Defense-in-Depth Security in Azure

Learn how Microsoft designs and operates Azure and get an overview of Azure services and capabilities to secure, manage and monitor your data, apps and infrastructure.

As a managed service, Microsoft designs and operates its cloud services with security at the core and provides you with the built-in controls and tools to meet the security needs of your infrastructure, apps and data. You also benefit from the service level intelligence from Microsoft’s global scale cyber defense operations.

Defense in Depth Security

In Azure, all services are designed and operated to support multiple layers of defense spanning your data, apps, virtual machines, network, perimeter, all the way through to the physical security within our datacenters. Together, this layered approach comprises a comprehensive defense in-depth strategy.

As we move from the center of our defense in depth approach, from data to the perimeter, one of the most important built-in services to familiarize yourself with is the Azure Active Directory (Azure AD) which provides role-based access control over your Azure resources. Next is Azure Security Center which gives you centralized and real-time monitoring into the security state of your Azure workloads, with actionable recommendations and controls. Azure Security Center provides unified visibility and control, adaptive threat protection, as well as intelligent threat detection and response.
Protecting Your Data

Data protections are built for both structured and unstructured Data. For structured data, all data is encrypted at rest and machine learning can be used to proactively look for and alert you on potential security vulnerabilities.

These can be related to data encryption, enabling security telemetry and extend to capabilities in data services themselves to recommend and enable sensitive information discovery and classification, dynamic data masks to obscure data fields, and more.

Database services in Azure can be configured to run these checks automatically and Azure Security Center will alert you on any potential issues it finds to keep your data protected.

For unstructured data, Storage accounts spanning blobs, files, tables and queues are also encrypted at rest by default and each account is geo-redundant. You can also apply further protections using Access Keys to control authentication, Shared Access Signatures for secure delegated access and granular Network firewall settings.

Azure Security Center will report its findings when security is at risk or protections have been disabled by an admin.

Additionally the Azure Key Vault service helps safeguard cryptographic keys and secrets used by cloud applications and services. By using Key Vault, you can encrypt keys and secrets (such as authentication keys, storage account keys, data encryption keys, .PFX files, and passwords) using keys protected by hardware security modules (HSMs).

Protecting Your App

Apps are the front end for accessing and presenting data and their security is generally governed through data, VMs or compute and platform services in Azure.

Your web apps can be configured to use Azure managed service identities to streamline secure communication with other services connected to Azure AD.

You can manage SSL certificates for your apps and even require that clients connecting to your apps have valid certificates for inbound requests.
Protecting Your Virtual Machines

As you move into Virtual Machines and compute, the Azure Security Center uses machine learning to continuously assess security and vulnerability levels of your VMs, networks and service configurations. It also gives you actionable recommendations to prevent exploits before they occur, and dynamically applies both allow and block lists to keep out unwanted traffic. You can also benefit from intelligent threat detection and response.

The Azure Security Center leverages the Microsoft Intelligent Security Graph to discover and take action against attacks. The security graph combines the cyber intelligence Microsoft collects across all of its services and industry data to block known attack patterns. We also give you the controls you need to prioritize alerts and incidents important to you.

Intelligent threat detection and response in Azure

We give you a unified view for forensics analysis and the ability to search across all your compute resources. You can even visualize threat intelligence down to the trending attack techniques and the geographic regions affected.

Protecting Your Network

The Azure Security Center will assess and report on potential networking security issues related to open ports and firewall settings and network security groups. Azure provides additional security when designing and architecting your apps to enforce logical network boundaries and limit permissions to network security groups.

You can also control network and other resources like VMs with just-in-time controls for opening management and internet ports, with intelligent recommendations to reduce exposure to brute force attacks.

Just in time controls for admin access
Perimeter Level Security

Beyond your network controls, Azure’s protection against Distributed Denial of Service attacks (DDoS) is available at a basic level by default. The standard version of Azure’s DDoS protection adds additional protection and mitigations against:

**Volumetric Attacks** – where the attacker’s goal is to flood the network with traffic in efforts to disable your services.

**Protocol Attacks** – where the attacker tries to find and exploit weaknesses in layer 3 and 4 protocol stacks.

**Application Layer Attacks** – where web application packets are used to disrupt transmission of data between hosts, like cross-site scripting or HTTP protocol violations.

As your hub for visibility and control, many of the capabilities that we give you in Azure Security Center also extend to your VMs in other clouds or in your data centers.
Security Policies and Access Management

Azure has a comprehensive set of services to securely manage security policies and access to your resources – whether accessed by people or programmatically via your code.

These controls are more than just the front door to who or which processes can access your apps, files or data, and extend to how granular access is delegated to your IT and development teams using role-based access controls, to ensure your team members only have access to what they need. For more information, check out the Azure Essentials on Identity and Access Management.

To automate the response to specific security events you can also use a security playbook. Powered by Logic Apps, you can use these to automate workflows. This orchestrates the set of actions that need to happen when a pre-defined event is detected by the Azure Security Center.

Azure Service Level Security by Design

Beyond the policies that you can set, security is infused in everything we do as we develop Azure services – from the planning and design phase all the way to development and delivery, using the Secure Development Lifecycle process.

Fabric admins operate Azure services with zero standing privilege and use just-in-time approval processes to gain temporary access to sensitive data or controls when needed.

Azure services comply with both international and industry-specific compliance standards and are subject to rigorous third-party audits that verify Azure security controls.
Physical Security

Finally, we extend our layered approach to physical security. Datacenters managed by Microsoft have extensive layers of protection: access approval at the facility’s perimeter, at the building’s perimeter, inside the building and on the datacenter floor.

This layered approach reduces the risk of unauthorized users gaining physical access to data and the datacenter resources.

Microsoft Azure operates datacenters in 43 regions

So that completes our overview of defense-in-depth security in Azure. The controls that we give you are all part of the shared responsibility model in Azure. This comprises the security that Microsoft manages as the service provider, built-in controls for you to protect your data, apps and infrastructure and the intelligence that Microsoft can provide you from its global scale cyber defense operations.

Continued Learning

Microsoft Mechanics

Steps to securing and managing your VMs in production with Azure
End-to-end updates for securing and managing your virtual machines in Azure
Application Insights – Live telemetry across app lifecycle
An overview of Azure Monitor

Additional Learning Resources

Microsoft Trust Center
Azure Essentials: Defense in Depth Security in Azure
Azure Essentials: Managing Identity

Quickstarts:

Azure Security Center Quickstart
Get Started with Key Vault

Training

Getting Started with Microsoft Azure Security
Azure Security Services