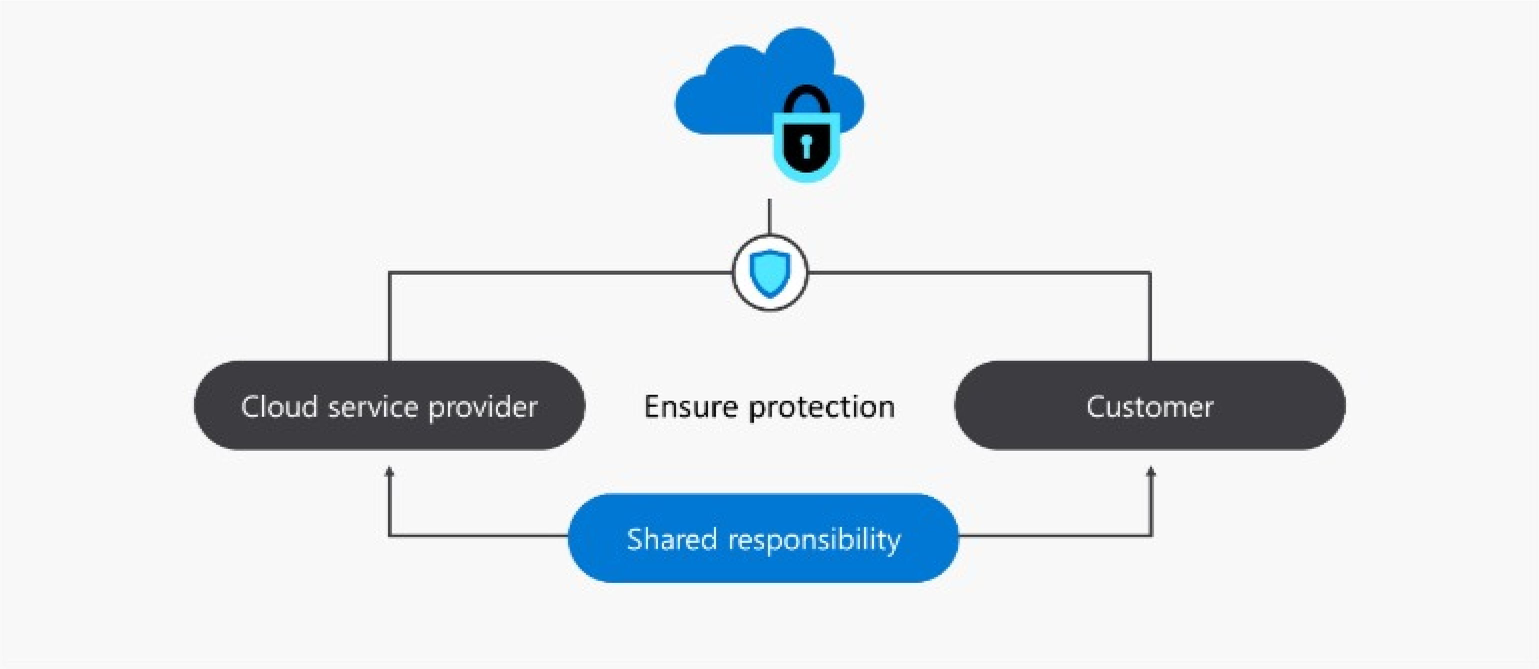
Cloud security and defense in depth

The move to cloud-based services necessitates a shift in security responsibilities, also known as the cloud responsibility matrix, with the cloud service provider and the customer playing crucial roles. It's a shared responsibility that demands cooperation and understanding to ensure comprehensive and effective protection.

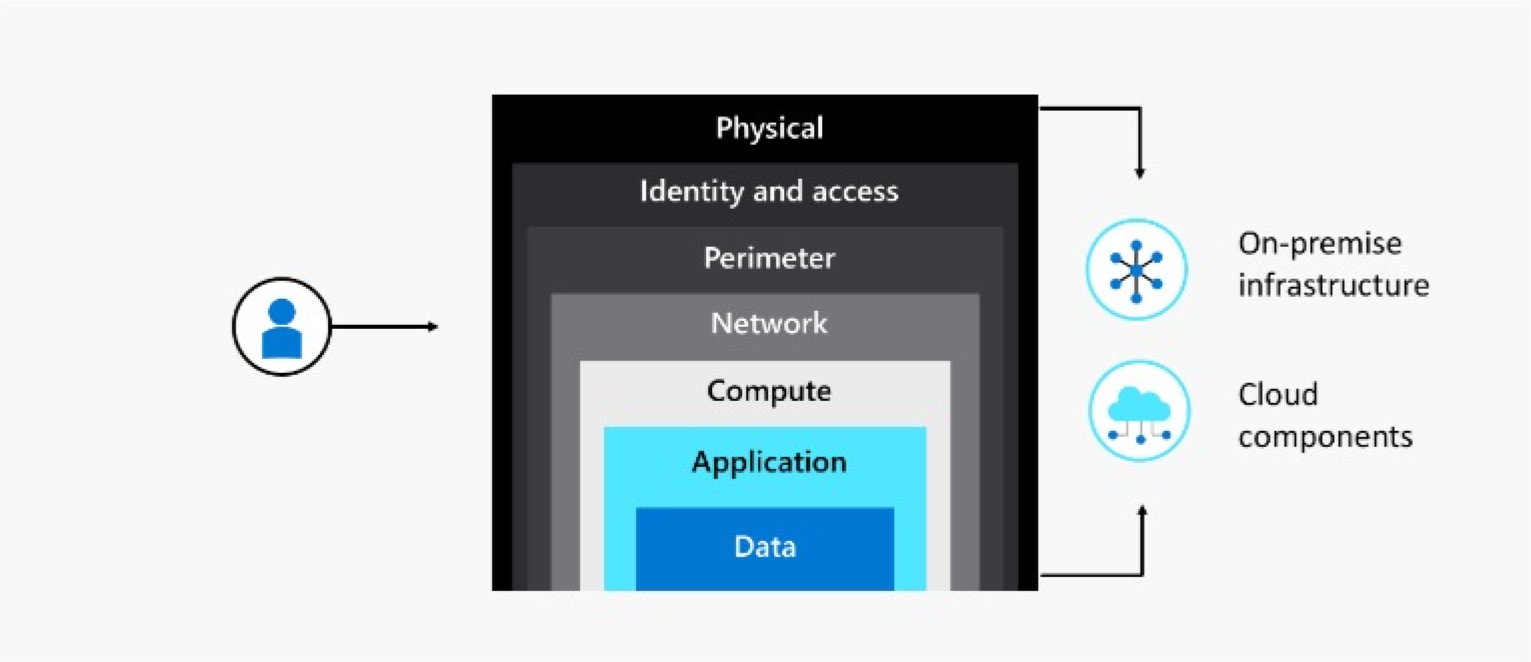


However, it's worth remembering that the security landscape is dynamic and constantly evolving. This evolution requires security strategies to adapt and improve in response to new threats and challenges. Regular monitoring, evaluation, and enhancement of security architecture are crucial to staying ahead of potential threats.

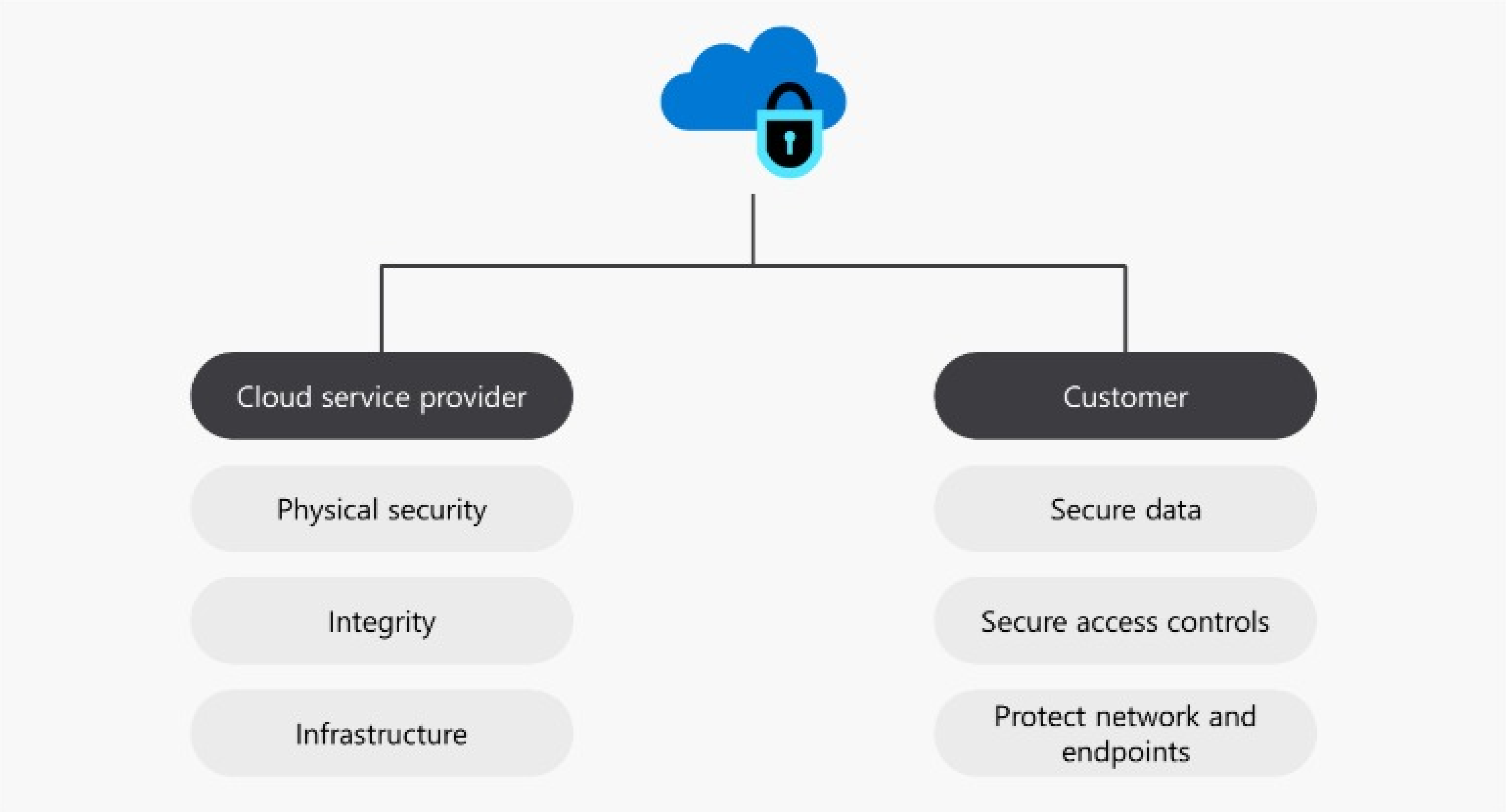
In this reading, you'll review the shift in security responsibilities when moving to cloud-based services.

Responsibilities of cloud service provider and customer

When dealing with cloud services, customers need to apply the principles of defense in depth both to their on-premises infrastructure and the cloud components. The provider may have robust security measures in place from the cloud perspective. Still, it is the responsibility of the customer to ensure that their use of the cloud services is secure and that they have implemented appropriate measures at their end.



For instance, the cloud provider may ensure the physical security of the data centers, the integrity of the network, and the underlying infrastructure. On the other hand, the customer is often responsible for securing the data they store and process in the cloud, setting up secure access controls, and protecting their own networks and endpoints.



Conclusion

When it comes to cloud-based services, both the customer and the provider have important roles to play. It's a shared responsibility to ensure security.