Is Antivirus Software a Waste of Money?

Companies spent more than $3 billion on antivirus last year. Were they wasting their money? *Photo: PopCultureGeek.com/Flickr*

Jeremiah Grossman is the kind of guy you'd expect to be super paranoid when it comes to computer security. He was on the front lines at Yahoo more than a decade ago when a hacker named MafiaBoy was abusing the site with DDoS attacks. Now Chief Technology Officer at security consultancy White Hat Security, Grossman spends his time fighting web intruders for his company's clients. When it comes to computer security, he's paranoid — and for good reason. He's seen what the bad guys can do. But when he met with Wired at the RSA Conference in San Francisco this week, he said something surprising: He doesn't use antivirus software.

As it turns out, many of his security-minded peers don't use it either. The reason: If someone is going to try and attack them, they're likely to use a new technique, one that most antivirus products will miss. "If you asked the average security expert whether they use antivirus or not," Grossman says "a significant proportion of them do not."

Dan Guido, the CEO of security startup Trail of Bits also doesn't use AV. Some security pros use it because they're in regulated industries, or because they work with customers who require it. "If it weren't for that," he says, "almost nobody in the security industry would run it."

It's a story we heard again and again at RSA this week. The pros are generally smart enough to avoid the things that will get them hacked — visiting malicious websites or opening documents from untrusted sources. But even if they get fooled, the odds are their antivirus software catching it are pretty low. But many of these pros also believe that antivirus isn't always that useful to the average business either.

"Ten years ago if you were to ask someone the question, 'Do you need antivirus?' the overwhelming response would be, 'Absolutely, my entire security strategy is based on endpoint antivirus,'" says Paul Carugati, a security architect with Motorola Solutions. "Today … I don't want to downplay the need for it, but it has certainly lost its effectiveness."

The problem is that most criminals are smart enough to test their attacks against popular antivirus products. There's even a free website called Virus Total that lets you see whether any of the most popular malware scanning engines will spot your Trojan program or virus. So when new attacks pop up on the internet, it's common for them to completely evade antivirus detection. Consumers and small businesses can get good antivirus software for free, but do businesses even need antivirus software?

You Do and You Don't

The short answer is: yes they do. Most companies can't just drop AV. First of all, it's a line of defense protecting employees who do the stupid things that the security experts tell us to avoid: clicking on dubious attachments, visiting untrustworthy websites. Second, companies often must have desktop security software to meet industry regulations, such as the Payment Card Industry (PCI) Data Security Standard. Those folks simply have no choice but to pay the Symantecs and McAfees of the world.

But according to some, businesses should probably spend less on antivirus and other security software. Much of the money they're spending is better spent somewhere else, such as analyzing the mountains of data logged by software on computer networks for signs of attack. "Save that money," says Andy Ellis, Chief Security Officer with Akamai, a company that helps websites deliver content on the internet. "Do your own log analysis because that is what's going to catch the problems."

White Hat's Grossman agrees. "I think we overspend on the wrong security products," he says. "Particularly antivirus. I think we overspend on firewalls and antivirus." Corporations do spend a lot of money on antivirus and firewalls. Research firm Gartner pegs the corporate desktop security software market at $3.4 billion worldwide. Consumers will spend even more — nearly $5 billion — on antivirus this year. Biggest of all, though, is the $6.5 billion firewall market.

Gartner Analyst Ruggero Contu doesn't quite buy the argument that companies are spending too much money on antivirus. According to him, the antivirus vendors have been doing a good job lately of beefing up their products and delivering new features beyond basic malware protection adding new features to encrypt files on disk and prevent data from leaking out. "Not to have malware protection would be foolish," he says.

But spending money on learning how attackers are working, and changing your business to thwart common attack techniques may be a better investment.

"We need to be smart, we need to be more agile," says Motorola's Carugati. "My biggest concern right now and one of the things we're focusing on is information sharing." That means figuring out from his peers what attacks are really happening, and working out ways to stop them.

Dan Guido describes it as going "offensive on security." Figure out who is likely to attack you — hacktivists, online banking thieves, so-called advanced persistent threat groups — and make sure that you can stop the known attacks that these people use. "You need to attack the system that they have developed to take advantage of your flaws," he says. "That's the name of the game."

Mark Patterson learned that lesson the hard way back in 2009. That's when hackers managed to install a variant of the widely used Zeus Trojan horse program on his construction company's computers and steal the username and password to his corporate bank account. Over the next eight days, the criminals moved more than half a million dollars out of his account. Some of that cash was recovered, but at the end of the day, about $345,000 went overseas and is gone forever. To make matters worse, Patterson's bank, Ocean Bank, says he's responsible for the theft. (Patterson sued; last year, a court sided with the bank, but the case is being appealed.)

Patterson said his company, Patco, had "good AV" at the time of the attack, but nevertheless it missed the password-stealing Trojan. Now, two years later, he's taken an inexpensive step that every small business should take to prevent his company from becoming victim to this type of fraud: He's told his bank give him a call before it authorizes any big money transfers. Patco still uses antivirus, but as Patterson puts it: "I think an AV is worth the investment," he says. "I just would not rely on it as my protection for those transactions."