

# Defense in depth

🕒 10 minutes

There's no "easy button" for security and no solution that solves all your problems from a security perspective. Let's imagine that Lamna Healthcare has neglected security in its environment. The company has realized it needs to put some major focus in this area. Lamna is not exactly sure where to start, or if it's possible to just buy a solution to make the environment secure. The company knows it needs a holistic approach but is unsure what really fits into that. Here, we'll identify key concepts of defense in depth, identify key security technologies and approaches to support a defense in depth strategy, and discuss how to apply these concepts when architecting your own Azure services.

## Defense in depth



## A layered approach to security

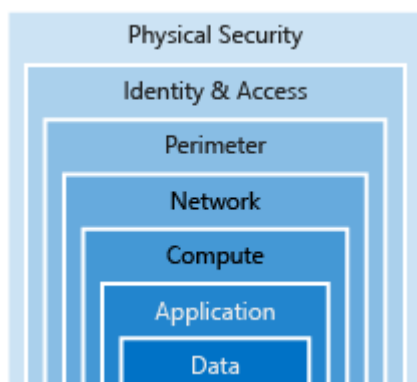
*Defense in depth* is a strategy that employs a series of mechanisms to slow the advance of an attack aimed at acquiring unauthorized access to information. Each layer provides protection so that if one layer is breached, a subsequent layer is already in place to prevent further exposure. Microsoft applies a layered approach to security, both in our physical datacenters

and across Azure services. The objective of defense in depth is to protect and prevent information from being stolen by individuals not authorized to access it. The common principles used to define a security posture are confidentiality, integrity, and availability, known collectively as CIA.

- **Confidentiality** - Principle of least privilege. Restricts access to information only to individuals explicitly granted access. This information includes protection of user passwords, remote access certificates, and email content.
- **Integrity** - The prevention of unauthorized changes to information at rest or in transit. A common approach used in data transmission is for the sender to create a unique fingerprint of the data using a one-way hashing algorithm. The hash is sent to the receiver along with the data. The data's hash is recalculated and compared to the original by the receiver to ensure the data wasn't lost or modified in transit.
- **Availability** - Ensure services are available to authorized users. Denial of service attacks are a prevalent cause of loss of availability to users. Natural disasters also drive system design to prevent single points of failure and deploy multiple instances of an application to geo-dispersed locations.

## Security layers

Defense in depth can be visualized as a set of concentric rings, with the data to be secured at the center. Each ring adds an additional layer of security around the data. This approach removes reliance on any single layer of protection and acts to slow down an attack and provide alert telemetry that can be acted upon, either automatically or manually. Let's take a look at each of the layers.



### Data

In almost all cases, attackers are after data:

- Stored in a database
- Stored on disk inside virtual machines
- Stored on a SaaS application such as Office 365

- Stored on a SaaS application such as Office 365
- Stored in cloud storage

It's the responsibility of those storing and controlling access to data to ensure that it's properly secured. Often there are regulatory requirements that dictate the controls and processes that must be in place to ensure the confidentiality, integrity, and availability of the data.

## Applications

- Ensure applications are secure and free of vulnerabilities
- Store sensitive application secrets in a secure storage medium
- Make security a design requirement for all application development

Integrating security into the application development life cycle will help reduce the number of vulnerabilities introduced in code. Encourage all development teams to ensure their applications are secure by default. Make security requirements non-negotiable.

## Compute

- Secure access to virtual machines
- Implement endpoint protection and keep systems patched and current

Malware, unpatched systems, and improperly secured systems open your environment to attacks. The focus in this layer is on making sure your compute resources are secure, and that you have the proper controls in place to minimize security issues.

## Networking

- Limit communication between resources through segmentation and access controls
- Deny by default
- Restrict inbound internet access and limit outbound where appropriate
- Implement secure connectivity to on-premises networks

At this layer, the focus is on limiting the network connectivity across all your resources to only allow what is required. Segment your resources and use network level controls to restrict communication to only what is needed. By limiting this communication, you reduce the risk of lateral movement throughout your network.

## Perimeter

- Use distributed denial-of-service (DDoS) protection to filter large-scale attacks before they can cause a denial of service for end users
- Use perimeter firewalls to identify and alert on malicious attacks against your network

At the network perimeter, it's about protecting from network-based attacks against your

## Policies & access

- Control access to infrastructure, change control
- Use single sign-on and multi-factor authentication
- Audit events and changes

The policy & access layer is all about ensuring identities are secure, and that access granted is only what is needed, and changes are logged.

## Physical security

- Physical building security and controlling access to computing hardware within the data center is the first line of defense.









































With physical security, the intent is to provide physical safeguards against access to assets. This ensures that other layers can't be bypassed, and loss or theft is handled appropriately.



Each layer can implement one or more of the CIA concerns.

#	Ring	Example	Principle
1	Data	Data encryption at rest in Azure blob storage	Integrity
2	Application	SSL/TLS encrypted sessions	Integrity
3	Compute	Regularly apply OS and layered software patches	Availability
4	Network	Network security rules	Confidentiality
5	Perimeter	DDoS protection	Availability
6	Policies & Access	Azure Active Directory user authentication	Integrity
7	Physical Security	Azure data center biometric access controls	Confidentiality

## Shared responsibilities

As computing environments move from customer-controlled datacenters to cloud datacenters, the responsibility of security also shifts. Security is now a concern shared by both cloud providers and customers.

responsibility	prem	iaas	paas	saas
Data governance & rights management				
Client endpoints				
Account & access management				
Identity & directory infrastructure				
Application				
Network controls				
Operating system				
Physical hosts				
Physical network				
Physical datacenter				

 Microsoft
  Customer

## Continuous improvement

The threat landscape is evolving in real time and at massive scale, therefore a security architecture is never complete. Microsoft and our customers require the ability to respond to these threats intelligently, quickly, and at scale.

[Azure Security Center](#) provides customers with unified security management and advanced threat protection to understand and respond to security events on-premises and in Azure. In turn, Azure customers have a responsibility to continually re-evaluate and evolve their security architecture.

## Defense in depth at Lamna Healthcare

Lamna Healthcare has put a strong focus on defense in depth across all IT teams. Since the organization is responsible for a substantial amount of sensitive health care data, they realize that a comprehensive approach is their best path forward.

They've formed a virtual team, with representatives from each IT team along with their security team, that is focused on driving this across the organization. They work on educating

engineers and architects on vulnerabilities, how to address them, and provide guidance as projects move through the organization.

They realize that this effort is never done, and have put in place regular policy, process, technical and architectural reviews to ensure they are constantly looking at ways to improve

technical, and architectural reviews to ensure they are constantly looking at ways to improve security.

## Summary

We've looked at what a defense in depth approach to security looks like, what the layers of this approach look like, and what each layer is focused on. Using this approach to secure your architecture will put you on a path forward to ensure you're addressing security comprehensively across your environment instead of focusing on one single layer or technology.

## Check your knowledge

1. True or false: *defense in depth* is a strategy aimed to protect you against attacks attempting to gain access to your information?

- ☐ True
- ☐ False

2. True or false: by moving to the cloud, my architecture is fully secure and I can hand off all security responsibilities to my cloud provider?

- ☐ True
- ☐ False

[Check your answers](#)

---