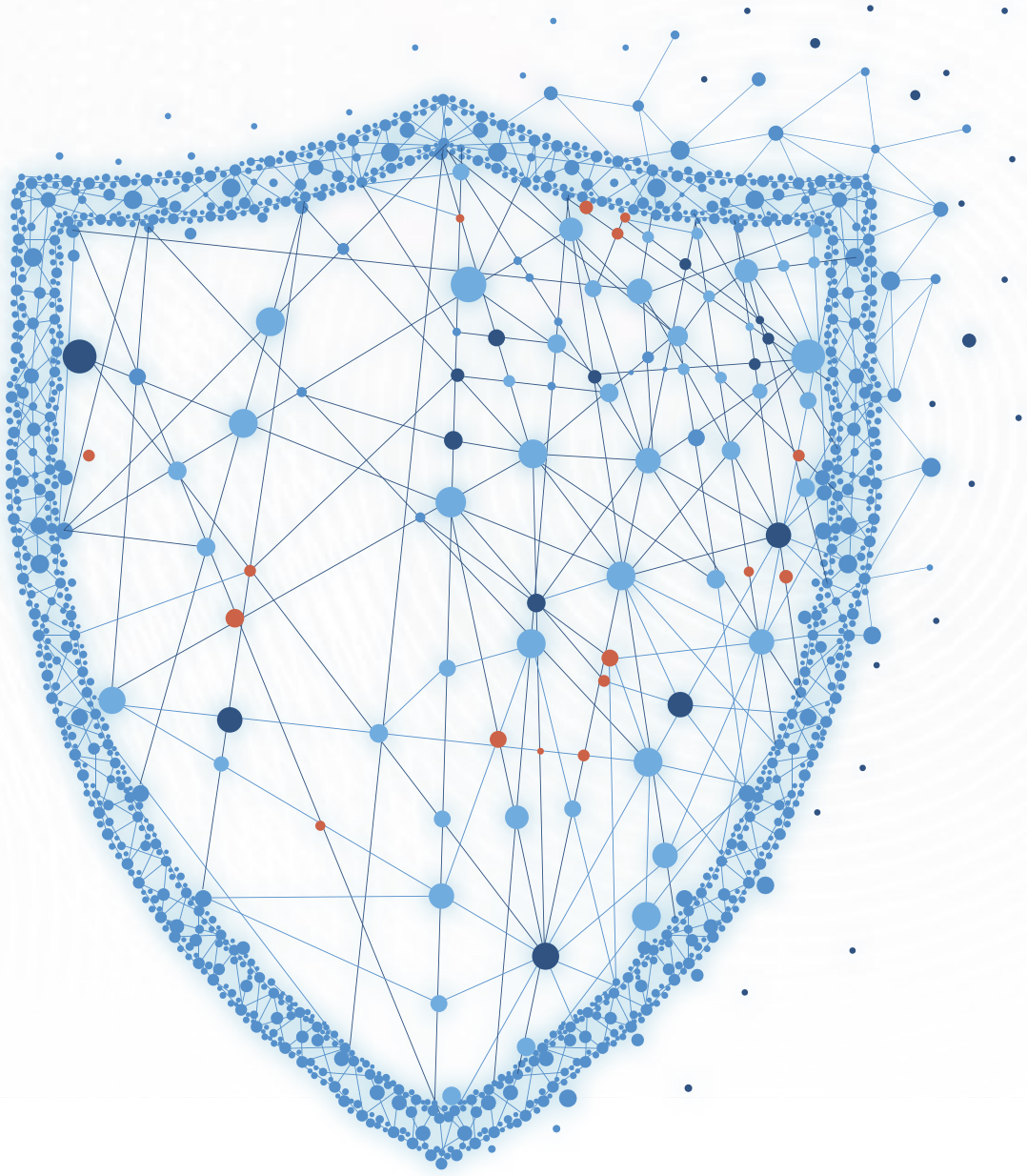

GoDgtl
by PruTech

AZURE **COMPLIANCE AND SECURITY**

Table Of Contents

Introduction

Compliance is one of the prime reasons why most businesses hesitate to adopt a cloud-first strategy. When moving to cloud environments, enterprises must know in which countries their data will get processed, what data protection and privacy laws will apply, and what impact these laws will have on non-compliance. It is also crucial to know what security measures these laws require for businesses to put in place. However, with a clear understanding of attaining compliance in the public cloud, enterprises that require following even the most rigorous standards can operate in an ever-changing regulatory environment.

Public clouds like Microsoft Azure consider security of prime importance. One of the prominent reasons to use Azure for your applications and services is to take advantage of its wide array of security tools and capabilities. These tools and capabilities help make it possible to create secure solutions on the safe Azure platform. In addition, Microsoft Azure provides confidentiality, integrity, and availability of customer data while also enabling transparent accountability.

This whitepaper explores how the capabilities of the Azure platform enable businesses to achieve compliance and security when moving to the cloud. This paper also discusses some of the security best practices that you can follow when using Azure as your cloud platform.

Azure: A Secure Public Cloud

Azure is a public cloud service platform that supports a broad selection of operating systems, programming languages, frameworks, tools, databases, and devices. It can run Linux containers with Docker integration, build apps with JavaScript, Python, .NET, PHP, Java, and Node.js, and build backends for iOS, Android, and Windows devices.

Azure public cloud services support the same technologies that millions of developers and IT professionals already rely on and trust. When you build on or migrate IT assets to a public cloud service provider, you rely on that organization's abilities to protect your applications and data with the services and controls they provide to manage the security of your cloud-based assets.

Azure's infrastructure is designed from facility to applications for hosting millions of customers simultaneously. Moreover, it provides a trustworthy foundation upon which businesses can meet their security requirements.

In addition, Azure provides you with a wide array of configurable security options and the ability to control them so that you can customize security to meet the unique requirements of your organization's deployments. This document helps you understand precisely how Azure security capabilities can help you fulfill these requirements.

How Azure Helps Keep Customer Data Secure

Automated Azure processes in the cloud can reduce or eliminate human error that is often responsible for any security breaches. State-of-the-art physical security protecting Microsoft datacenters is designed, built, and operated as per internationally recognized standards. Moreover, Microsoft continuously invests in making the Azure infrastructure resilient to attack, safeguarding user access to the Azure environment, and helping keep customer data secure.

Here are some of the ways Azure helps in securing customer data:

PHYSICAL SECURITY

Microsoft datacenters have extensive layers of protection to reduce the risk of unauthorized physical access to datacenter resources.

SECURITY DESIGN AND OPERATIONS

Microsoft makes Azure security a priority at every step, including code development that follows the Security Development Lifecycle (SDL), a company-wide, mandatory process based on a rigorous set of security controls that govern operations, as well as robust incident response strategies. Operational Security Assurance (OSA) makes Microsoft business cloud services more resilient to attack by decreasing the amount of time needed to prevent, detect, and respond to actual and potential internet-based security threats.

INFRASTRUCTURE PROTECTION

The guiding principle of our security strategy is to “assume breach.” The Microsoft global incident response team works around the clock to mitigate the effects of any attack against our cloud services.

NETWORK PROTECTION

Azure provides the infrastructure to connect Virtual Machines (VMs) to one another securely and connect on-premises datacenters with Azure VMs. The Azure infrastructure ensures that all infrastructural communications (for which Microsoft is responsible) carrying customer information are encrypted over the wire. In addition, the Distributed Denial-of-Service (DDoS) protection at every Azure datacenter helps protect against the largest DDoS attacks observed on the internet to date.

DATA PROTECTION

Azure safeguards customer data for applications, platforms, systems, and storage using four specific methods: segregation, encryption, redundancy, and destruction. Azure offers protection for customer data both in transit and at rest, and supports encryption for data, files, applications, services, communications, and drives.

IDENTITY AND USER ACCESS MANAGEMENT & CONTROL

Azure manages and controls identity and user access to enterprise environments, data, and applications byfederating user identities to Azure Active Directory and enabling multi-factor authentication for more secure sign-ins. Microsoft uses stringent identity management and access controls to limit data and systems access to those with a genuine business need (least-privileged).

Privacy and Ownership of Data

Microsoft defines customer data as “all data, including all text, sound, video or image files, and software that are provided to Microsoft by, or on behalf of, the customer using the online7 service.” This includes data that you upload for storage or processing and the applications you run in Azure.

For many organizations, keeping data private is no longer merely desirable—it’s mandatory.Government and industry regulations require that you protect the privacy of certain types of data. Breaches that expose personal information can have serious consequences. The Microsoft approach to privacy is grounded in its commitment to give you control over the collection, usage, and distribution of your customer data.

Knowledge is the key to controlling your data, and with Azure:

- You know how Microsoft manages your data. Microsoft uses your customer data only to provide the agreed-upon services and does not mine it for marketing or advertising. If you leave the service, Microsoft takes the necessary steps to ensure you have full ownership of your data.
- You know where your data resides. Customers willing to maintain their data in a specific geographic location can rely on the expanding network of Azure datacenters worldwide. Microsoft also complies with international data protection laws regarding transfers of customer data across borders.
- You know who can access your data and on what terms. Microsoft takes strong measures to protect your data from inappropriate access, including restrictions that limit access for Microsoft personnel and subcontractors. However, you can access your customer data anytime and for any reason.
- You know how Microsoft responds to government and law enforcement requests to access your customer data. Microsoft will not disclose customer data hosted in the Microsoft Cloud to a government or law enforcement except as you direct or where required by law.

How Azure Security Works

The Azure Security documentation shows that Microsoft Azure Security infrastructure operates under a shared security responsibility model. It means that the security is a joint effort between Azure and the customers, except in an on-premise setting where the customers carry all the responsibilities. However, as customers move to the cloud, some Azure customer security responsibilities do get transferred.

The division of responsibilities changes across different cloud service models in the following ways:

- **In IaaS (Infrastructure as a Service)**, Azure takes over physical security (hosts, networks, and datacenter).
- **In PaaS (Platform as a Service)**, Azure takes over physical security and the operating system. Azure also shares identity and directory infrastructure, network controls, and applications with customers.
- **In SaaS (Software as a Service)**, Azure takes more responsibilities such as physical security, operating system, network controls, and application. The cloud platform still shares identity and directory infrastructure with the customer.

In a nutshell, Azure secures the physical infrastructure, and then the division of responsibility changes depending on the cloud delivery model. It is evident that customers have more responsibilities in IaaS compared to PaaS or SaaS. However, regardless of whether it is on-premise, IaaS, PaaS, or SaaS, customers are always responsible for these three aspects: data governance and rights management, account and access management, and endpoint protection.

Azure Security Best Practices

The Azure Security documentation is a handy source for security recommendations and best practices. **Here are some tips to get you started quickly:**

- Upgrade your Azure subscription to Azure Security Center Standard to enjoy more functionality, like finding and fixing security vulnerabilities, detecting threats with analytics and intelligence, and quick response to an attack.
- Store your keys in the Azure Key Vault designed to support passwords, database credentials, and other secrets.
- Install a web application firewall.
- Use Azure MFA (Multi-Factor Authentication), especially for admin accounts.
- Encrypt virtual hard disk files.
- Connect Azure VMs (virtual machines) to other networked devices by placing them on Azure virtual networks.
- Use Azure's DDoS services to prevent and mitigate DDoS (Distributed Denial of Service) attacks.
- Have security policies in place to prevent abuse. To help you get started, Azure can auto-generate a security policy per an Azure subscription.
- Regularly review the Azure Security Center dashboard. The dashboard provides a central view of your Azure resources and recommends actions.
- Implement Azure Security Center's Role-Based Access Control (RBAC). There are five built-in roles (Subscription Owner, Resource Group Owner, Subscription Contributor, Resource Group Contributor, and Reader) and two unique security roles (Security Administrator and Security Reader). These roles vary in permissions.

> Remember that cloud security is a shared responsibility between you and Azure. Depending on the cloud delivery model, the responsibilities you share with Azure will change. Don't forget to implement the security practices recommended by Microsoft!

How GoDgtl Collaborates With Microsoft Azure

GoDgtl brings a team of experienced cloud experts who work directly with Microsoft Azure to bring value and real solutions for your cloud projects. With direct access to Microsoft Azure resources and in-house cloud consulting talent, GoDgtl is ready to guide you through your cloud journey regardless of where you are on that path. Whether it's more knowledge-based information on cloud topics such as security, or governance and compliance, or basic cloud migration aspects, or even if an assessment is needed, GoDgtl can provide a roadmap for your path to project completion and success.

Sources

https://digitalguardian.com/blog/what-azure-security

https://docs.microsoft.com/en-us/azure/security/fundamentals/overview

https://docs.microsoft.com/en-us/azure/security/fundamentals/services-technologies

https://azure.microsoft.com/en-us/blog/trusted-cloud-security-privacy-compliance-resiliency-andip/

GoDgtl by PruTech

Our mission is to **help client organizations like yours access the latest resources and make their DX goals a reality.** Connect with our teams at Go-Dgtl to embrace new ideas and key enablers. **We promise to make your digital acceleration journey a success.**

go-dgtl.com/contact-us

ENABLE | TRANSFORM | ACHIEVE | ANALYZE | ADAPT

OUR LOCATIONS // Charlotte | Bangalore | Hyderabad | Mexico City | New Jersey (Iselin) | New York | Washington DC

CONTACT US // info@go-dgtl.com | (646) 536-7777 | go-dgtl.com