WORKPLACE TRANSFORMATION, SECURITY & MAXIMIZING EMPLOYEE EXPERIENCE

WORKPLACE TRANSFORMATION AND SECURITY

What is your strategy to enable seamless & secure remote work for your employees?

In this COVID-19 Scenario, availability and security are the two most important angles. Seamless and Secured remote work from any where is the need of the hour.

Being Manufacturing conglomerate, idea of working from anywhere was very restricted to mostly for front end jobs like Sales, Marketing. Core job function being Manufacturing all the workforce is expected to work from office premise. This sudden requirement of almost everyone required to work from home (WFH) was a big challenge, but we were quickly able to ramp-up in terms of technology and capacity.

One part of the readiness, we had already deployed VPN technology with two factor authentication. While VPN gives connectivity, but on Non-company devices if login name and password is cached, it may provide a unauthorised person connection company network.

We deployed 2 Factor authentications (2FA) coupled with Microsoft Authenticator mobile App. This ensured even if login name and password is cached, unauthorized person cannot connect to company network. We used MS SCCM to quickly deploy VPN clients wherever required remotely.

Post VPN, we deployed Remote Desktop (RDP) technology on our highly scalable On-Premise Private Cloud. We ensured that all connections will get terminated on WFH RDP setup and users will connect to Intranet, ERP, HR and other resources over RDP only. RDP setup is equipped with Data Copy prevention so any other company data could not be leaked through this door.

We also have another department which work with Defense and Aviation. Their data is highly confidential and bound by Legal terms.

They have Email system which is internal to that department only. These emails cannot be even routed outside of that department. Challenge was on how to ensure that these email accounts cannot be operated from outside, at the same time email should not be leaked. Their network is also not accessible for any other department within the Company.

We created double RDP setup; Use connects to one setup RDP common for the company and another jump host to connect to that specific network. This double RDP Setup then connected to users Design Workstation, which then connects to Fileserver. User passing these two RDP lands on Design Workstation, and then only can open design file on that workstation. Person working on these files cannot copy files to home devices. This was an additional security measure deployed in the solution.

For O365 setup, these users OneDrive and Email access is also disable over internet. When users connect to RDP, and open O365 with in RDP setup, it checks for Company LAN IP. If IP is within the Local VLAN range, then only it allows to connect to O365 which is enabled with Multifactor authentication and Geo Tagging and restricts users to open email from locations other than the pre-defined location.

Wakeup on LAN (WoL) technology enabled us to power on office workstation sitting at remote location and shutdown at the end of the shift, ensuring Power consumption optimization as well as avoiding fire or short circuit due to overheating of devices kept on for 24x7.

At Firewall level, each users access is defined to ensure that users can not wonder any where on the network other than what is authorized for that person. Firewall Setup in enable to check the Hostname of the device to distinguish between company provided device and user's personal device and accordingly access is granted.

More than 5000 users connect to VPN setup and to RDP setup who needs to connect to intranet resources and other users connect to MS O365 Outlook, OneDrive & TEAMS.

This entire setup provided all the IT users could get connected to company network on the very next day of lockdown announcement without compromising Security and ensuring data Availability and Integrity.