TSPlus Advanced Security - Cloud IT/Infrastructure Default Settings

05/24/2024 8:29 am EDT

This tool should be administrated by the customer. They will have a designated IT, MSP, or Admin to login to unlock users IPs as needed in lieu of whitelisting.

Default Settings

Homeland: Allow connections from anywhere

Bruteforce: Maximum failed logon attempts from a single IP address :10

Bruteforce: Reset counters of failed logon attempts after : 2 hours

IP Addresses: 83.166.153.206, localhost private IP, localhost IPv6 IP, localhost loopback, localhost ::1

Permissions: None [Lets the company establish NTFS permissions on specific folders] This should not be offered/used

Working Hours: None [Lets the company set specific hours for allowing users to work on the server]

Secure Desktops: Not Configured [Allows the company to established prohibited actions/application access even in full desktop mode]

Endpoints: None [Allows the company to enter employee Machine names that will bypass whitelisting everytime] Not recommended as machine names can be spoofed/ non unique

Ransomware Protection: Disabled [Additional Ransomware Protection] Not required as we are using Cylance on every machine. Redundancy in this area could cause performance and unexpected issues in SO Client

Settings: Users: Not Configured [Whitelist for 1st login/sedonaasp credentials to be bypassed for TSPlus Advanced Security] Should remain empty sans the BoldGroup Admins and potentially 1 designated Admin within the company

Settings: Programs: Not Configured [Whitelist for programs in Ransomware check] Should not be used as Ransomware Protection will not be used

Settings: Advanced: Not Configured [Has information on other items such as port watching, process monitoring, firewall changes, logging, etc]