Contoso in the Microsoft Cloud

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

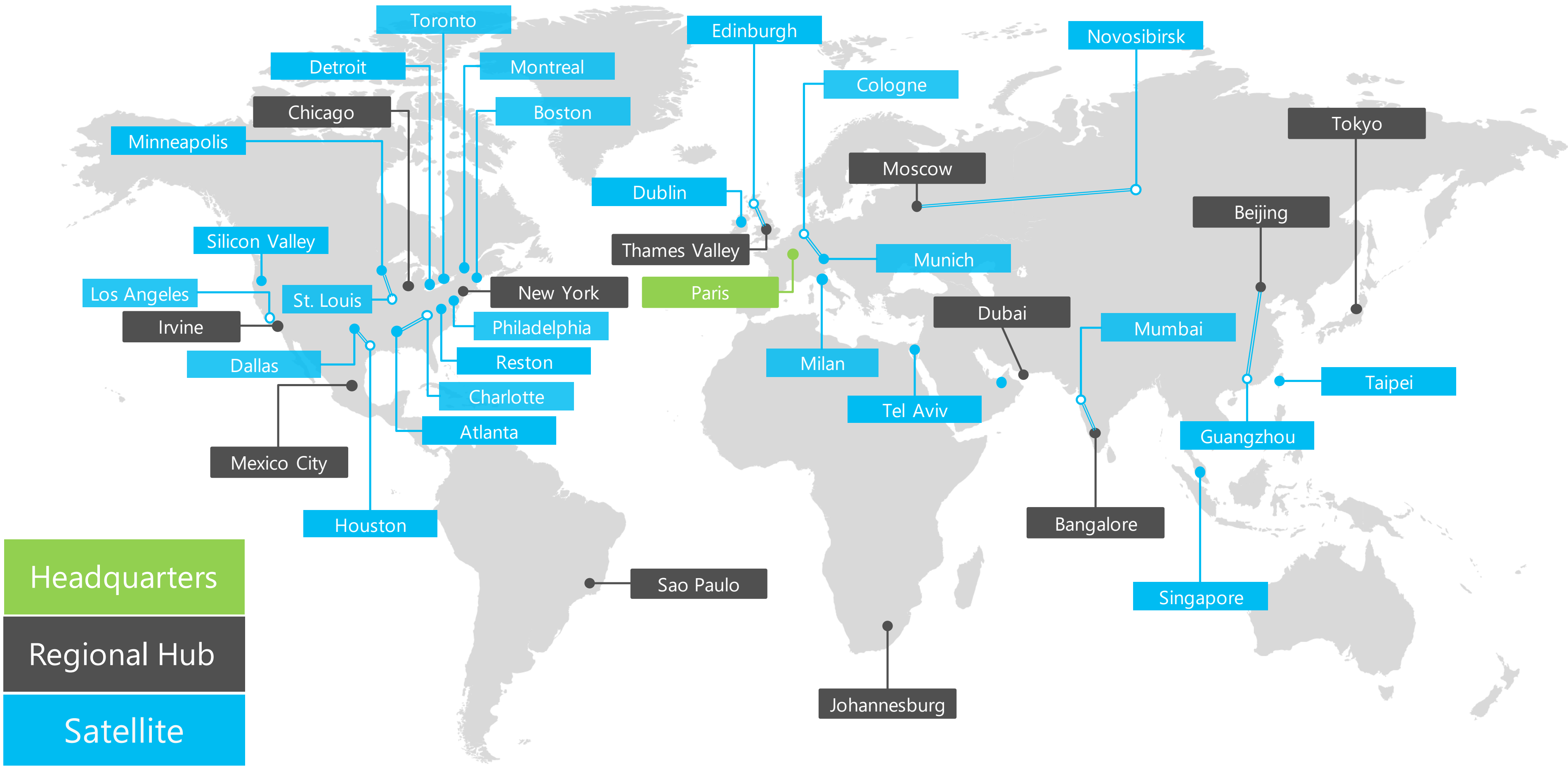
This topic is 1 of 7 in a series 1 2 3 4 5 6 7

The Contoso Corporation

The Contoso Corporation is a global business with headquarters in Paris, France. It is a conglomerate manufacturing, sales, and support organization with over 100,000 products.

Article version of this poster

Contoso's worldwide organization



Contoso's offices around the world follow a three tier design.

Headquarters

The Contoso Corporation headquarters is a large corporate campus on the outskirts of Paris with dozens of buildings for administrative, engineering, and manufacturing facilities. All of Contoso's datacenters and it's Internet presence are housed in the Paris headquarters.

The headquarters has 15,000 workers.

Regional hubs

Regional hub offices serve a specific region of the world with 60% sales and support staff. Each regional hub is connected to the Paris headquarters with a high-bandwidth WAN link.

Each regional hub has an average of 2,000 workers.

Satellite offices

Satellite offices contain 80% sales and support staff and provide a physical and on-site presence for Contoso customers in key cities or sub-regions. Each satellite office is connected to a regional hub with a high-bandwidth WAN link.

Each satellite office has an average of 250 workers.

25% of Contoso's workforce is mobile-only, with a higher percentage of mobile-only workers in the regional hubs and satellite offices.

Providing better support for mobile-only workers is an important business goal for Contoso.

Elements of Contoso's implementation of the Microsoft cloud

Contoso's IT architects have identified the following elements when planning for the adoption of Microsoft's cloud offerings.

Networking

Networking includes the connectivity to Microsoft's cloud offerings and enough bandwidth to be performant under peak loads. Some connectivity will be over local Internet connections and some will be across Contoso's private network infrastructure.

Microsoft Cloud Networking for Enterprise Architects

Identity

Contoso uses a Windows Server AD forest for its internal identity provider and also federates with third-party providers for customer and partners. Contoso must leverage the internal set of accounts for Microsoft's cloud offerings. Access to cloud-based apps for customers and partners must leverage third-party identity providers as well.

Microsoft Cloud Identity for Enterprise Architects

Security

Security for cloud-based identities and data must include data protection, administrative privilege management, threat awareness, and the implementation of data governance and security policies.

Microsoft Cloud Security for Enterprise Architects

Management

Management for cloud-based apps and SaaS workloads will need the ability to maintain settings, data, accounts, policies, and permissions and to monitor ongoing health and performance. Existing server management tools will be used to manage virtual machines in Azure IaaS.

September 2017

Microsoft

Contoso in the Microsoft Cloud

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

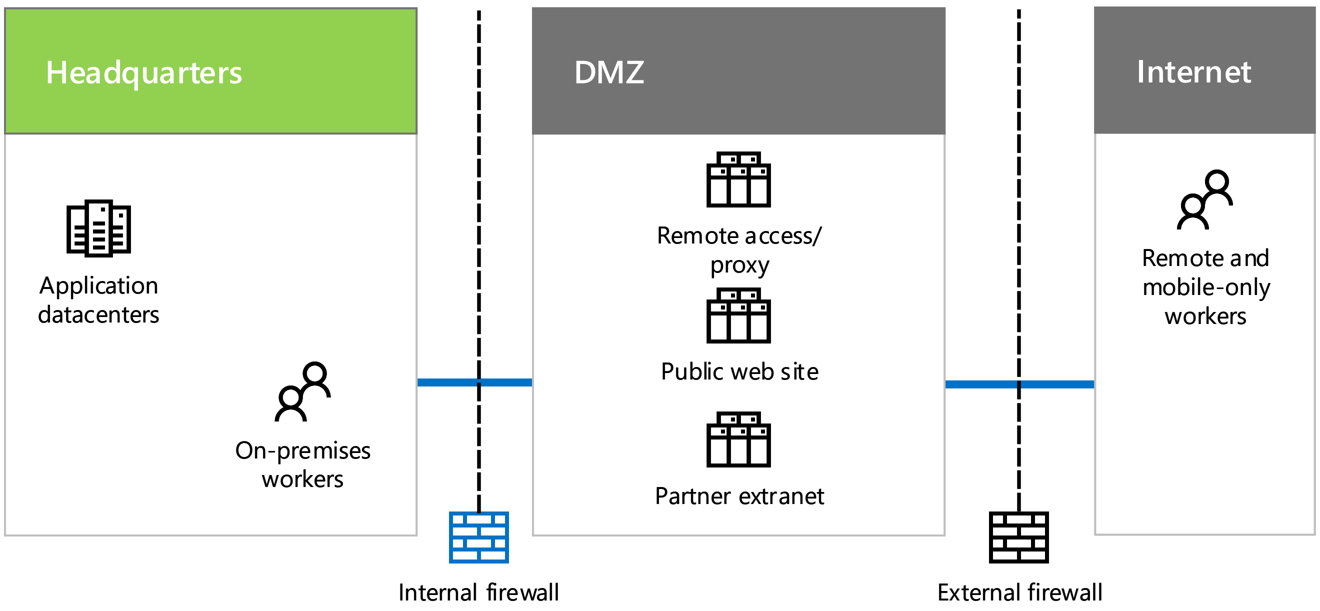
This topic is 2 of 7 in a series ① ② ③ ④ ⑤ ⑥ ⑦

Contoso's IT infrastructure and needs

Contoso is in the process of transitioning from an on-premises, centralized IT infrastructure to a cloud-inclusive one that incorporates cloud-based personal productivity workloads, applications, and hybrid scenarios.

Contoso's existing IT infrastructure

Contoso uses a mostly centralized on-premises IT infrastructure, with application datacenters in the Paris headquarters.



Headquarters

Application datacenters

On-premises workers

Internal firewall

DMZ

Remote access/ proxy

Public web site

Partner extranet

External firewall

Internet

Remote and mobile-only workers

In Contoso's DMZ, different sets of servers provide:

- Remote access to the Contoso intranet and web proxying for workers in the Paris headquarters.
- Hosting for the Contoso public web site, from which customers can order products, parts, or supplies.
- Hosting for the Contoso partner extranet for partner communication and collaboration.

Contoso's business needs

① **Adhere to regional regulatory requirements**

To prevent fines and maintain good relations with local governments, Contoso must ensure compliance with data storage and encryption regulations.

② **Improve vendor and partner management**

The partner extranet is aging and expensive to maintain. Contoso wants to replace it with a cloud-based solution that uses federated authentication.

③ **Improve mobile workforce productivity, device management, and access**

Contoso's mobile-only workforce is expanding and needs device management to ensure intellectual property protection and more efficient access to resources.

④ **Reduce remote access infrastructure**

By moving resources commonly accessed by remote workers to the cloud, Contoso will save money by reducing maintenance and support costs for their remote access solution.

⑤ **Scale down on-premises datacenters**

The Contoso datacenters contain hundreds of servers, some of which are running legacy or archival functions that distract IT staff from maintaining high business value workloads.

⑥ **Scale-up computing and storage resources for end-of-quarter processing**

End-of-quarter financial accounting and projection processing along with inventory management requires short-term increases in servers and storage.

Mapping Contoso's business needs to Microsoft's cloud offerings

SaaS
Software as a Service

- **Office 365:** Primary personal and group productivity applications in the cloud. ① ③ ⑤
- **Dynamics 365:** Use cloud-based customer and vendor management. Remove partner extranet in the DMZ. ②
- **Intune/EMS:** Manage iOS and Android devices. ③

Azure PaaS
Platform as a Service

- Host sales and support documents and information systems using cloud-based apps. ③
- Mobile applications are cloud-based, rather than Paris datacenter-based. ③ ④

Azure IaaS
Infrastructure as a Service

- Move archival and legacy systems to cloud-based servers. ⑤
- Migrate low-use apps and data out of on-premises datacenters. ⑤
- Add temporary servers and storage for end-of-quarter processing needs. ⑥

September 2017

Microsoft

Contoso in the Microsoft Cloud

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

This topic is 6 of 7 in a series 1 2 3 4 5 6 7

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