Microsoft Fabric

avanade

Do what matters

Security assessment & enablement

Do what matters

Securing Fabric is not just important, it's fundamental.

At Avanade, we view the introduction of Fabric as a **pivotal shift in the digital landscape**, with its private preview adoption by over 20,000 organizations marking it as a cornerstone for business operations.

It's a beacon of innovation, **but with its brilliance comes the magnetism for potential threats**.

Do what matters

avanade

Fabric security challenges

Organizations are tasked with seamlessly integrating Fabric's analytics solutions into existing infrastructures, enhancing multi-layered security protocols, elevating data governance and readiness, and tapping into expert knowledge for robust security across the Microsoft ecosystem.

Navigating technology interdependencies
It can be difficult to have a comprehensive understanding of Fabric's all-in-one analytics solution, how it interacts with your existing services, and how to best configure the systems effectively to enable enhanced data security and compliance.

Achieving data-readiness
Data quality, governance and access policies may be substandard and can be difficult to identify and even harder to improve ahead of integration into OneLake and Fabric.

Mastering SaaS security principles
Taking on the task of assessing and applying a multi-layered security model across the platforms can be challenging but is critical for improving governance access and safeguarding sensitive data against unauthorized access or cyber threats.

Leveraging expertise for enhanced security
The implementation of security best practices across the Microsoft landscape requires the expertise of professionals in cloud security, data engineering, and analytics who possess a profound knowledge and understanding of Microsoft Fabric and its supporting services. But these experts can be difficult to come by.

avanade

Do what matters

Securing Fabric is akin to safeguarding the lifeblood of an organization

Imagine Fabric as the repository of your most valuable secrets, a vault that, if breached, could unravel the very threads of your organization. It holds the power to drive your business forward, yet it bears the vulnerability of exposure.

Azure AD

Microsoft Fabric

Purview

Defender for Cloud

Sentinel

Microsoft Synapse

Data Factory · Data Engineering · Data Warehouse · Data Science · Real-Time Analytics · Power BI

OneLake

Shortcut

Azure ML · Azure Databricks

ADLS Gen2
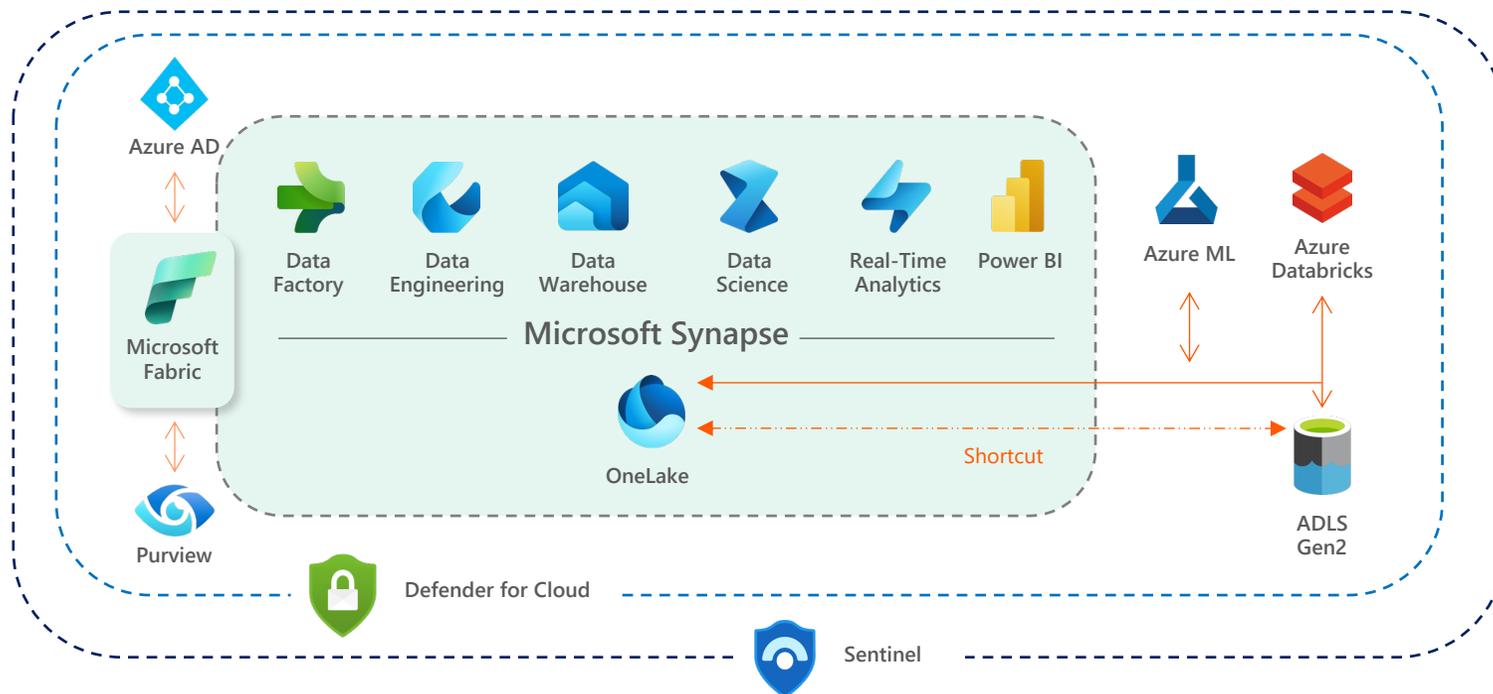
It's crucial to use the available Microsoft features protect your data in Fabric, but how can you be sure that you have all of your most sensitive information covered?

Establish a security mindset with Avanade.

avanade

Put security at the forefront of your Fabric journey

Learn | Explore | Build

Work together with Avanade SMEs to understand and realize the business value of securing Microsoft Fabric.

Avanade will join your team on-site (or remotely) cover in-depth the security requirements for Fabric deployment within your enterprise.

Avanade teams involved:

Security Architect, Data & AI Fabric Architect

Important focus areas:

- Azure security maturity
- Source data readiness
- Data access models & permissions
- Implementation/operational plans & procedures

1

1-hour learning session & discussion
Take part in a Fabric introduction and opening discussion to identify any questions you may have spanning risks, compliance and current posture/readiness for broad scale deployment.

2

Fabric security assessment (3 to 6 weeks)
We'll help you evaluate your existing security controls that support Microsoft Fabric and deliver recommendations and plans to remediate gaps and uplift deficiencies to support a secure Fabric implementation.

⌄ Depending on workshop outcomes ⌄

3

Follow-on activities

Fabric Security Controls Uplift
Analyze the outputs from the Fabric Security Assessment recommendations and deploy relevant changes.

Operations Support & Fabric Security Monitoring
We'll support you in enabling a secure transformation and adoption of Microsoft Fabric to realize the power of the platform and address your regulatory and compliance requirements.

Do what matters

avanade

Establish a security mindset

Over a 3-to-6-week period, we'll help you evaluate your existing security controls that support Microsoft Fabric and deliver recommendations and plans to remediate gaps and uplift deficiencies to support a Secure Fabric implementation.

Plan
Outline and assemble assessment prerequisites, such as tenant and subscription access and documentation

Assess
Gather inventory and assess tenant security, fabric services and data sources
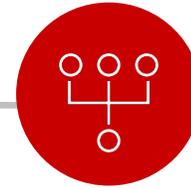
Define
Receive a high-level gaps and deficiencies report and undergo a briefing with Avanade
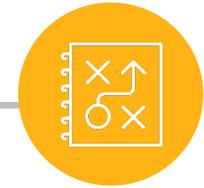
Report & strategize
Receive a complete report and define next steps

Final deliverables/work products

1. Assessment report on discovered risks and detail on resolutions

2. Next steps proposal highlighting an approach to address gaps and deficiencies and identify quick wins through strategic pieces of work

avanade

Do what matters

We **think global**, **act local** and **scale** to meet our clients' needs

1000+ Security Clients **globally**

1700+ Security Professionals **globally**

NetHope Founding Member Digital box

Member of Microsoft Intelligent Security Association
Microsoft Security

Microsoft Intelligent Security Association (MISA) member

Member of Microsoft Intelligent Security Association
Microsoft Security | Microsoft Verified Managed XDR Solution

Microsoft-verified MXDR solution by Microsoft Intelligent Security Association

CSA
Cloud Security Alliance Member

Member of the Microsoft Security Copilot Design Advisory Council

IDC
Leader IDC Marketscape for Worldwide Microsoft Implementation Services[6]

avanade

No 1. for security certifications
Accenture / Avanade have the highest number of Microsoft security certified people[5]

82 locations Globally
across 5 continents in 26 countries supported by on and offshore capabilities

300+ Industry Security Certifications

Advanced Microsoft security specializations

Cloud security

Identity and access management

Threat protection

Information protection and governance

Do what matters