# Choosing the best enterprise malware protection for your business

**DANIEL MILLER** on December 06, 2018

|

Few things are more of a setback for your business than a security breach. Global damage from cybercrime is predicted to cost $6 trillion by 2021. Faced with these statistics, keeping your enterprise safe from cybercriminals should be a priority.

Many security breaches are the result of malware. Hence, effective enterprise anti-malware solutions are an obvious first step to securing your business against attack. Choosing the best enterprise anti malware protection from the plethora of options available may seem like a daunting task – but it doesn't have to be difficult. Here's how:

## Choosing the right security software for your business

There is no one-size-fits-all approach to choosing security software. Yet one key point is to recognize that a multilayered approach, using a combination of different types of security software, provides the best protection against the widest possible variety of cyber threats. A basic anti-virus/anti malware software program is a critical layer of endpoint protection for most businesses, but this layer alone won't provide complete protection from security threats. There are many other endpoint protection tools available, including URL filters, email encryption software and secure browsing solutions. Some vendors offer various enterprise 'security suites' that combine a core anti malware and firewall feature with built-in management tools. Whatever you choose, make sure you are covered from every angle. Don't rely on just one solution.

A good way to go about choosing software is to download a free trial and see how it works for your business, before making a final decision. Ask yourself the following questions:

- What features are included? What threats does the software protect against?
- Is performance adequate, without any slow-down or crashes?
- Is it easy for you and your employees to use?
- Can it be customized to suit your requirements?
- Is it compatible with your other software and devices?
- Is it competitively priced?
- Does the vendor provide support for setup and ongoing maintenance?

## The first layer of protection – anti malware software

The first layer of protection should consist of the best enterprise anti malware software. Common forms of malware include viruses, adware, Trojans, rootkits and ransomware. Anti-malware tools may cover some or all of these threats. It's important to check that the combination of software you choose will detect all types of threat. Often, what is called 'anti-virus' software actually detects more than just viruses. An enterprise-grade anti-malware solution should combine both anti-virus/anti malware software and management tools so you can manage the software from one central server or PC – this means you don't need to rely on your employees to keep the software up-to-date on their own machines. Many of these solutions also provide network protection tools.

The number of client machines you have may determine the type of software you need – many leading vendors offer business or enterprise anti-malware software suited for different size businesses. Licensing is generally available per user or device, allowing you to buy more licenses as needed. If your employees use their mobile devices at work, ensure the software you choose will protect those devices too.

Anti-virus and anti-malware software shouldn't slow your computers down, even during scheduled virus scans and updates. Software should be able detect the latest viruses and other forms of malware. Most enterprise malware tools use databases of known malware to identify threats. Some more advanced types of software can also identify suspicious code, enabling them to recognize new 'zero-day' threats that have not yet been added to a database. In both cases, the software should quarantine and remove potential threats.

## Filling in the gaps

Many malware threats originate from emails or web browsers. With the modern employee checking their email and browsing the web continuously throughout the day, it's vital that you have these channels covered. One of the most impactful ways to secure your organization from these threats is to isolate all web browsing from the user device, as well as the rest of the enterprise network and systems.

Remote browser isolation (RBI) solutions, such as Ericom Shield, protect your network by allowing your clients to access the web though a remote browser. This browser runs all active web code in an isolated virtual container, away from your network, while seamlessly delivering an interactive content stream to the user's local browser. Once a browsing session is over, the virtual container is destroyed, along with all web code, suspicious or otherwise. This means that if there was malware or malicious code on a website your employee visited, it will never reach your network or any of the computers in it. When using RBI, you're protected from web-based threats that often evade detection by typical anti malware software. Ericom Shield is compatible with security software from many different vendors – designed to work seamlessly with anti-malware solutions from McAfee, Check Point, Trend Micro, and others.

## It's all about those layers

Start a thorough investigation into the anti-malware solutions available to protect your business from cyber security threats. Test them carefully using the provided free trials. Remember to choose a multilayered approach, without relying on one software vendor or solution. With a basic layer of malware endpoint protection, and additional layers such as email encryption and RBI, you'll protect your business from cyber threats, wherever they come from.

Source: http://blog.ericom.com/Choosing-the-best-enterprise-malware-protection-for-your-business/