Contoso in the Microsoft Cloud

How a fictional but representative global organization has implemented the Microsoft Cloud

Security

Contoso is serious about their information security and protection. When transitioning their IT infrastructure to a cloud-inclusive one, they made sure that their on-premises security requirements were supported and implemented in Microsoft's cloud offerings.

Contoso's security requirements in the cloud

Strong authentication to cloud resources	Cloud resource access must be authenticated and, where possible, leverage multi-factor authentication.
Encryption for traffic across the Internet	No data sent across the Internet is in plain text form. Always use HTTPS connections, IPsec, or other end-to-end data encryption methods.
Encryption for data at rest in the cloud	All data stored on disks or elsewhere in the cloud must be in an encrypted form.
ACLs for least privilege access	Account permissions to access resources in the cloud and what they are allowed to do must follow least-privilege guidelines.

Contoso's data sensitivity classification

Using the information in Microsoft's Data Classification Toolkit, Contoso performed an analysis of their data and determined the following levels.

Level 1: Low business value	Level 2: Medium business value	Level 3: High business value
Data is encrypted and available only to authenticated users Provided for all data stored on premises and in cloud-based storage and workloads, such as Office 365. Data is encrypted while it resides in the service and in transit between the service and client devices. Examples of Level 1 data are normal business communications (email) and files for administrative, sales, and support workers.	Level 1 plus strong authentication and data loss protection Strong authentication includes multi-factor authentication with SMS validation. Data loss prevention ensures that sensitive or critical information does not travel outside the on-premises network. Examples of Level 2 data are financial and legal information and research and development data for new products.	Level 2 plus the highest levels of encryption, authentication, and auditing The highest levels of encryption for data at rest and in the cloud, compliant with regional regulations, combined with multi-factor authentication with smart cards and granular auditing and alerting. Examples of Level 3 data are customer and partner personally identifiable information and product engineering specifications and proprietary manufacturing techniques.

Data classification toolkit

Mapping Microsoft cloud offerings and features to Contoso's data levels

	SaaS	Azure PaaS	Azure IaaS
Level 1: Low business value	• HTTPS for all connections • Encryption at rest	• Support only HTTPS connections • Encrypt files stored in Azure	• Require HTTPS or IPsec for server access • Azure disk encryption
Level 2: Medium business value	• Azure AD multi-factor authentication (MFA) with SMS	• Use Azure Key Vault for encryption keys • Azure AD MFA with SMS	• MFA with SMS
Level 3: High business value	• Azure Rights Management System (RMS) • Azure AD MFA with smart cards • Intune conditional access	• Azure RMS • Azure AD MFA with smart cards	• MFA with smart cards

Continued on next page

Contoso's information policies

	Access	Data retention	Information protection
Level 1: Low business value	• Allow access to all	6 months	Use encryption
Level 2: Medium business value	• Allow access to Contoso employees, subcontractors, and partners • Use MFA, TLS, and MAM	2 years	Use hash values for data integrity
Level 3: High business value	• Allow access to executives and leads in engineering and manufacturing • RMS with managed network devices only	7 years	Use digital signatures for non-repudiation

Contoso's path to cloud security readiness

1. **Optimize administrator accounts for the cloud**

   Contoso did an extensive review of the existing Windows Server AD administrator accounts and set up a series of cloud administrator accounts and groups.

2. **Perform data classification analysis into three levels**

   Contoso performed a careful review and determined the three levels, which was used to determine the Microsoft cloud offering features to protect Contoso's most valuable data.

3. **Determine access, retention, and information protection policies for data levels**

   Based on the data levels, Contoso determined detailed requirements, which will be used to qualify future IT workloads being moved to the cloud.

Cloud security resources

Microsoft Cloud Security for Enterprise Architects
http://aka.ms/cloudarchsecurity

Information Protection for Office 365
http://aka.ms/o365infoprotect

Security in a Cloud-Enabled World Microsoft Virtual Academy Course
http://aka.ms/securecustomermva

Microsoft