Data#3 | Microsoft Security

Microsoft Hybrid Cloud Security Workshop

Get a customised threat & vulnerability analysis of your hybrid and multi-cloud environment and learn how to build a more robust cloud security system.

Workshop highlights

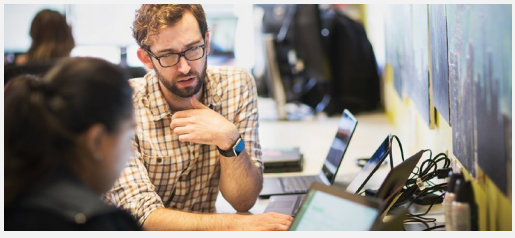
- Discover threats and vulnerabilities in your hybrid environment.
- Learn how to prioritise and mitigate potential threats to your servers and services.
- Understand what can be done to reduce the attack surface area for hybrid workloads.
- Learn about benefits and capabilities of Azure Defender and Azure Network Security.
- Develop defined next steps based on your needs and objectives.

Do you have a good understanding of security vulnerabilities in your hybrid and multi-cloud environment including VMs, databases, Azure storage and more? Are you aware of the number of suspected authentication activities across your multi-cloud environment? In short, are you confident about the cloud security posture of your organisation?

Improve your cloud security posture with a Microsoft Hybrid Cloud Security Workshop

As the use of cloud services continues to grow, cyber risks and threats continue to evolve. Get help achieving your hybrid and multi-cloud security objectives – and identify current and real threats – by scheduling a Microsoft Hybrid Security Workshop.

We can help you develop a strategic plan customised for your organisation and based on the recommendations of Microsoft cybersecurity experts. You'll gain visibility into immediate threats and vulnerabilities across Azure, on-premises and multi-cloud environments, plus clarity and support on how to improve your security posture for the long term.



Why you should attend

Given the volume and complexity of identities, data, apps, endpoints, and infrastructure, it's essential to learn how secure your organisation is right now, and how to mitigate and protect against threats moving forward. By attending this workshop, you can:

Identify current, security threats and vulnerabilities in your hybrid and multi-cloud environment.	Walk away with actionable next steps based on your specific needs and objectives.	Document your security priorities and needs for the benefit of key stakeholders.	Better understand how to accelerate your security journey using the latest tools.

What to expect:

During this-workshop, we'll partner with you to strengthen your organisation's approach to hybrid cloud security. We'll help you better understand how to prioritise and mitigate potential attacks:

- **Analyse** your requirements and priorities for a hybrid cloud security detection and response solution.
- **Define Scope** & deploy Azure Defender in the production environment, onboarding servers and other selected services.
- **Explore** Azure Network Security capabilities and experience selected Azure Network Security products in a demonstration environment.
- **Discover** existing hybrid workload vulnerabilities and learn how to reduce the attack surface area.
- **Discover** threats to the included hybrid workloads and demonstrate how to investigate and respond to threats.
- **Recommend** next steps on proceeding with a production deployment of Azure Defender and Azure Network Security.

Who should attend

The workshop is intended for security decision-makers such as:

- Chief Information Security Officer (CISO)
- Chief Information Officer (CIO)
- Chief Security Officer (CSO)
- Data Protection Officer
- Data Governance Officer
- IT Security, IT Compliance, and/or IT Operations
- Data Governance

Why Data#3?

When it comes to hybrid cloud security you need an experienced partner. We are Microsoft's largest Australian business partner with the highest certified level of competency across the Microsoft ecosystem. Our hundreds of accredited consultants are ready to help. From enhancing productivity and collaboration with Microsoft 365, Meeting Rooms, and the latest Surface devices, to transforming business processes with Dynamics 365, and getting the most value from Azure cloud, Data#3 has you covered.