How to get started with Third Wall

So now you have Third Wall, and you're trying to figure out the best way to use all of that power at your fingertips. Not a bad problem to have! We have a good suggestion on how to get started.

You'll notice that, with 56 different policies to apply, some will impact end-users more than others. The ones that impact end users the least (while still providing great protection, of course!) are what we call "no-brainers." That is, you should be deploying many of these across ALL of your managed computers - right now. And, using our Profile feature, we make that easy for you to do.

How do you do that? Simply create a Profile in Third Wall with the following no-brainer policies that are appropriate for you. Once you have done that, apply the Profile and select the "All Clients" option, which will then turn these policies on at ALL of your managed Locations - just like that. Pretty slick. Then, you can customize each of your clients by setting up a separate Profile for each of them, then deploy those Profiles by single client on top of your original deployment of the no-brainers. Since Profiles are additive, this will allow you to layer your Profile deployments like this for maximum protection in minimum time.

So here is our suggested list of no-brainer policies:

1. Rename Local Administrator Account
   Why would you ever leave the name of this as default (Administrator)? Hide the name – make it harder for malware to find.

2. Disable Local Guest Account
   Nobody needs to be using Guest Account. This account, by default, is already turned off – adding Third Wall policy monitoring makes sure it stays off, and then gives you the tracking you need for audit validation.

3. Set Minimum Local Password Length
   Required by most compliance protocols. Even if your users are mostly domain accounts, you should ensure that, if and when they are on a Local account, they have password policy enforced.

4. Set Maximum Local Password Age
   Same as above!

5. Enforce Password Protected Screensaver
   Again required by most compliance protocols.

6. Restrict Local Admin Tools (Registry Editor, Powershell Script and Run as Admin)
   Whew – do you really want ANY end users having access to these tools? We thought not. You may want to restrict other options in this policy, but at the least do these three.

7. Enforce User Account Control Settings – level 3
   Give end users notification when they are about to have something modify their

computer. While a little annoying, it could save everyone a ton of trouble.

8. Disable Windows 10 Keylogger
   Need we say why?

9. Disable Autorun (Autoplay)
   No need for that box to pop up every time they insert a thumb drive or DVD. If they really want to run an executable, make them go find it. Don't let them mindlessly select a dangerous option on a popup.

10. Schedule Secure Free Space Delete
    You can select a long schedule (monthly), but don't leave "ghost" files lying around on their hard drives. Deleted files should be fully deleted – so critical data is not pilfered later.

11. Disable Windows Store
    Hmm, prevent Windows from marketing? Maybe most valuable as a productivity enhancer!

12. Disable Google Play
    Same again…

13. Disable Apple App Store
    And once more…

14. Log All Logon and Logoff Events
    Because…this is a prerequisite for the next one:

15. Enable User Logon Reporting
    Filters and stores the data needed to create Logon report (a full history of Logon / Logoff / Unlock / Lock events, by user!) and Logon dataview (now you can answer the question within seconds: "did anybody log on to a computer last night after hours?")

16. Monitor Event Log Clearing
    Unless you are doing this on a schedule, there are only two actors who would do this: a sophisticated user trying to cover tracks (what did they do?); or malware that has just buried itself, waiting to strike, and wants to cover its tracks. BIG RED FLAG!

17. Monitor for Ransomware
    Find it when it starts encrypting. Ransomware seems to find its way in – this gives you a way to see it as soon as it acts, and also gives you the ability to auto-react right from Third Wall.

So – there you have it. Seventeen policies that you can, and should, deploy today. Without them, your protection is sub-optimal. With them, you and your clients will avoid a ton of trouble.