will be. But it is clear that the use of "white lists" will be a major part of the solution, and that one of the leaders in this movement is a vastly enhanced PC Matic.

Dave McClure • Jan. 04, 2016

The field of computer security is in disarray, leaving individuals and businesses alike largely unprotected and confused as how to fend off attacks by so-called "black hat" hackers. That's a problem for tax and accounting firms, which are required by law to safeguard the information of their clients.

Several companies are proposing solutions, but it is uncertain how successful these will be. But it is clear that the use of "white lists" will be a major part of the solution, and that one of the leaders in this movement is a vastly enhanced PC Matic.

Law enforcement officials who work against the "dark Internet" of hackers and other criminals estimate that there are thousands of organized rings of hackers who are

able to steal billions of dollars each year. The Internet is an almost ideal

- The creation of programs that contain malicious code ("malware"), such as the infamous Cryptolocker, which locks up the computer until its owner pays a ransom.

Helping firms counter these kinds of attacks are three resources — law enforcement, the cadre of computer security specialists, and the companies that produce security software and hardware, including the anti-virus companies. Unfortunately, these three are at a disadvantage themselves:

- Law enforcement is out-gunned, under-staffed and in some cases hampered by laws. When the criminal element is a government, for example, it is difficult for law enforcement in many countries to act even if they wished to. Even when this is not the case, there are too many scammers, with new persons and schemes erupting daily across the Internet.
- Computer security specialists can help, but their services are often too costly for individuals or small businesses. Moreover, while they are able to suggest best practices and perform other services, they are not able to assure protection.
- The anti-virus and computer security hardware and software companies are hampered by a whole host of problems. They are, in general, reactive rather than proactive. That is, they can't do much to protect a computer until a new virus or scheme is already loose in the environment, so they are constantly left playing catch-up.

With more than 100 major computer security hardware and software vendors, it is virtually impossible to tell whose products will best suit the needs of a specific industry, company or individual. It is clear that the days of traditional anti-virus applications and firewalls are over. Worse yet, the market has been flooded with fake anti-virus programs, and one leading company has been accusing of trying to cause competitors to misidentify harmless and necessary applications as malware.

In August of 2015, Reuters (www.reuters.com/article/2015/08/14/us-kaspersky-

into their software.

If traditional anti-virus and anti-malware programs are ineffective, how can tax and accounting protect their clients. Indeed, if the Internal Revenue Service is itself incapable of protecting that data, what chance can a small firm or solo practitioner have?

The answer may lie in the aggressive use of application and email whitelists.

Whitelists and blacklists have been a part of the computing industry from the beginning. A blacklist is a list of persons, web sites or applications that are not accessible by a computer or network. A whitelist is that group of users, web site, email domains or applications that have been approved for use on a computer or network.

Old timers will remember when whitelists and blacklists were widely used – but those memories are not good ones. Email whitelists for small businesses virtually ensured that new customers would be blocked from communicating with the firm. The firms themselves had to maintain the whitelist, which added expense and bother for the firm's IT staff. Also, if a firm used an Internet Service Provider whose other clients sent commercial pitches via email, that firm could find itself blacklisted and unable to send email. Getting off a blacklist often required a short trip to hell and back.

Today is different. While law enforcement struggles to catch up, and traditional forms of protection proving virtually worthless, security vendors – from Symantec and McAfee to Trend Micro and more — have again turned to whitelisting as a solution. They may not all do it in the same way, but they are uniformly in favor of trying application whitelisting as a critical part of a firm's security schema.

The surprising part of all of this is not that the old is new again, but rather the

threats to computer security as well as tips for Windows users..
- The web site is enhanced with features and utilities.
- The company makes some valid points about the origin of malware (generally in the same countries in which anti-malware software is developed, increasing the possibility of contamination of the anti-malware products.)
- The software generally gets positive reviews from professional evaluators, and there are numerous positive reviews on Amazon.com and from other sources to balance the bad reviews.

Of course, there are still some negatives – a high number of false positives in some tests, for example. Note that the worst of the complaints about this product, however, are 3-5 years old — long before the renovation of PC Matic. In addition, the company is unlikely to whitelist many of the freeware or obscure third-party applications some PC gurus prefer. Finally, don't waste time with utilities such as hard drive defraggers and registry cleaners, which do little to improve product performance.

On the other hand, there are few products on the market today that I would trust entirely, even the so-called market leaders.

I do like the whitelist approach PC Matic has taken. And for a solo practitioner or very small practice, PC Matic is an economical security program.

The best advice for these accounting offices is to try the security features of PC Matic with other tools we have recommended in the past, including LavaSoft's Ad-Aware free version, and SpyBot's Search-And-Destroy. At the same time, make no changes (other than critical patches and tax software updates) between January 1 and May 1 of next year.

Sponsors.