

One Page Security Guide: Using What You Have

In many cases, you can significantly improve your security by better leveraging technology that you already have. The following points may not all apply to you, but if you are like the vast majority of businesses, many of them will.

Use Your Firewall

Firewalls are, at their heart, just special computers. The more rules you have in your firewall, the more slowly they run and the harder they are to maintain. Prune down your rules regularly. If your technical people cannot give you a business justification for each and every rule, you have a problem. Spend a few hours each month identifying and removing rules that you do not need. This will improve both your protection and your troubleshooting time.

Fully Leverage Anti-malware

Modern anti-malware solutions go far beyond the old style signature-based designs. If you have a modern system, you should configure and enable features like Intrusion Prevention, Application Control, Cloud-based Protection, Data Control / Loss Prevention, Device Control and Endpoint Firewall. If your system does not offer these features, you may wish to reallocate your budget towards a system that does.

Fully Leverage Anti-spam

Much as with antimalware, anti-spam systems have begun to evolve. If you have a modern system, look into features like Directory Harvesting Protection, Email Encryption and Outbound Controls. It is important to have protection on outgoing email as well as incoming. If your system does not offer these features, you may wish to reallocate your budget towards another system.

Restrict Admin Rights

If you have a Microsoft subscription contract, update every possible workstation to Windows 7. If not, plan to do this at license renewal time. The security in Windows 7 is much improved over earlier versions. In the meantime, protect your legacy XP systems by removing administrative rights from every user that you can. This one step can often make the difference between minor annoyances and business-wide malware infections.

Patch Your Systems

You should already be familiar with the fact that all systems should be patched regularly. Microsoft systems require minimal monthly patching and other software and systems will require it weekly to quarterly. If you have a patch management system, use it. If you do not, at least check every system on a monthly basis and make sure that all operating system (Windows...) and application (Adobe, Java...) patches are applied. Network devices (switches...) should also be patched.

Shrink Your Environment

The more systems you have in your environment, the more potential areas of attack. Identify legacy systems and, if you can, eliminate them. If not, consider isolating them. If your network infrastructure supports VLANs and multiple DMZs, segment the network into different zones to make it easier to secure the network.

End User Training

An untrained user can be the weak point of any security system. All of your users should understand why restrictions are in place and the risks that the company is exposed if they attempt to work around them. While there are robust training programs available online, you can also engage in monthly or quarterly user awareness training. Using email and newsletters to get the word out is not as complete as a system that educates and verifies, but they are a whole lot better than nothing.

Replace/Add Firewall

Lastly, while not a free solution, bear in mind that firewalls do reach end-of-life. Modern firewalls that could replace your existing and aging device can include features like Web Filtering, Data Loss Prevention, Log Monitoring and Intrusion Detection and Prevention – all for a similar price as what you paid for your existing solution. When replacement time rolls around, look to other products with an eye towards maximizing security.