The smart devices making the Internet of Things (IoT) can expose sensitive customer data to hackers, the Tor Project says-- and as such it would be best to hide such networking using layers of encryption and network stealth.

How does one hide such networking? Using anonymous onion services, of course, specifically in the form of the "Home Assistant." A free, open-source platform, Home Assistant runs on Raspberry Pi and other smart home hubs, and can control and network the various devices making the IoT as a Tor hidden service, the same system Tor uses to obscure the locations of servers running on the so called darknet.

The result, according to The Guardian Project, is a stealthier and more secure system for the connection of smart homes to the internet. Adding further security is Home Assistant running as an authenticated hidden service, meaning Tor intermediary computers require a passcode (or "cookie") in order to connect to the destination computer.

"Too many 'Things' in our homes, at our hospitals, in our businesses and throughout our lives are exposed to the public internet without the ability to protect their communication," the Guardian Project says. "Tor provides this, for free, with real-world hard ended, open-source software and strong, state of the art cryptography."

Tor cites a number of cases showing how prone the IoT is to hacking-- for instance, an HVAC system provided a backdoor to a national retailer, allowing attackers to reach its computer systems and customers.

Currently Home Assistant exists in prototype form, but can already be set up on customer networks.

Watch Using Tor to Securely Access to Your Home Network of Things

Go A Quick, Simple Guide to Tor and the IoT (So Far)