It is a great post about controlling cyber threats, Edward. It pointed out the next-generation firewall (NGFW) and segmented by networks could mitigate the threat by the vulnerabilities and the employee abuse case commonly.

The protection of vulnerabilities in NGFW is primarily determined by the nature of the vulnerability and if it lends itself to such defence. The NSS labs test results found that there were limitations when confronted with unknown variants of known exploits (Help Net Security, 2019).

The traditional architecture design is network segmentation, partitioning services in different trusted networks with the firewall (Cisco, 2021). Network segmentation is a foundational component to mitigate data breaches and reduce risk with the different layers. However, it creates a significant security concern if malware gets past the perimeter, the infection and attack other devices inside the trusted network are uncontrollable.

For the network segmentation enhancement, John Kindervag developed the Zero Trust Network architecture in 2010 (John, 2010). The concept is to pretend all interfaces and users are untrusted, and all traffic is encrypted. Despite implementation from trust to untrust network can be painful for the existing organization and require taking the phased approach, it is much convenient and maturational to set up this architecture nowadays. Encryption is a build-in function or enabled by default on the software designed, Multi-factor Authentication has become a common practice and option in web service.

References:

Help Net Security (2019) NSS Labs test exposes weaknesses in NGFW products. Available from: https://www.helpnetsecurity.com/2019/07/19/nss-labs-2019-ngfw-group-test/ [Accessed 25 September 2021].

Cisco (2021) What Is Network Segmentation?. Available from: https://www.cisco.com/c/en/us/products/security/what-is-network-segmentation.html [Accessed 25 September 2021].

John, K. (September 17, 2010) No More Chewy Centers: Introducing The Zero Trust Model Of Information Security. *For Security & Risk Professionals*. Available from: https://media.paloaltonetworks.com/documents/Forrester-No-More-Chewy-Centers.pdf [Accessed 25 September 2021].

Edward van Biljon

<https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=274692>