Third Wall™ – Powerful Cybersecurity Protection

OnBoarding your Clients - what you can expect

We know you strive to be the best MSP you can be for your clients, providing them world-class service and products to keep them running smoothly. They depend on your expertise and advice – and Third Wall will simplify the management and implementation of top-shelf security policies. It's inexpensive, high value, and easy to implement.

So just why do your clients need Third Wall protection? Isn't a good firewall, a powerful antivirus, and Automate patching enough? If only that were the case. Hackers, malware and data thieves don't passively sit back and say "oh well, guess I can't get past these defenses." Instead, they are continually probing, developing new viruses, finding new ways into their target environments. And where is the soft underbelly? In the realm of "Operational Cybersecurity," which is where they find weaknesses in end users, in inadequately protected protocols and entry points, and in simple lack of discipline. Third Wall gives an array of amazing tools to protect this soft underbelly, by turning good intentions into ConnectWise Automate®-enforced policies.

You can improve cybersecurity in the following ways using Third Wall:

1. Prevent data theft / loss
2. Stop phishing
3. Prevent malware / ransomware from getting in
4. Stop malware / ransomware from spreading
5. Enforce Passwords
6. Eliminate unwanted software
7. Prevent risky behavior
8. Improve auditing and logging
9. Improve productivity (which is a byproduct of ALL of Third Wall's policies)

This document will help you engage in a conversation with each of your clients about cybersecurity, and the value of truly protecting their environment in ways you couldn't easily do prior to Third Wall. We strongly suggest you do that in person, if possible, and determine the correct Third Wall settings for each client. In doing so, you will get to demonstrate your expertise in a crucial way.

There is a spreadsheet that accompanies this document, where you can record the policy settings for each client.

From a strict cybersecurity perspective, it is BEST PRACTICE to implement ALL of the policies for any given environment, but we realize that is not practical for all of your clients – which is why we made Third Wall to give you tremendous flexibility. And remember, there is not any extra charge to you for enabling additional Third Wall policies – so use them as much as you are able.

Note: Asterisk* indicates the policy will not be applied to Windows Servers

Local Built-in Account Management Policies

1. **Rename Local Administrator Account***
    a. Why this is important: hides the account from malware, which often wants to take control of the Local Admin account once it gets in.
    b. Impact on end users: None
2. **Set Local Administrator Password***
    a. Why this is important: prevents malware from taking control of the Local Admin account.
    b. Impact on end users: None
3. **Disable Local Administrator Account***
    a. Why this is important: prevents malware from taking control of the Local Admin account.
    b. Impact on end users: If Local Admin Account is required on a given computer, this will disable that functionality. Apply an Exception for those computers.
4. **Disable Local Guest Account**
    a. Why this is important: keeps malware from controlling the Local Guest Account as an access point or an avenue for spreading.
    b. Impact on end users: None. This Account is disabled by default; Third Wall monitoring ensures that it stays that way.
5. **Disallow Microsoft Accounts**
    a. Why this is important: For computers running Windows 8 or later, anyone with a Microsoft account (such as Hotmail) can log onto that computer. That can allow unauthorized access, and this policy prevents that.
    b. Impact on end users: None, unless they are allowed to logon to a company computer using personal MS credentials.

Local User Account Management

6. **Set Minimum Local Password Length***
    a. Why this is important: prevent access / theft due to easily compromised password. Required for most compliance regulations (HIPAA, PCI, etc.).
    b. Impact on end users: may have to reset password to more characters.
7. **Set Maximum Local Password Age***
    a. Why this is important: prevent access / theft due to easily compromised password. Required for most compliance regulations (HIPAA, PCI, etc.).
    b. Impact on end users: may have to reset passwords more frequently.
8. **Enforce Password Complexity***

a. Why this is important: prevent access / theft due to easily compromised password. Required for most compliance regulations (HIPAA, PCI, etc.).

    i. This setting requires characters from 3 of the following: Uppercase letters; Lowercase letters; Number; non-alphanumeric character; a Unicode character.

b. Impact on end users: may have to reset password to meet minimum complexity requirement.

9. Enforce Password Protected Screensaver

a. Why this is important: protects access to computer / data if logged-on user is away from the computer. Required for most compliance regulations (HIPAA, PCI, etc.).

b. Impact on end users: will have to log back in from locked screensaver to continue working.

10. Restrict Local Admin Tools*

a. Why this is important: malware often tries to use Local Admin Tools for spreading; most companies prefer to let end users have Local Admin privileges. This policy allows selective disabling of key privileges that, in most cases, should not be available to end users. This policy thus also has the benefit of preventing end users from malicious or inadvertent damage to their computer or the system by using these risky tools.

b. Impact on end users: they will have certain privileges denied to them. If any given end user needs access to one or more, apply Exception for that computer.

    i. Registry Editor
    ii. WinRun
    iii. Command Prompt
    iv. Powershell Script
    v. Management Console
    vi. Run as Admin
    vii. Task Manager
    viii. Control Panel

11. Enforce User Account Control Settings*

a. Why this is important: a powerful speed-bump to warn end users if something or someone is trying to modify the computer itself in potentially dangerous ways.

b. Impact on end users: they will not be able to turn off the warnings, or may be required (depending on settings) to have admin privileges to proceed.

12. Disallow Running 'setup.exe' and 'install.exe'*

a. Why this is important: prevent installation of unauthorized software that should not be on a computer.

b. Impact on end users: will deny them the ability to install software they may want or need. It will also deny running of these types of files by sys admins. Use Computer Exceptions or Location UNDO function as needed; we recommend temporary Exceptions or UNDOs, where possible.

13. Disable Windows Installer*

a. Why this is important: prevent installation of unauthorized software that should not be on a computer.

b. Impact on end users: will deny them the ability to install software they may want or need. It will also deny running of these types of files by sys admins, other than Managed MSI files (if selected). Use Computer Exceptions or Location UNDO function as needed; we recommend temporary Exceptions or UNDOs, where possible.

OS Security

14. **Disable Windows 10 Keylogger***

    a. Why this is important: prevent Microsoft from collecting keystroke and voice information.

    b. Impact on end users: none

15. **Enable Logon Message**

    a. Why this is important: provide branding opportunity and allow for legal disclaimer that any person logging on to a computer will see. Required for most compliance regulations (HIPAA, PCI, etc.).

    b. Impact on end users: They will see an extra screen on logon where they will have to click OK to continue.

16. **Enable SmartScreen***

    a. Why this is important: for Microsoft Edge and Internet Explorer users only, helps identify and avoid navigation to reported phishing and malware sites, and also helps make informed decisions about downloads.

    b. Impact on end users: If using Microsoft Edge, users may encounter warnings and / or blocked actions if detected by SmartScreen.

17. **Disable UPnP**

    a. Why this is important: prevent malware from accessing this long-exploited avenue for entry into a computer, often going right through a firewall.

    b. Impact on end users: UPnP compatible devices will no longer automatically plug-n-play.

18. **Disable Autorun (Autoplay)**

    a. Why this is important: prevent the popup box from appearing whenever an end-user inserts a disk or USB drive, removing the temptation by end users to click to allow malware (probably disguised) program from running.

    b. Impact on end users: No autoplay popup will appear; they will have to navigate to the disk or USB drive to find and select a program or file that they want to run / open.

19. **Disable .exe Running from AppData**

    a. Why this is important: malware hides deep in the AppData folder, and will launch as an .exe file under certain conditions. This prevents that.

    b. Impact on end users: none

20. **Disable Terminal Server Services**

a. Why this is important: malware is able to use RDP / Terminal Server to gain access to a computer. This prevents that. It does not impact the Terminal Client services.

b. Impact on End Users: will not be able to use RDP / Terminal Server.

Data I/O Security

21. Disable Write to Optical Media*

a. Why this is important: prevents a common and easy path for data theft.

b. Impact on end users: they will not be able to write to a DVD or CD.

22. Disable Read/Write to Optical Media*

a. Why this is important: prevents a common and easy path for data theft, and prevents embedded malware from inserting itself from a DVD or CD.

b. Impact on end users: they will have no ability to use a DVD or CD drive.

23. Enable USB Wall

a. Why this is important: prevents a common and easy path for data theft.

b. Impact on end users: they will not be able to write to a USB device for storage except for specifically registered USB storage devices. However, they will be able to use USB-connected devices such as keyboards, mouse, etc.

24. Disable Write to USB Storage Devices*

a. Why this is important: prevents a common and easy path for data theft.

b. Impact on end users: they will not be able to write to a USB device for storage. However, they will be able to use USB-connected devices such as keyboards, mouse, etc.

25. Disable Read/Write to USB Storage Devices*

a. Why this is important: prevents a common and easy path for data theft, and prevents embedded malware from inserting itself from a USB device.

b. Impact on end users: they will have no ability to use a USB drive. However, they will be able to use USB-connected devices such as keyboards, mouse, etc.

26. Disable Common Cloud Storage*

a. Why this is important: prevents a common and easy path for data theft. You can select from a list of which ones you want to disable:

i. Google Drive, OneDrive, iCloud, iDrive, Dropbox, BackBlaze, SugarSync, Box, Amazon Drive.

b. Impact on end users: they will not be able to access selected cloud storage sites. Some selections, particularly for Google, will likely impact access to other features / tools from that provider.

27. Schedule Secure Free-Space Delete

a. Why this is important: to fully overwrite (full deletion, 3 pass) all previously deleted files. Causes "deleted" files to be truly deleted. This makes storage drives less susceptible to data theft.

b. Impact on end users: They will not be able to ever recover these files, even forensically.

Application Security

28. Uninstall Blacklisted Applications*

a. Why this is important: gets rid of unwanted applications in a very timely fashion, without need for action by the Sys Admin (in most cases).

b. Impact on end users: applications that they install that are on the Automate Blacklist will be removed very shortly after they are installed, usually with silent deinstallation.

29. Prevent Public Webmail Access*

a. Why this is important: to prevent Phishing events from personal email running on work computers. You may select from a list of email programs to block. Also prevents data thieves from using personal email to email data to themselves. Also improves productivity of many end users.

i. Gmail, Yahoo, Outlook.com, Hotmail, AOL, iCloud, Windows Live, Mailbox, Mail.com, GMX Mail, Inbox.com, Zoho, Lycos, Hushmail, Yandex.

b. Impact on end users: will not be able to access selected personal / outside email. Some selections, particularly for Google, will likely impact access to other features / tools from that provider.

30. Prevent Social Media Access*

a. Why this is important: to prevent infection and Phishing from social media sites. You may select from a list of social media programs to block. Also improves productivity of many end users.

i. Facebook, YouTube, Twitter, Linkedin, Pinterest, Google+, Tumblr, Instagram, Reddit, VK, Flickr, Vine, Meetup, Snapchat, Foursquare, Periscope, Tinder, WhatsApp, Yelp, Musical.ly.

b. Impact on end users: will not be able to access selected social media sites. Some selections, particularly for Google, will likely impact access to other features / tools from that provider.

31. Disable Windows Store*

a. Why this is important: prevent download of unwanted, possibly infected, software. Will likely improve productivity for many users.

b. Impact on end users: will not be able to access Windows Store and will not be able to download apps.

32. Disable Google Play*

a. Why this is important: prevent download of unwanted, possibly infected, software. Will likely improve productivity for many users.

b. Impact on end users: will not be able to access Google Play Store and will not be able to download apps.

33. Disable Apple App Store*

a. Why this is important: prevent download of unwanted, possibly infected, software. Will likely improve productivity for many users.

b. Impact on end users: will not be able to access Apple App Store and will not be able to download apps.

34. Disable Office Macros from Internet*

a. Why this is important: prevents infection via macros embedded within an Office document – a favorite trick of malware.

b. Impact on end users: will not be able to run embedded macros they receive from outside sources (email, etc.).

35. Disable OLE in Office Documents*

a. Why this is important: prevents infection via OLE features within an Office document – an increasingly common tactic of malware.

b. Impact on end users: will not be able to use OLE features in documents they download or receive.

Protocol Security

36. Enable Windows Firewall – Workstations*

a. Why this is important: allows you to configure the local firewall to maximum impact.

b. Impact on end users: depends on what configuration you select and upload.

37. Enable Windows Firewall – Server

a. Why this is important: allows you to configure the local firewall to maximum impact.

b. Impact on end users: depends on what configuration you select and upload.

38. Disable Local LM Hash Storage

a. Why this is important: prevents storage of account password with the obsolete / weak LM Hash technique.

b. Impact on end users: none

39. Audit All NTLM Traffic

a. Why this is important: provides IT a window into current usage of NTLM, to determine if restricting NTLM is appropriate. Kerberos is the preferred authentication method, but some applications may still use NTLM.

b. Impact on end users: none

40. Disable LM NTLMv1

a. Why this is important: disables an obsolete and highly vulnerable authentication method.

b. Impact on end users: none

41. Disable NetBios

a. Why this is important: disables an interface / convention that has become vulnerable to various types of malware attacks.

b. Impact on end users: Applications and services that depend on NetBIOS over TCP/IP no longer function once NetBIOS over TCP/IP is disabled. Therefore, verify that any clients and applications no longer need NetBIOS over TCP/IP support before you disable it. If so, then no impact on end users.

42. Disable IPv6

a. Why this is important: disables a vector used by malware to enter computers / networks. Disable if not necessary in a given environment.

b. Impact on end users: test to ensure no adverse impacts on applications / communications prior to implementing. If none, then no impact on end users.

43. Disable IGMP

a. Why this is important: disables a obsolete IP multicast protocol that has shown substantial vulnerability to malware. Should be disabled if multicast is not used.

b. Impact on end users: none, if multicast not required by end users. We recommend you verify that IGMP is not used for each environment.

44. Disable SMBv1

a. Why this is important: disables an obsolete version of SMB protocol that has shown substantial vulnerability to malware. Should be disabled if not in use by legacy applications.

b. Impact on end users: check to determine if any application dependencies on SMBv1; if not, no impact to end users.

Security Monitoring & Logging

45. Log all Logon and Logoff Events

a. Why this is important: creates a locally stored log trail for user logons and logoffs, for future forensic analysis if needed.

b. Impact on end users: none

46. Enable User Logon Reporting

a. Why this is important: provides full capture and reporting capability for logon / logoff and unlock / lock events initiated by Users (not applications), by User or by Computer.

b. Impact on end users: none

47. Enhance Security Event Logging

a. Why this is important: creates a locally stored log trail of many security events that Windows does not normally capture, for future forensic analysis if needed.

b. Impact on end users: none

48. Monitor Event Log Clearing

a. Why this is important: Event Log Clearing is a strong indication that malware has embedded itself and is trying to hide its tracks, or that an end user knows how to clear the event log and is trying to hide something. Both are major red flags.

b. Impact on end users: none

49. Alert on Excessive Logon Failures

a. Why this is important: IT needs to know if an unauthorized user or program is attempting to log on to a computer, to prevent unauthorized access and brute force attempts. You may set parameters / thresholds.

b. Impact on end users: may log users off or take other action, depending on actions set during Third Wall configuration, to interrupt their access to computer / network if threshold crossed.

50. Monitor for Ransomware

a. Why this is important: to protect access to critical data and prevent ransom situations.

b. Impact on end users: may interrupt their work if a detection occurs, depending on actions set during Third Wall configuration.

51. Alert on Unencrypted Disk

a. Why this is important: Ensure knowledge if unsecured disk (BitLocker encryption only).

b. Impact on end users: none

Emergency Buttons:

1. Emergency Isolate

a. Why this is important: prevent spread of suspected malware by isolating a computer from the network and internet, except for connections to Automate server and ScreenConnect server.

b. Impact on end users: will disconnect them from the network / internet if selected.

2. Emergency Lockout

a. Why this is important: prevents unauthorized access to lost / stolen / compromised computers, until recovered.

b. Impact on end users: will lock them out if selected, and they may not be able to log back in without Sys Admin assistance. If full logoff option is selected, end users may lose unsaved data.

3. ScreenSaver Lock

a. Why this is important: prevents unauthorized access to lost / stolen / compromised computers, until recovered.

b. Impact on end users: will force them back to password-protected Screensaver – they will have to log back in to regain access. No loss of unsaved data.

4. Annihilate

a. Why this is important: prevents unauthorized access to lost / stolen / compromised computers, with no recovery possible in most cases.

b. Impact on end users: will not be able to use their computer again, all data may be lost if selected.