Recommendations and potential mitigations:

1st priority. Brute Force attack: A passwordless MFA solution can mitigate the Brute Force attack completely. Microsoft (2021) able to deploy a passwordless MFA solution with Windows Hello; the Microsoft or Google authenticator can do the 2nd sign in with a mobile phone; and FIDCO2 security keys can be the last authentication. No more password is involved during the authentication process.

2nd priority. Wi-Fi being cracked down and hacked: A WPA2 enterprise solution can be deployed: By using RADIUS/802.1x-based authentication, which is based on 802.11i standard, with the latest AES-CCMP encryption. The Aps don't contain any authentication credential in this case: A Wireless LAN Controller and the AP will be the 802.1X authenticator, by using the LWAAP split MAC architecture, while the AAA server is the authentication server. Usually, it is the Microsoft AD Server (Cisco, 2021)

3rd priority. DDOS: A stateful firewall can mitigate the DDOS. But other specific anti-DDOS appliance, such as Checkpoint DDOS protector, by using new techniques to provide zero-day DDOS protection and SSL attack with hardware engines. It compliant to the industry standards such as PCI, HIPAA, as well as cloud security standards such as ISO 27001, ISO 27017, ISO 27018, ISO 27032 and others. (Checkpoint, 2021).

References:

Microsoft (2020) How it works: Azure AD Multi-Factor Authentication, Available at: https://docs.microsoft.com/en-GB/azure/active-directory/authentication/concept-mfa-howitworks (Accessed: 5th May 2021).

Cisco (2021) *Cisco Unified Wireless Network Architecture—Base Security Features. Enterprise Mobility 4.1 Design Guide* [Online]. Available at: *https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/emob41dg/emob41dg-wrapper/ch4_Secu.html* (Accessed: 24th May 2021).

Checkpoint (2021) *DDoS Protector,* Available at: *https://www.checkpoint.com/quantum/ddos-protector/* (Accessed: 24th May 2021).