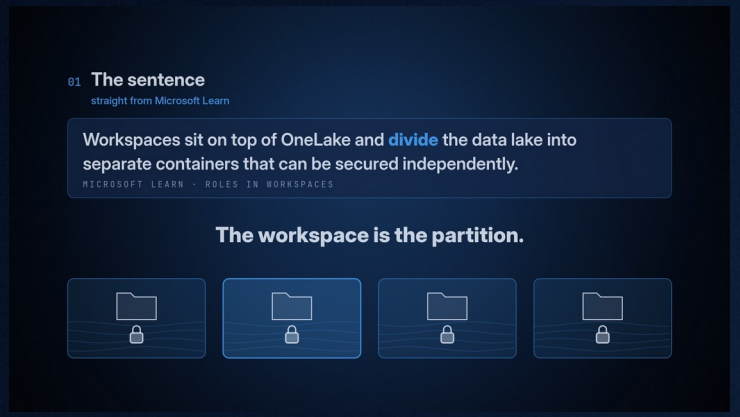
APPENDIX

All scenes

The scenes of each architecture film that the evening skipped, in film order. The full films play in the episodes.

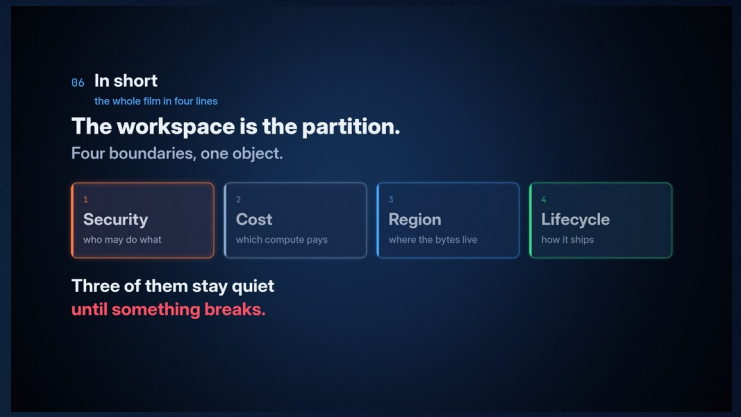
ALL SCENES · 01 · WORKSPACE

Four Boundaries in One Object



SCENE 1 Source: Microsoft Learn, Roles in workspaces

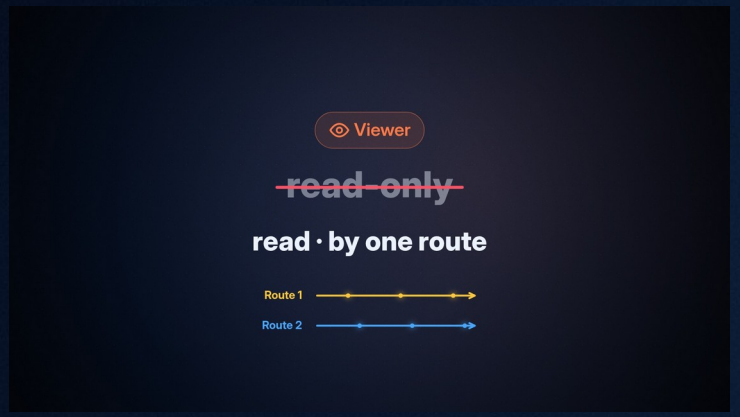
SCENE 3 Roles: Admin, Member, Contributor, Viewer



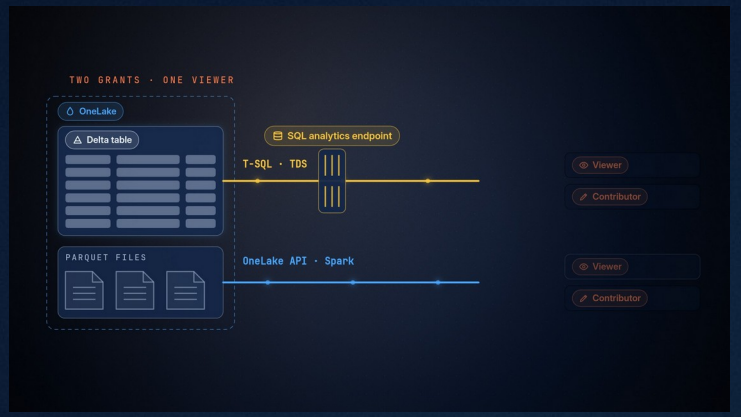
SCENE 6 Summary of the film

ALL SCENES · 01 · WORKSPACE

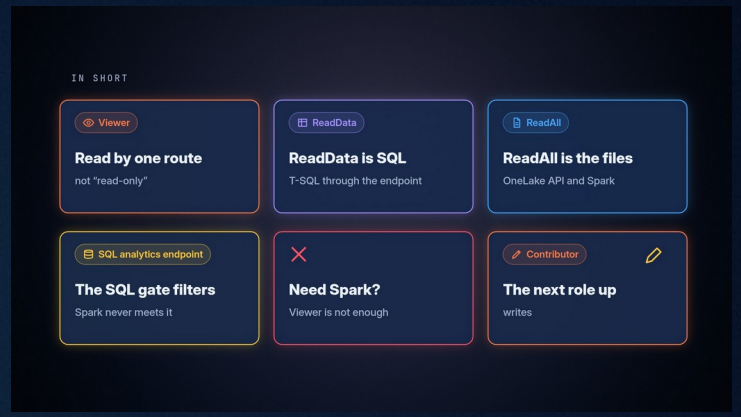
The Viewer Line: One Table, Two Routes



SCENE 1 Viewer = read via SQL only



SCENE 2 Same bytes, two routes

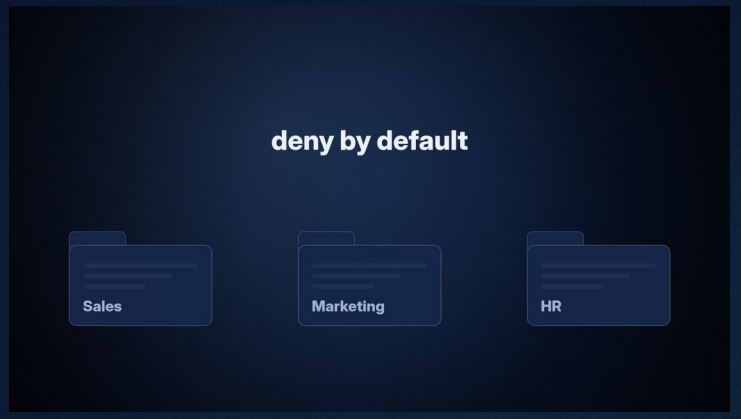


SCENE 6 Summary of the film

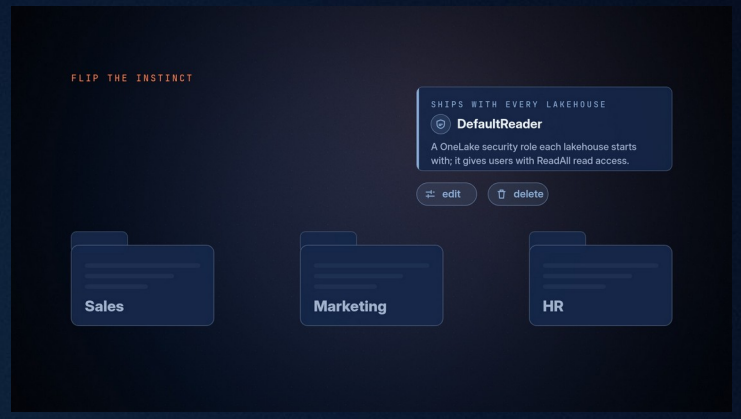
ALL SCENES · 01 · WORKSPACE

Why OneLake Security Cannot Fence In a Contributor

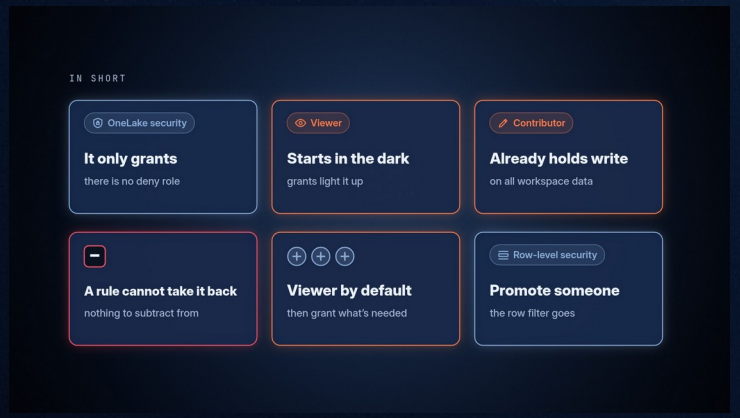
SCENE 1 The design people reach for



SCENE 2 OneLake security has no deny



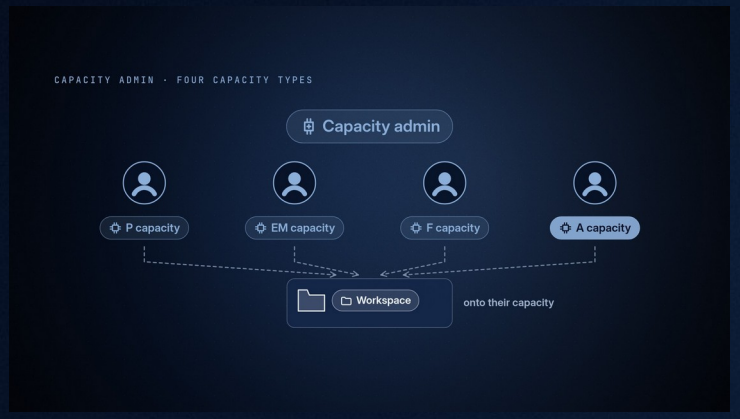
SCENE 6 Lakehouses ship a default reader role



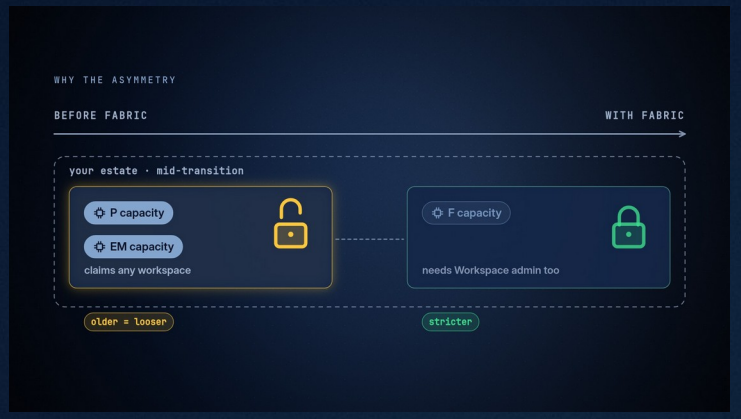
SCENE 8 Summary of the film

ALL SCENES · 01 · WORKSPACE

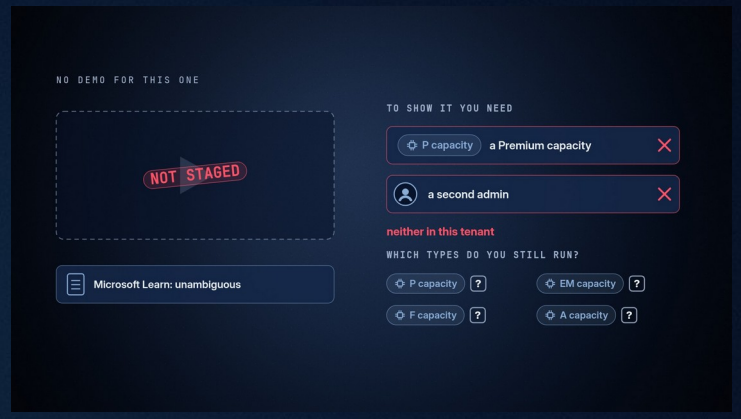
Who Can Claim Your Workspace



SCENE 1 Capacity type decides



SCENE 3 Older rule = looser rule



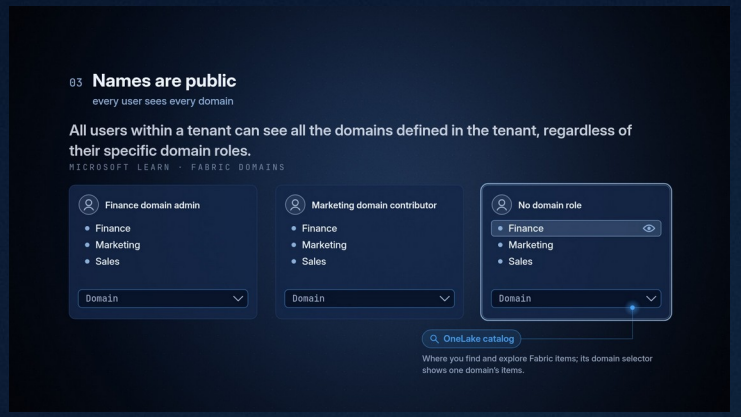
SCENE 6 Docs are unambiguous

SCENE 7 Summary of the film

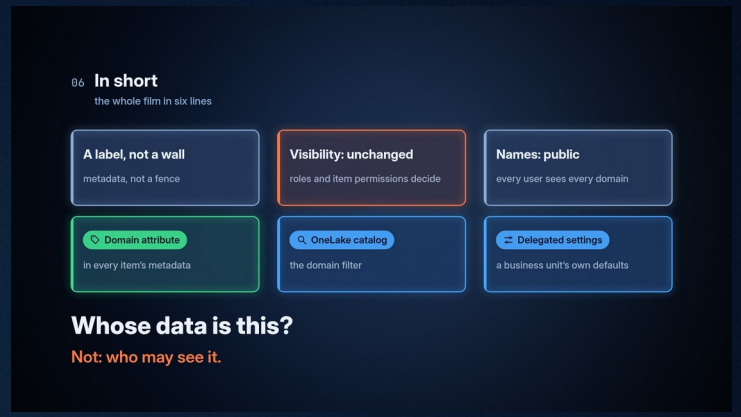
ALL SCENES · 02 · DOMAIN

What a Domain Does, and What It Does Not

SCENE 2 The domain is a label



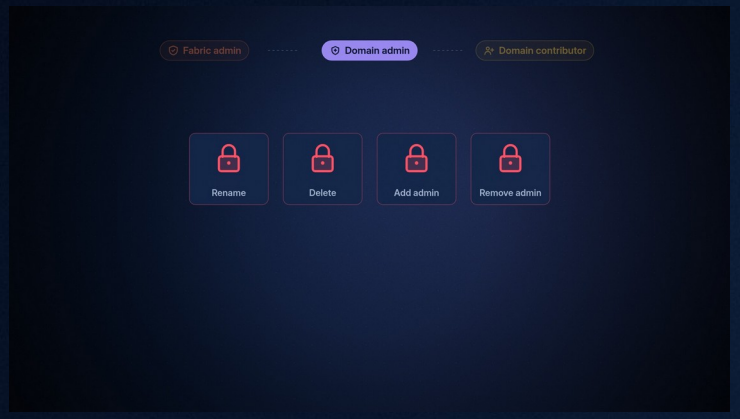
SCENE 3 All domain names are public in the tenant



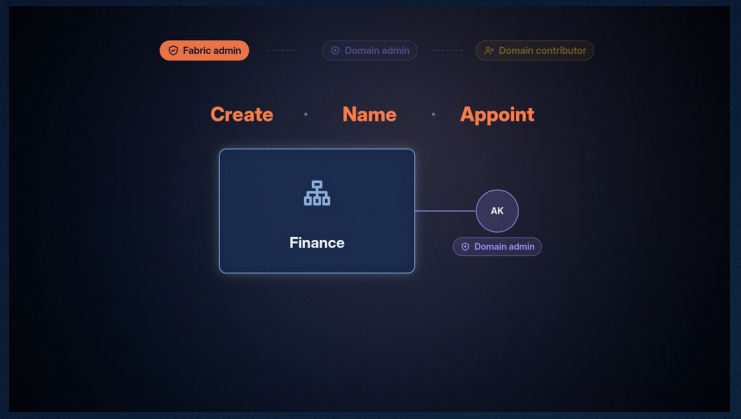
SCENE 7 Summary of the film

ALL SCENES · 02 · DOMAIN

Three Roles, and the Four Things an Admin Cannot Do

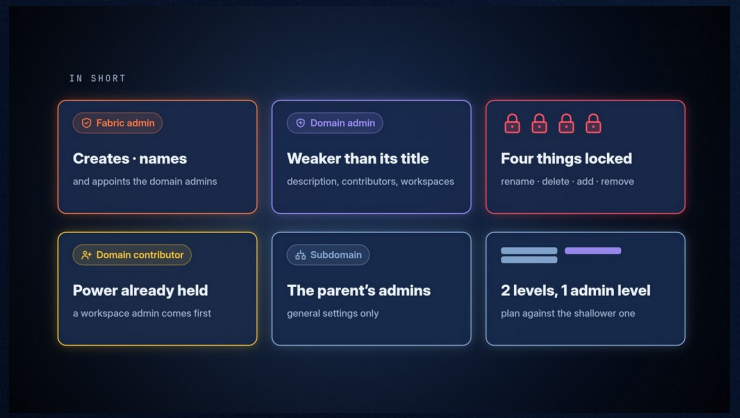


SCENE 1 Three roles



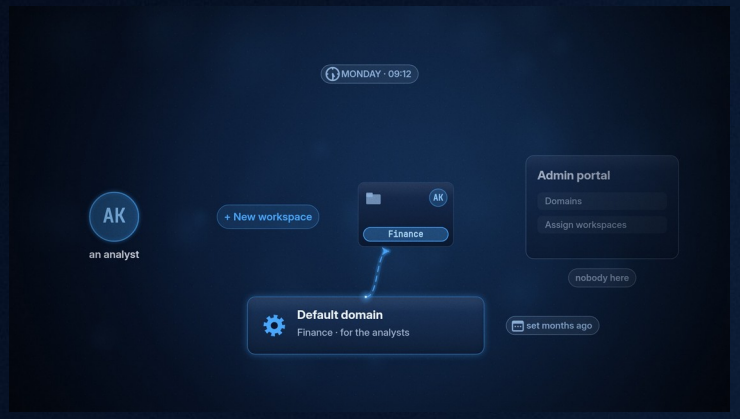
SCENE 2 Top of the ladder

SCENE 6 Why the rule is right

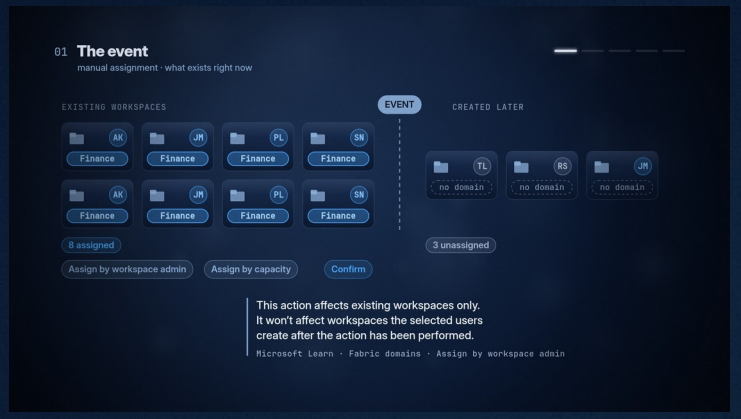


SCENE 8 Summary of the film

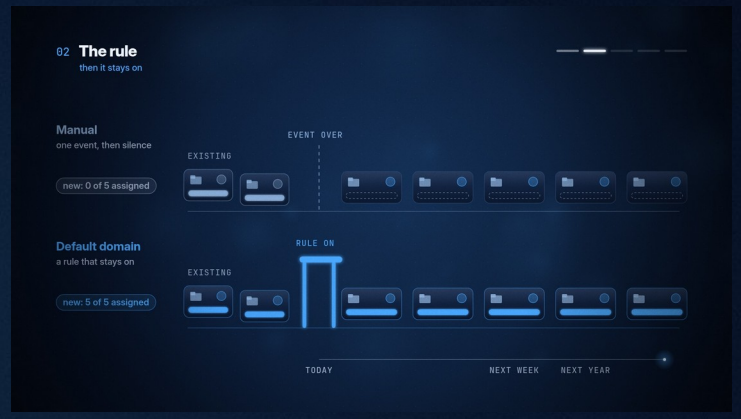
The Default Domain Assigns Workspaces For You



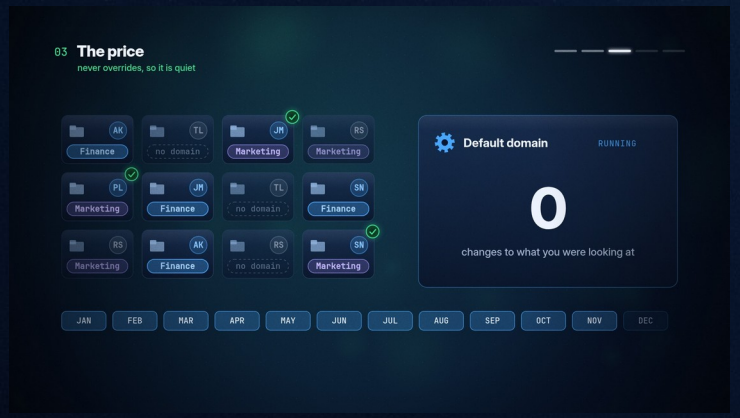
SCENE 1 A setting, months ago



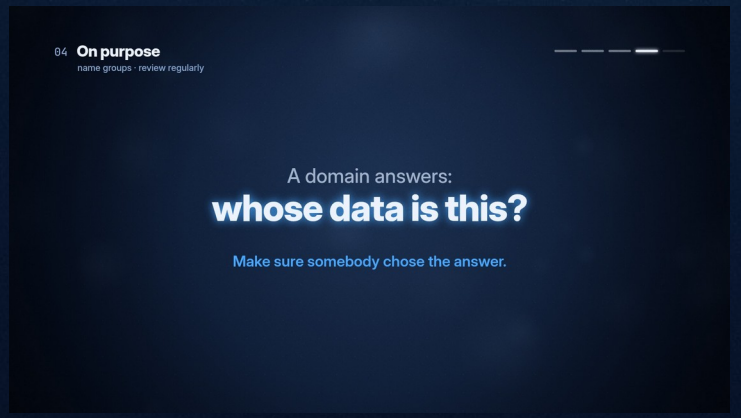
SCENE 2 Learn: affects existing workspaces only



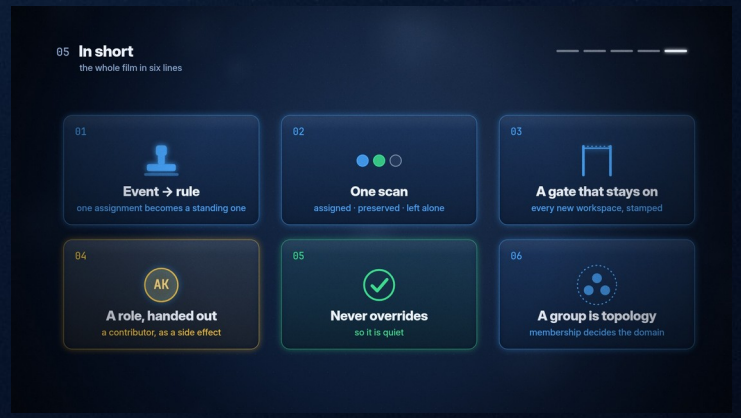
SCENE 4 Next week, next year



SCENE 6 Zero visible changes



SCENE 9 Make sure somebody chose the answer

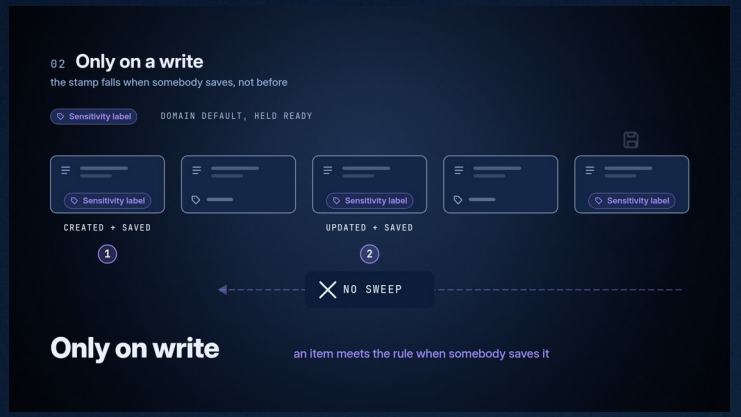


SCENE 10 Summary of the film

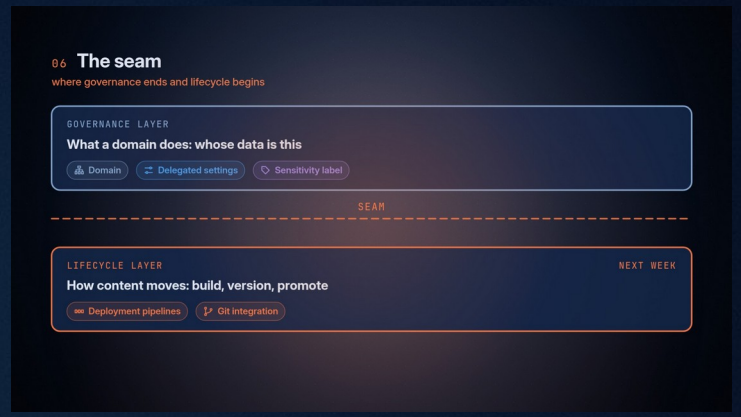
ALL SCENES · 02 · DOMAIN

The Sensitivity Label Override Ladder

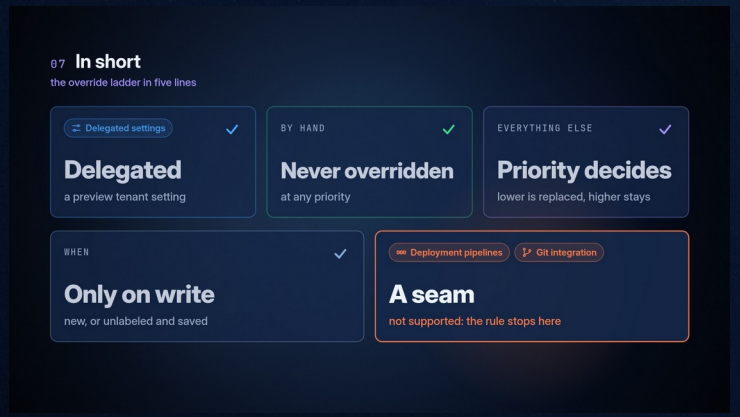
SCENE 1 Tenant setting must be switched on



SCENE 2 Only on write

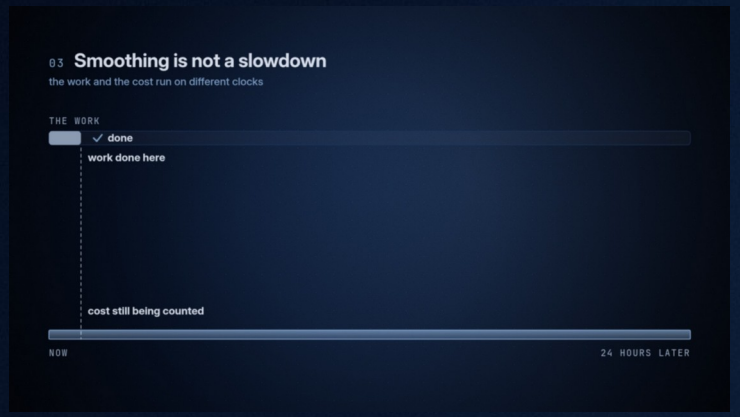


SCENE 6 Know where the seam is



SCENE 7 Summary of the film

Where a CU Second Actually Lands

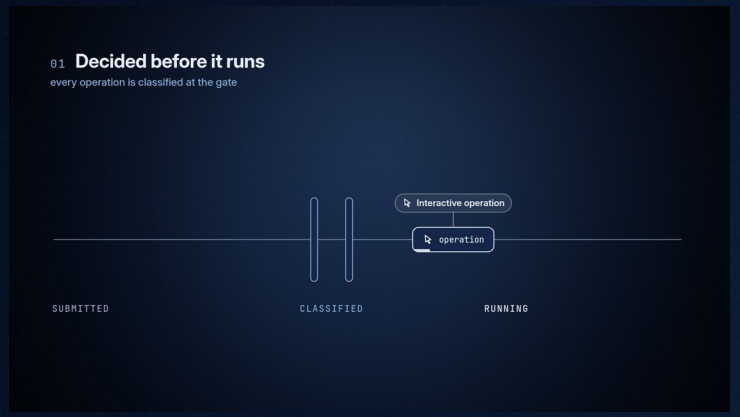


SCENE 3 Learn: no effect on execution time

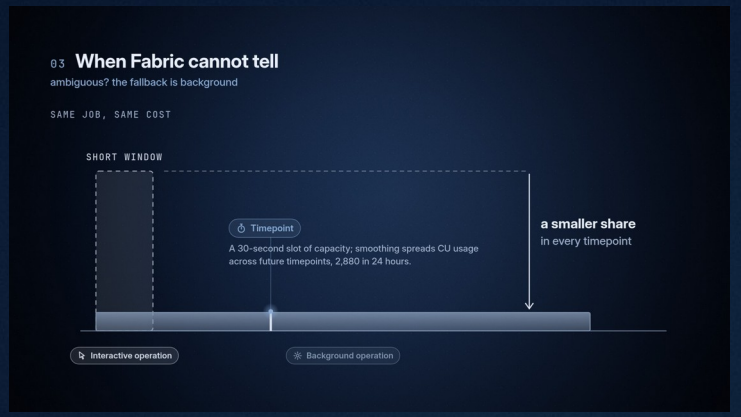
SCENE 6 Summary of the film

ALL SCENES · 03 · CAPACITY

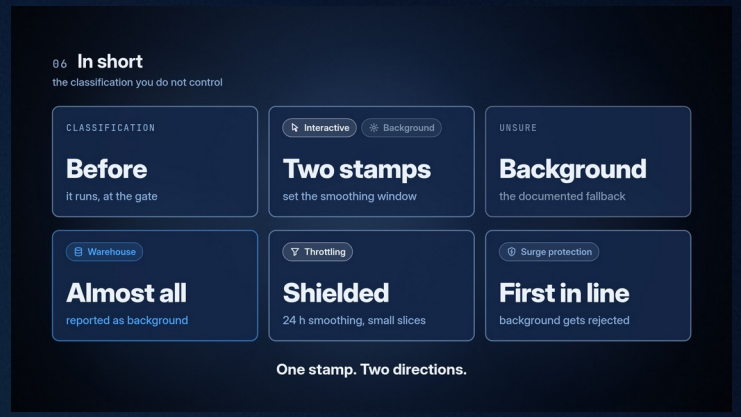
The Classification You Do Not Control



SCENE 1 Classified at the gate



SCENE 3 Documented fallback



SCENE 6 Summary of the film

ALL SCENES · 03 · CAPACITY

The Throttling Staircase, and Who Skips Steps

SCENE 1 The symptoms users report

SCENE 3 Overage protection: 10 minutes

SCENE 4 "Fabric is slow"

SCENE 5 "Fabric is down"

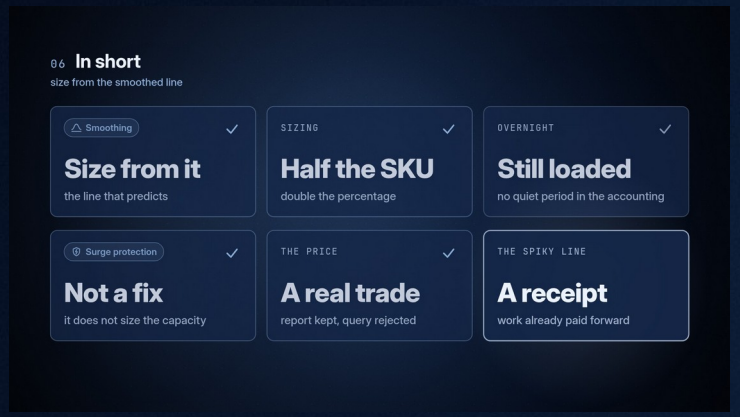
SCENE 7 Real-Time Intelligence: no delay step

SCENE 8 Starved, not throttled

The Throttling Staircase, and Who Skips Steps

SCENE 11 Summary of the film

Sizing From the Smoothed Line



SCENE 6 Summary of the film

06 Cheat Sheet – Workspace

The One "Why"

A workspace is not a folder. It is a cut through OneLake – and the cut has to carry everything.

Once you partition the lake, that partition is the only place to hang security, cost, residency and lifecycle. That is why one object has four owners, and why three of the four stay invisible until they are expensive.

Roles at a Glance

Capability	Admin	Member	Contributor	Viewer
Delete workspace · add admins	yes			
Connect to Git · create workspace identity	yes			
Add members and lower	yes	yes		
Allow others to reshare	yes	yes		
Create / modify items	yes	yes	yes	
Execute notebooks · pipelines	yes	yes	yes	

Capability	Admin	Member	Contributor	Viewer
View execution output	yes	yes	yes	yes
T-SQL read via TDS (`ReadData`)	yes	yes	yes	**yes**
Spark / OneLake API read (`ReadAll`)	yes	yes	yes	**–**

> **`ReadData` ≠ `ReadAll`.** "Read-only" is a route, not a level.

Limits

Limit	Value
Items per workspace	**1,000** – parent *and* child items
Movable across regions	**7 item types**
Permission change latency	**Next sign-in**
Post-migration wait for non-movable types	up to **1 hour**

The seven that cross a region: Report · Semantic model (small storage) · Dashboard · Dataflow Gen1 · Paginated Report · Datamart · Scorecard

---

Who Can Claim Your Workspace

Capacity type	Can move ANY workspace?	Needs Workspace Admin?
P Premium	**Yes**	No
EM Embedded	**Yes**	No
F Fabric	No	**Yes**
A Azure	No	**Yes**
Fabric / Global Admin	**Yes**, any type	No

> P and EM predate the Fabric permission model. During a Premium-to-Fabric transition both rules run at once, and the older one is looser.

Don't Confuse These

Name	What it actually is
Workspace role	Access to items in one workspace. Says nothing about the capacity or tenant
OneLake security	Fine-grained folder/table rules. Works *downward* from Viewer only
Capacity admin	Controls the compute. May or may not be able to take your workspace
Domain	A grouping *above* workspaces. Next-but-two in this series

Name	What it actually is
My workspace	Personal, on shared capacity, and its owner can move it out of region

---

The Traps

#	Trap	Fix
1	Viewer cannot read via Spark	Grant with OneLake security, not a role bump
2	OneLake restriction ignored for Contributor	**Viewer + explicit grants** – there is no "Contributor, but only this folder"
3	RLS silently stops applying	Enforced for Pro users only in the **Viewer** role
4	Git connect grayed out	**Admin only**, not Member
5	Access audit misleading	Highest permission wins across **nested** groups
6	Offboarding lag	Revocation applies at **next sign-in**
7	Cannot create item	1,000 cap counts **children** – a lakehouse brings its SQL endpoint (default semantic models stopped being auto-created 2025-09-05)
8	Workspace moved without you	**P/EM** capacity admins can claim it by name
9	Items gone after a region move	Non-movable types must be **deleted** first

---

Decision Rules

Splitting workspaces. Split on a *boundary you actually need* – a different security audience, a different capacity to bill, a different region, a different release cadence. Splitting for tidiness buys you nothing and costs you cross-workspace access management.

Restricting access. Start at Viewer and grant upward with OneLake security. Never start at Contributor and try to restrict downward: the documentation says plainly it will not hold.

Planning a region change. Treat it as a migration project: inventory the non-movable items, capture their definitions, expect running jobs to be canceled, and budget an hour before you can recreate what you removed.

Three Links

- Roles in workspaces
- OneLake security access control model
- Capacity reassignment restrictions

SQL analytics endpoint identity mode

A newly created lakehouse endpoint starts in **delegated identity mode**, where OneLake security is not enforced on the way out. An Admin or Member has to switch it to **user's identity mode** before the endpoint applies object-level and row-level security. Until that switch, the endpoint is not a security boundary – it is a bypass.

Source: https://learn.microsoft.com/fabric/onelake/security/get-started-onelake-security

06 Cheat Sheet – Domain

The One "Why"

A domain answers "whose data is this?", not "who may see it?"

> "Domain assignment doesn't affect item visibility or accessibility for tenant users."

Everything a domain does is discovery, metadata and settings delegation. All three are real. None is a boundary.

Gives you / does not

Gives you	Does not give you
A domain attribute on every item's metadata	Visibility control
A OneLake catalog filter	Access control
Delegated tenant settings	Privacy of the domain *name*
A place to name a business owner	A second domain per workspace

All users see all domain names, regardless of role. If a business unit's existence is confidential, do not encode it here.

Roles

	Fabric admin	Domain admin	Domain contributor
Create domain	yes		
Rename domain	yes	**no**	
Edit description	yes	yes	
Delete domain	yes	**no**	
Add/remove domain admins	yes	**no**	
Define contributors	yes	yes	
Assign workspaces (admin portal)	yes	yes	
Assign own workspaces	yes	yes	yes
Delegated settings	yes	yes	
Domains tab	yes	own only	**no**

> **A domain contributor must already be a workspace Admin.** The role is permission to use power you have, not a grant of new power.

Subdomains

- **General settings only** – name and description

- **No admins of their own** – they inherit the parent's
- No contributors, no delegated settings, no default-domain behavior

Hierarchy two deep. Administration one deep.

Default Domain

Situation	Result
Workspace already in a domain	**Preserved** – default never overrides
Workspace unassigned	Assigned to the default
New workspace by a listed user	Assigned automatically, indefinitely
Side effect	Those users **become domain contributors**

Contrast: assigning **by name** in the admin portal *can* override an existing assignment (with a warning). Assigning **by workspace admin** excludes *My workspaces*.

Sensitivity Label Override

Applied on create, and when an **unlabeled** item is updated and saved.

Existing label	Overridden?
Manual, any priority	**No**
Automatic, lower priority	Yes
Automatic, higher priority	No
Policy default, lower priority	Yes
Policy default, higher priority	No

A human decision always wins. Everything else is a priority comparison.

> **Deployment pipelines and Git integration are not supported.** The one governing behavior a domain has does not follow content through its lifecycle.

The Traps

#	Trap	Fix
1	Domains built as a security boundary	Use workspace roles and item permissions
2	Confidential business unit named as a domain	Every user sees every domain name
3	Workspace needed in two domains	Not expressible – choose one or split
4	Domain contributor can do nothing	They must also be **workspace Admin**

#	Trap	Fix
5	Domain admin cannot rename their domain	Fabric admin only
6	Subdomain has no separate governance	It has a name and a description
7	Workspaces appearing in a domain unbidden	A **default domain** is configured
8	Labels not flowing through CI/CD	Documented limitation, not a fault

---

Three Links

- Fabric domains
- Best practices for planning and creating domains
- Domain-level default sensitivity labels

06 Cheat Sheet – Capacity

The One "Why"

Fabric does not charge you when work happens. It spreads the cost forward.

Interactive work pays over 5 to 64 minutes; background work pays over 24 hours. Every confusing thing about capacity follows: the moment you are throttled is not the moment you caused it, and last night's refresh is still paying into this afternoon.

The Numbers

Fact	Value
Timepoint length	**30 seconds**
Timepoints per day	**2,880**
Interactive smoothing	**5 – 64 minutes**
Background smoothing	**24 hours**
Throttle stage 1	10 min future capacity → **20 s delays**
Throttle stage 2	60 min future capacity → **interactive rejected**, background runs

Fact	Value
Throttle stage 3	24 h future capacity → **all new requests rejected**
Azure quota buffer (subscription CUs, not capacity headroom)	**25 – 50 %**

Worked example, from the docs: an F2 has 60 CU s per timepoint. A background job of 1 CU hour spreads to 1.25 CU s per timepoint = **~2.1%**. The job consumed **six times** the CU available in the next ten minutes and throttled nothing.

Classification

	Interactive	Background
Window	5 – 64 min	24 h
Decided	**before the operation runs**	same
Ambiguous case	–	**falls back here**, "in your best interest"
Warehouse	rarely	**nearly everything**
Copilot	–	**yes**
API for GraphQL	**yes**	–

> Same fact, two consequences: background classification **protects** you from throttling and **exposes** you to surge-protection rejection.

Who Skips Which Step

Workload	Stage 1 (20 s delay)	Stage 2 (interactive rejected)	Stage 3 (all rejected)
Interactive operations	applies	applies	applies
Background operations	–	keep running	applies
Real-Time Intelligence	**skipped**	applies	applies
Eventstreams	never throttled – **CU starved** instead	–	–

A degraded eventstream does not throw an error. It gets slower at keeping up, which is much harder to notice than a failure.

Surge Protection – the honest version

- Limits background compute when 24-hour usage is high
- **Rejects** background jobs – they need delaying or rerunning
- **Many SQL queries count as background** and can be rejected
- **Not a substitute** for correct sizing or content optimization
- Critical workloads still need **dedicated capacity**

It protects the report someone is looking at by sacrificing the query someone is waiting on.

Scaling Down

The rule as arithmetic: halving the SKU doubles the percentage.

At	Smoothed usage	After scale-down
F128	**< 40 %**	≈ 80 % on F64 – safe
F128	50 %	100 % on F64 – no headroom; throttling after 10 min of future capacity

Read the **smoothed** line in the Metrics app, not the spikes you remember. The spiky line is a record of work already paid forward.

Autoscale Billing for Spark

Turning it on **disables bursting and smoothing** – Spark becomes pay-as-you-go.

	Behavior
Interactive Spark	**throttled** when CUs are used up
Background Spark	**queued** – queue size = CU limit (2048 CU → 2048 jobs)

The trade: you give up a predictable bill to get a predictable absence of self-inflicted throttling.

Don't Confuse These

Name	What it actually is
Bursting	Using more CU than the SKU allots, briefly
Smoothing	Spreading the *cost* of that forward in time
Throttling	The consequence when a timepoint is over-full
Surge protection	A setting that rejects background work to protect interactive work
Autoscale billing	Turns bursting and smoothing off entirely for Spark

---

Three Links

- Understand the Fabric capacity throttling policy
- Capacity planning: manage growth and governance
- Smoothing and throttling in Fabric Data Warehouse