✓ 200 XP ▶

Design for security

🕒 10 minutes

Your healthcare organization stores personal and potentially sensitive client data. A security incident could expose this sensitive data, which could cause personal embarrassment or financial harm. How do you ensure the integrity of their data and ensure your systems are secure?

Here, we'll talk about how to approach the security of an architecture.

What should I protect?

The data your organization stores or handles is at the heart of your securable assets. This data could be sensitive data about customers, financial information about your organization, or critical line-of-business data supporting your organization. Along with data, securing the infrastructure it exists on, and the identities we use to access it, are also critically important.

Your data may be subject to additional legal and regulatory requirements depending on where you are located, the type of data you are storing, or the industry that your application operates in. For instance, in the healthcare industry in the US, there is a law called the Health Insurance Portability and Accountability Act (HIPAA). In the financial industry, the Payment Card Industry Data Security Standard is concerned with the handling of credit card data. Organizations that store data that is in scope for these laws and standards are required to ensure certain safeguards are in place for the protection of this data. In Europe, the General Data Protection Regulation (GDPR) lays out the rules of how personal data is protected, and defines individuals' rights related to stored data. Some countries require that certain types of data do not leave their borders.

When a security breach occurs, there can be substantial impacts to the finances and reputation of both organizations and customers. This breaks down the trust customers are willing to instill in your organization, and can impact its long-term health.

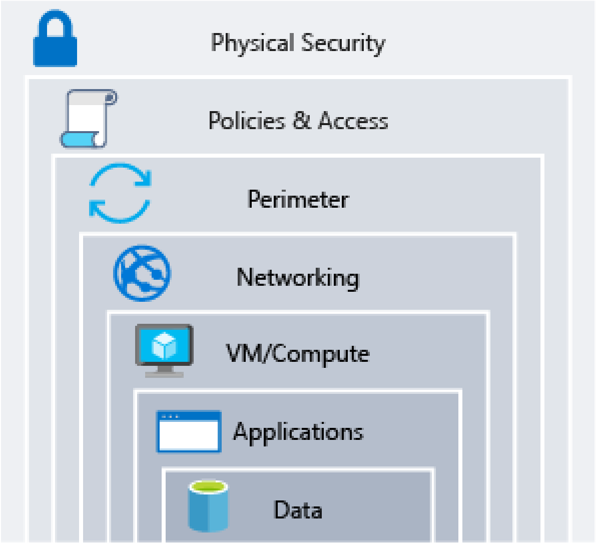
Defense in depth

A multilayered approach to securing your environment will increase the security posture of your environment. Commonly known as *defense in depth*, we can break down the layers as follows:

- Data

- Data
- Applications
- VM/compute
- Networking
- Perimeter
- Policies & access
- Physical security

Each layer focuses on a different area where attacks can happen and creates a depth of protection, should one layer fail or be bypassed by an attacker. If we were to just focus on one layer, an attacker would have unfettered access to your environment should they get through this layer. Addressing security in layers increases the work an attacker must do to gain access to your systems and data. Each layer will have different security controls, technologies, and capabilities that will apply. When identifying the protections to put in place, cost will often be of concern, and will need to be balanced with business requirements and overall risk to the business.



Defense in-depth security layers

There is no single security system, control, or technology that will fully protect your architecture. Security is more than just technology, it's also about people and processes. Creating an environment that looks holistically at security, and making it a requirement by default will help ensure your organization is as secure as possible.

Common attacks

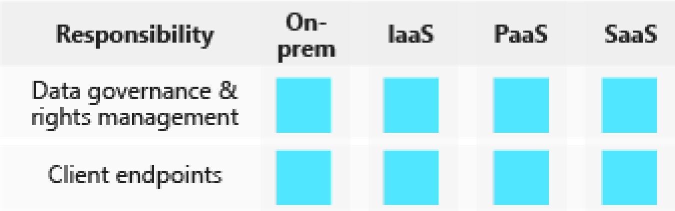
At each layer, there are some common attacks that you will want to protect against. These are not all-inclusive, but can give you an idea of how each layer can be attacked and what types of protections you may need to look at.

- **Data layer**: Exposing an encryption key or using weak encryption can leave your data

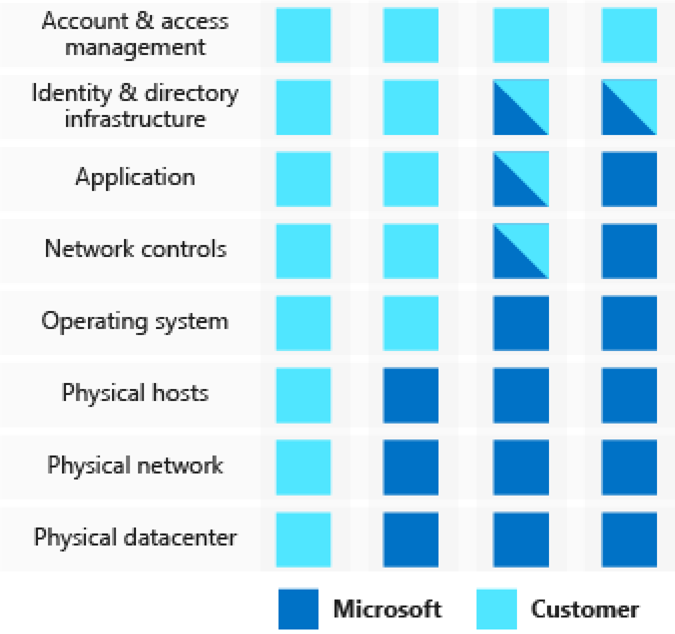
- **Data layer**: Exposing an encryption key or using weak encryption can leave your data vulnerable should unauthorized access occur.
- **Application layer**: Malicious code injection and execution are the hallmarks of application-layer attacks. Common attacks include SQL injection and cross-site scripting (XSS).
- **VM/compute layer**: Malware is a common method of attacking an environment, which involves executing malicious code to compromise a system. Once malware is present on a system, further attacks leading to credential exposure and lateral movement throughout the environment can occur.
- **Networking layer**: Unnecessary open ports to the Internet are a common method of attack. These could include leaving SSH or RDP open to virtual machines. When open, these could allow brute-force attacks against your systems as attackers attempt to gain access.
- **Perimeter layer**: Denial-of-service (DoS) attacks are often seen at this layer. These attacks attempt to overwhelm network resources, forcing them to go offline or making them incapable of responding to legitimate requests.
- **Policies & access layer**: This is where authentication occurs for your application. This could include modern authentication protocols such as OpenID Connect, OAuth, or Kerberos-based authentication such as Active Directory. Exposed credentials are a risk here and it's important to limit the permissions of identities. We also want to have monitoring in place to look for possible compromised accounts, such as logins coming from unusual places.
- **Physical layer**: Unauthorized access to facilities through methods such as door drafting and theft of security badges can be seen at this layer.

Shared security responsibility

Revisiting the model of shared responsibility, we can reframe this in the context of security. Depending on the type of service you select, some security protections will be built in to the service, while others will remain your responsibility. Careful evaluation of the services and technologies you select will be necessary, to ensure you are providing the proper security controls for your architecture.



Responsibility	On-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

Check your knowledge

1. Which of the following types of data may need to have security protections?

○ Customer data that contains personal information

○ Financial data supporting business operations

○ Intellectual property

○ All of the above may need security protections ✓

All of the above may merit additional security protections.

2. Which of the following is an example of an attack you might see at the policies & access layer?

○ Exposed credentials posted online ✓

Exposed credentials are a huge risk to an organization and apply at the policies & access layer.

○ A SYN flood attack

○ Following an employee into a datacenter without presenting credentials

○ Ransomware that encrypts the disks of a virtual machine

Next: Design for performance and scalability

Continue >