Data Security

Security of data in the cloud is one of the biggest concerns for IT departments looking to take advantage of cloud computing.

Physical Layer- Facility and Network Security

Microsoft starts by providing security for the physical access of the data. Microsoft stores its customer data in data centers distributed geographically, restricts access to the data centers job function, and uses physical security measures.

At the network level, Microsoft only allows connections that are necessary for the systems to operate, blocking other ports, protocols and connections. Tiered Access Control Lists and firewall rules put security restrictions on communication, protocols, and port numbers. There are also security features that detect intrusions and vulnerabilities at the network layer.

Logical Layer- Host, Application and Admin Users

Microsoft has automated most of the operations performed on the hosts and apps by administrators in order to reduce human intervention. Access to Office 365 data is strictly controlled where least privilege is granted to perform specific operations by role. Microsoft's Lock Box process greatly limits human access to data.

Microsoft employs anti-malware software to protect data from malicious applications by both detecting and preventing such software from entering the systems. If malware enters a system, Microsoft quarantines infected systems to prevent additional damage. Additionally, they perform regular updates, hotfixes, and patches.

Data Layer- Data

Office 365 is a multi-tenant service. This means multiple customers use some of the same hardware resources, which is one of the primary benefits of cloud computing that allows for lower operating costs. Microsoft isolates co-tenant data through Active Directory and has other features specifically designed to secure multi-tenant environments.

In order to protect data from security threats, Microsoft adheres to an "Assume Breach" approach. Microsoft assumes a breach has already occurred and is not known yet, while their security team attempts to detect and mitigate the threat. The assume breach mentality rests on four pillars of security:

1- **Prevent Breach**
2- **Detect Breach**
3- **Respond to Breach**
4- **Recover from Breach**

Office 365 Email Threat Protection

Due to the evolving nature of the threat landscape, Microsoft offers its threat protection for Exchange Online, which goes beyond protection against spam, viruses and malware and includes:

- **Protection against unknown malware**

  By using a feature called Safe Attachments, Exchange Online users can be protected against malware not known to Microsoft as well as other zero-day threats. Microsoft routes all messages and attachments without a known malware signature to a sandbox environment that employs machine learning to detect malicious patterns/intent, and if none are detected, the message is delivered to its destination.

- **Real time protection against malicious URLS**

  This feature goes beyond the traditional security feature of Exchange Online where each message in transit is scanned to detect and block malicious URLs in an email. With threat protection, malicious URLs, even when disguised as normal URLs, can be identified/blocked, and users who click them will remain protected.

- **Robust reporting URL tracking**

  Office 365's advanced threat protection also lets organizations see who is being targeted by unknown malware and malicious links, which messages are being blocked due to the unknown malware, and trace those malicious URLs in message that have been clicked.

For these reasons and more, Microsoft has invested significant resources in building its security stack. At the same time, Microsoft has partnered with third-party security vendors to provide additional layers of security for organizations with more complex requirements.