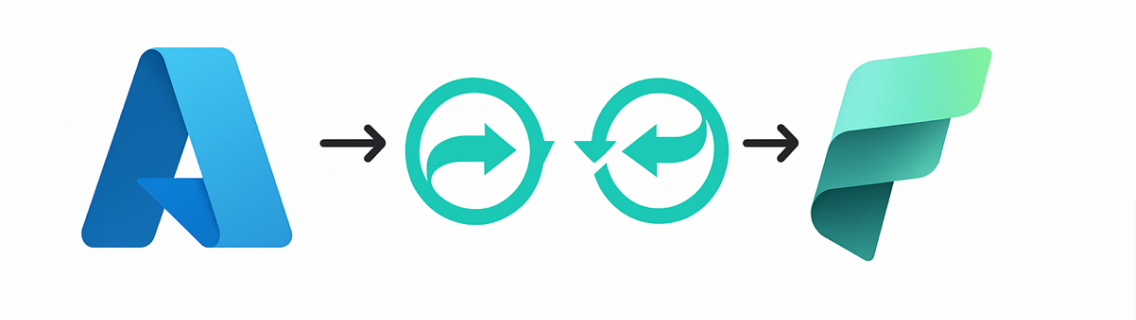
Securing the infrastructure beneath Fabric?

Microsoft Fabric has quickly become the analytical backbone for many organizations, unifying Power BI, Synapse, and Data Factory into one SaaS platform. But every Fabric deployment still depends on one critical Azure component: **the Fabric Capacity**.

That capacity is the compute engine behind the entire Fabric experience. It's the virtual computer running inside Azure that delivers every dataset refresh, every warehouse query, every pipeline job. Without it, Fabric doesn't run.

As each capacity lives in the customer's Azure tenant, **the responsibility for governance, risk, and compliance (GRC) at that layer still belongs to the customer**. That's exactly where **MyPlatform** operates.



The Invisible Layer of Fabric

Under the Fabric interface sits a full Azure infrastructure:

- **Fabric Capacities (F-SKUs)** providing the CPU and memory pools for workloads.
- **Key Vaults** storing connection secrets and managed identities.
- **Networking, storage, and logging resources** that Fabric uses but doesn't expose directly in the SaaS portal.

For most customers, these components appear "invisible". Microsoft manages the SaaS, but the Azure resources still exist inside their tenant.

That means they require the same discipline as any other production workload: **RBAC, PIM, tagging, monitoring, backup, and compliance enforcement**.

Many organizations overlook this crucial aspect. Although Fabric operates as a service, it relies on underlying infrastructure that requires careful oversight; without proper governance, expanding or monitoring this infrastructure can expose significant risks.

Where GRC Risks Emerge

Even though Fabric hides much of the complexity, the underlying Azure resources remain fully active. When capacities are created manually or through multiple environments, common governance gaps appear:

- **Over-privileged identities** – Fabric capacity admins are often assigned broad Contributor or Owner rights in subscriptions, far beyond what's required.
- **Lack of tagging and cost governance** – Capacities consume significant compute, but without policy enforcement they often bypass FinOps tagging or cost controls.
- **Compliance** – Key Vaults, storage accounts, and diagnostic settings used by Fabric may fall outside of organizational policy frameworks such as NIS2, CIS, or ISO 27001.
- **Shadow scaling** – Fabric automatically adjusts compute usage. Without policy limits and monitoring, this can drive unplanned cost or breach compliance thresholds.
- **Inconsistent audit trails** – While Fabric itself logs activity at the SaaS layer, the Azure resources beneath it may lack consistent diagnostics or retention policies.

In short: **Fabric doesn't remove governance work - it hides it - and what's hidden, often isn't secured.**

MyPlatform's Role: GRC for Fabric Infrastructure

MyPlatform was designed for exactly this layer, as the Azure foundation that powers Microsoft's cloud services.

Through an automated, code-based model deployed from **Azure Marketplace**, **MyPlatform** builds a **governed and compliant infrastructure baseline** that includes Fabric Capacities and related Azure resources.

MyPlatform & Fabric

MyPlatform

Automated Governance Foundation
MyPlatform applies an opinionated management-group and policy structure across the tenant. Fabric Capacities are discovered and automatically aligned with the same controls as other production workloads.

This includes enforced tagging, diagnostic settings, backup retention, and network configuration. Capacities inherit the organization's compliance framework from day one, as no or limited manual setup required.

Least-Privilege and PIM Controls
MyPlatform implements **least-privilege RBAC** and integrates **Azure Privileged Identity Management (PIM).**

Capacity admins gain just-in-time elevation with approval and expiry. No permanent Owner or Contributor roles exist on subscriptions hosting Fabric resources. This protects against accidental or malicious privilege escalation while still allowing Microsoft's managed operations to function transparently.

Policy-as-Code Compliance
MyPlatform encodes compliance baselines such as **ISO 27001**, **NIS2**, and **CIS Benchmarks** directly into Azure Policy. For Fabric Capacities, that means continuous validation that:

- Diagnostic logs are enabled and retained.
- Key Vaults are secured with soft delete and purge protection.
- Encryption, tagging, and network policies stay aligned with corporate standards.

Have an always-compliant infrastructure beneath Fabric and **evergreen governance.**

FinOps and Cost Governance
Fabric compute consumption can be substantial. MyPlatform integrates FinOps tagging, budget alerts, and capacity monitoring to ensure financial control without manual tracking.

By enforcing policies for cost allocation and rightsizing, MyPlatform converts uncontrolled consumption into **predictable, transparent OPEX**.

Continuous Compliance Dashboard
All Fabric-related Azure resources appear within MyPlatform's compliance dashboard.

Security teams can see exactly which capacities comply with policy and where remediation is pending unified with other Azure workloads for a single governance view.

Why This Matters

Fabric democratizes analytics, but governance must democratize too.

In large enterprises, Fabric is often deployed by data teams, not cloud architects. Without automated governance, that decentralization creates fragmented security and unpredictable cost exposure.

MyPlatform closes that gap. It ensures that every Fabric deployment inherits the same **secure, compliant, and auditable foundation** as any mission-critical Azure workload.

That protects not only the compute layer, but the trust behind every insight Fabric delivers.

From Invisible Risk to Governed Foundation

Microsoft Fabric is the future of data unification. But like every Azure service, its reliability depends on the integrity of the infrastructure beneath it.

MyPlatform turns that hidden layer into a governed one — secure, compliant, and continuously aligned with Microsoft's best practices.

By automating GRC for Fabric Capacities, MyPlatform gives organizations the confidence to scale analytics safely, knowing their compute foundation is protected by design.

From invisible risk to visible governance — that's the Fabric layer MyPlatform secures.