A layered security assumes focus solely on the origin of the threats in a category of attacks predefined in the system. For example, a Norton internet security product focus on detecting and preventing users from internet threats from certain parameters specified. On the other hand, defense in-depth takes a broader approach to network security such as forensic recovery, intrusion prevention and alarm system. Common application of layered security includes the antivirus applications, firewall application, parental control, and privacy control and anti-spam packages. On the other hand, defense in depth strategies include other security covering preparation rather than directly protective such as monitoring, alerting, and emergency response; authorized personnel activity accounting; disaster recovery; criminal activity reporting; forensic analysis.

The disadvantages of defense in depth are that implementing this strategy can be more expensive than a layered approach as many components go into it. Another disadvantage of defense in-depth is that it is difficult to Implement the three tenet of security; confidentiality, integrity and availability because increasing confidentiality makes it more difficult to implement and manage integrity in a system. Also, to many complexities in the security makes it availability difficult for users.

On the other hand, the drawback of layered security is that its simplicity can make the system more prone to attack and penetration. A layered security strategy is not as flexible as the defense in-depth strategy.