Harmony-IoT Remote

More companies than ever are offering the option of working from home — or even requiring it. Remote work has become part of the new normal way of working.

Remote work brings with it a number of new security issues and threats, a key one being the inability to control or ensure the security of the remote network employees use, and the prevalence of WiFi at home.

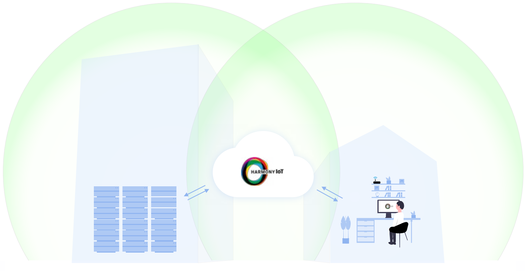
Widespread WiFi remote work opens a new organizational attack surface – employee WiFi devices and off-premise home WiFi networks. The top threats generated by off-premise WiFi usage are: misconfigured and rogue access points, home IoT, suspicious connected devices and man-in-the-middle attacks.

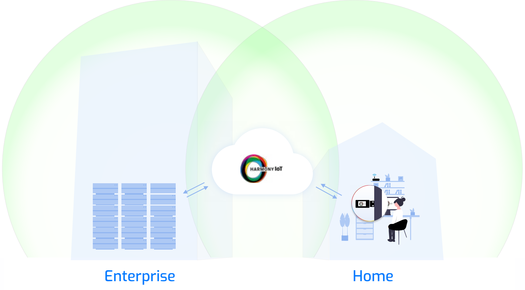
Harmony-IoT protects on premise WiFi networks. Harmony-IoT remote extends corporate on-premise wireless protection to the employee's remote work location, incorporating it into Harmony-IoT's on-premise protective shield and dashboard.

HARMONY-IOT REMOTE COMES IN MULTIPLE VERSIONS:

HARMONY-IOT
REMOTE LITE

An agent is installed on the employee's laptop or home computer. The agent executes periodic scans of the WiFi and Bluetooth neighborhood to find suspicious SSID's and unknown wireless devices connected to or around the home network. It also checks to make sure that the home access point is recognized and securely configured.





HARMONY-IOT
REMOTE CONTINUOUS

Adds a WiFi usb dongle to the employee laptop to enable continuous scanning of the WiFi neighborhood without disturbing the employee's wireless connection.

HARMONY-IOT
PATH PROTECT

Requires the installation of a Harmony virtual server in the data center or organizational cloud. Includes all of the capabilities of Harmony-IoT Remote Lite or Continuous, adding Attack Path Scenarios (APS) analyzes the corporate network for remote device attack paths. Harmony APS can also be licensed for Attack Path Scenarios for all on-premise devices.