You brought up some great points within your post. There is a major issue in the cyber security world with the speed at which technology is changing. These rapid changes bring forth the possibility of zero-day attacks. In particular, in environments such as the medical community, where there is a significant lack of preparedness for these attacks (Glisson et al, 2015).

For brute force attacks, account lockout after a certain number of incorrect password attempts is very effective in stopping them. It should be noted though, that as shown in an OWASP article, this can cause other problems. The biggest problem is that users who need to access a device or system could also be locked out (Sheridan, 2021). In a medical environment, this could be particularly disastrous. However, for training material, such as a mannequin it could be a possible solution since the consequences aren’t physically harmful. However, combined with other solutions such as IP address filtering and zero trust architecture, it could be successful in protecting against both brute force and Dos attacks (Rose et al, 2020) Overall, being such a complex and high-risk environment, the most secure system is necessary, Given the varying medical environments, certain technologies may be more necessary than others.

References:

Glisson, W., Andel, T., McDonald, T., Jacobs, M., Campbell, M. & Mayr, J. (2015) [Compromising a Medical Mannequin**.**](https://aisel.aisnet.org/amcis2015/HealthIS/GeneralPresentations/5/) Healthcare Information Systems and Technology (Sighealth).

Rose, S., Borchert, O., Mitchell, S., Connelly, S. (2020) *Zero Trust Architecture.* Available from: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf> [Accessed 20 November 2021].

Sheridan, E.(2021) Blocking Brute Force Attacks.Available from: [**https://owasp.org/www-community/controls/Blocking\_Brute\_Force\_Attacks#**](https://owasp.org/www-community/controls/Blocking_Brute_Force_Attacks) [Accessed 20 November 2021].