Microsoft Cloud Workshop

Security baseline on Azure
Whiteboard design session student guide
November 2019

Contents

Security baseline on Azure whiteboard design session student guide

Abstract and learning objectives

In this whiteboard design session, you will work with a group to design an end-to-end solution that leverages many of Microsoft Azure's security features.

At the end of this session, you will be better able to design and recommend solutions that help organizations properly secure their cloud-based applications while protecting their sensitive data.

Step 1: Review the customer case study

Outcome

Analyze your customer's needs.

Timeframe: 15 minutes

Directions: With all participants in the session, the facilitator/SME presents an overview of the customer case study along with technical tips.

1. Meet your table participants and trainer.
2. Read all of the directions for steps 1–3 in the student guide.
3. As a table team, review the following customer case study.

Customer situation

Contoso Ltd. is a multinational corporation, headquartered in the United States that provides insurance solutions worldwide. Its products include accident and health insurance, life insurance, travel, home, and auto coverage. Contoso manages data collection services by sending mobile agents directly to the insured to gather information as part of the data collection process for claims from an insured individual. These mobile agents are based all over the world and are residents of the region in which they work. Mobile agents are managed remotely through regional corporate offices.

The fundamental workflow for Contoso is as follows:

1. Contoso support staff process the incoming claims (which sometimes requires scrubbing) through the *corporate website*, and create a work order assigned to a mobile agent in the region of the insured.

2. Mobile agents log in daily to the *data collection website* and retrieve the list of insured customers they are responsible for visiting. They communicate directly with the insured, schedule a time for a home visit, and ultimately during that visit collect information and input it into the data collection website. The sensitive information collected always includes Personally Identifiable Information (PII) and may include Protected Health Information (PHI) about the insured customer. This data is sent over the public Internet securely over TLS (SSL).

3. When the data collection for an insured is completed, the mobile agent marks the task completed so that the corporate system can process those results.

4. Support staff processes complete work orders and submits results through the corporate website requiring another transfer of sensitive data. They also tend to utilize Microsoft Support when tough issues arise and want to know what options they have to engage and log support activities with VMs and other Azure resources.

Contoso currently hosts their systems at co-locations facilities within each geopolitical region and manages all IT operations for the systems. In the United States, they have achieved SOC 1 and SOC 2 compliance and follow required HIPAA regulations to protect PHI. Because of the new European GDPR laws, Contoso must evaluate their computing environments for compliance gaps. Contoso has concerns about maintaining their SOC 2 certification and HIPAA compliance with respect to moving to Azure. They would like to specifically address concerns about regional issues of data sovereignty for sensitive data within the context of the GDPR and want to ensure that if they move to Azure, they will be able to continue to have isolation between components.

In addition to the GDPR compliance requirements, they are expecting significant growth within the United States and abroad. They foresee the need to scale their system and are exploring moving their web applications (corporate and data collection web apps) to Microsoft Azure via lift and shift and other applicable methods to simplify some of the operations management overhead and associated costs, beginning with their U.S. data center and then those in Europe. They would also like to ensure that the corporate website and external facing web apps are sufficiently isolated. Lastly, they want to ensure that resources are created using best practices and that those practices are followed during the resource provisioning process.

Contoso has been using their on-premises SIEM to do most of their auditing and log reporting. They are wondering what options they have to monitor their on-premises and future cloud-based resources. They have thoughtfully tuned their on-premises SIEM to reduce false positives and normalize the metadata across different log types. They are worried about the amount of logs and potential for unnecessary work when they move workloads to Azure.

Jack Tradewinds, the CIO of Contoso Ltd, has heard a great deal of positive news about Azure and its progress in terms of security and compliance. He would like to learn more about the security features and if they can move some of their data and applications away from their on-premises datacenter. Given his long-standing relationship with Microsoft, he would like to see if Azure can meet his needs.

Customer needs

1. Assure data privacy and protection across all aspects of the system; in transit and at rest.

2. Address issues of data sovereignty with respect to the location of sensitive data.

3. Ability to scale as the company grows and system load increases.

4. Contain hosting and operational costs associated with running the system.

5. Enable method to continually review and assign legal compliance tasks to the appropriate individuals and provide a compliance reporting ability for Azure resources.

6. Enforce subscription owners to configure Azure resources with compliance and security while disallowing the creation of specific resources.

7. Limit access to the corporate site to users on the Contoso domain, and continue to support VPN access.

8. Extract all web applications that have configuration or embedded connection strings to a more secure implementation.

9. Migrate current database applications to Azure PaaS solution with the appropriate data backup features implemented to prevent catastrophic data loss due to intentional or unintentional acts.

10. Implement all security best practices on the migrated databases such as encryption at rest and during transport as well as ensure that sensitive data is not exposed to non-admin database users and applications.

11. Ensure network segregation between Azure admin and the lift and shifted web and database tiers.

12. Enable logging across all components (identity, virtual network, virtual machine, web, and database) to support an all-encompassing monitoring solution.

13. Ensure that Azure admins utilize best practices when accessing the Azure virtual machine resources and that all logins are logged for identity theft analysis activities.

14. Ensure ease of use by syncing appropriate admin username and passwords for on-premises and cloud resources.

15. Ensure that only authorized users can access specific Azure resources when logged into the Azure Portal.

16. Setup auditing such that software installs are monitored across Azure virtual machine resources.

17. When specific security events are detected (such as a port scan), allow for the execution of actions to remediate, start the investigative process or prevent further information leakage or damage.

Customer objections

1. Can Azure support the lift and shift of their web and database applications?

2. Admins are worried that they won't have the bandwidth to perform deployments of the corporate website and other supporting web applications.

3. Can Azure help contain costs for minimally used costly production and development resources?

4. Does Azure support the ability to allow VPN connections to specific resources?

5. Can Microsoft employees or government entities access our data?

6. How does Azure protect against threats?

7. Does Azure allow enough granular RBAC controls to meet our least privilege needs?

8. Is Azure virtual networking flexible enough to meet our requirements?

9. Can Azure supplement on-premises and third-party SIEM systems for auditing and compliance tasks?

10. What certifications does Azure have and can Azure hosted applications meet the US and European compliance goals?

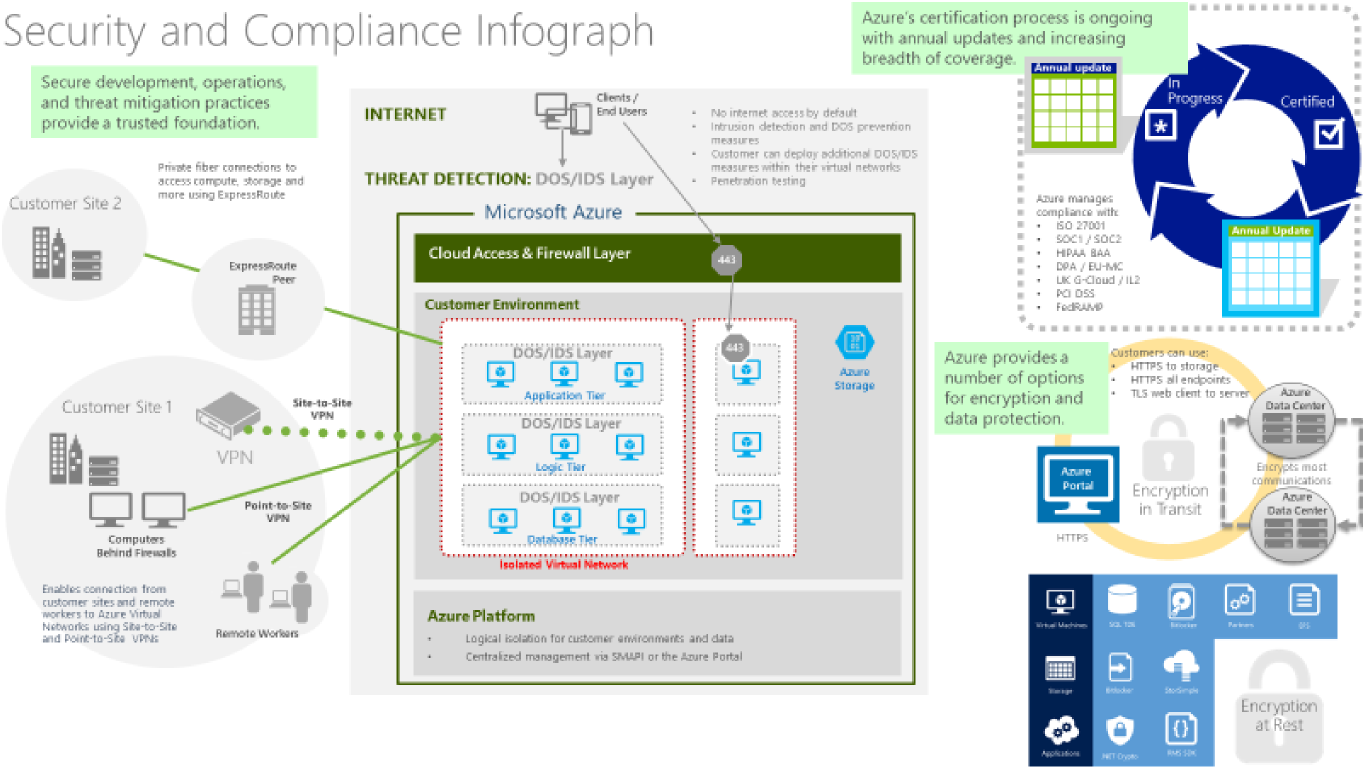
11. Is Azure flexible enough to support data sovereignty needs and issues like those referenced in GDPR articles?

12. How can we ensure continued SOC 1 and SOC 2 compliance?

13. Does Azure permit penetration testing as a part of a security assessment?

Infographic for common scenarios

This Infographic shows an example of a generic implementation of various security Azure technologies in action that can be used as a reference in your design:



Security and Compliance Infograph

Secure development, operations, and threat mitigation practices provide a trusted foundation.

Private fiber connections to access compute, storage and more using ExpressRoute

Enables connection from customer sites and remote workers to Azure Virtual Networks using Site-to-Site and Point-to-Site VPNs

- No internet access by default
- Intrusion detection and DOS prevention measures
- Customer can deploy additional DOS/IDS measures within their virtual networks
- Penetration testing

Azure Platform

- Logical isolation for customer environments and data
- Centralized management via SMAPI or the Azure Portal

Azure's certification process is ongoing with annual updates and increasing breadth of coverage.

Azure manages compliance with:
- ISO 27001
- SOC1 / SOC2
- HIPAA BAA
- DPA / EU-MC
- UK G-Cloud / IL2
- PCI DSS
- FedRAMP

Azure provides a number of options for encryption and data protection.

Customers can use:
- HTTPS to storage
- HTTPS all endpoints
- TLS web client to server

Step 2: Design a proof of concept solution

Outcome

Design a solution and prepare to present the solution to the target customer audience in a 15-minute chalk-talk format.

Timeframe: 60 minutes

Business needs

Directions: With all participants at your table, answer the following questions and list the answers on a flip chart:

1. To whom should you present this solution? Who is your target customer audience? Who are the decision makers?

2. What customer business needs do you need to address with your solution?

Design

Directions: With all participants at your table, respond to the following questions on a flip chart.

High-level architecture

Briefly sketch-out and propose a high-level solution that meets the customer's business and technical needs and mitigates their objections. For this workshop, you may choose from the following technologies (you may not need all of them in the correct solution):

1. Azure Virtual Machines and Networks, Network Security Groups

2. Virtual Private Networks (Point to Point, Site to Site) and Express Route

3. Azure Web Apps

4. Azure Firewall

5. Azure Front Door

6. Azure SQL DB Security Features (Threat Detection, TDE, Column Level Encryption, Service Endpoints, etc.)

7. Azure Storage Encryption

8. SQL Server in a Virtual Machine

9. Azure Security Center, Azure Monitor and Log Analytics

10. Azure Sentinel and Azure Policy

11. Azure Key Vault

12. Microsoft Azure Active Directory (Connect, IAM, etc.)

13. Microsoft Intune

Securing Sensitive Data

On your diagram, indicate how you would secure any sensitive data at rest and in transit with respect to the following:

1. Web Tier (corporate vs. data collection)

2. Database Tier

3. Network, Internal, and External Communications

Ensuring auditing and compliance

Describe how you will use Azure features to ensure the following:

1. How will you monitor and audit VM access?
2. How will you monitor and audit network traffic across Virtual Networks?
3. How will you monitor and audit Azure SQL?
4. Create custom alerts and execute remediation and investigation activities on detection?
5. What tools would you setup to surface audit and for compliance reporting to IT Executives?

Ensuring availability and business continuity

Describe how you would ensure that the following resources would be available in the unlikely event of an attack or intentional or unintentional data loss?

1. Virtual Machines
2. Azure SQL

Ensuring protection

Describe how you would secure each Azure resource from internal and external attacks:

1. Ensure that admin credentials are sufficiently protected and monitored
2. Prevent admins from causing intended and unintended harm to the environment such as unapproved software installs
3. Admins access Azure resources from secured and/or compliant corporate assets and do not directly access any production Virtual Machines from the internet
4. Prevent Denial of Service (DoS) and common web application attack vectors from reaching the web applications

Prepare

Directions: With all participants at your table:

1. Identify any customer needs that are not addressed with the proposed solution.
2. Identify the benefits of your solution.
3. Determine how you will respond to the customer's objections.

Prepare a 15-minute chalk-talk style presentation to the customer.

Step 3: Present the solution

Outcome

Present a solution to the target customer audience in a 15-minute chalk-talk format.

Timeframe: 30 minutes

Presentation

Directions:

1. Pair with another table.
2. One table is the Microsoft team and the other table is the customer.
3. The Microsoft team presents their proposed solution to the customer.
4. The customer makes one of the objections from the list of objections.
5. The Microsoft team responds to the objection.
6. The customer team gives feedback to the Microsoft team.
7. Tables switch roles and repeat Steps 2–6.

Wrap-up

Timeframe: 15 minutes

Directions: Tables reconvene with the larger group to hear the facilitator/SME share the preferred solution for the case study.

Additional References

Description	**Links**
Azure Virtual Machines	https://docs.microsoft.com/en-us/azure/virtual-machines/windows/
Azure Virtual Networks	https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview
Azure DDoS	https://docs.microsoft.com/en-us/azure/virtual-network/ddos-protection-overview
Network Security Groups	https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-nsg
Azure VPN Gateway	https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal
Azure Firewall	https://docs.microsoft.com/en-us/azure/firewall
Azure Front Door	https://docs.microsoft.com/en-us/azure/frontdoor/front-door-overview
Azure Application Gateway	https://docs.microsoft.com/en-us/azure/application-gateway
Azure Web Apps	https://docs.microsoft.com/en-us/azure/app-service/
Azure SQL	https://docs.microsoft.com/en-us/azure/sql-database/

Azure SQL documentation, TDE, data masking and encryption at rest	https://docs.microsoft.com/en-us/azure/sql-database/sql-database-always-encrypted-azure-key-vault
Express Route	https://docs.microsoft.com/en-us/azure/expressroute/expressroute-introduction
Azure Storage Encryption	https://docs.microsoft.com/en-us/azure/storage/common/storage-service-encryption
SQL Server (IaaS)	https://docs.microsoft.com/en-us/azure/virtual-machines/windows/sql/virtual-machines-windows-sql-server-iaas-overview
Azure Identity Access Management (IAM)	https://docs.microsoft.com/en-us/azure/active-directory/role-based-access-control-configure
Azure Monitor and Log Analytics	https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/monitoring-overview
Azure Sentinel	https://azure.microsoft.com/en-us/services/azure-sentinel/
Azure Policy	https://azure.microsoft.com/en-us/services/azure-policy/
Azure Lockbox	https://azure.microsoft.com/en-us/blog/approve-audit-support-access-requests-to-vms-using-customer-lockbox-for-azure/
Azure Key Vault	https://docs.microsoft.com/en-us/azure/key-vault/
Microsoft Azure Active Directory Connect	https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnectsync-whatis
Lift and Shift (IaaS)	https://docs.microsoft.com/en-us/dotnet/standard/modernize-with-azure-and-containers/lift-and-shift-existing-apps-azure-iaas
Microsoft Intune	https://docs.microsoft.com/en-us/intune
Conditional Access	https://docs.microsoft.com/en-us/azure/active-directory/active-directory-conditional-access-azure-portal
Azure, Office 365, Azure SQL and Cloud App references	https://docs.microsoft.com/en-us/azure/active-directory/active-directory-conditional-access-no-modern-authentication
SQL Database Conditional Access	https://docs.microsoft.com/en-us/azure/sql-database/sql-database-conditional-access
SQL Database Service Endpoints	https://docs.microsoft.com/en-us/azure/sql-database/sql-database-vnet-service-endpoint-rule-overview
Azure AD Conditional Access Technical Reference	https://docs.microsoft.com/en-us/azure/active-directory/active-directory-conditional-access-technical-reference
Advanced Threat Analytics	https://docs.microsoft.com/en-us/advanced-threat-analytics
Microsoft Cloud App Security	https://docs.microsoft.com/en-us/cloud-app-security

Compliance Commitments	http://azure.microsoft.com/en-us/support/trust-center/services/
Azure Trust Center	http://azure.microsoft.com/en-us/support/trust-center/