TIP SHEET

3 Ways to Ensure Cloud Platform Security

Microsoft Azure provides many native security features and services focusing on operations, applications, storage, networking, compute, and identity. Even though you have access to these built-in capabilities, there are steps you can take to ensure that your enterprise-grade cloud workload is protected from breaches, data leaks, and targeted attacks. Essentially, security concerns and obligations that occur in an on-premises environment are still a factor in the cloud as well. On the other hand, with the limitless power of cloud scalability, environment perimeters are less defined.

Ensuring your data is protected in the cloud means that you must secure it in every possible state it can occur, and consider what controls are available for that specific state. **Here are 3 easy methods to ensuring that your data is secure across your cloud platform:**

1 Policy-Based Granular Management

This is critical to secure your cloud environment. You can set up groups and roles instead of having to maintain permissions on an individual basis, granting only the necessary access to each unit rather than blanket permissions.

2 Azure Virtual Network (VNet)

This enables you to deploy business-critical resources and apps in logically isolated sections of Azure. VNet allows your various Azure resources to safely connect with each other, the internet, and any on-premises networks with the added advantages of Azure's infrastructure including scale and availability.

3 Data Encryption

You can protect your data by encrypting it at all its various levels of usage. You can use several different methods of encryption with Azure, including server-side encryption that relies on service-managed keys, customer-managed keys in Key Vault, or customer-managed keys on customer-controlled hardware. If you choose to go with the client-side encryption method, you can keep your keys on-premises or in a different secure location.