Contributions to the discussion helped to get an overview of methods capable of securing a network and to discuss the pro and cons of some of the individual solutions in detail.

To minimise the attack surface of a network, filtering traffic via firewalls was agreed to be a must have, although firewalls cannot mitigate all threats. (Ross 2008)

It was of no dispute, that antivirus (AV) software is an effective tool for intrusion detection and therefore should also be a key element of your defence strategy. Other tools are however also available here. (Ross 2008; Koret & Bachaalany 2015)

It was also mentioned that an additional element to your defence should be encryption, because if the first two measures fail, the attacker now still needs to decrypt your data, which if done right, is not economic for most attackers. (Mustafa et al 2015)

Updating systems was only touched by the discussion but was also seen as a key element of any defence strategy. (Ross 2008)

Bottom line the discussion pointed out that every technology has its pros and cons. The implementation of most security features will always be a trade of between factors such as money, security, performance, and usability. A recommendation on the ideal set up therefore cannot be given, since the best solution is very case depending. If you take firewalls for example, it can be said that large cooperation with high value assets will have a very different firewall landscape, than a home network. (Ross 2008)

The technology also does have its limitation. Although present-day signature scanning of AV software is very complex, they still cannot detect most of the unknown malware (i.e., Zero-day attacks) (Suttard & Pinto 2011). This is however not an argument to not deploy certain tools, it is rather an argument to have as many effective tools within your layered defence as economically achievable.

References:

Koret, J. Bachaalany E. (2015) *The Antivirus Hacker's Handbook*. First Edition. Indianapolis: Wiley Publishing Inc.

Ross, A. (2008) *Security Engineering: A Guide to Building Dependable Distributed Systems*. Second Edition. Indianapolis: Wiley Publishing Inc.

Suttard, D. Pinto, M. (2011) *The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws*. Second Edition. Indianapolis: Wiley Publishing Inc.

Mustafa, A.S., Mohammed, J. M. & Thajeel, A.M. (2015). *Layered Defence Approach: Towards Total Network Security*. International Journal of Computer Science and Business Informatics. 15. Available from: https://www.researchgate.net/publication/321622160_Layered_Defense_Approach_Towards_Total_Network_Security [Accessed on 20.03.2021].