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

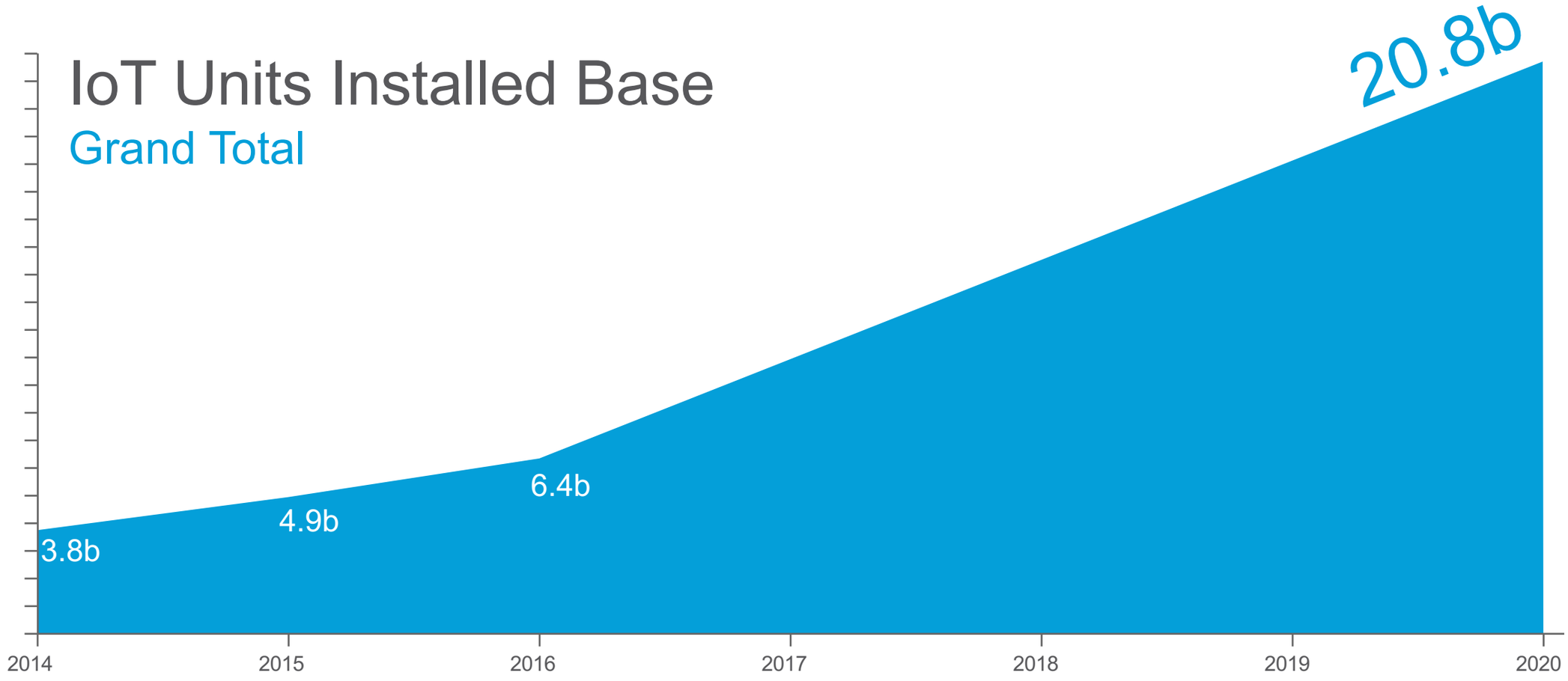
- Interoperability concerns cited as one of the top factors that prevent or delay IoT deployments, while customers wait for the ”dust to settle”.
- **Enterprise IoT –** Drive a standard for Enterprise IoT application comm/data/resource models
  - It matters less which open standard wins, so much as there 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

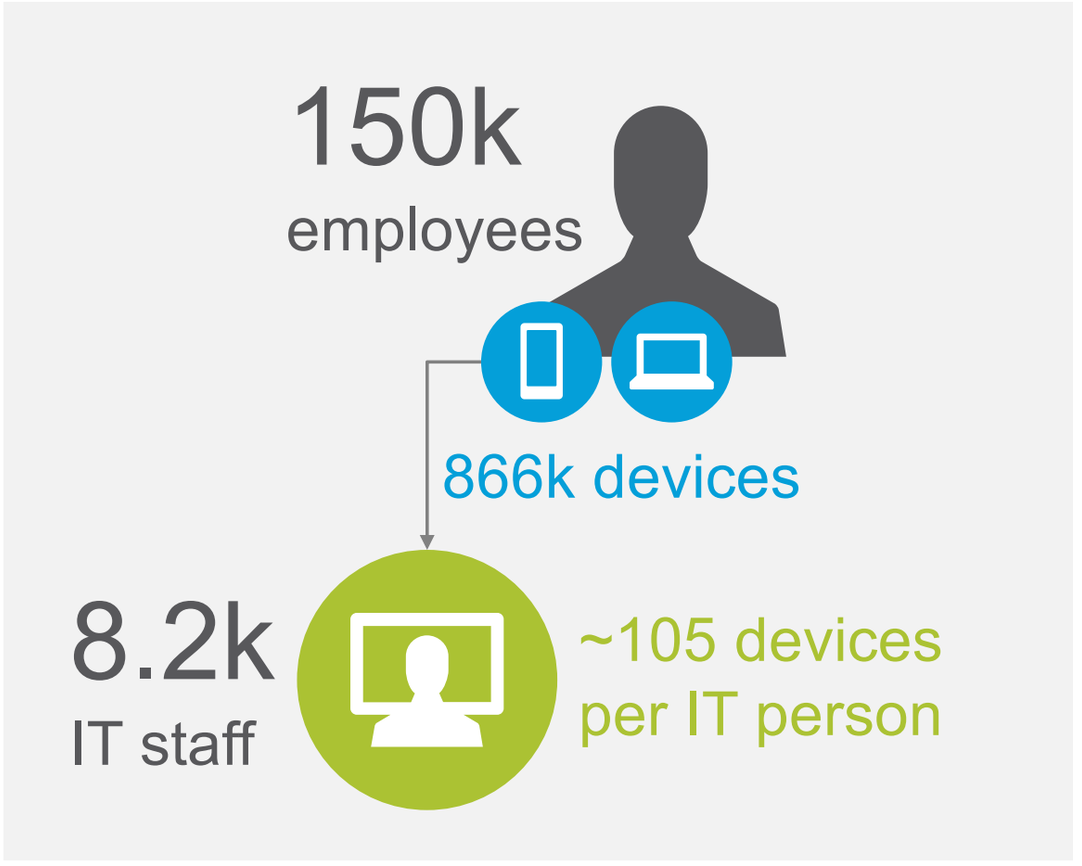
Gratuitous IoT Growth Chart



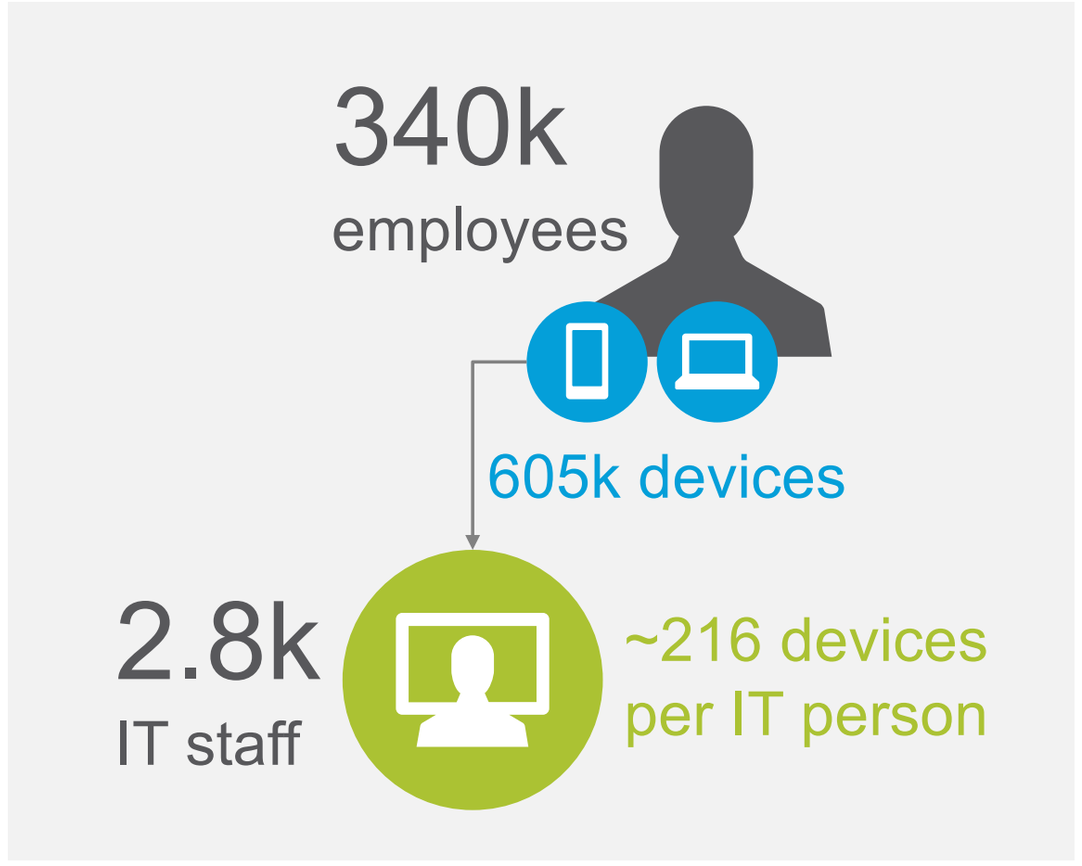
Source: Gartner, November 2015
https://www.gartner.com/newsroom/id/3165317

Humans can’t scale to manage networks of this size

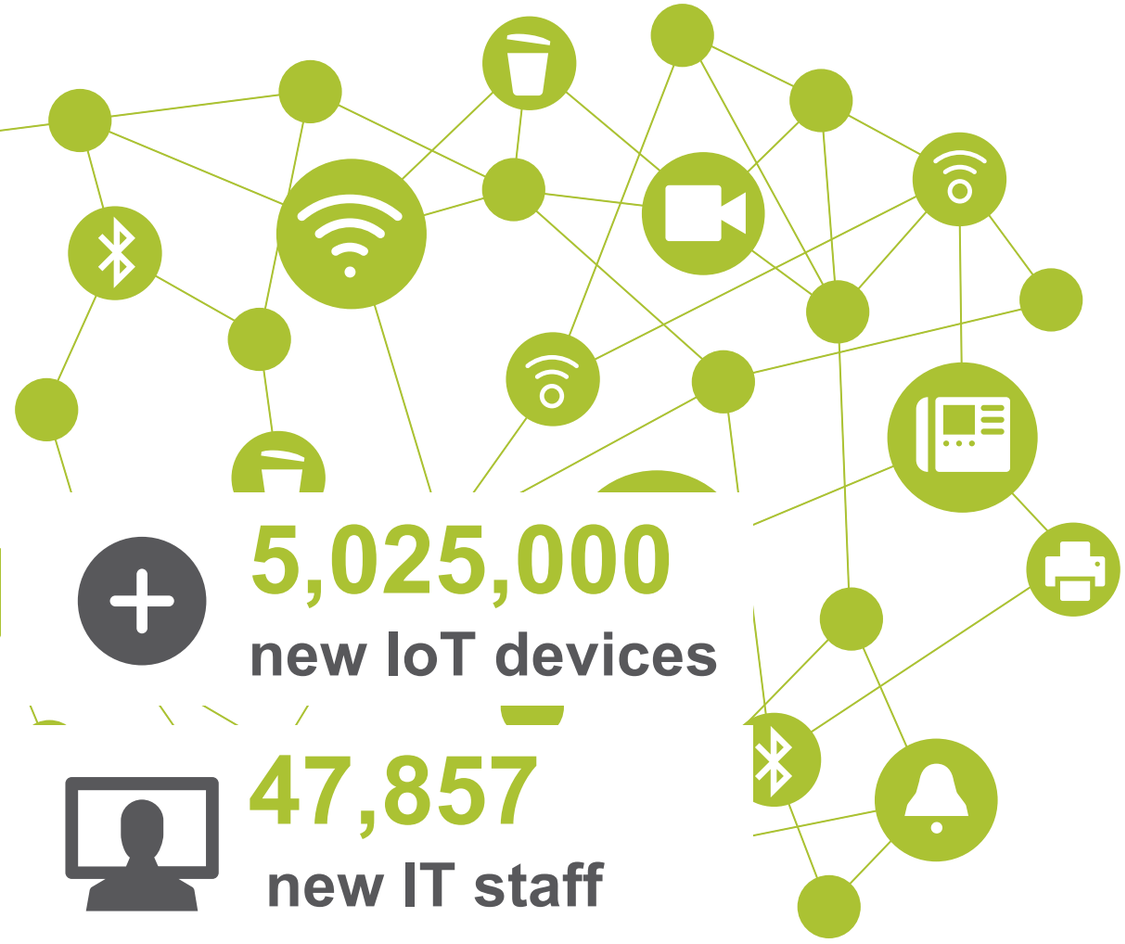
Major Bank
Today



Major Retailer
Today



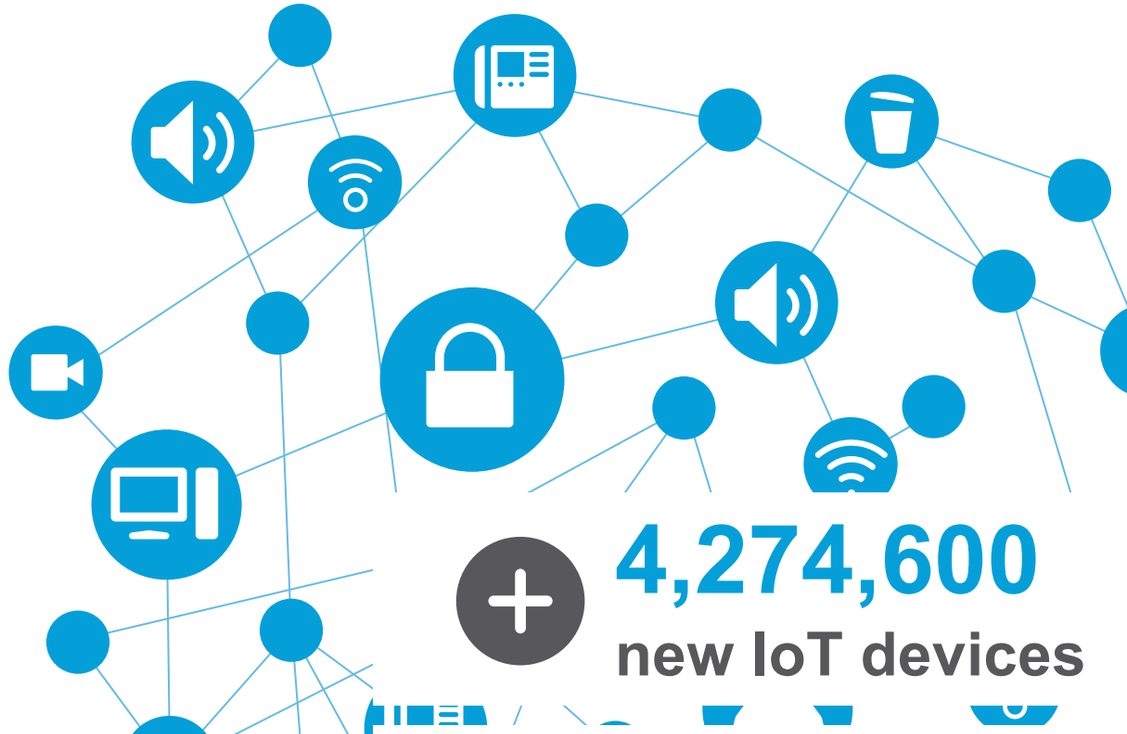
Major Bank



5,025,000
new IoT devices

47,857
new IT staff

Major Retailer



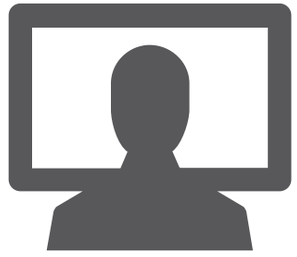
4,274,600
new IoT devices

19,789
new IT staff

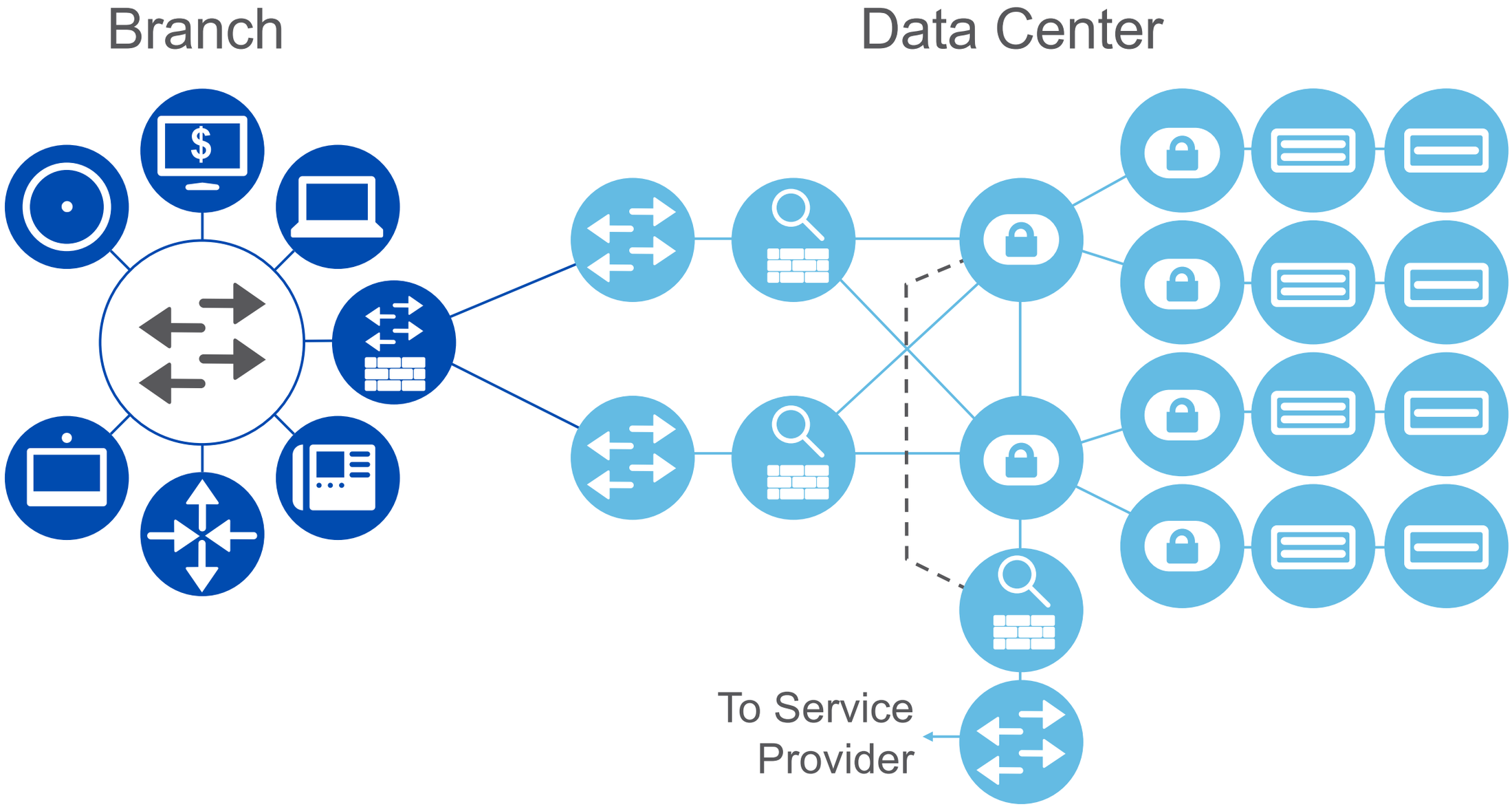
1:200

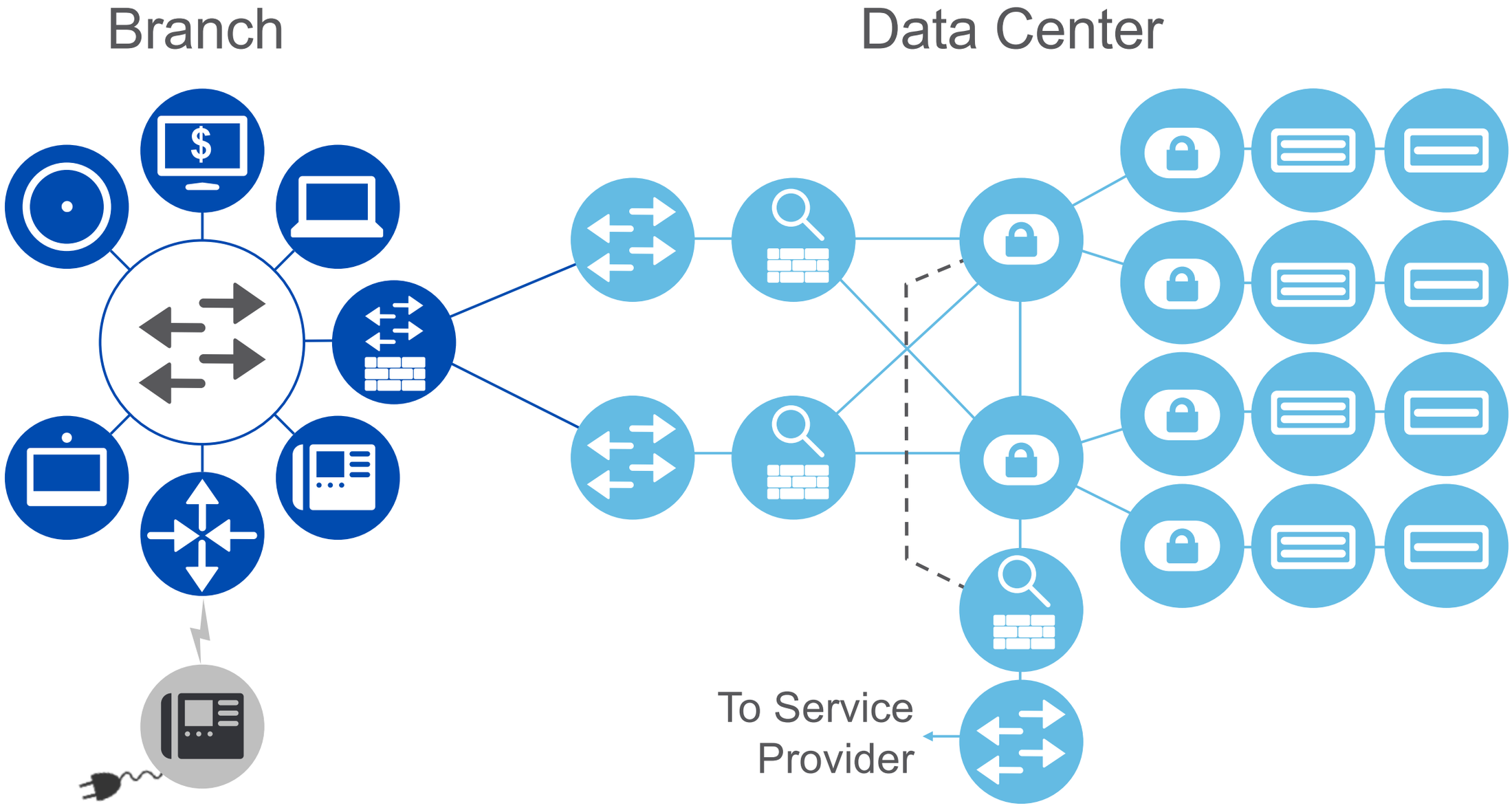
This doesn’t scale.

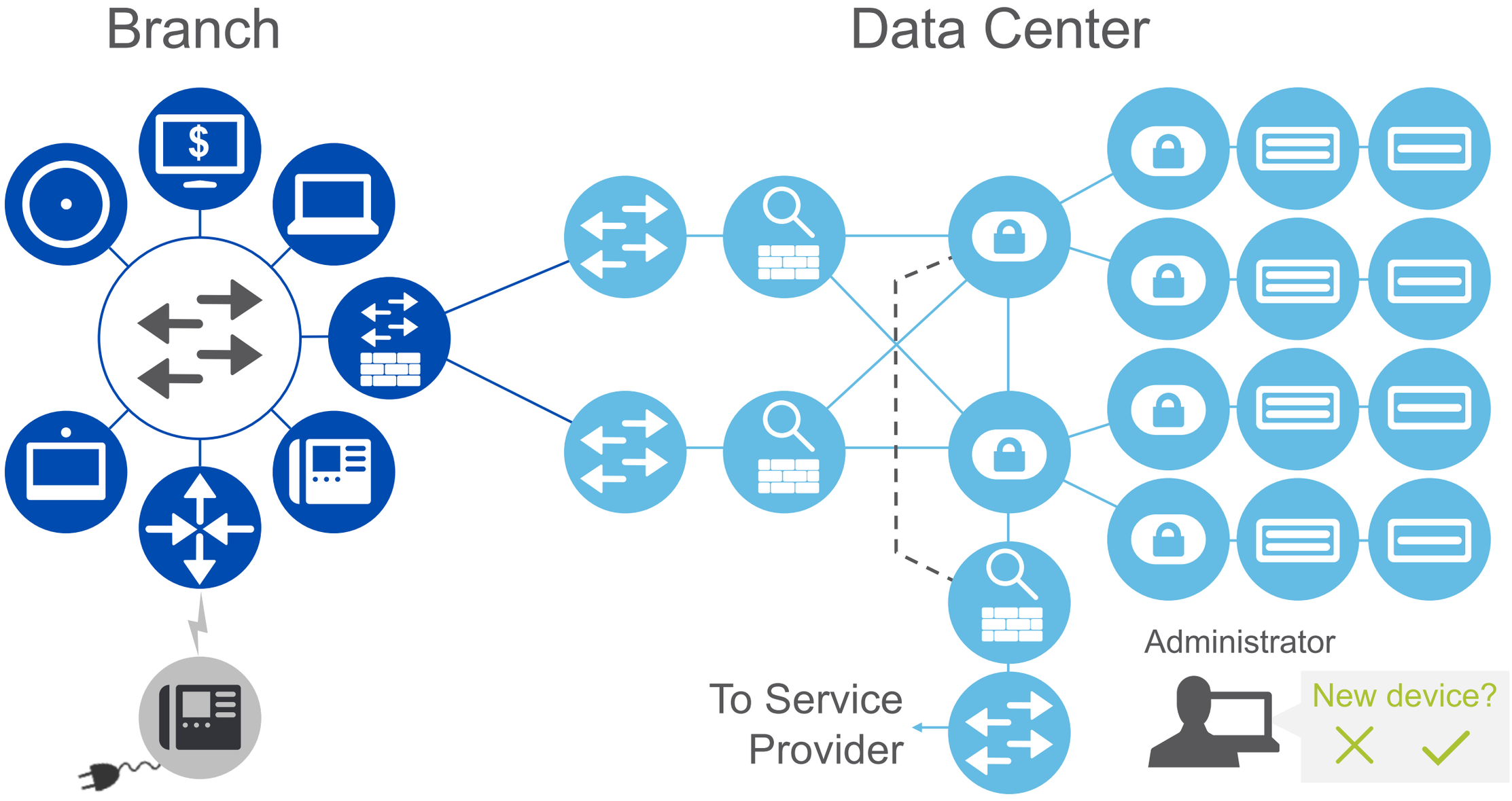
1:1,000,000

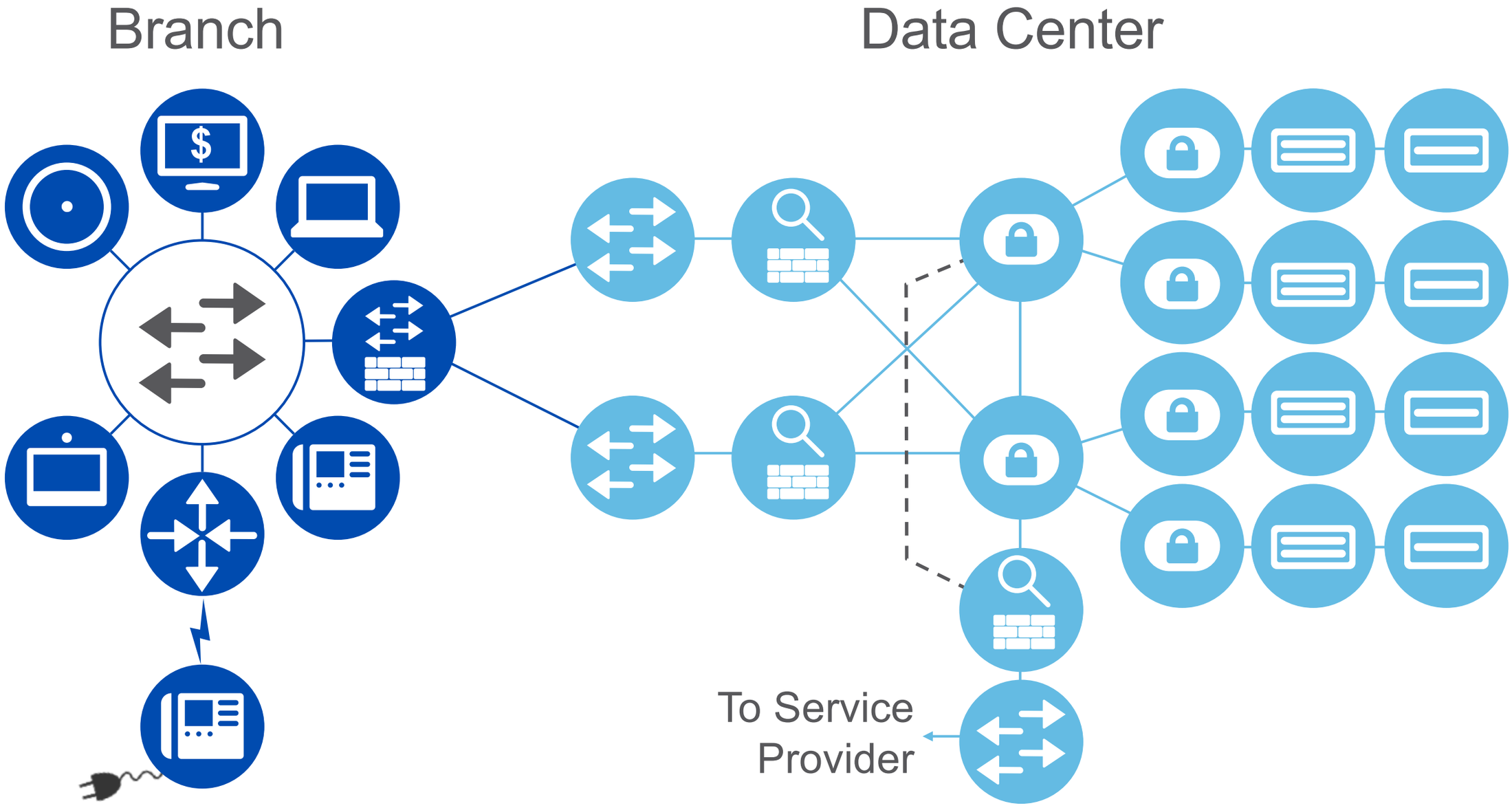


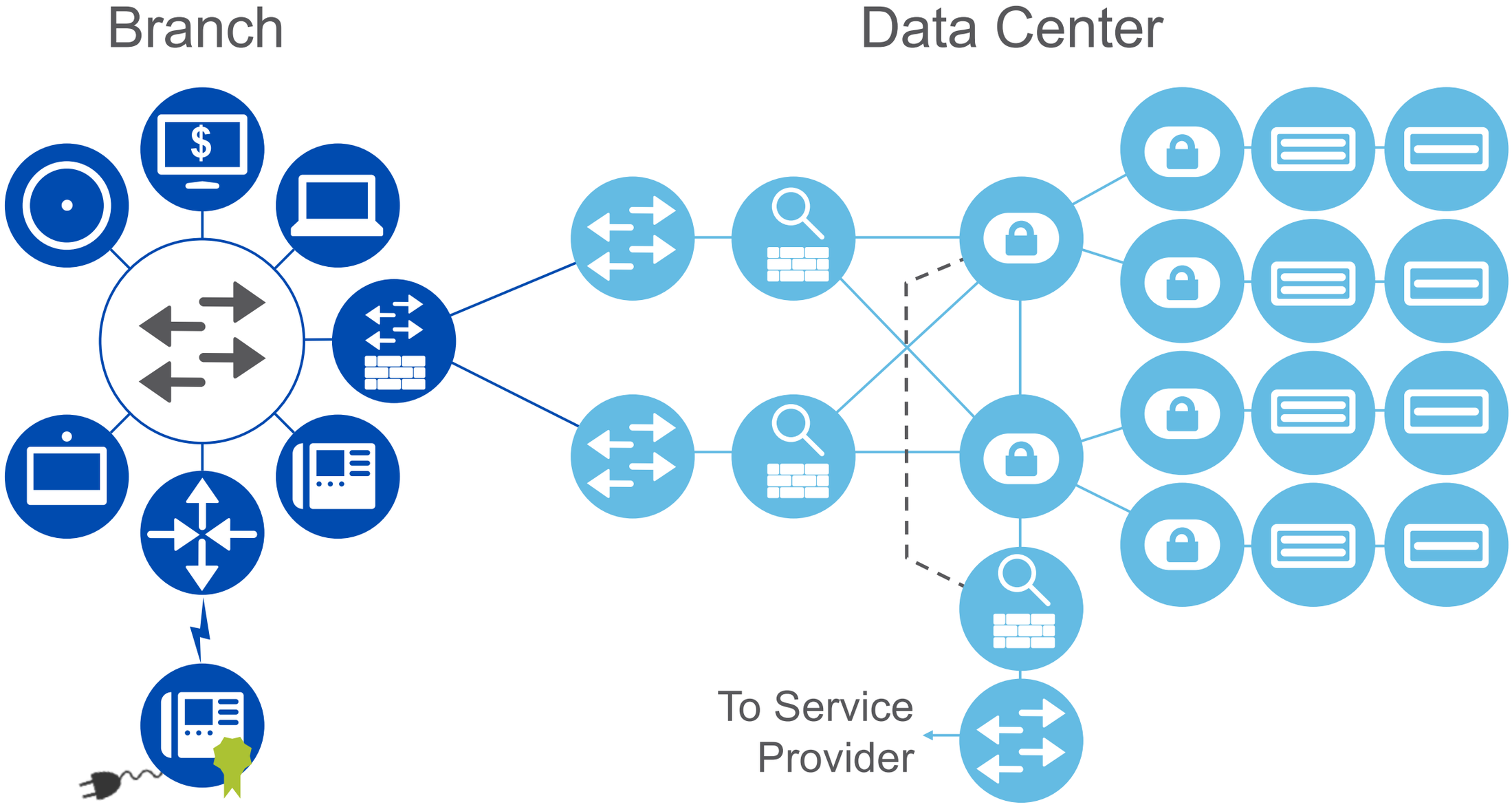
What does this future look like?

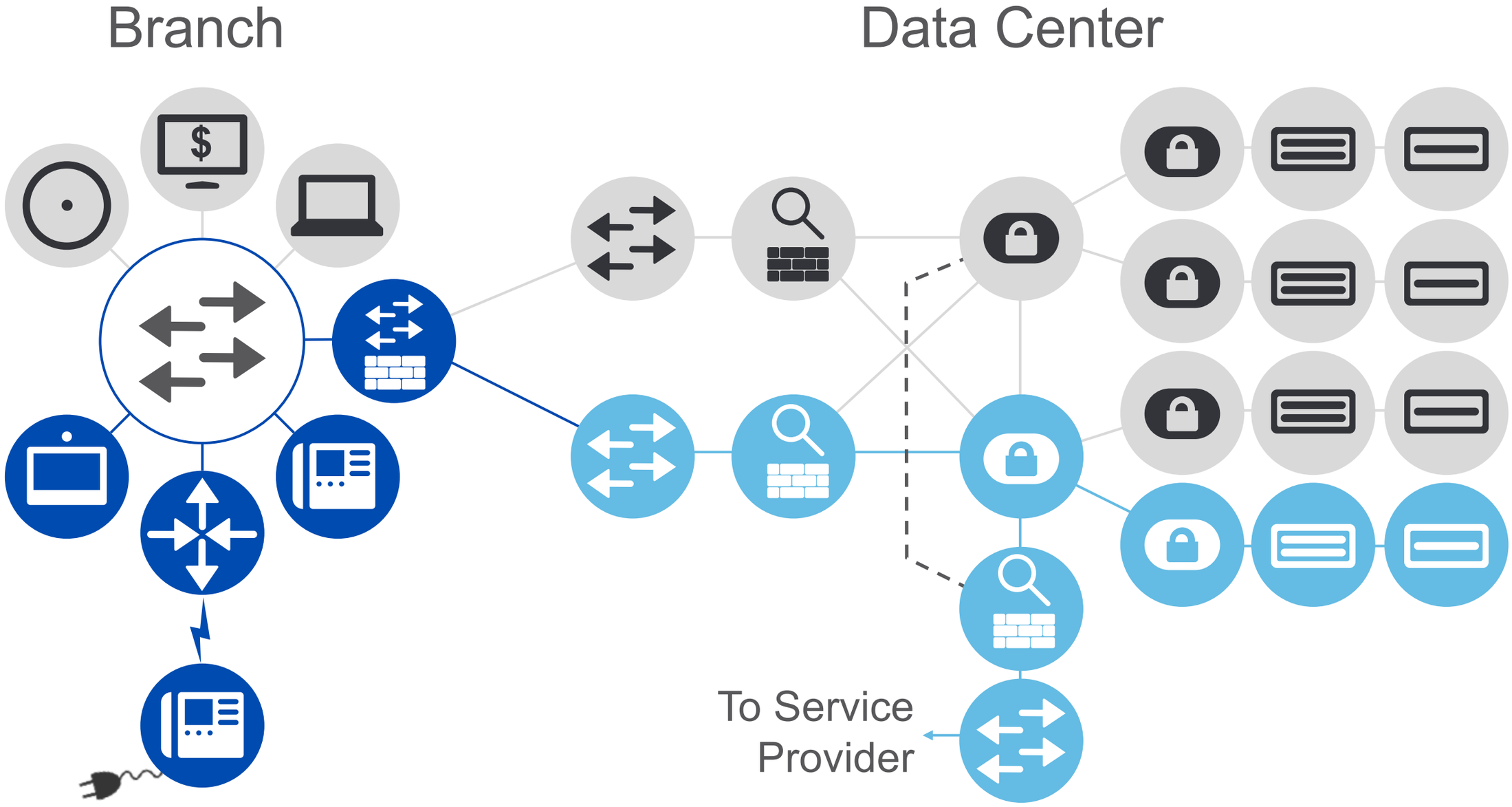


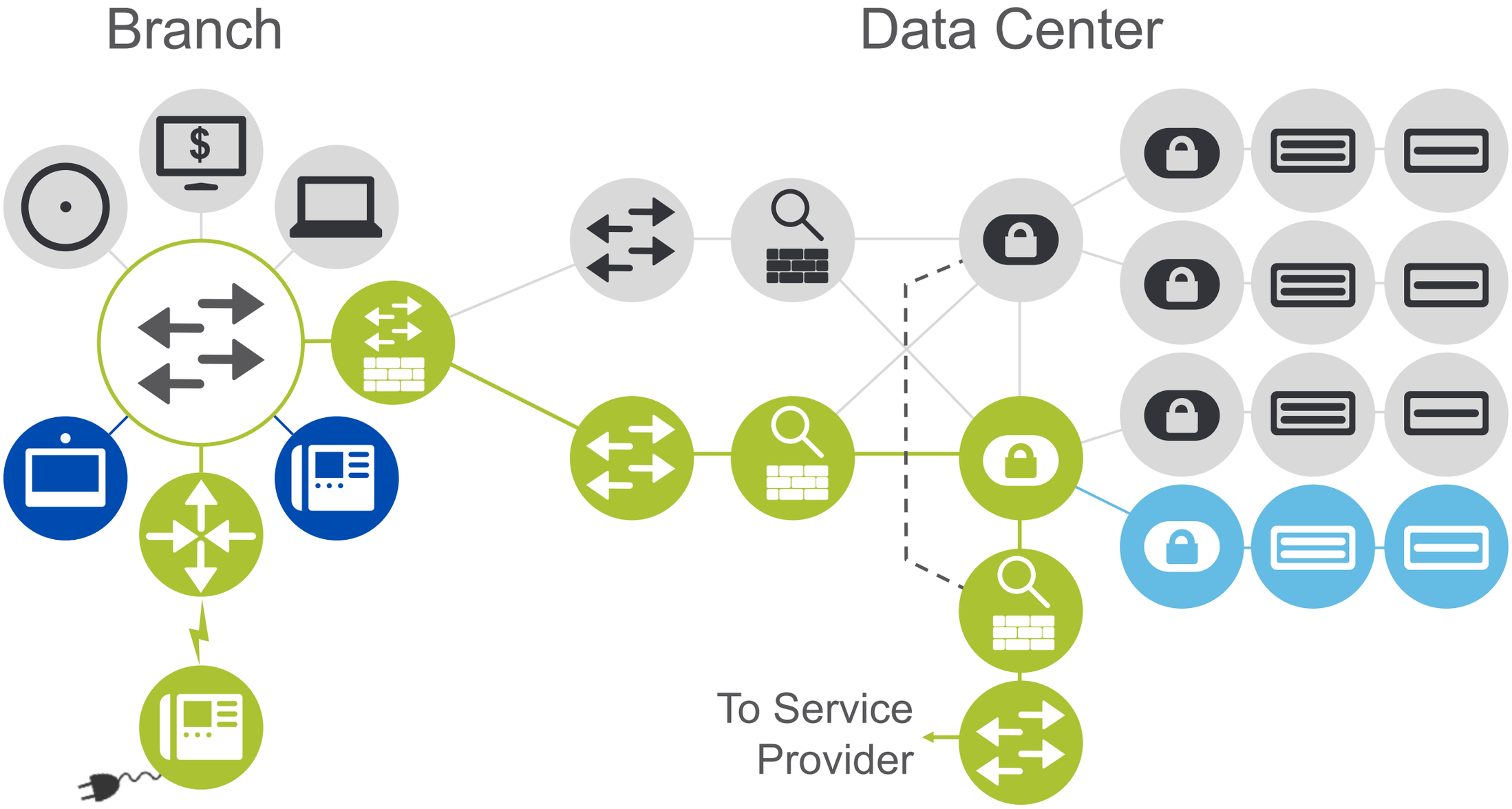


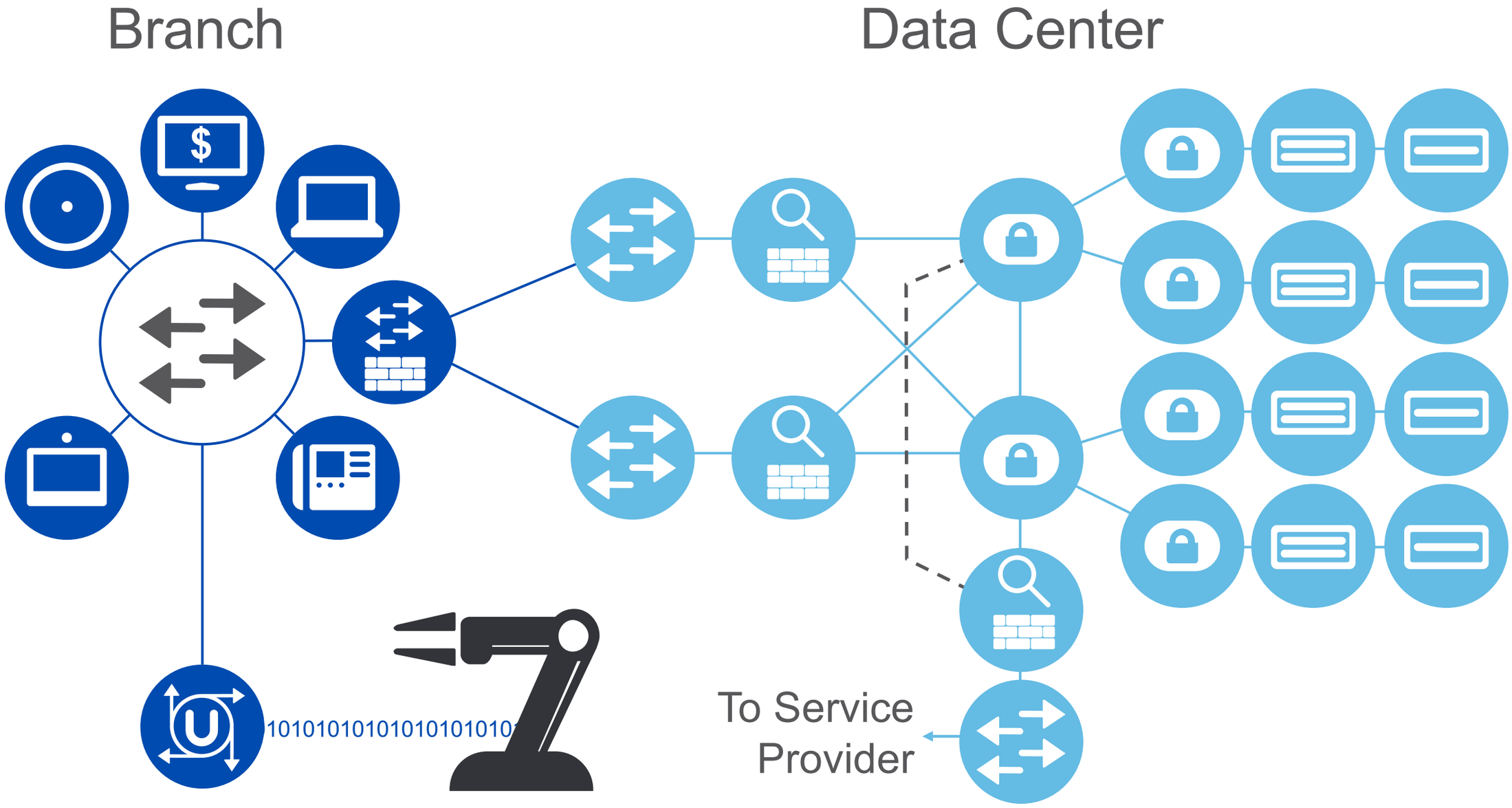


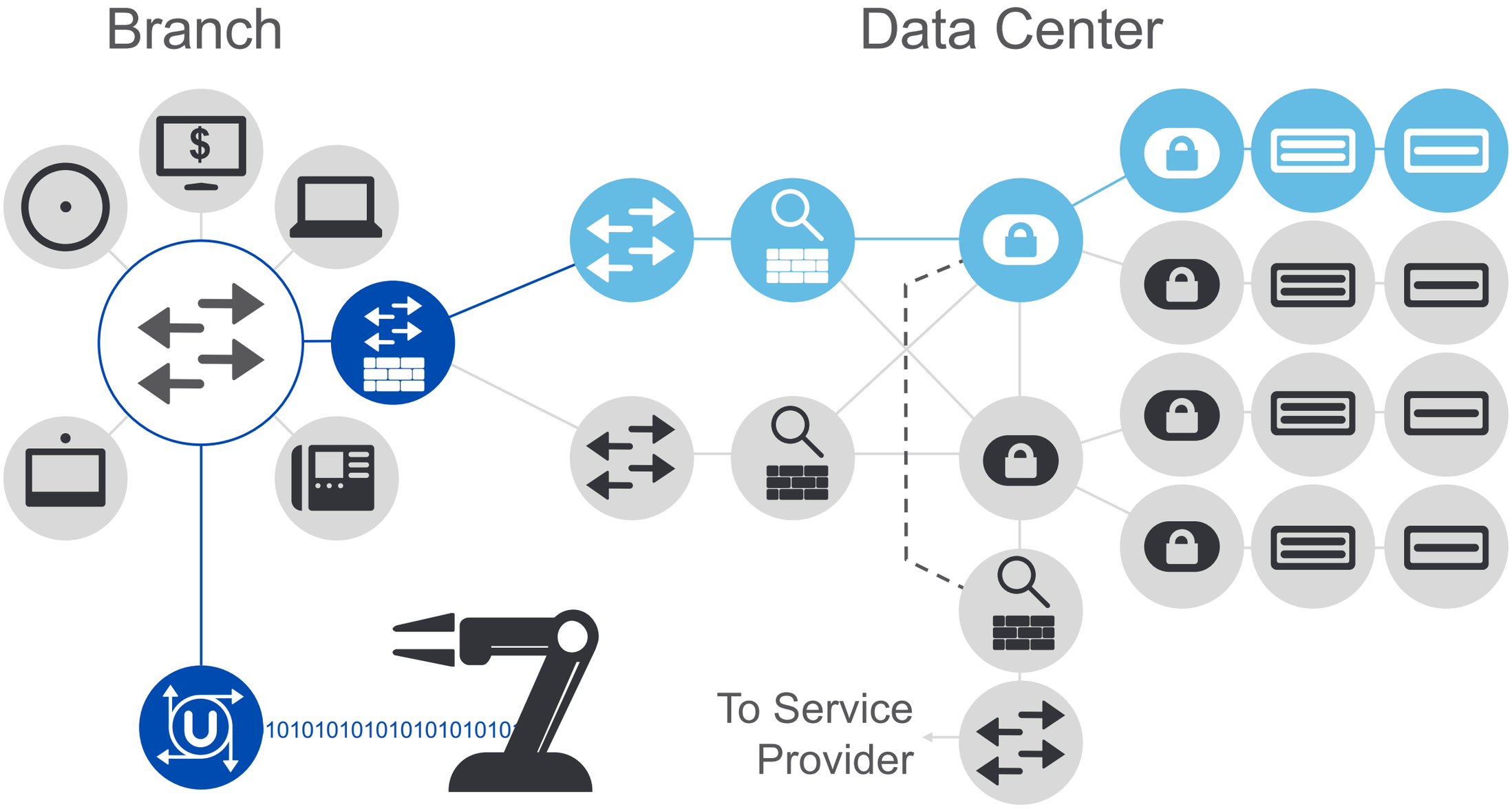










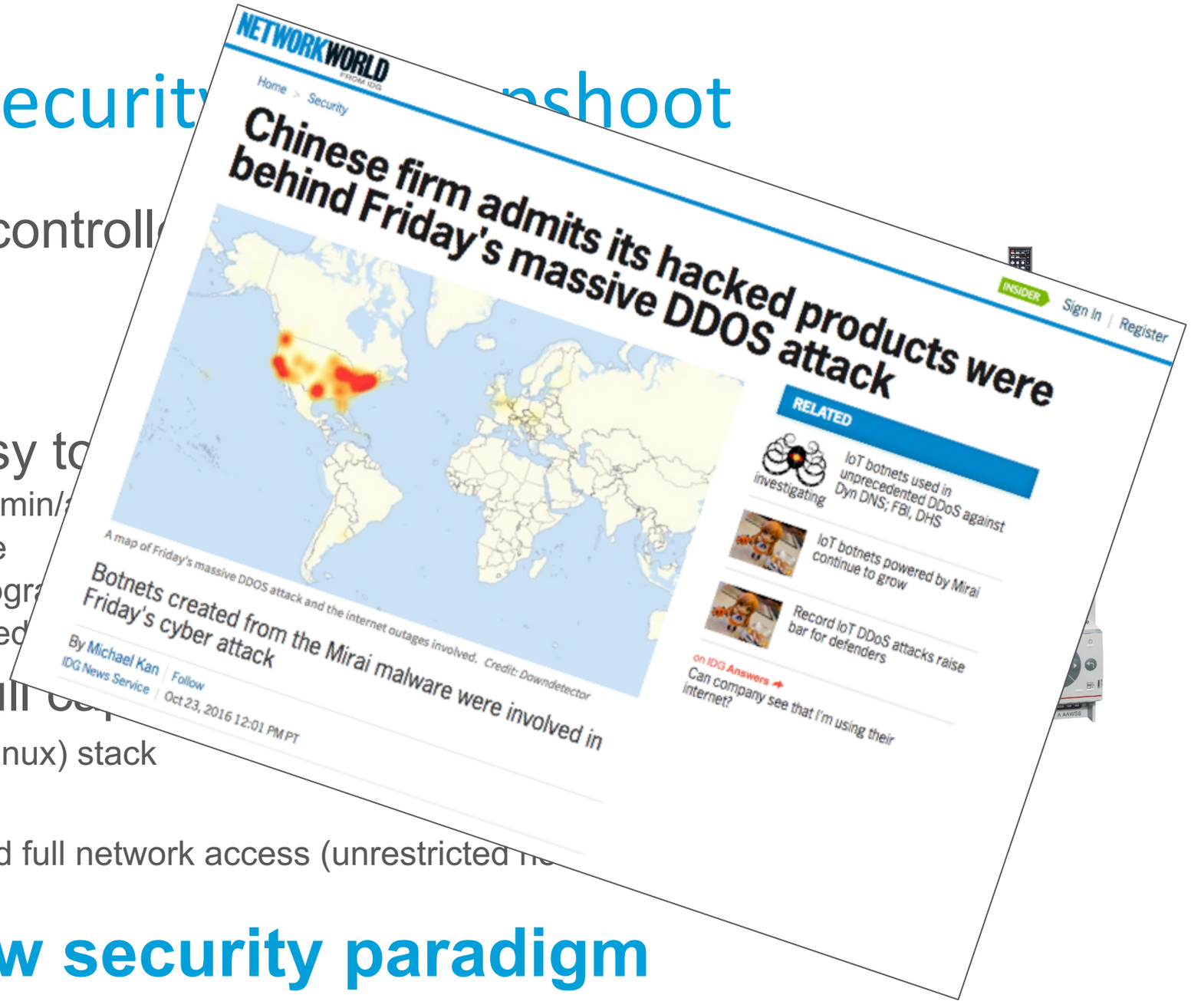


But IoT Device Security is a Crapshoot

- 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)

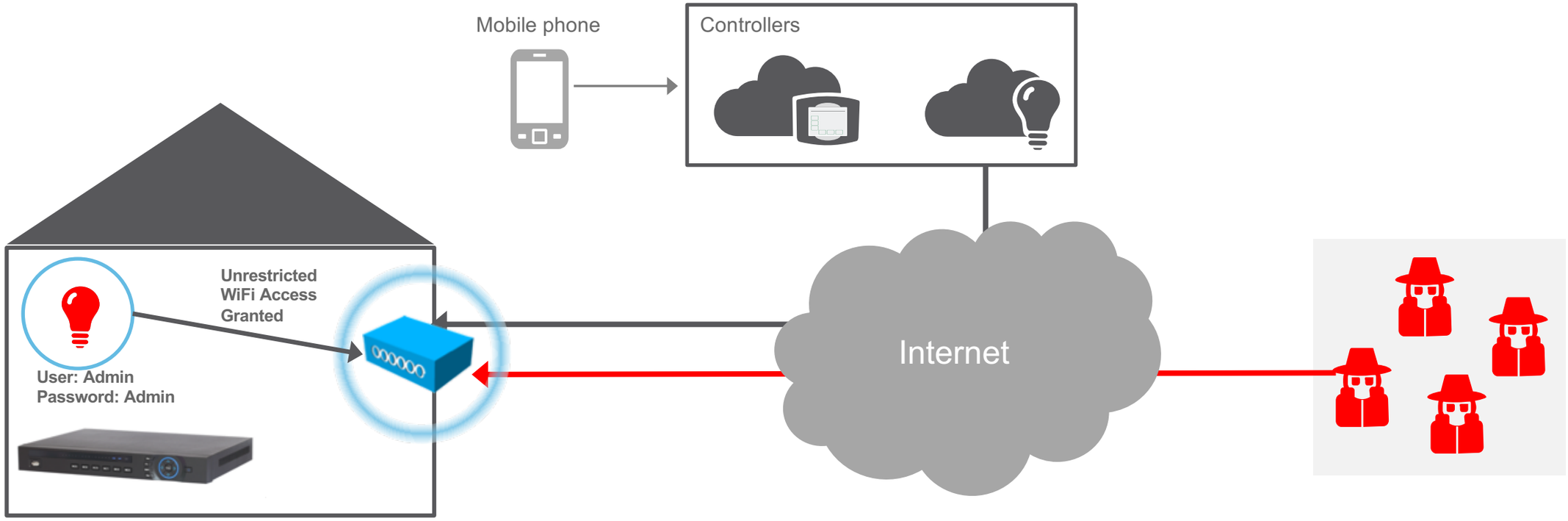
But IoT Device Securit nshoot

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

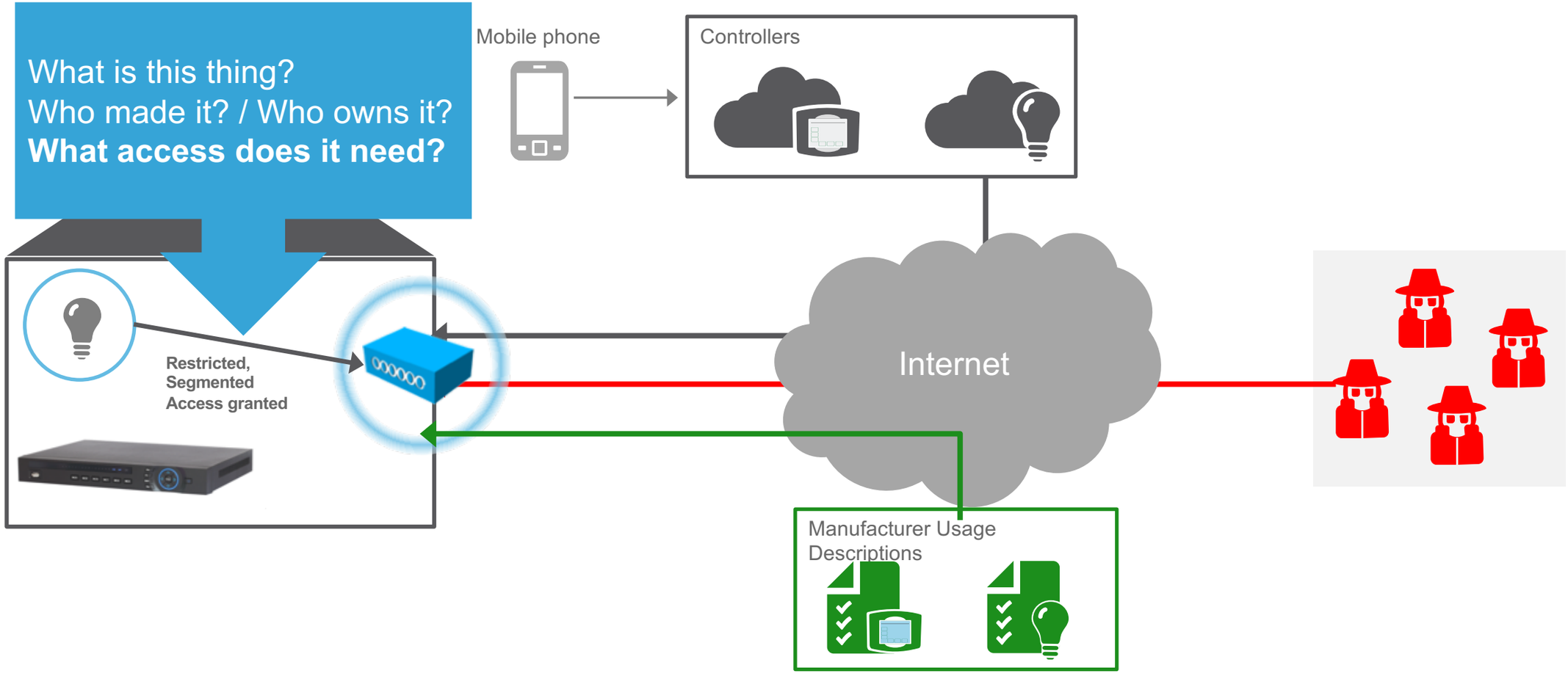


We need a new security paradigm

Device Onboarding Today



Autonomous Onboarding via Manufacturer Usage Descriptions (MUD)



Assumptions and Assertions

Assumptions	Assertions
A Thing has a single use or a small number of uses.	Because a Thing has a single or a small number of intended uses, all other uses must be unintended
Things are tightly constrained. Resource constraints are tight.	Any intended use can be clearly identified
Even those Things that can protect themselves today may not be able to do so tomorrow	All other uses can be warned against in a statement
Network administrators are the ultimate arbiters of how their networks will be used	Manufacturers are in a generally good position to make the distinction

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)


CISCO