



Managing 50 Billion Things

Chris Steck

Head of Standards -IoT & Industries

Cisco Systems

csteck@cisco.com

Agenda

- Brief overview of Cisco's Key IoT Standards Initiatives (~10 min)
- Feature Presentation: Massive Onboarding (<15 min)

Cisco's Key IoT Standards Initiatives

Objective: Clear roadblocks to Enterprise & Industrial IoT deployments

- **Massive onboarding** – Drive seamless, scalable automatic onboarding and network provisioning standards, and incorporate into all of the IoT standards we participate in.
- **Security** – Provide clear guidance to **protect the things from the network and the network from the things**: What existing security mechanisms/standards should be repurposed for IoT, what's different, and drive validated solutions where IoT-specific standards are needed
- **Interoperability** - Expedite enterprise deployments by driving consolidation of IoT app frameworks, data models, interworking formats and compliance to same.
- **Device [Lifecycle] Management** – Promote & extend existing standards for FOTA/SOTA and DM (=OMA LwM2M) to maximize the devices that can be managed.
- **Network Service Exposure** - Ensure service capabilities exposed by core network APIs are comprehensive, but avoid orchestration that prevents innovation
- **Enable Next Gen IP-based IoT Networks**– Drive deterministic networking standards enabling new industrial markets for IP. Drive IP[v6] in IoT networking to leverage IT network management advances in the IoT.

Enterprise IoT vs Industrial IoT Initiatives

- Industrial IoT has existed for decades as M2M with de jure & de facto standards already in place in each vertical.
 - Convergence on common platforms began years ago, & Cisco is already there. (e.g. OPC-UA in Factory Automation)
 - Very few “IoT” led standards in CE/Smarthome space are getting traction in industrial verticals. (e.g. oneM2M, OCF have zero uptake in industrial despite attempting to address automotive, manufacturing, energy, etc.)
- Enterprise IoT = IoT in the IT domain
 - Digital Ceiling/Connected Lighting, Building Automation, Inventory Mgmt, etc.
 - Peer to peer connection/information models from Smarthome can be leveraged/enhanced for Enterprise (=Open Connectivity Foundation)
- Line between Enterprise/Industrial is blurred as IP hourglass fans out below transport
 - Thread/802.15.4, LoRaWAN, Mobile IoT (NB-IoT, LTE-M), etc.



Interoperability Goals

- Interoperability concerns cited as one of the top factors that prevent or delay IoT deployments, while customers wait for the “dust to settle”.
- **Enterprise IoT** – Drive a standard for Enterprise IoT application comm/data/resource models
 - It matters less which open standard wins, so much as there is a clear winner
 - But we feel Open Connectivity Foundation best positioned to deliver.
- **Certification** - Make sure strong certification programs exist for meaningful customer-facing logo programs & run-time cert.
- **Testbeds** -Leverage testbeds for both interop and proving grounds
 - IIC Time Sensitive Networking Testbed

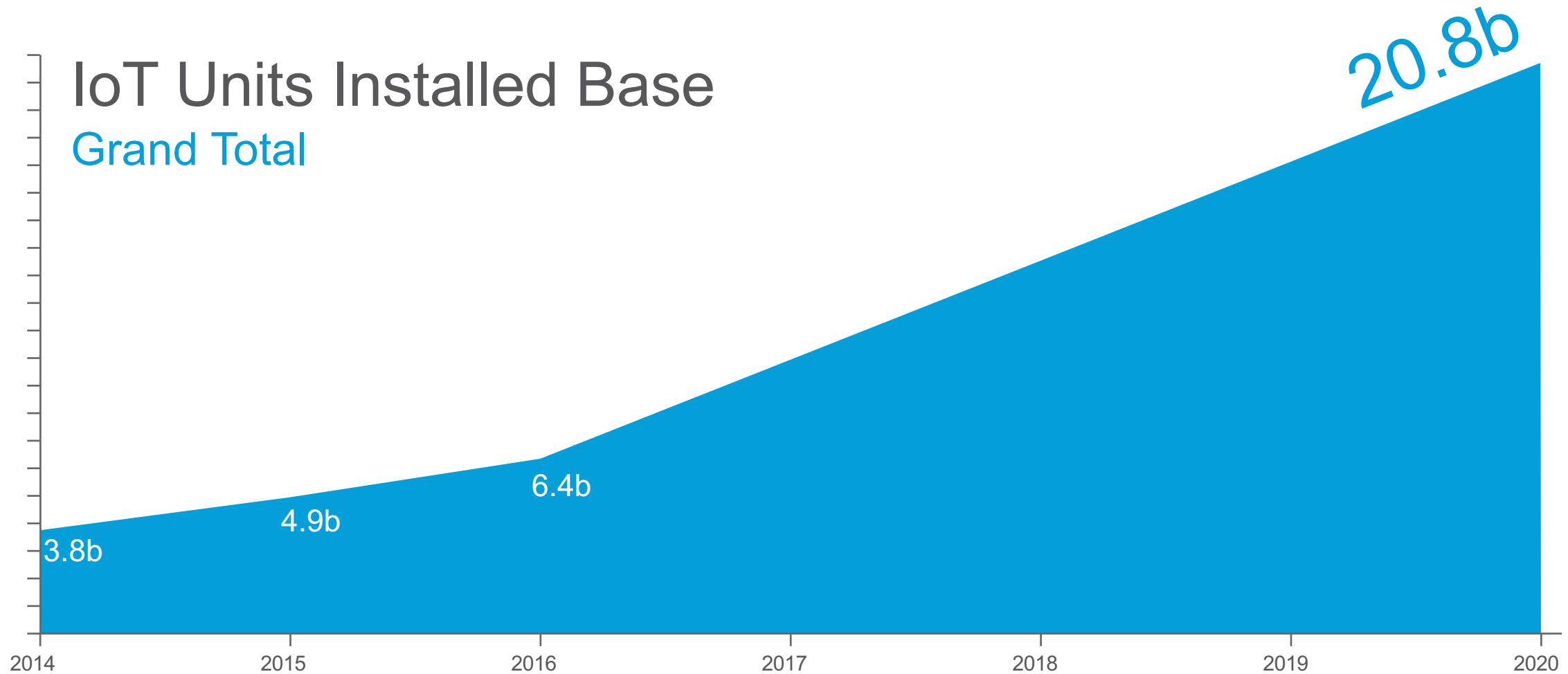
Why OCF for Enterprise IoT?



- Makes it easy for developers to deal with the complexity of IoT comms
- Provides a common data model that developers can use to interface with all IoT devices and their underlying data
- Establishes an architectural foundation that can achieve the necessary scalability
- Focuses the architecture around interoperability
- Supports the needs of multiple vertical markets (since many use cases span multiple vertical markets)
- Provides a path towards future consolidation of standards
 - OCF = (UPnP+AllSeen+OIC) + ??? (<--watch this space)
 - oneM2M & OMA LwM2M bridging
- Best positioned to move directly into Enterprise IoT after Smarthome
 - Security model forces Cloud and other Interworking through secure bridge/gateway model

Massive Onboarding

Gratuitous IoT Growth Chart



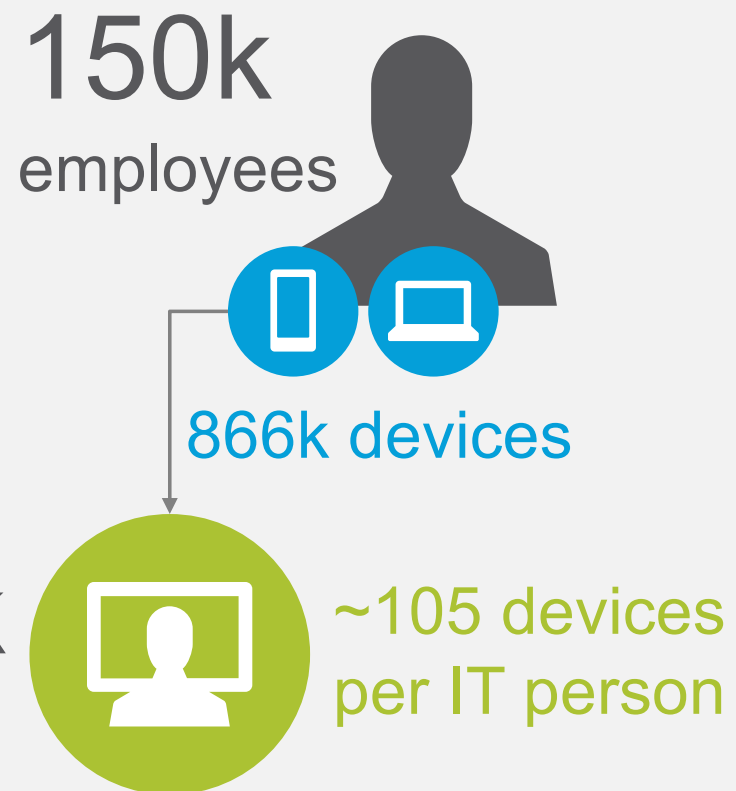
Source: Gartner, November 2015

<https://www.gartner.com/newsroom/id/3165317>

**Humans can't scale to
manage networks of
this size**

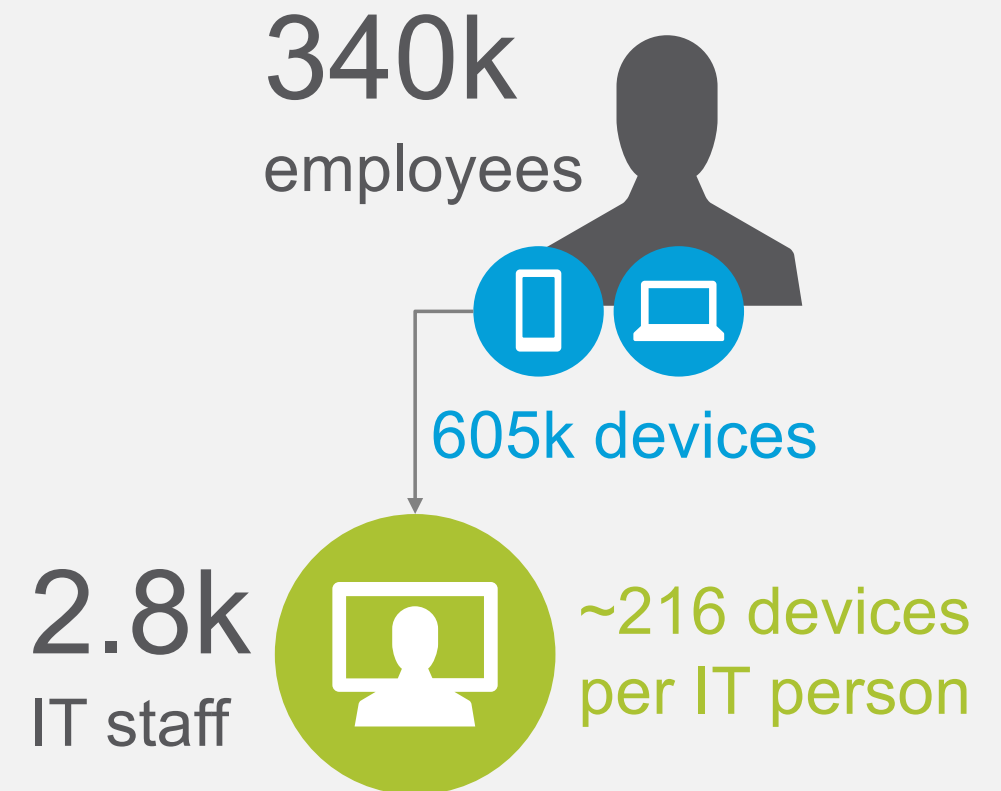
Major Bank

Today

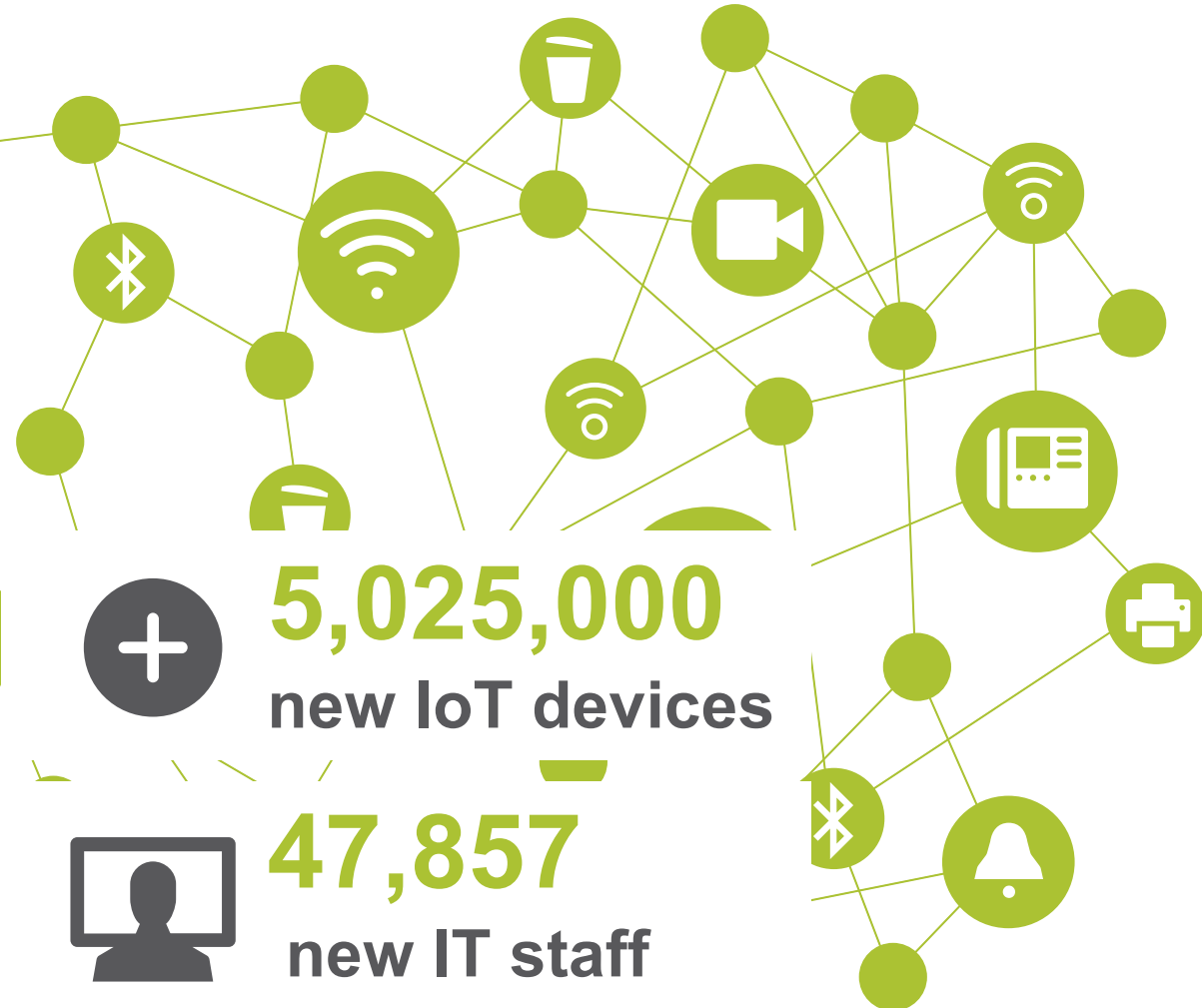


Major Retailer

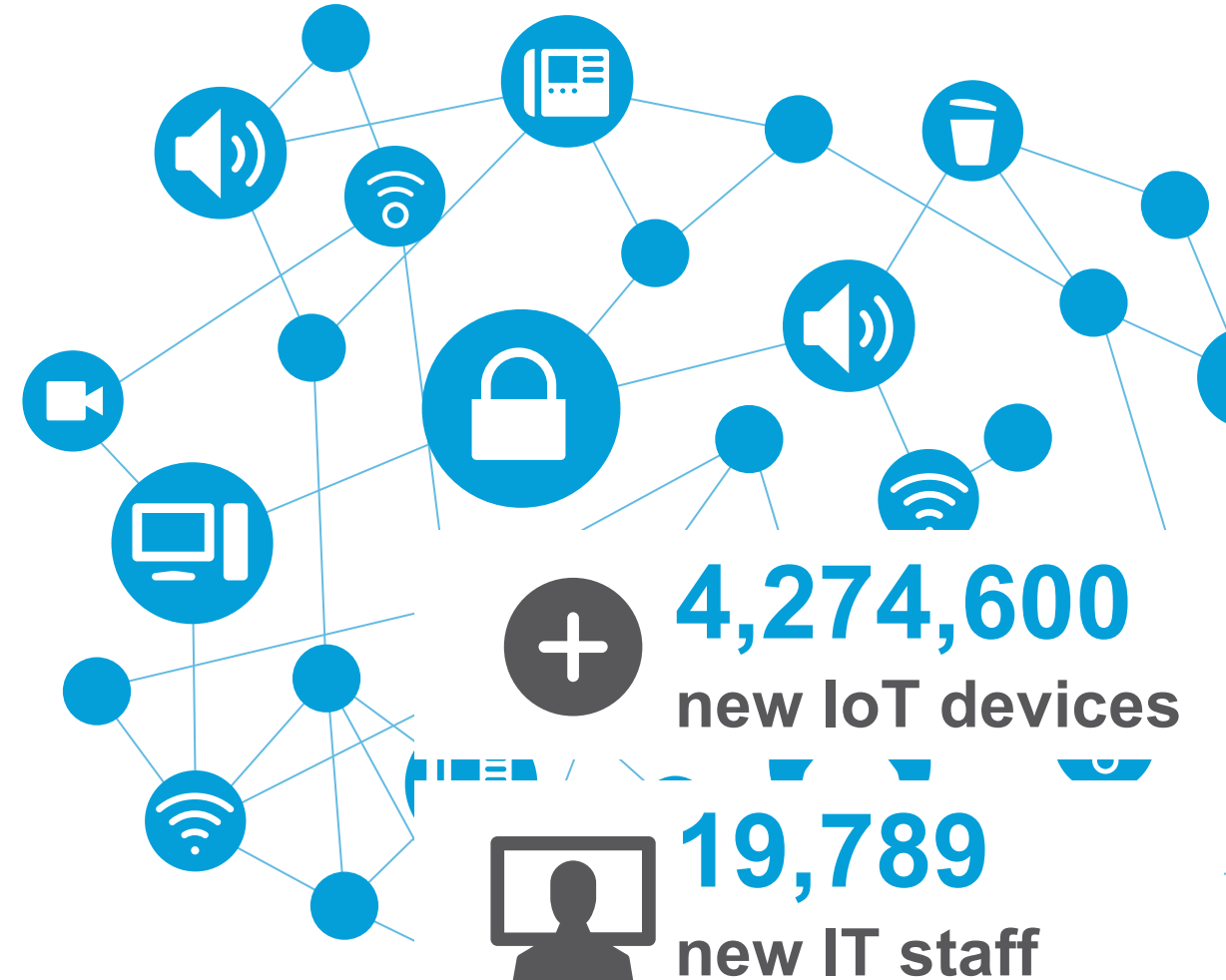
Today



Major Bank



Major Retailer

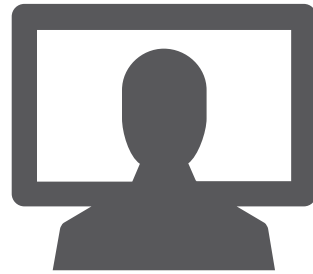


1:200



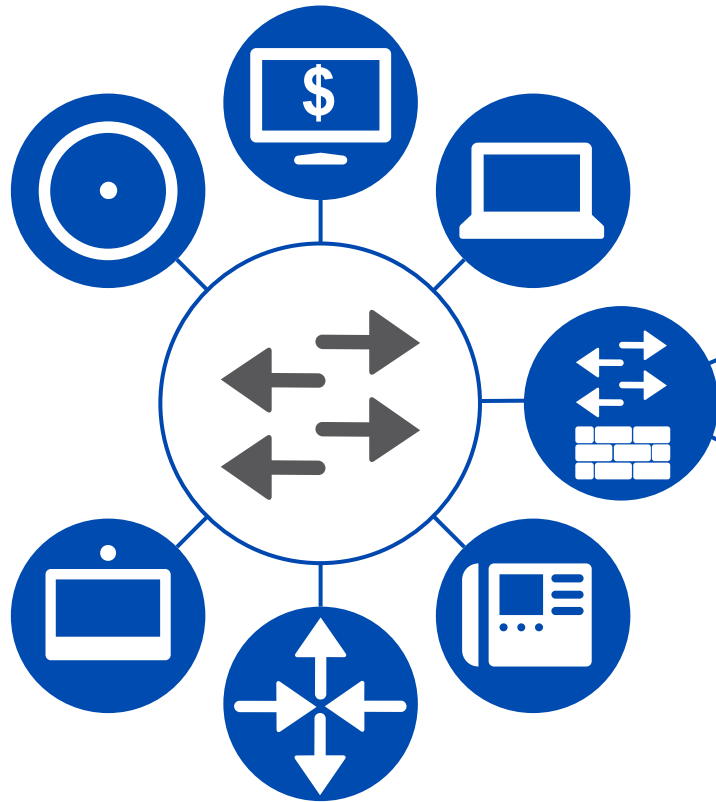
This doesn't scale.

1:1,000,000

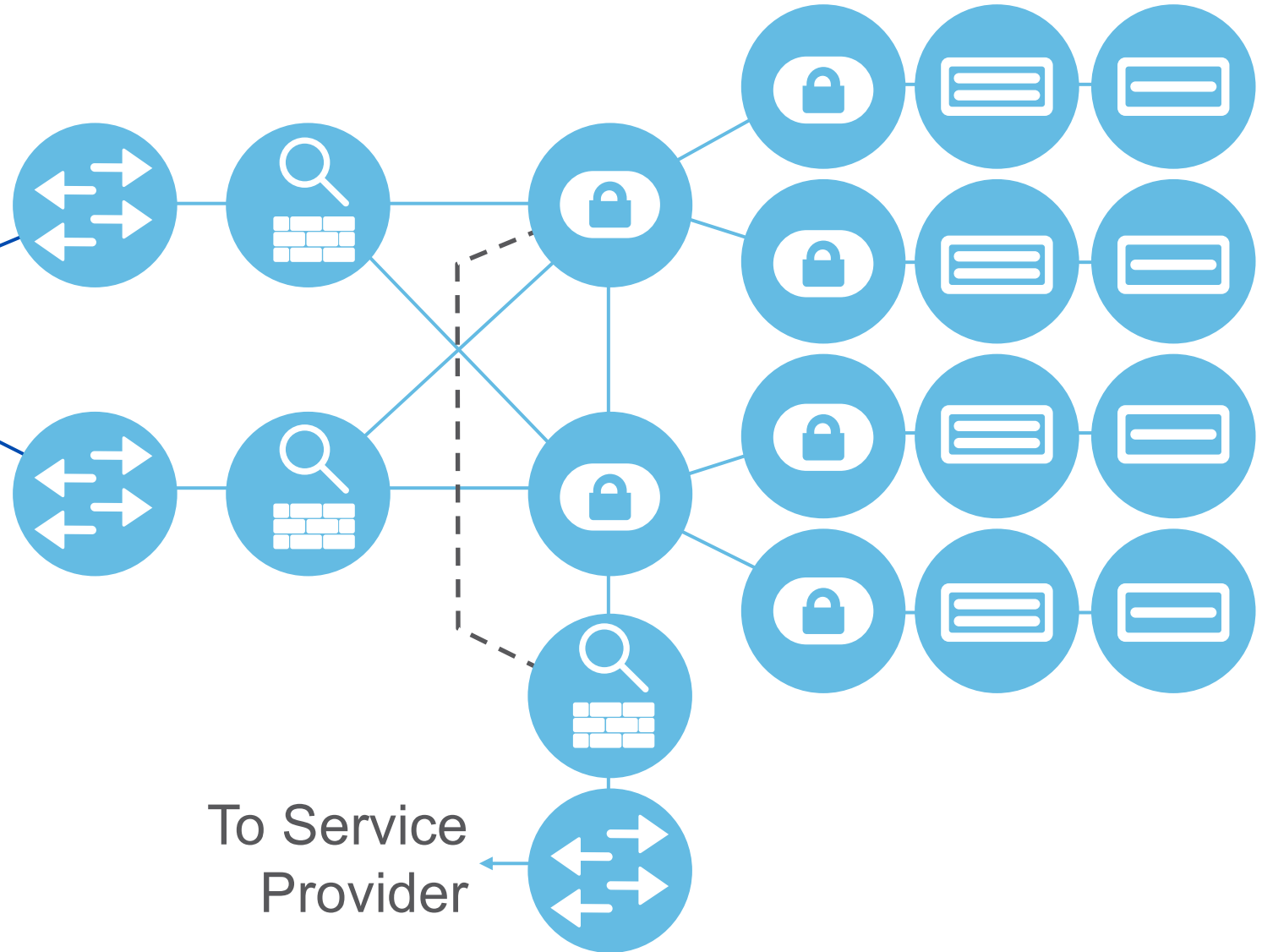


What does this future look like?

Branch

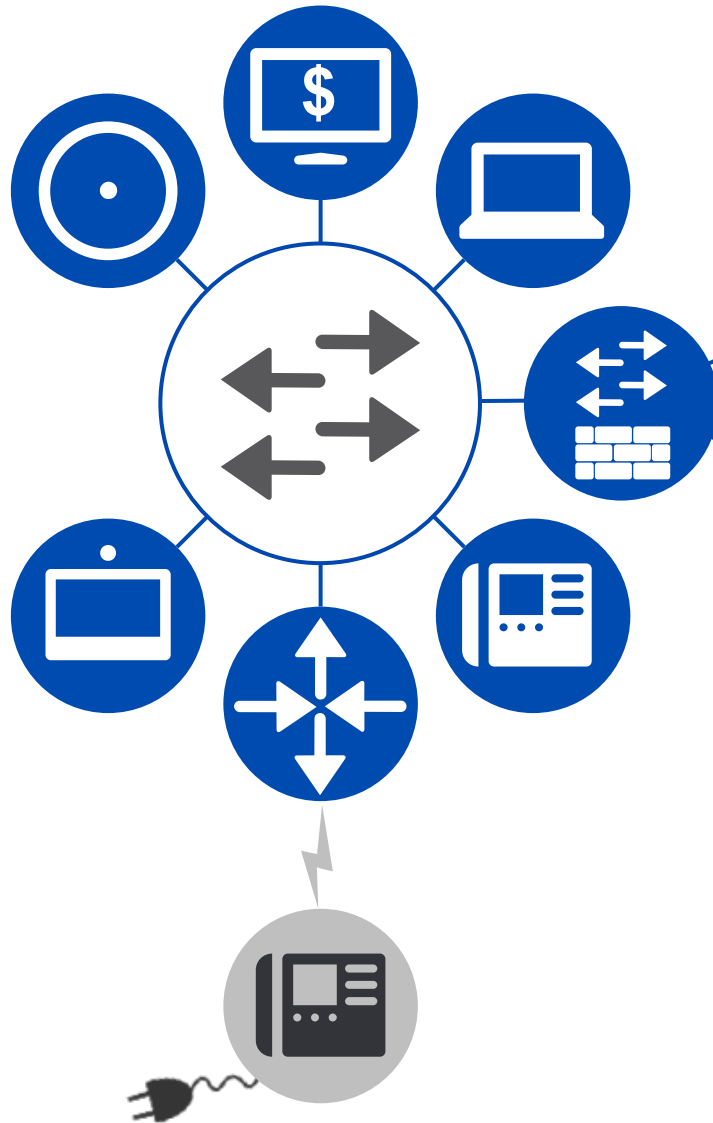


Data Center

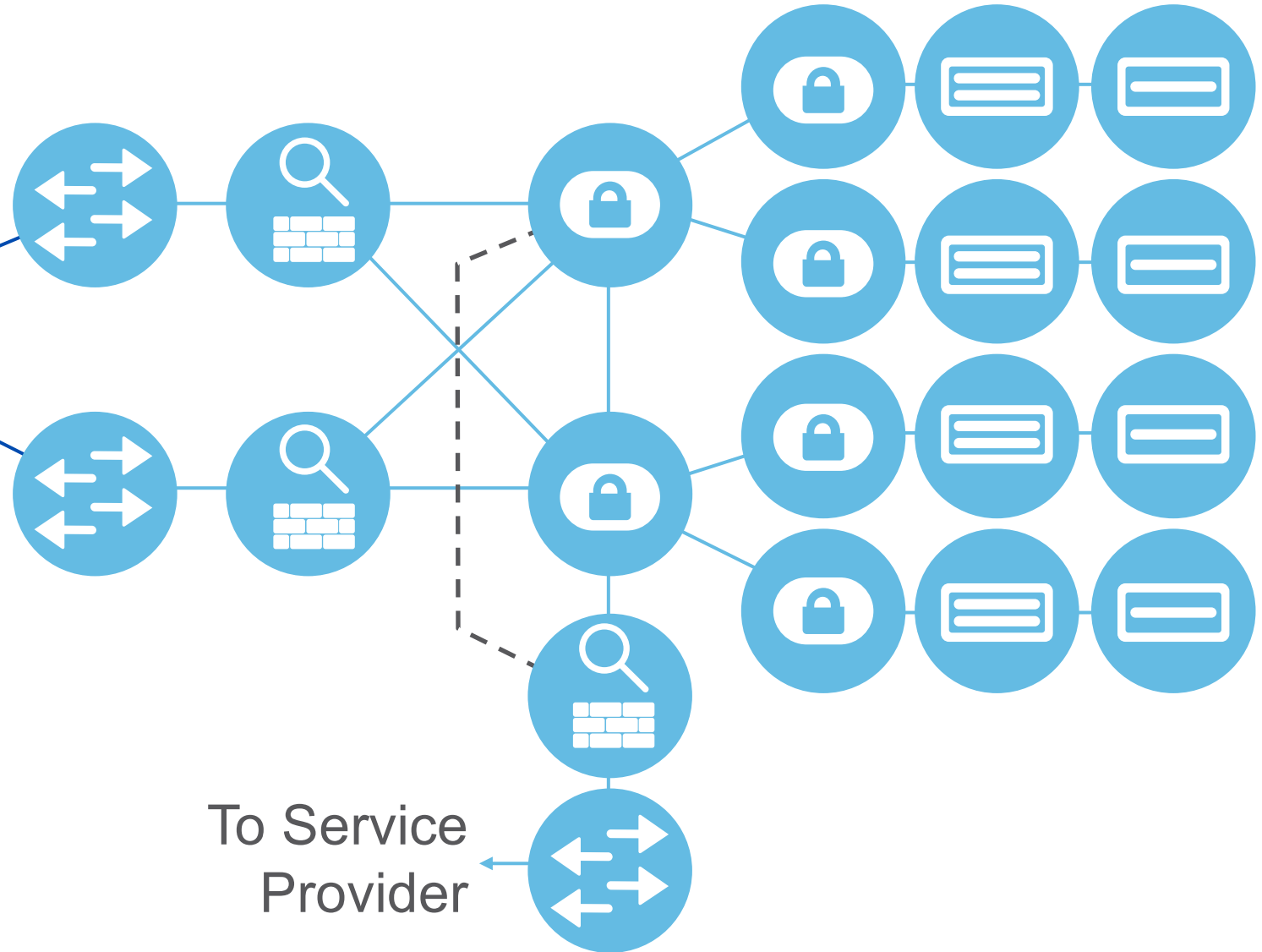


To Service
Provider

Branch

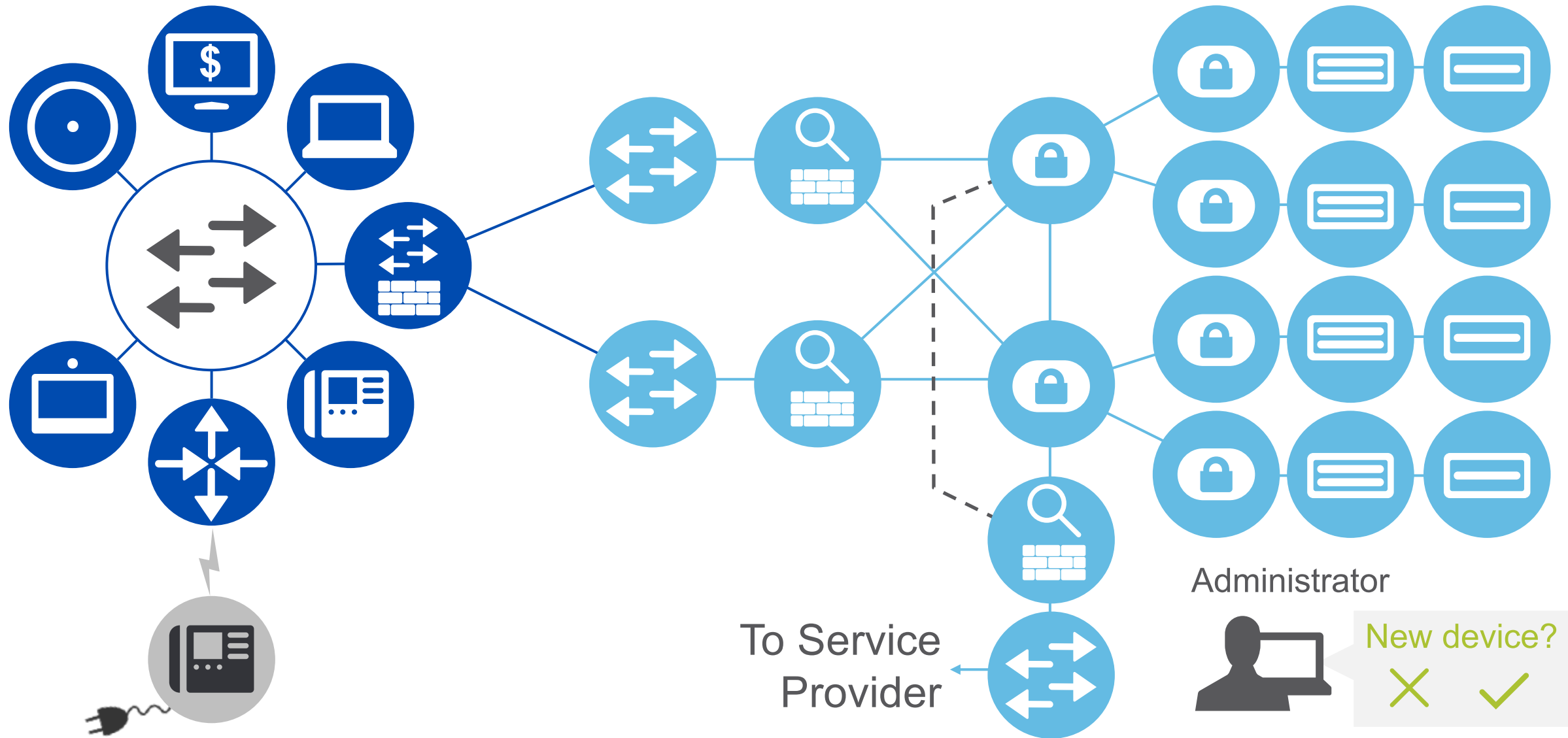


Data Center

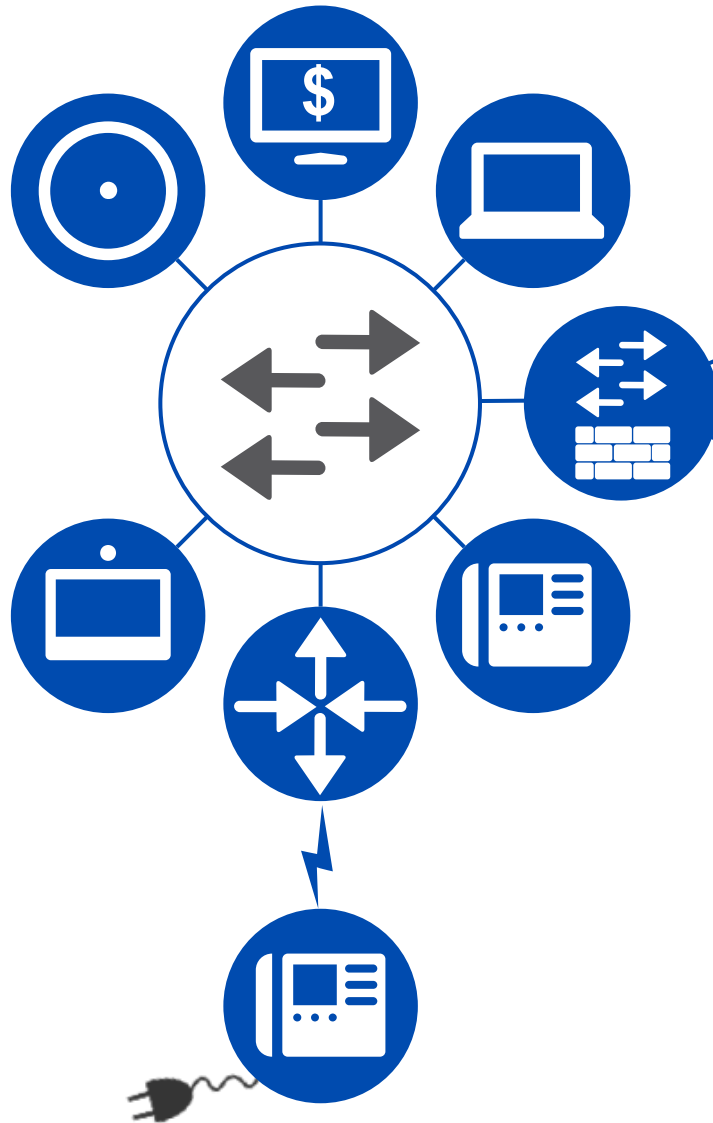


Branch

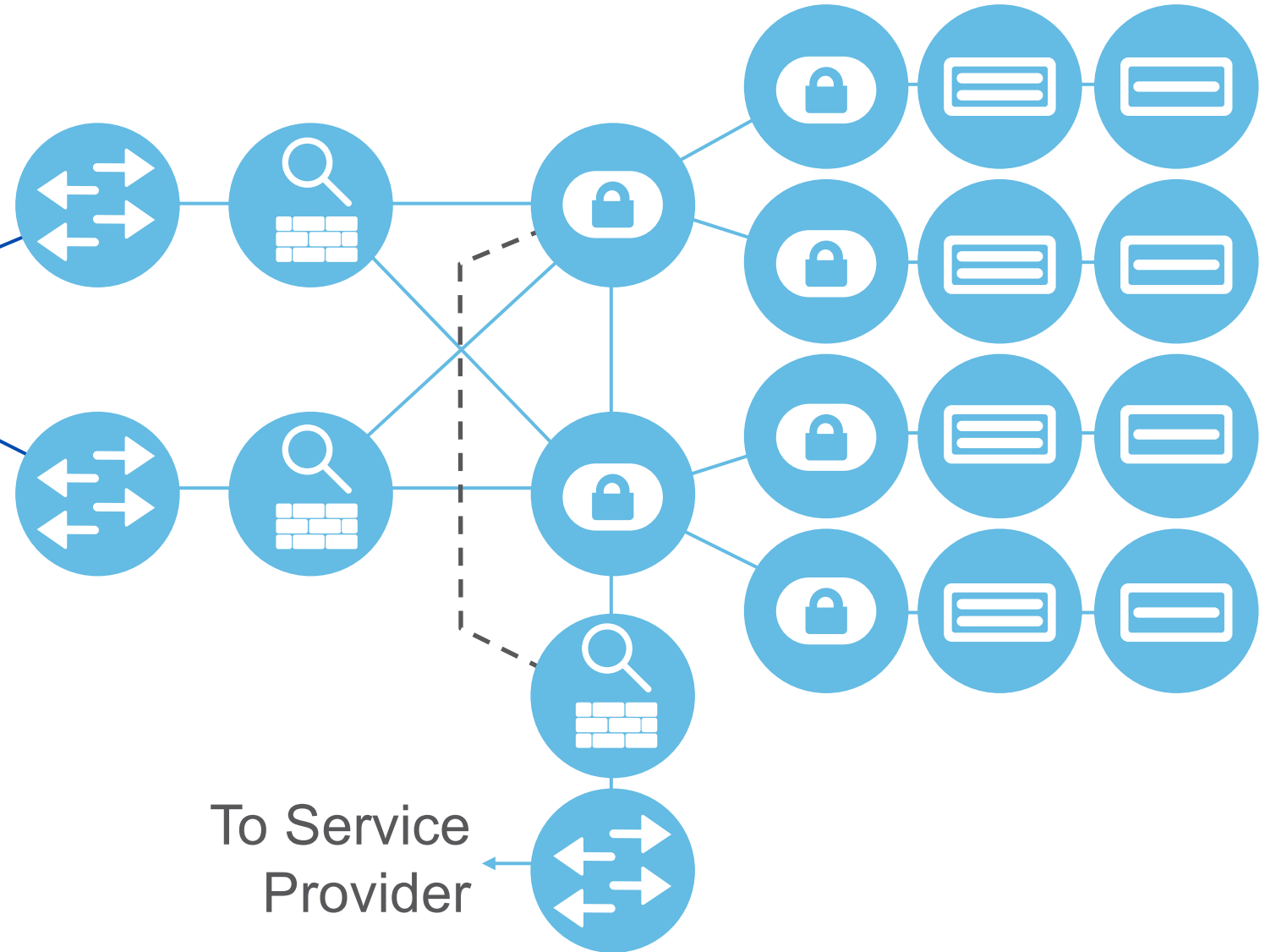
Data Center



Branch



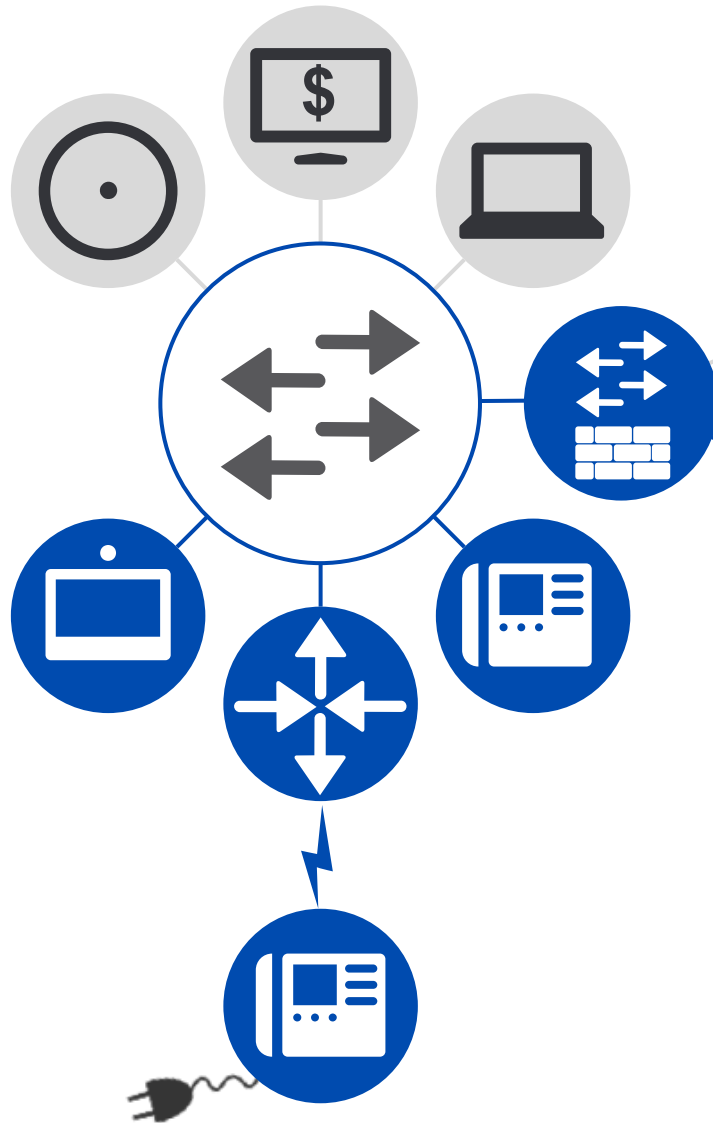
Data Center



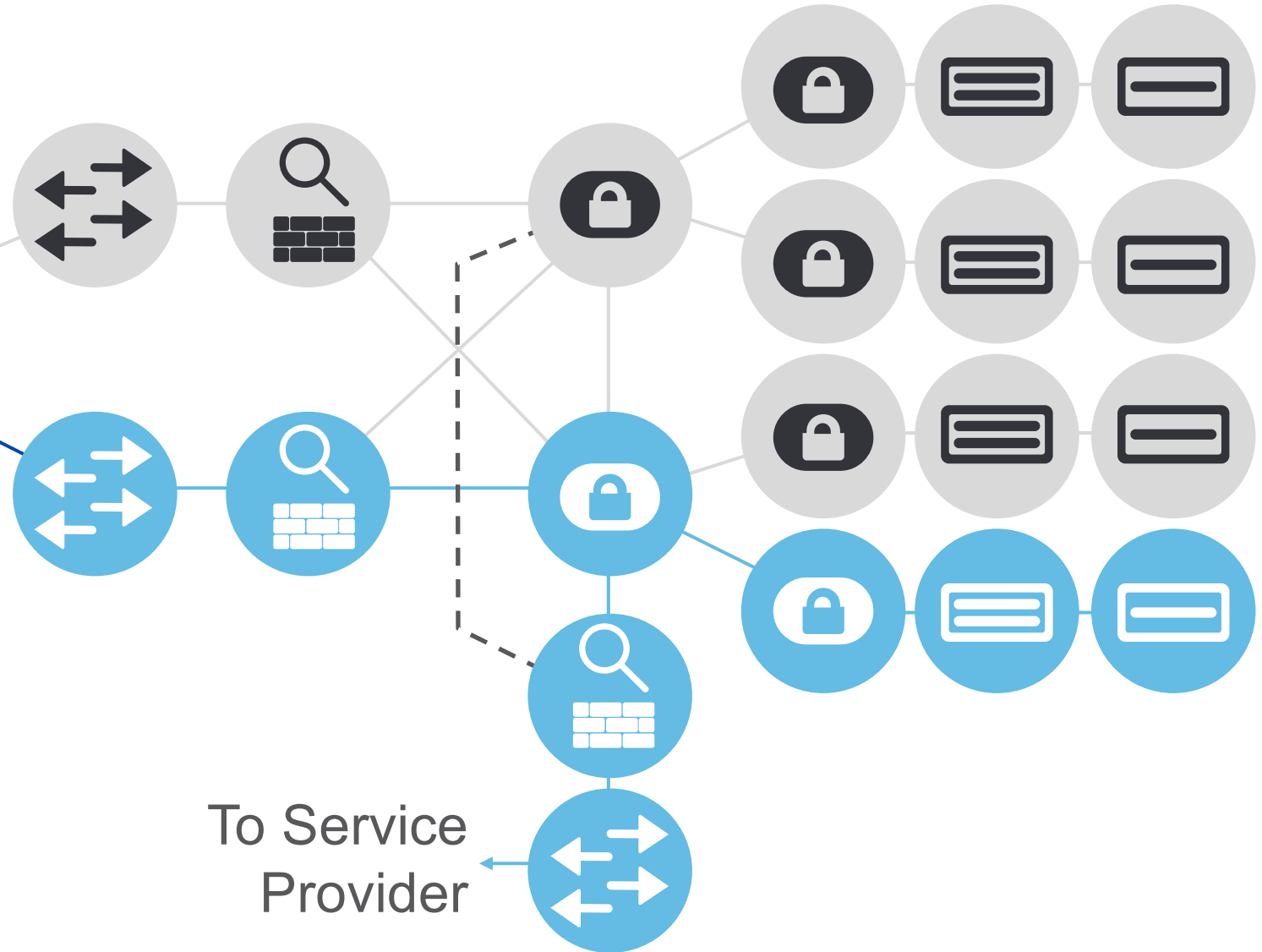
To Service
Provider

The diagram illustrates a multi-tier network architecture. On the left, there are two identical vertical stacks of three circular nodes. Each stack consists of a top node with a double-headed arrow, a middle node with a magnifying glass over a brick wall, and a bottom node with a padlock. These stacks are connected to a central column of three nodes: a top padlock node, a middle padlock node, and a bottom magnifying glass over a brick wall node. A dashed line connects the middle node of the left stacks to the middle padlock node in the central column. To the right of the central column is a 4x3 grid of circular nodes. The top two rows of this grid contain padlock nodes, while the bottom two rows contain magnifying glass over a brick wall nodes. Each node in the grid is connected to the central column nodes. At the bottom, a circular node with a double-headed arrow is connected to the bottom magnifying glass node in the central column. An arrow points from this node to the text 'To Service Provider'.

Branch

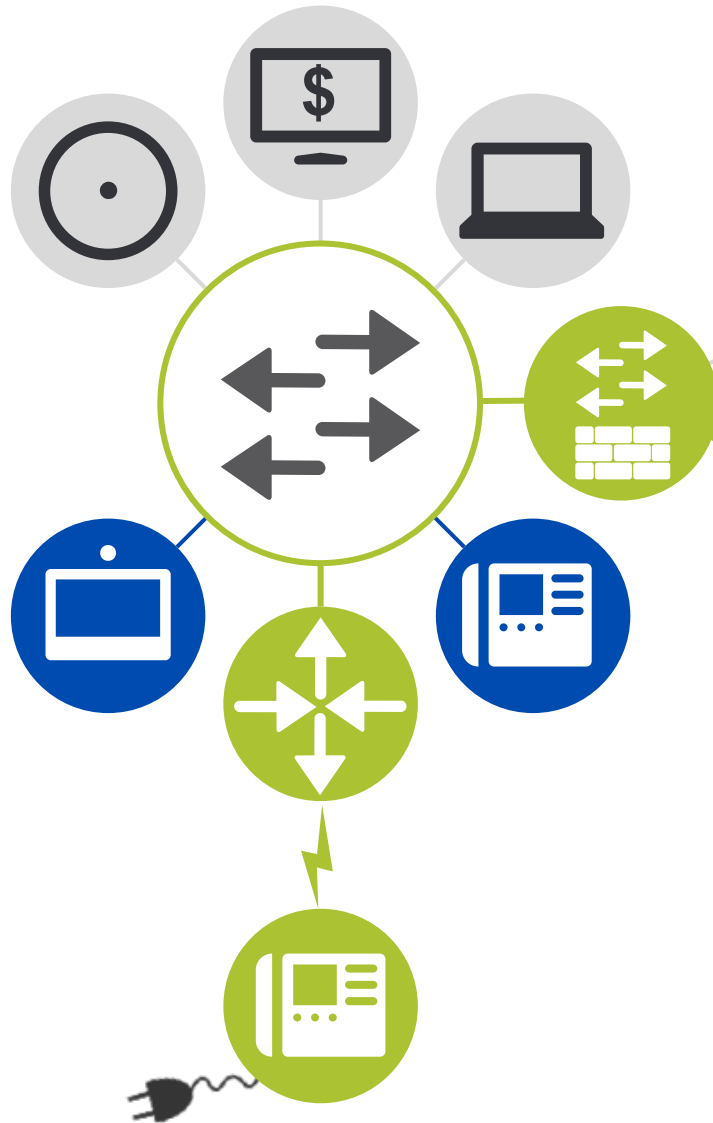


Data Center

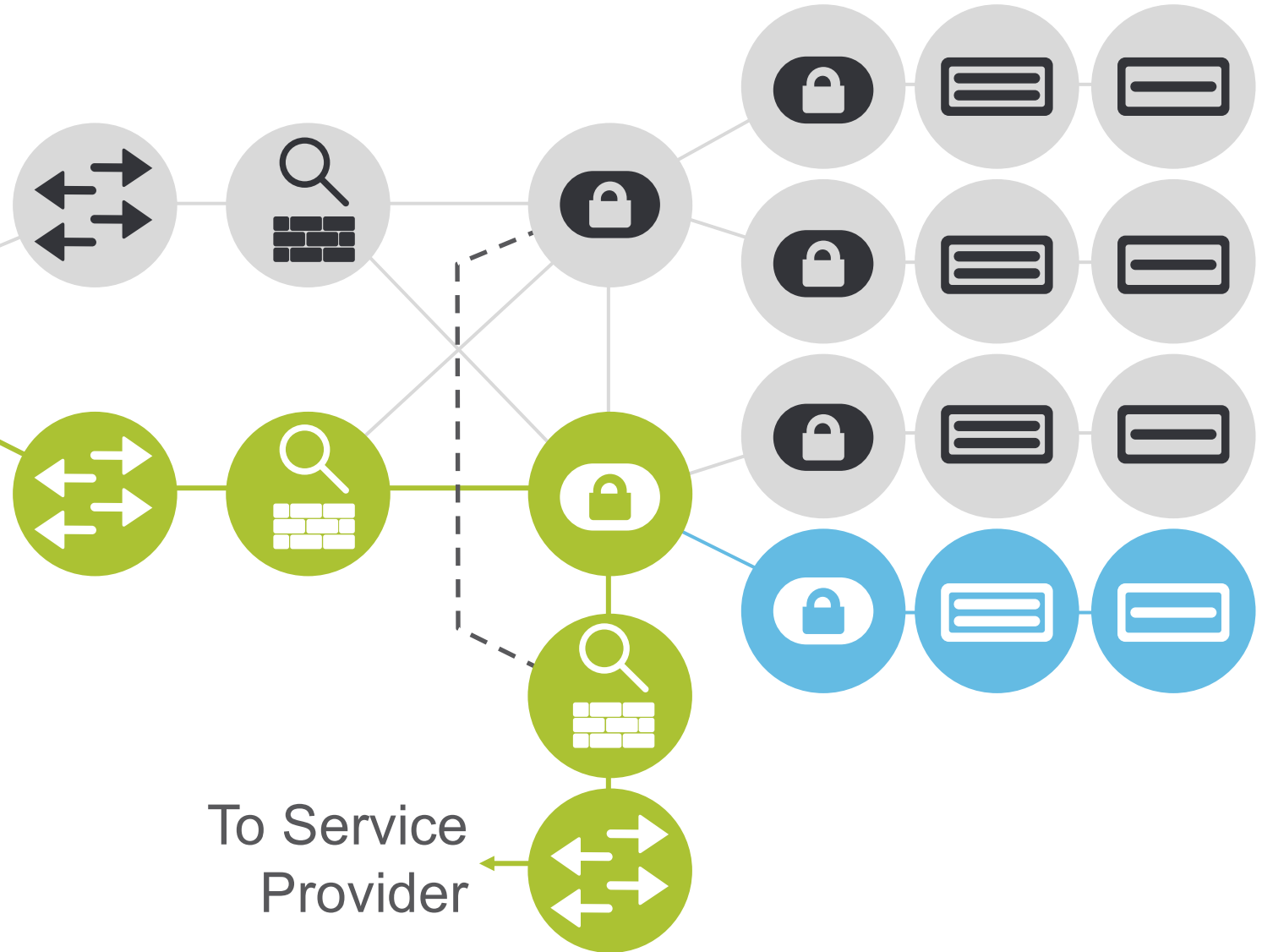


To Service
Provider

Branch



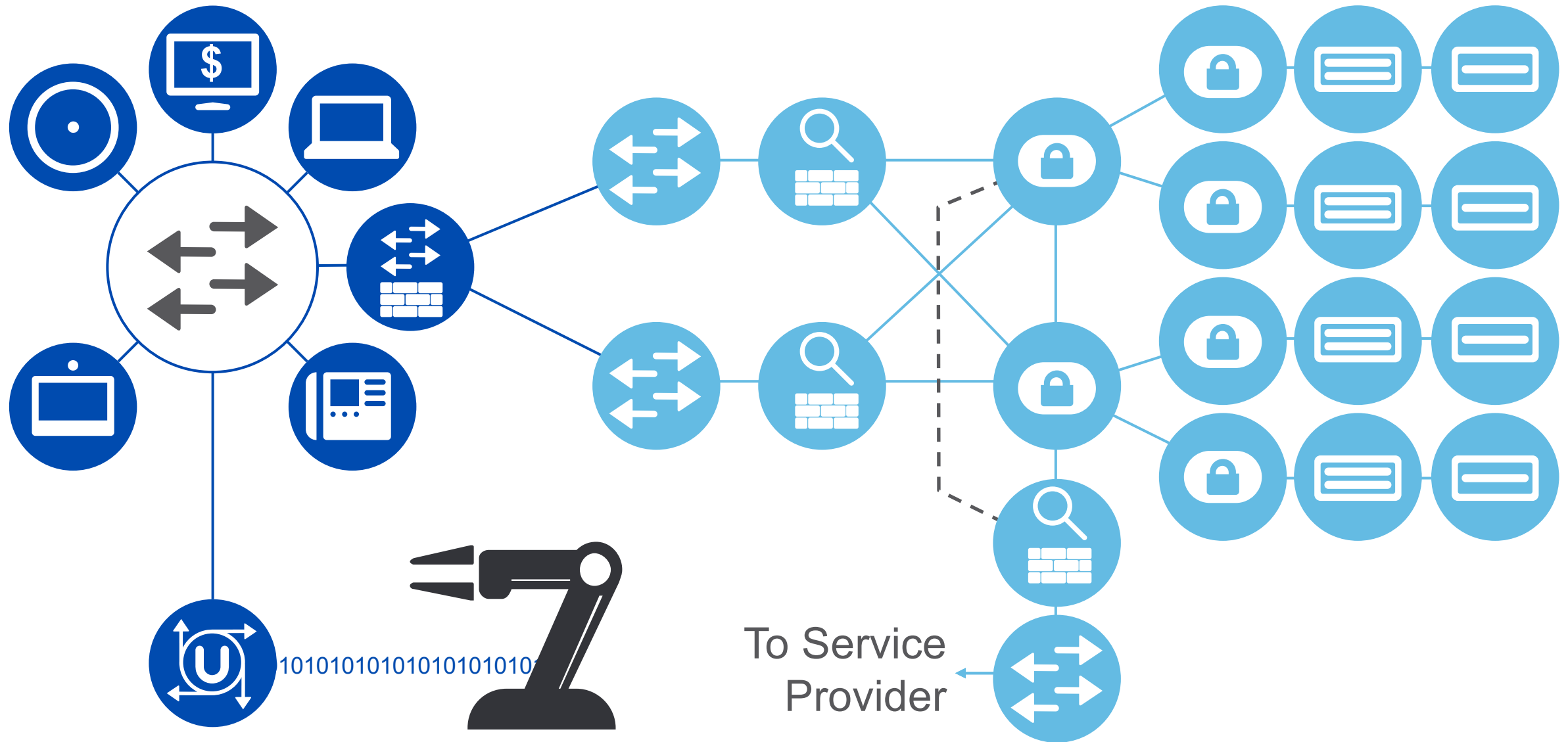
Data Center



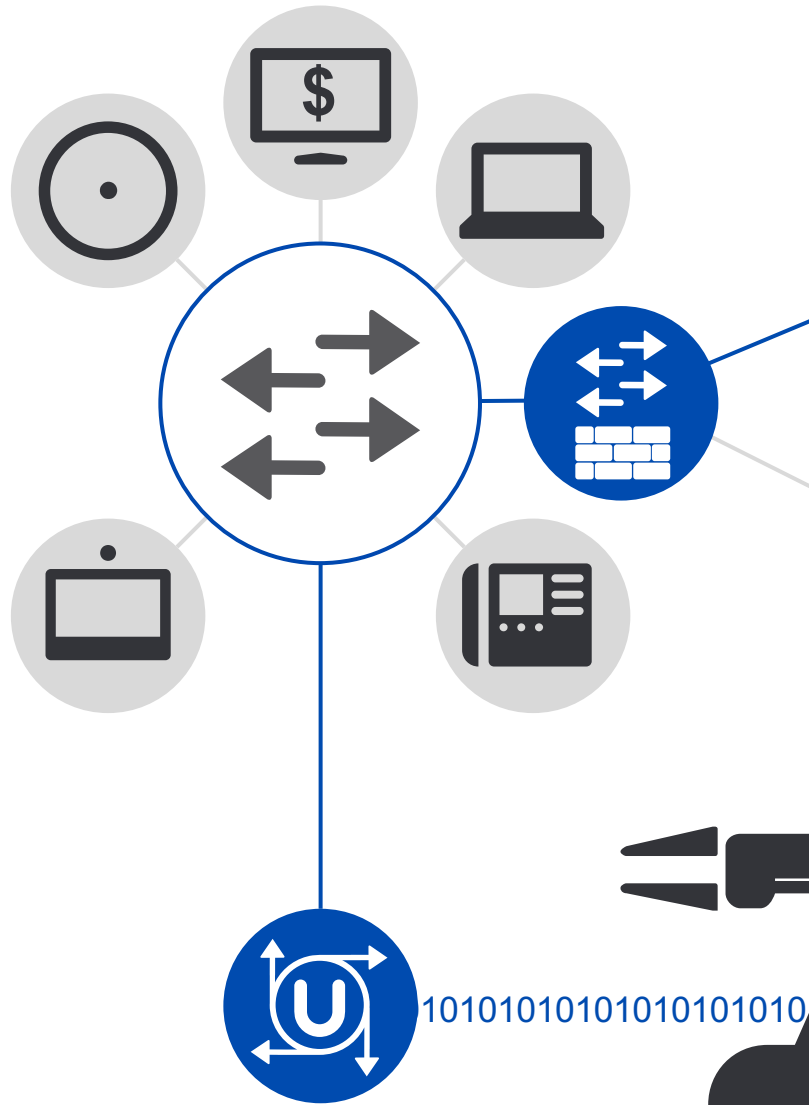
To Service
Provider

Branch

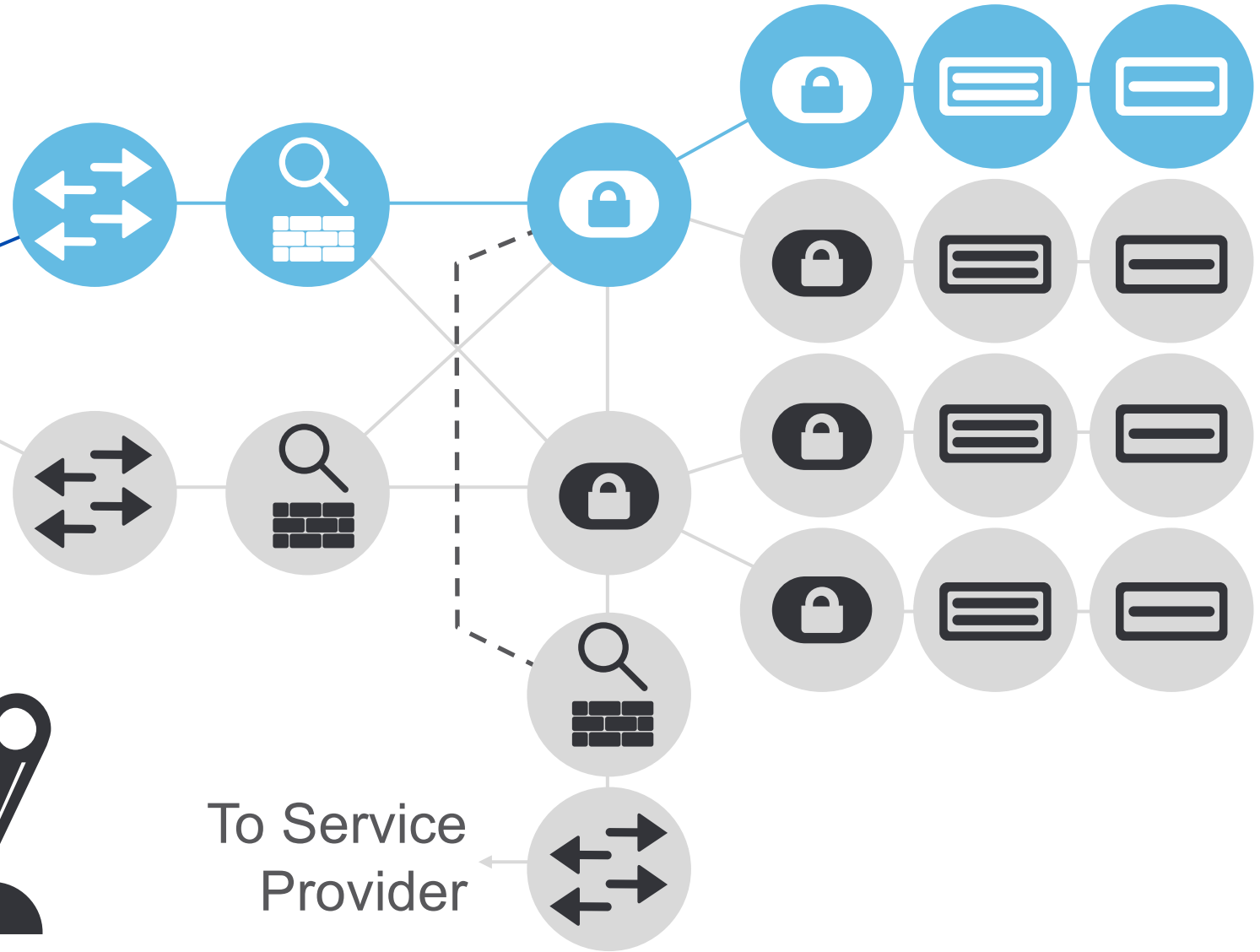
Data Center



Branch



Data Center



To Service
Provider

But IoT Device Security is a Crapshoot

- IOT devices are uncontrolled
 - Software – firmware
 - Manufacturing process
 - Maintenance process
- IOT devices are easy to compromise
 - Poor access protection (admin/admin, even nothing ...)
 - No anti-virus / anti malware
 - Limited (if any) software upgrade capability
 - Compromises go undetected
- IOT devices have full capability of causing harm
 - They often have a full (linux) stack
 - Large numbers, Diverse
 - They are frequently granted full network access (unrestricted network access)



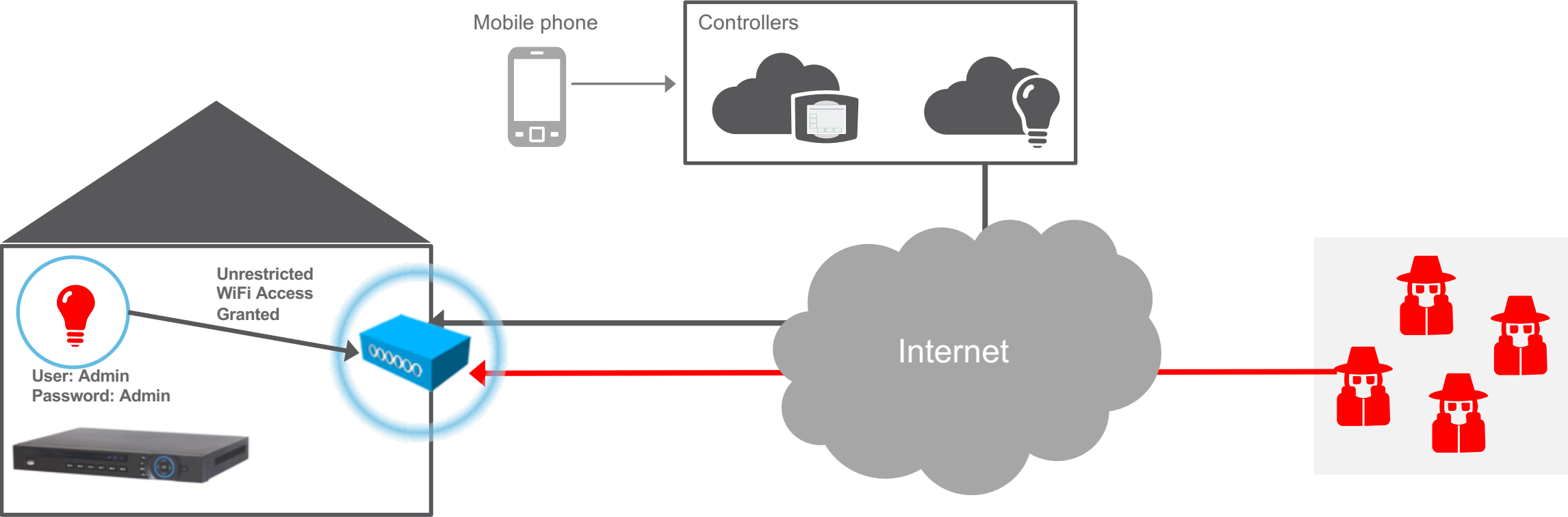
But IoT Device Security is a Shoot

- IOT devices are uncontrollable
 - Software – firmware
 - Manufacturing process
 - Maintenance process
- IOT devices are easy to exploit
 - Poor access protection (admin/)
 - No anti-virus / anti malware
 - Limited (if any) software upgrades
 - Compromises go undetected
- IOT devices have full access to the network
 - They typically have a full (linux) stack
 - Large numbers, Diverse
 - They are frequently granted full network access (unrestricted network access)

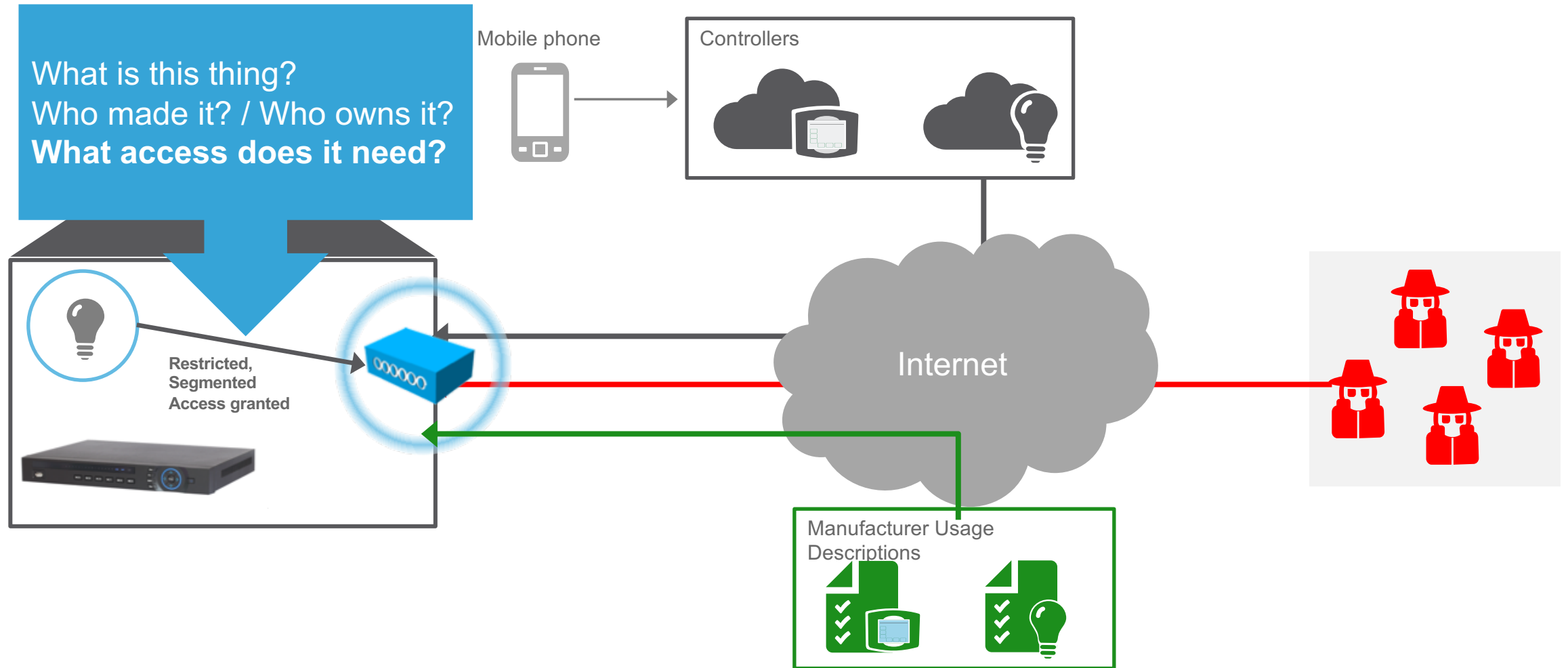


We need a new security paradigm

Device Onboarding Today



Autonomous Onboarding via Manufacturer Usage Descriptions (MUD)



Assumptions and Assertions

Assumptions

A Thing has a single use or a small number of uses.

Things are tightly constrained.
Resource constraints are tight.

Even those Things that can protect themselves today may not be able to do so tomorrow

Network administrators are the ultimate arbiters of how their networks will be used

Assertions

Because a Thing has a single or a small number of intended uses, all other uses must be unintended

Any intended use can be clearly identified

All other uses can be warned against in a statement

Manufacturers are in a generally good position to make the distinction

| Drug Facts | |
|--|---------------|
| Active Ingredient (in each tablet) | Purpose |
| Aspirin 81 mg | Pain reliever |
| Uses for the temporary relief of minor aches and pains or as recommended by your doctor. Because of its delayed release action, this product will not provide fast relief of headaches or other symptoms needing immediate relief. | |
| Do not use -if you have ever had an allergic reaction to any other pain relievers/ fever reducers. | |
| Warnings Reyes syndrome: Children and teenagers who have or are recovering from chicken pox or flu-like symptoms should not use this product. When using this product, if changes in behavior with nausea and vomiting occur, consult a doctor because these symptoms could be an early sign of Reyes's syndrome, a rare but serious illness. | |
| Ask a doctor before use if you have -stomach problems (such as heartburn, upset stomach, or stomach pain) that last or come back -bleeding problems -ulcers -asthma | |
| Ask a doctor or pharmacist before use if -you are taking a prescription drug for -diabetes -gout -arthritis | |
| Allergy alert: Aspirin may cause a severe allergic reaction which may include: -facial swelling -asthma (wheezing) -shock -hives | |
| Alcohol warning: If you consume 3 or more alcoholic drinks every day. Ask your doctor whether you should take aspirin or other pain relievers/fever reducers. Aspirin may cause stomach bleeding. | |
| Stop use and ask doctor if an allergic reaction occurs. Seek medical help right away. -Pain gets worse or lasts more than 10 days -redness or swelling is present -new symptoms occur -the ears or loss of hearing occurs | |
| If pregnant or breast-feeding, ask a health professional. It is especially important not to use aspirin during the last 3 months of pregnancy unless definitely directed to do so because it may cause problems in the unborn child or complications during delivery. | |
| Keep out of the reach of children. In case of overdose, get help or contact a Poison Control Center immediately. | |
| Directions -drink a full glass of water with each dose. -At 12 years of age and over: take 4 to 8 tablets every 4 to 6 hours. Do not exceed 48 tablets in 24 hours unless directed by a doctor. -Children under 12 years: consult a doctor | |
| Other information -store at room temperature | |
| Inactive ingredients colloidal silicon dioxide, sodium, FD&C Yellow #10 aluminum lake, FD&C Yellow #6, methacrylic acid copolymer, microcrystalline cellulose, talc, titanium dioxide, triethyl citrate | |



The MUD File

```
{
  "ietf-acl:access-lists": {
    "ietf-acl:access-list": [
      {
        "acl-name": "mud-10387-v4in",
        "acl-type": "ipv4-acl",
        "ietf-mud:packet-direction": "to-device",
        "access-list-entries": {
          "ace": [
            {
              "rule-name": "clout0-in",
              "matches" : {
                "ietf-mud:direction-initiated" : "from-device"
              },
              "actions": {
                "permit": [
                  null
                ]
              }
            },
            {
              "rule-name": "entin0-in",
              "matches": {
                "ietf-mud:controller":
                  "http://lightbulb.example.com/controller",
                "ietf-mud:direction-initiated" : "to-device"
              },
              "actions": {
                "permit": [
                  null
                ]
              }
            }
          ]
        }
      }
    ]
  }
},
{
  "acl-name": "mud-10387-v4out",
  "acl-type": "ipv4-acl",
  "ietf-mud:packet-direction": "from-device",
  ....
}
```

We must protect the Things from the network, and the network from the Things

- Networks need to have automated means to know how to protect the devices: the manufacturer is key.
 - Use IETF [Manufacturing Usage Descriptions \(MUD\)](#) to aid in providing the maximum access control possible for the device.
 - Deploy protection at the Ethernet Access Switch, edge router, or IoT Gateway connecting the Things to the rest of the network.
 - Deploy Port-Based Network Access Control (e.g., IEEE 802.1X, MAB)
- Devices and networks need a way to establish trust with one another: again, the manufacturer is key.
 - Use a device's IEEE 802.1AR IDevID manufacturer's certificate to establish trust between the Device and the Network.
 - Use IETF ANIMA [Bootstrapping Remote Secure Key Infrastructures](#) (BRSKI)

