

Advantage: you.



THE WALL STREET JOURNAL.

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers visit <http://www.djreprints.com>.

<http://www.wsj.com/articles/does-your-whole-home-need-antivirus-now-1429036789>

PERSONAL TECHNOLOGY

Does Your Whole Home Need Antivirus Now?

Bitdefender Box has the right idea about smart-home security, but it still needs work



The Bitdefender Box, shown here next to a Linksys router, monitors traffic on your network in search of dangerous software. *PHOTO: EMILY PRAPUOLENIS/THE WALL STREET JOURNAL*



By

GEOFFREY A. FOWLER

Updated April 14, 2015 2:54 p.m. ET

Lots of people spend money on a home security system. So why are we leaving more and

more of our digital property defenseless?

If you're diligent, you've kept the bad guys at bay by running antivirus software on a home PC. These days, though, we've also got phones, e-readers and smart TVs. And what about connected thermostats, security cameras and garage doors? They're all secret passageways into our living rooms.

We know these security and privacy threats lurk all over the house because good-guy hackers have found plenty. These vulnerabilities just haven't turned into major criminal targets. Yet.

A new type of Internet security product is designed to stand guard over the whole smart home full of gadgets. Rather than counting on antivirus on every device, they scan all the activity in your house for signs of trouble. If you click on a malicious link, or your thermostat starts sending a thousand emails per hour, your sentry will hoist a red flag.

These products are in their infancy, and their promise outweighs their present effectiveness. But they offer a glimpse of how home network security is going to change for all of us. And while they develop, there are steps you can take with existing home routers and security software to stay safe.





One of the first products comes from Bitdefender, a company known for excellent antivirus software. For the past week, I've been using Box, a slim, \$200 device that attaches to your Wi-Fi router to make it more security conscious. (Two startups, Itus Networks and Nodal Industries, have announced similar products. They aren't yet shipping, though, and I didn't test them.)

Box is a breakthrough idea. I just wish it worked better—especially for its price, which requires an additional \$100 annual subscription after the first year. My test Box was temperamental, sporadically giving me unhelpful alarms and likely causing my home's Internet connection to slow to a crawl several times.

It found most malware—malicious software designed to disrupt or spy on you. But its filters can't identify evil lurking in traffic that's been encrypted (locked behind a secret code) and in some other situations.

Box's premise is simplicity, but setting it up might turn off people without networking experience. An app guides you through steps that can vary depending on your gear. It required me to dig around in settings, and crashed during setup, sending me back to Square One.

Risky Business
Smart-home security risks are just beginning to emerge. Here are some ways Bitdefender's Box tries to keep your devices safe:

				
Devices:	Connected thermostats, cameras, smart-home devices	Smart TVs and game consoles	iOS and Android tablets and smartphones	Windows or Mac computers
Risk:	Mostly limited to lab studies now, but an attacker could take control or use it for nefarious purposes (like sending spam).	Devices with browsers can lead you to malware or phishing sites.	Malware, bad apps and websites that might phish for your private information.	Viruses, malware, websites that might phish for your private information.
How Box tries to help:	Monitors the data coming in and out for unusual patterns and suspected malware.	Keeps you from loading known dangerous websites.	Prevents you from visiting known bad websites when on the home network. On iOS, it gives you VPN access when away from home; prevents Android users from downloading known bad apps.	Prevents you from visiting known bad websites when on the home network; VPN access for when you are away from home; scans traffic for signatures of known viruses; installed software identifies viruses on drives, even USB sticks.

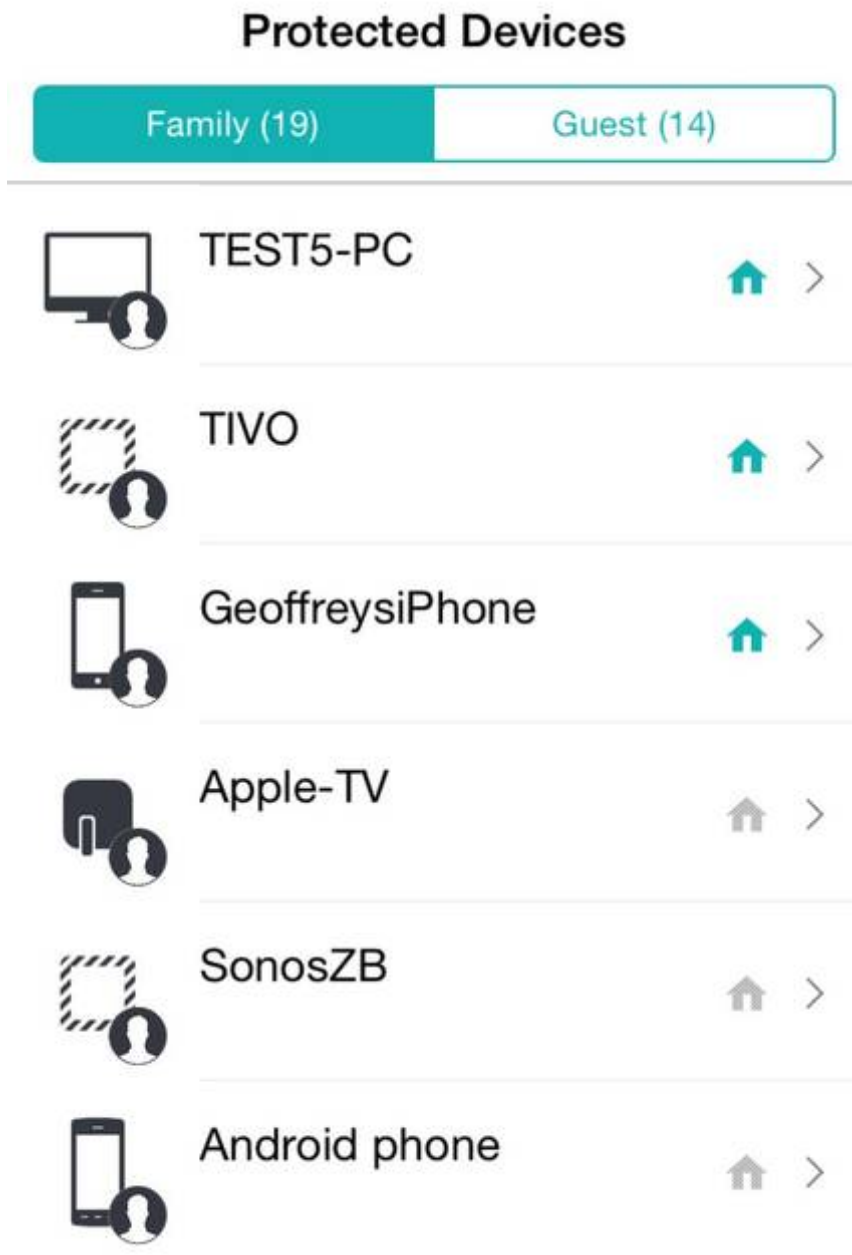
Source: Bitdefender
THE WALL STREET JOURNAL.

Once it was running, Box did some things that made me feel more secure. First, it scoured my network, producing a list of everything that's connected. There's more than you might think! One of the biggest smart-home risks today is somebody sneaking onto the network you thought was locked. (More tips on keeping it closed in a minute.)

With Box, when a new device logs in, an alert pops up on your phone. You can kick things off the network with two taps.

Box also does other things that home routers should already be able

The Box app lists all devices on your home network—even ones you don't know about. PHOTO: BITDEFENDER



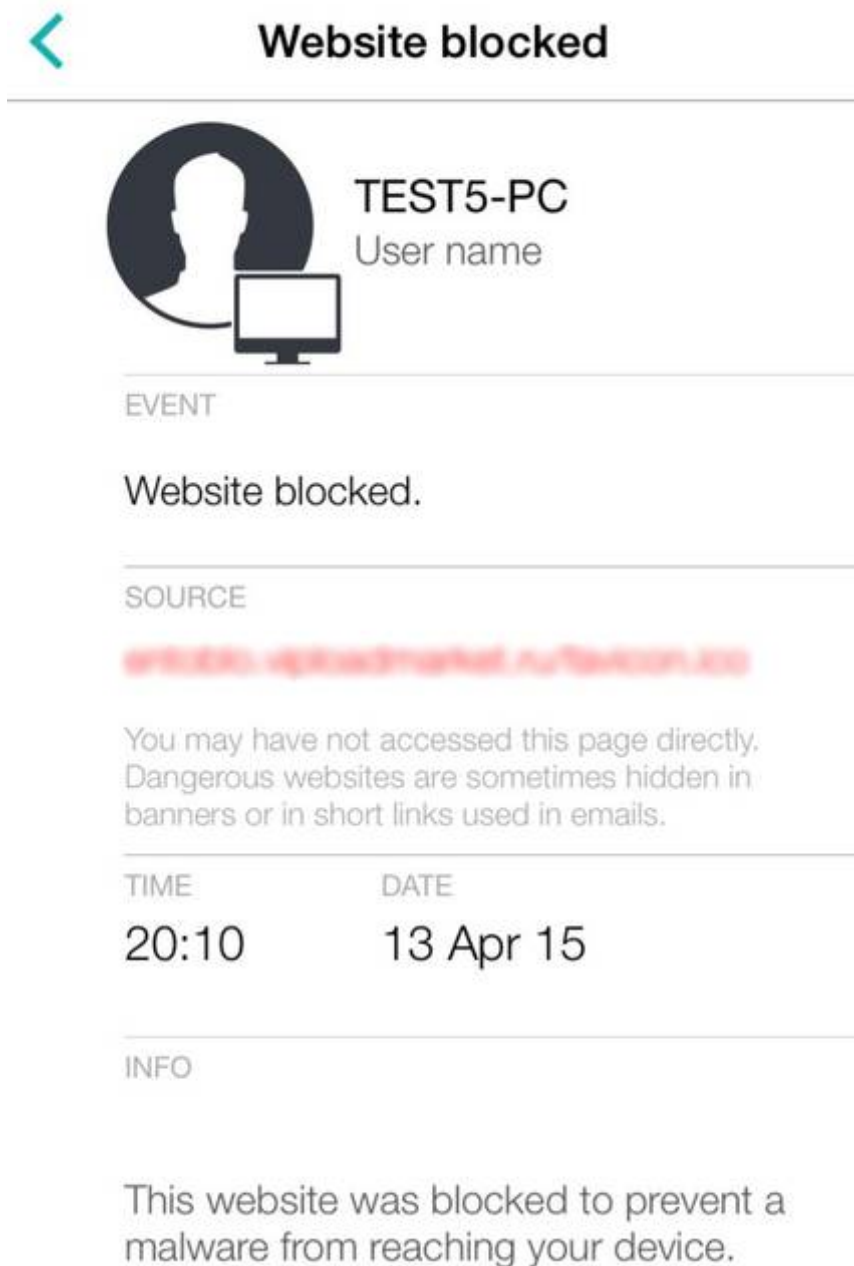
to do but don't. Most routers can stop direct inbound attacks. But Box also inspects all the data that does make it through,

comparing it against Bitdefender's ever-growing database of known threats. It also notices when devices aren't behaving as they should.


To test this, I pointed a retired laptop at some of the darker corners of the Internet, where sites push malware or try to phish for personal information. Box stopped them and alerted my phone.

If you let it, Box can install additional security software onto computers, phones and tablets. On PCs and Macs, for example, local protection software can detect a USB stick infected with malware. When you take a mobile device away from the home network, a Box system called private line lets you route traffic back through your Box—a miniature version of the VPN systems used by companies.

But Box has some work to do on its scanning system. The app alerted me to a few malware attacks that appeared to be delivered by advertising companies—but Box didn't tell me which Web page sent them.



Website blocked

 **TEST5-PC**
User name

EVENT

Website blocked.

SOURCE

[REDACTED URL]

You may have not accessed this page directly. Dangerous websites are sometimes hidden in banners or in short links used in emails.

TIME	DATE
20:10	13 Apr 15

INFO

This website was blocked to prevent a malware from reaching your device.

When any of your devices hits a known malicious website, you get a phone alert. (The URL here is obscured for reader safety.) *PHOTO: BITDEFENDER*

Box is also blind to some malware hidden in encrypted traffic. Using a zip file, the tech website Digital Trends managed to slip a virus that targets Internet security cameras past Box's filter and then install it on a camera. A Bitdefender spokesman says “no security solution available today” could have detected malware that way.

And too often, Box caused my Internet connection to become painfully slow,

particularly when I tried to stream video. A Bitdefender spokesman says that problem was likely the fault of my Internet service provider—but it didn't report any outages in my area.

What about all those still-unknown threats to connected cameras and thermostats? Box is one of the first products to at least attempt to track smart-home devices. Its makers say they'll be on high alert for malware designed to target these devices, while simultaneously gathering information about devices, so it can notify you when they start acting funny.

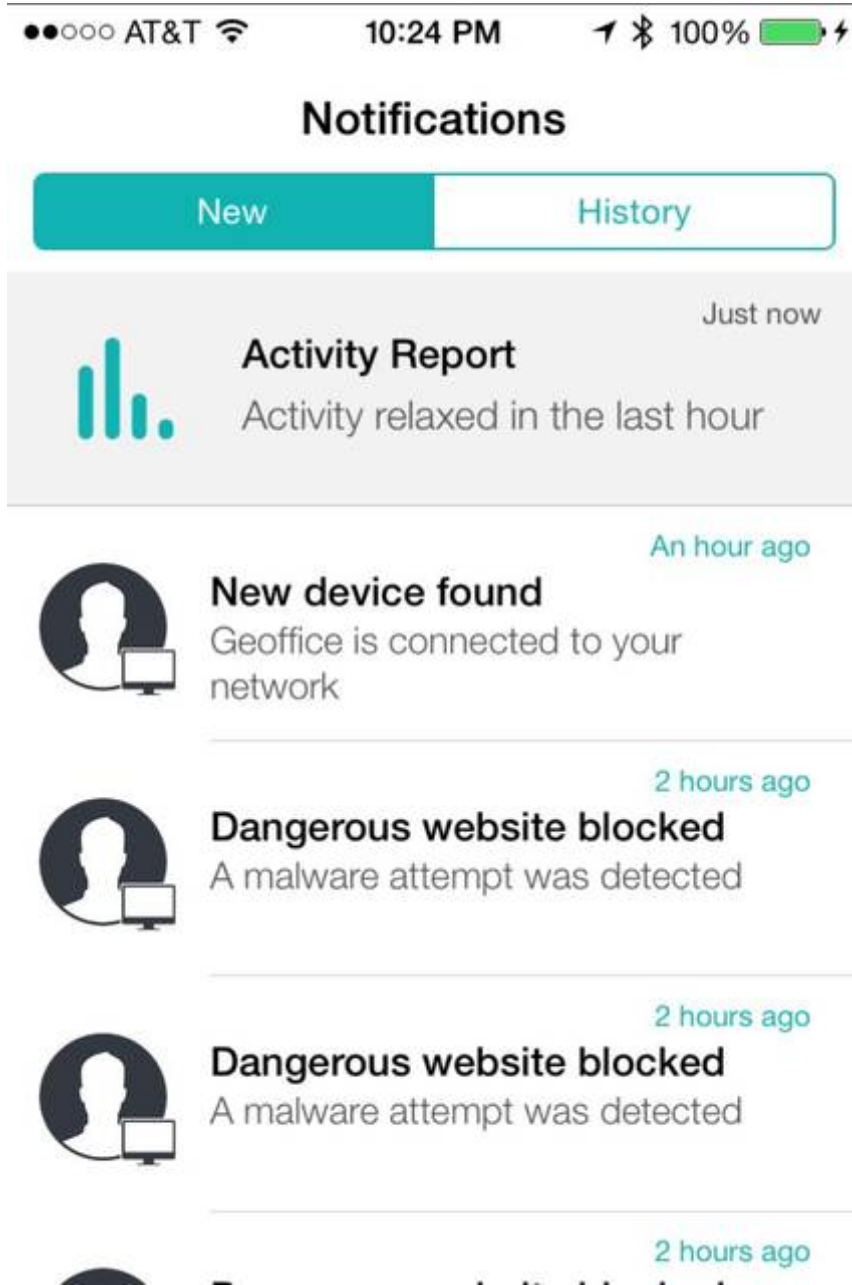
For wide-ranging attacks that might involve turning your devices into spambots, there's a chance Box could defend your device, or evolve to do it. But Box's defenses are far from 100%, security experts warn.

"The focus seems to be solely on blocking malware, as opposed to identifying when a hacker is doing nefarious things on the home network or any of the devices themselves," says Chris Eng, the vice president of research at Veracode. His security firm recently found worrying holes in a bunch of smart-home devices, none of which Box could have protected, he says.

Dan Berte, Bitdefender's vice president of design, says Box "goes leaps and bounds in protecting our most common devices," adding, "We couldn't be happier to have achieved this milestone, though we do agree it will be a bumpy ride to get things perfect."

The app provides a quick glance at all the activity on your network. *PHOTO: BITDEFENDER*

Box isn't worth it now, but I'm glad that Bitdefender is working on making home networks safer. And they're not alone: Norton antivirus maker Symantec and router maker Linksys (now owned by Belkin) say they're also working on smart-home protection.



The most important thing now is to make sure the lock on your home network is as secure as the one on your front door. Here's a checklist:

- Update the software on your router. Routers themselves have vulnerabilities, like a scary one last year called Misfortune Cookie. Many router makers fixed the problem, but you need to update your firmware—an option in your router's settings—to get the patch. The best new routers can install updates automatically.

• Use a strong password for your network—and for your router's administrative controls. It's important to use a WPA2-secured Wi-Fi network, protected by a good password. But the administrative controls for your router also need a better password than the default, which is often, terrifyingly, "admin."

- Don't give out your Wi-Fi password to friends and visitors. Instead, create a guest network with its own password. This minimizes the chances someone might, inadvertently or otherwise, give up direct access to the part of your network with your sensitive devices.

- Antivirus software still matters on your most important devices, like PCs and smartphones. Yes, Apple devices are less susceptible to the most common malware, but

if your home network's defenses are breached, you're going to want an extra wall.

Finally, amid the flurry of new kinds of connected devices it's worth taking stock of which ones are really worth the risk to you. "If it is a thing that sits on your table that you talk to and it gives answers, that means there's a microphone recording you all the time," Mr. Eng says.

If a smart-home device doesn't require a good password, that's a sign its makers don't take security seriously.

And you can try to turn off features that you don't find useful. Today, some smart TVs have the ability to listen out for voice commands on remote controls. If you don't use that feature very often, then why take on the risk of having it in your home? Turn it off, or if you can't—muffle it with tape.

Write to Geoffrey A. Fowler at Geoffrey.Fowler@wsj.com or on Twitter [@geoffreyfowler](https://twitter.com/geoffreyfowler).

Copyright 2014 Dow Jones & Company, Inc. All Rights Reserved

This copy is for your personal, non-commercial use only. Distribution and use of this material are governed by our Subscriber Agreement and by copyright law. For non-personal use or to order multiple copies, please contact Dow Jones Reprints at 1-800-843-0008 or visit www.djreprints.com.