Many deployed IoT devices have security vulnerabilities. Vulnerable devices can be used to compromise the whole network. Automatic identification and isolation of vulnerable devices mitigates such threats.

Challenges in coping with vulnerable devices
• Patches not provided by device vendors
• Missing facilities for automatic patching
• Technically unsavvy IoT device users

Solution: take a brownfield security approach – identify and isolate vulnerable devices
• Identify device-type (model + SW version) of connected device
• Link device-type to known vulnerabilities (CVE)
• Isolate and filter communications from vulnerable devices (SDN support)

Device-type identification
• Monitor traffic of newly introduced devices
• Fingerprint from device setup communications
• Random Forest + Edit distance classification

Isolation profile
• Strict: Complete isolation from rest of network
• Restricted: as in strict + restricted Internet access
• Trusted: unrestricted access