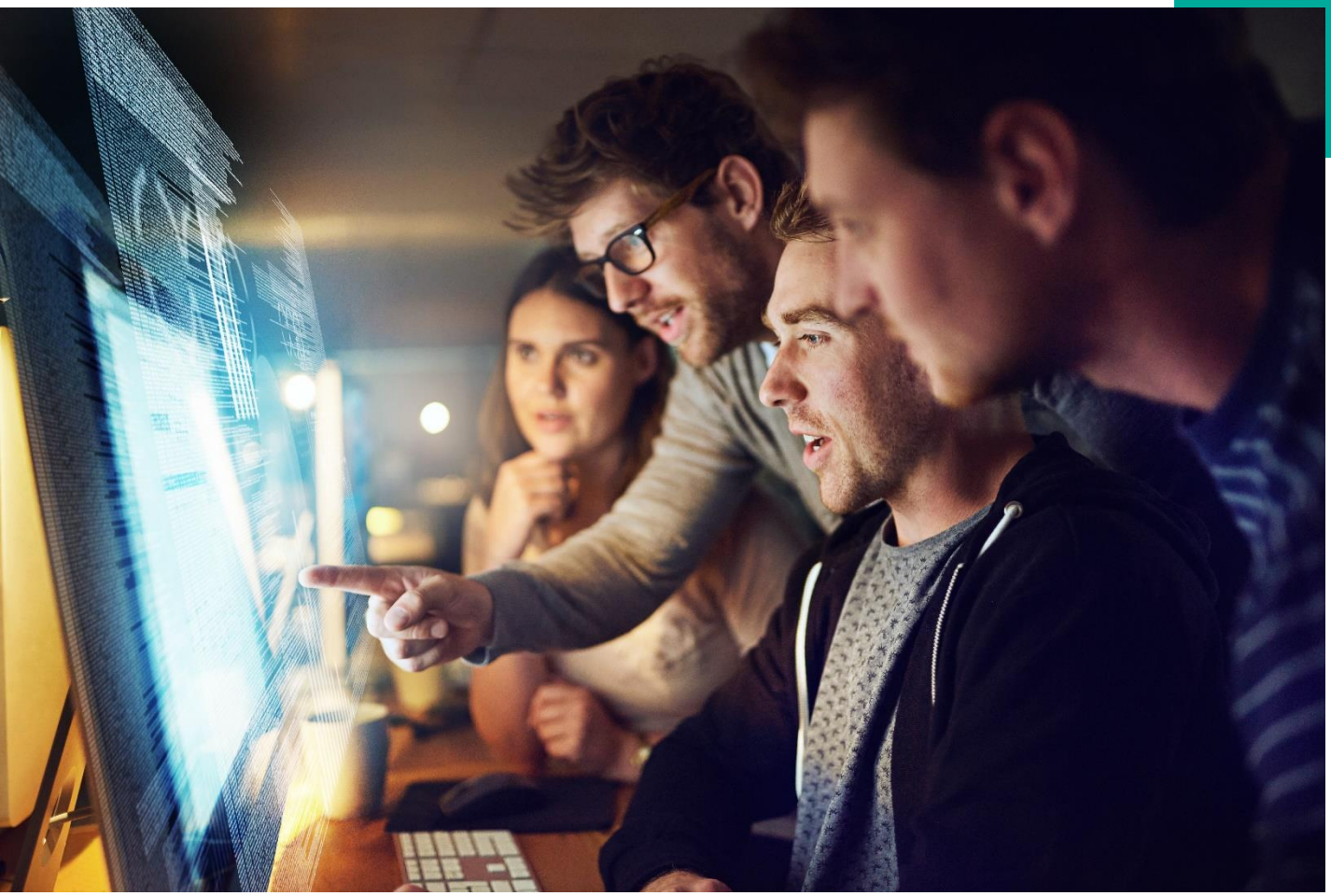
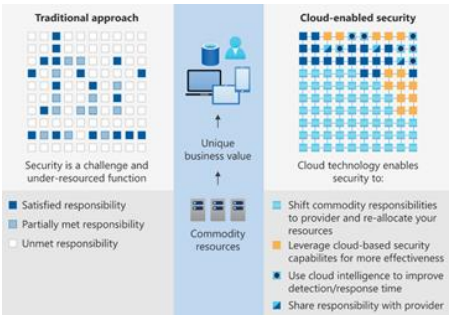


Azure Secure Networking Workshop

Protect your cloud workloads from network-based cyberattacks with Azure Secure Networking services

As organizations move workloads to the public cloud, they must pay special attention to protecting their assets from unauthorized access.
It is critical to understand the shared responsibility model and what security tasks are handled by the cloud provider and what tasks need to be handled by you or your partner.

The cloud offers significant advantages for solving long-standing information security challenges. In an on-premises environment, organizations are likely to have unmet responsibilities and limited resources available to invest in security, creating an environment where attackers can exploit vulnerabilities at all layers.
In the cloud-based approach, security is a shared responsibility: you can shift day-to-day security responsibilities to your cloud provider and reallocate your resources. You can leverage cloud-based security capabilities for greater effectiveness and use cloud intelligence to improve your threat detection and response time.



During our 3-days Azure Secure Networking Workshop, our experienced consultants will inform and inspire you about the advanced networking security capabilities in Azure and zoom in on those features that bring value for your environment.

inetum realdolmen
Positive digital flow

Azure Secure Networking Discovery Workshop
What will we cover?

Amongst others, we will cover the following:

- Overview of the Azure Secure Networking services such as Azure Firewall, Azure DDoS Protection, Azure Web Application Firewall, Azure Bastion, Azure Front Door, Azure Network Watcher and Azure Firewall Manager.
- Understand the risk and potential exposure of a conceptual network design and how to use Azure services and tools for network security improvement
- Network architecture best practices

The Secure Networking Workshop consists of following steps:

Kick-off workshop
We start this engagement by better understanding your security requirements. We select a critical workload that will be assessed and agree on the exact scope and expectations of the engagement.

Secure Networking services overview
We continue our engagement by discussing and explaining the capabilities and value of Azure Secure Networking services. Together we evaluate the value they can bring for your specific situation and requirements.

Network Architecture Review
We assess the network architecture of the cloud workload that was selected during the kick-off workshop. We will uncover the security risks on the network level and discuss how and which Azure Secure Networking services are valuable for this particular workload.

Closing workshop
We will summarize our finding of the review and our suggestions for bringing the network security to the next level. We will have a look at the pricing model of the selected services.

And afterwards?
You are ready now to better secure your cloud workloads from network-based cyberattacks. Of course our consultants can help you further with implementing the Network Security optimizations.

Microsoft Partner
Microsoft
Gold Cloud Platform
Gold Security

Microsoft Partner
Microsoft
Advanced specializations:
Windows Server and SQL Server Migration to Azure
Microsoft Windows Virtual Desktop
Modernization of Web Applications to Microsoft Azure
Kubernetes on Microsoft Azure
Calling for Microsoft Teams
Application and Change Management
Meetings and Meeting Rooms for Microsoft Teams

WANT MORE INFORMATION?

Contact our experts with any questions, suggestions, or challenges.
We are looking forward to informing you about other Azure services Inetum-Realdolmen can offer.

INFO@INETUM-REALDOLMEN.WORLD