ISLAND

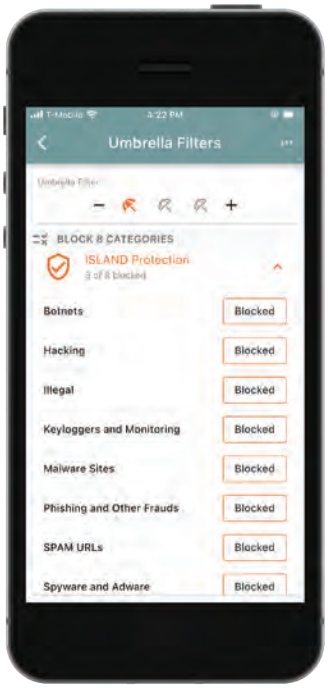
Security:
The Sum of Many Elements

Every router manufacturer touts security and privacy, but their specific means of accomplishing it are often vague. Generally, it takes a combination of factors to build a secure, private, network environment.

Toward this end, Island incorporates the following elements that contribute to security. Although some of these are ubiquitous to most routers today, they are nonetheless pillars of security worth mentioning. Some that come integrated into Island are considered add-ons by other routers, adding complication, expense, and almost always, degrading performance. It is 1) the number of and 2) the quality implementation of these elements that place Island in a unique position.

A Stateful Firewall

Not all firewalls are created the same. Island automatically includes a “stateful” firewall that monitors and detects states of all traffic on the network to track and defend based on traffic pattern-and-flow intelligence. You may not realize that Island has a firewall because, unlike most other routers, it requires no up-front configuration. It’s just there, ever vigilant from the moment Island boots up.



NAT

NAT contributes one aspect of security, enabling the use of private IP addresses that are fundamentally invisible and unreachable from outside the network.

Automated Threat Filtering

Island incorporates a best-in-class URL filtering product to protect both homes and offices. From boot-up, Island automatically prevents all devices on the network from reaching eight categories of known threat-ware. Island offers both preconfigured and customizable content filters to let the customer establish parental, guest, and employee controls.

Wholistic DNS

Island offers several options for DNS, but by default, provides DNS over HTTPS (DoH). It provides a wholistic DNS for the entire network that cannot be bypassed,* regardless of the configuration of individual devices. Importantly, it covers non-browsing, IoT devices (such as cameras, baby monitors, and thermostats) as well. Island’s DNS ensures privacy and protection from snooping and “man-in-the-middle” attacks that is not guaranteed when using other traditional DNS services, such as those of Google or of one’s ISP.

*The one exception occurs if a device has been configured to use another DoH service, as DoH itself does not permit in-transmission modifications. However, in this case, an Island filter (Proxy Avoidance and Anonymizers) listed under the category “Technical” can be set on a per-device basis that will revert all DNS requests back to Island’s DoH.

ISLAND®

Off-the-Cloud Database

Many device and service applications use the cloud to store and maintain data on activities occurring in your home or business. Island instead maintains all data pertaining to your network local to you. All inventories of your devices, user profiles, filters, network set-ups, and traffic and browsing histories live on your Island, both for performance and security reasons. It's always easier to protect your network data if it's not traversing the Internet or living on a server in the cloud.

Separately, Island's threat filtering database is also stored locally, a factor that not only improves privacy, but speed of threat detection.

Customizable Alerts and Pause

One aspect of security relates to how fast you can be notified of a potential problem, pinpoint the device in question, and respond. Island automatically sends a "red flag" alert to the app upon an attempt by any device to connect to a site considered unsafe: botnets, keyloggers, malware, spyware, and the like. Island identifies the device and with one tap, you can choose to pause its access to the Internet. In addition to the URL categories considered part of the Island protection shield, and on an "all" devices or specific-device basis, you can set up alerts based on URL visits, time on the Internet, volume of data used, or simply whether a device comes online/goes offline. Island thus allows each user to decide what constitutes a security or privacy breach in their own network and be alerted accordingly.

Easy VPN Access

Arguably the most secure means of communicating over the Internet is via VPN encrypted tunnels. While most routers can accommodate VPN clients on the network, not all of them come with Island's fast VPN functionality built in. Fewer still allow VPN access to the entire network on a per-device basis without burdening them with client software and impacting performance. Island's VPN access is granted to any user or device on a permission basis and can be scheduled for added security.

Scheduled VPN or Internet Access

Once again on a per-device basis, VPN access or Internet availability in general can be scheduled by time, day of week, or start/end dates. During time periods of known or desired inactivity, this feature can preclude access altogether.

USA

Island customers can be confident that all hardware, firmware, and software has been designed, assembled, and supported in the USA, enabling more security and oversight to the development and production process.