IoT in the Enterprise

An analysis of traffic and threats

by Zscaler™ ThreatLabZ™
May 2019

zscaler™

Overview

Enterprises around the globe have been adopting the use of IoT products to improve organizational efficiency, enhance communications, and to gain insight into system performance.

According to Gartner, 20.4 billion IoT devices will be in use worldwide by 2020, and more than 65 percent of enterprises will adopt IoT products..

The rapid adoption of these IoT devices has opened up new attack vectors for cybercriminals. As such, the ThreatLabZ research team began studying the use of IoT devices in the enterprise by analyzing IoT traffic across the Zscaler cloud.

The team analyzed one month of data for recent IoT device footprints based on traffic in the Zscaler cloud. This analysis looked at the types of devices in use, the protocols they used, the locations of the servers with which they communicated, and the frequency of their inbound and outbound communications, as well as IoT traffic patterns.

This report details the results of this analysis.

Background

IoT devices are nonstandard computing devices that connect wirelessly to a network and have the ability to transmit data. These devices can communicate and interact over the internet, and they can be remotely monitored and controlled.

Connected devices are part of a scenario in which every device talks to other related devices in an environment to automate home and industry tasks, and to communicate usable sensor data to users, businesses and other interested parties. IoT devices are meant to work in concert for people at home, in industry, or in the enterprise.

Market Size

IDC has predicted that IoT spending will reach $745 billion in 2019 and surpass the $1 trillion mark in 2022. That's a 15 percent increase over 2018's $646 billion.

According to the same report, the U.S. and China will be the spending the most at $194 billion and $182 billion, respectively. They are followed by Japan, Germany, Korea, France, and the UK.

Emerging Threats

As is often the case, IoT technology has moved more quickly than the mechanisms available to safeguard these devices and their users.

Researchers have already demonstrated remote hacks on pacemakers and cars. And, in October 2016, a large distributed denial-of-service (DDoS) attack, dubbed Mirai, affected DNS servers on the east coast of the United States, disrupting services worldwide. This attack was traced back to hackers infiltrating networks through IoT devices, including wireless routers and connected cameras.

In August 2017, the U.S. Senate introduced the IoT Cybersecurity Improvement Act, a bill addressing security issues associated with IoT devices. While it is a start, the bill only requires internet-enabled devices purchased by the federal government to meet minimum requirements, not the industry as a whole. However, it is being viewed as a starting point that, if adopted across the board, could pave the way to better IoT security industry-wide.

So, which devices constitute the most IoT traffic in the Zscaler cloud and what types of threats do they face? Let's take a look at what the Zscaler ThreatLabZ team discovered.

Results

This report provides a general overview of the most frequently seen device categories, then takes a deep dive into the transaction data for 10 specific types of IoT devices.

Category Overview

What kinds of devices are running in enterprise organizations?

- IP cameras
- Smart watches
- Smart printers
- Smart TVs
- Set top boxes
- Digital home assistants
- IP phones
- Medical devices
- Digital video recorders
- Media players
- Data collection terminals
- Digital signage media players
- Smart glasses
- Industry control devices
- Networking devices
- 3D printers
- Automotive (including smart cars)

Highlights of enterprise IoT traffic

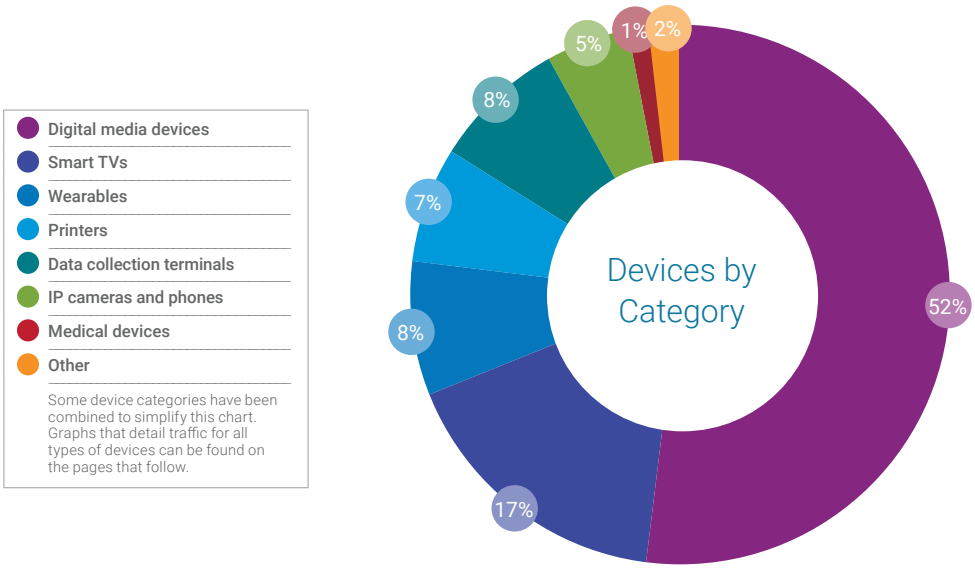
- **270** different IoT device profiles
- **153** different IoT device manufacturers
- **56 million** IoT device transactions were processed in the Zscaler cloud
- **1,051** organizations have at least one IoT device

Top IoT destinations

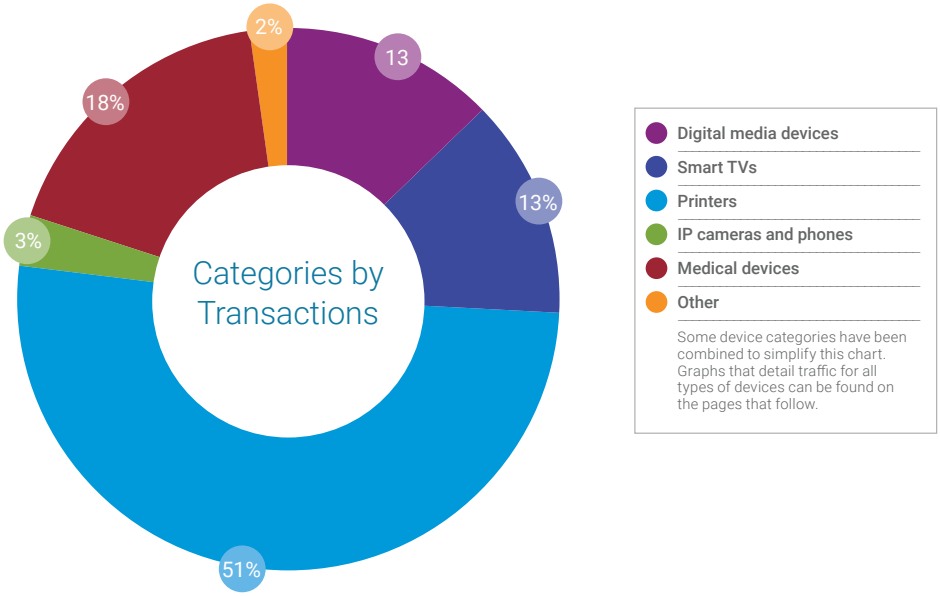
- **57%** of devices connect to Australia
- **37%** of devices connect to the United States
- **2%** of devices connect to the Republic of Ireland
- **1.5%** of devices connect to Namibia
- **0.8%** of devices connect to Japan

Devices by category and transactions

During the study period, the IoT devices seen most often in the Zscaler cloud were set-top boxes (generally used for decoding video), followed by smart TVs, smart watches, media players, and printers. The following chart shows the distribution of IoT devices across different categories.



When it comes to transactions, data collection terminals were the most active devices across all the categories, making up more than 80 percent of the IoT traffic in our cloud. Excluding data collection terminals, the most active category was printers, with more than 51 percent of the remaining IoT transactions coming from this category. Digital media devices, smart TVs, and medical devices were also major contributors. To get a better picture, the chart below shows the distribution of device categories by transactions excluding data collection terminals.



IoT devices insights

IP cameras and digital home assistants

IP cameras are network-connected smart camera devices used for surveillance in an enterprise. We saw eight different device profiles from seven different brands: **Nest, Foscam, Axis Camera, Yi Technologies, Samsung, Polaroid, and Dahua.**

Digital home assistant devices, such as **Amazon Echo** and **Apple HomePod**, were also found to be present in organizations.

Figure 1 shows the traffic distribution for IP cameras and smart home assistants from the Zscaler cloud.

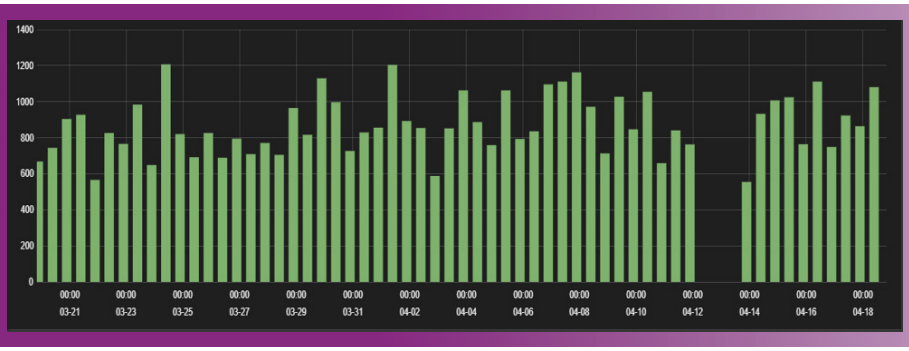


Fig 1
Transaction graph for IP cameras and smart home assistants

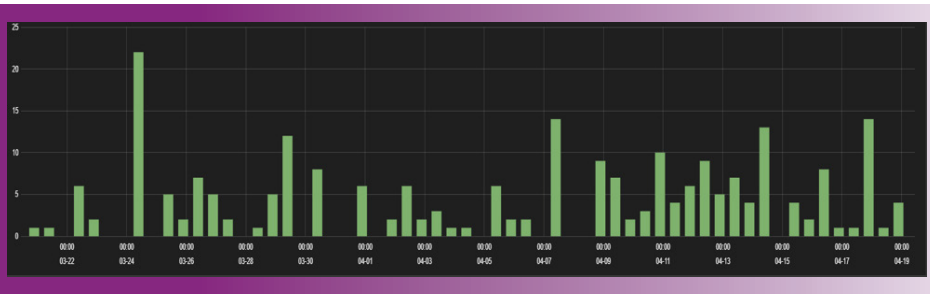
Smart watches and smart glasses

Smart watches are network-connected smart wrist watches that can be used for health monitoring, calling, texting, and more. We saw 18 different smart watches from 13 different manufacturers, including **Apple, Samsung, Pebble, Lemfo, Motorola,** and **Mobvoi.**

Along with smart watches, we noted a small presence of **Google** smart glasses in our cloud.

Figure 2 shows the traffic distribution from different smart watches.

Fig 2
Transaction graph for smart watches



Smart printers and 3D printers

Smart printers are network-connected printers used in offices and homes for printing and scanning documents. We observed printers from seven manufacturers: **Canon, HP, Xerox, Ricoh, Brothersoft, Zebra,** and **Toshiba.**

Along with smart printers, we saw transactions from 3D printers. 3D printers are smart network-connected devices used for crafting real objects. We observed 3D printers from **Ultimaker.**

Figure 3 shows the traffic distribution from different printers.

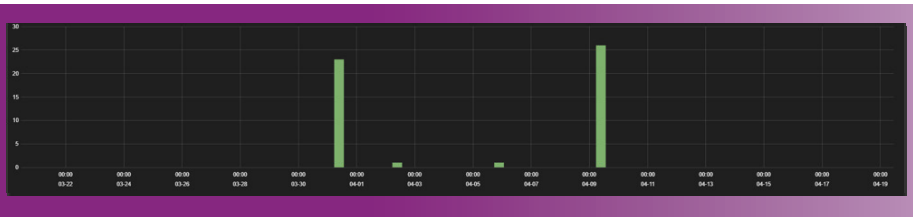


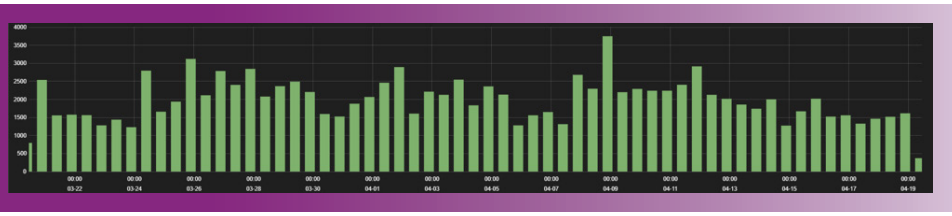
Fig 3
Transaction graph for smart printers and 3D printers

Smart TVs

Smart TVs are network-connected televisions used in offices and homes for entertainment and presentation purposes. We observed a total of 46 different TV models from 17 manufacturers, including **Hisense, Letv, LG, MStar, Panasonic, Philips, Realtek, Samsung, Sharp, Sony, TCL,** and **Xiaomi.**

Figure 4 shows the traffic distribution from different smart TVs.

Fig 4
Transaction graph for smart TVs



Set-top boxes and DVRs

Set-top boxes are network-connected devices used for streaming content to screens and TVs. We saw 109 different device profiles from 68 manufacturers, including **AerialBox, Alfawise, Amazon, Amlogic, Apple, Beelink, BenQ, Bomix, Bqeel, Foxtel Now,** and **Google.**

Along with set top boxes, digital video recorders (DVRs) have a strong presence in enterprise traffic. DVRs are network-connected smart devices used for recording and playing back digital videos. We saw three manufacturers: **TVT, EverFocus,** and **DIRECT TV.**

Figure 5 shows the traffic distribution from different set-top boxes and DVRs.

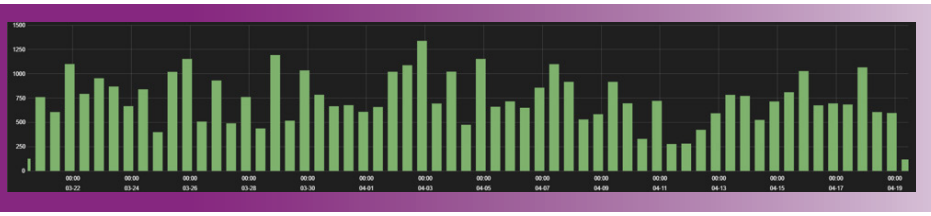


Fig 5
Transaction graph for set-top boxes and DVRs

IP phones and data collection terminals

IP phones are network-connected smart desktop phones used for communication that are commonly found in enterprise. We saw four different devices from **Polycom, Grandstream, Cisco,** and **Yealink.**

We also saw data collection terminal devices, which are used in enterprises for logging and storing data. We identified a total of 20 unique devices from five manufacturers: **Chainway, Coppernic, Honeywell, Motorola, Zebra.**

Figure 6 shows the traffic distribution from different IP phones and data collection terminals.

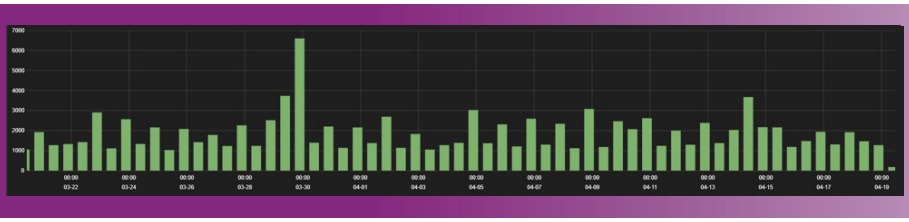


Fig 6
Transaction graph for IP phones and data collection terminals

Medical devices

Medical workstations were also present in the enterprise traffic during our analysis, and we saw smart medical devices such as insulin monitors that require internet connectivity.

Figure 7 shows the traffic distribution from medical devices.

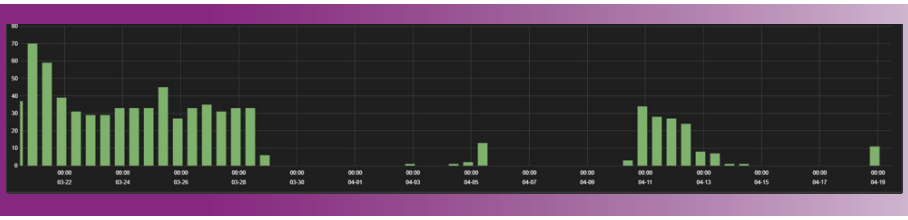


Fig 7
Transaction graph for medical devices

Media players and digital signage media players

Media players are entertainment devices for streaming videos and music. We found 24 device profiles from 18 different manufacturers, including **Bose, Sonos, Google, Pioneer, Sony,** and **Roku.**

Digital signage media players are used for automatically, wirelessly, and remotely managing televisions and monitor displays. We saw six different models from four manufacturers: **BrightSign, Navori, ViewSonic,** and **Promethean.**

Figure 8 shows the traffic distribution for media players and digital signage media players.

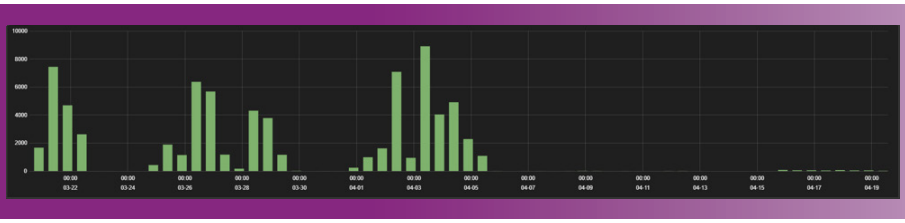


Fig 8
Transaction graph for media players and digital signage media players

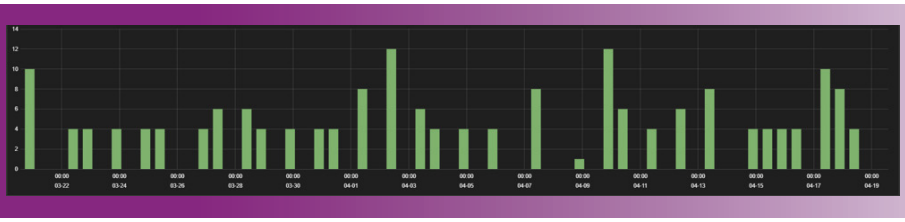
Industry control devices and networking devices

Devices used for different types of control systems and associated instrumentation include the devices and systems used to operate and automate industrial processes.

Smart networking devices from **IXON**, **Netbiter**, and **Synology** were also present in enterprise logs.

Figure 9 shows the traffic distribution from different industry control devices and networking devices.

Fig 9
Transaction graph for industry control devices and networking devices



Automotive devices

Interestingly, we saw some automobile media devices also connecting through the Zscaler cloud. We saw four car models from two different makers: **Tesla** and **Honda.**

Along with these cars, we saw transactions from **Chamberlain** smart garage door openers.

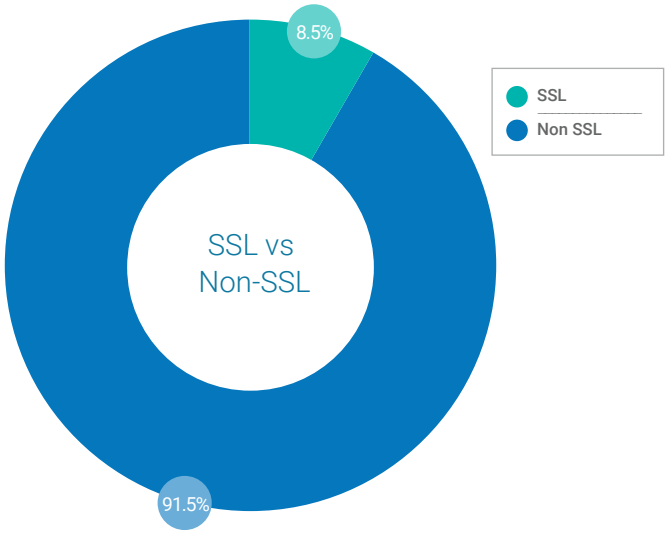
Security and privacy concerns

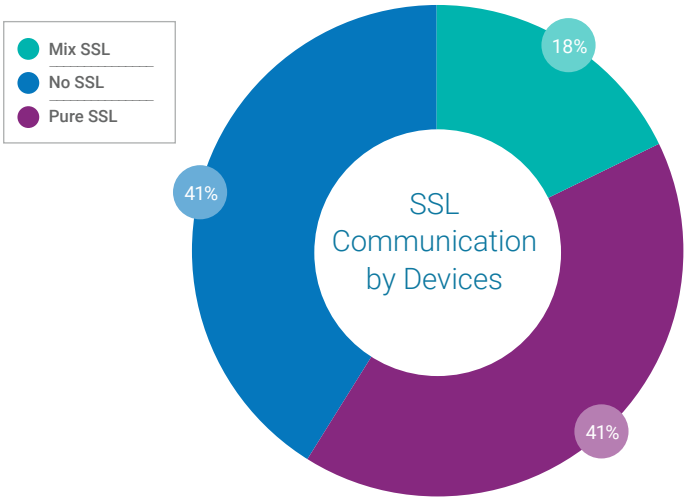
While looking IoT devices in the enterprise, we also observed that some devices are not following the proper security practices, making them vulnerable to further crafted attacks. The security issues we observed in our analysis include:

1. Plain-text HTTP communication to a server for firmware or package updates
2. Plain-text HTTP authentication
3. Use of outdated libraries
4. Weak default credentials

SSL vs. non-SSL

We also looked into how many devices are transacting in plain text and how many are doing so over encrypted channels. We saw that approximately 91.5 percent of transactions are occurring over a plain text channel whereas only 8.5 percent are using SSL.





From a device perspective, we saw 18 percent of total devices are using SSL exclusively to communicate. Forty-one percent of devices are using partial SSL (where some communication happens over SSL and some is over non-SSL channels), while the same percentage (41 percent) of devices were found to be using no SSL at all for any of the communication.

Malware in IoT enterprise traffic

Each quarter, the Zscaler cloud blocks approximately 6,000 transactions from IoT-based malware and exploits.

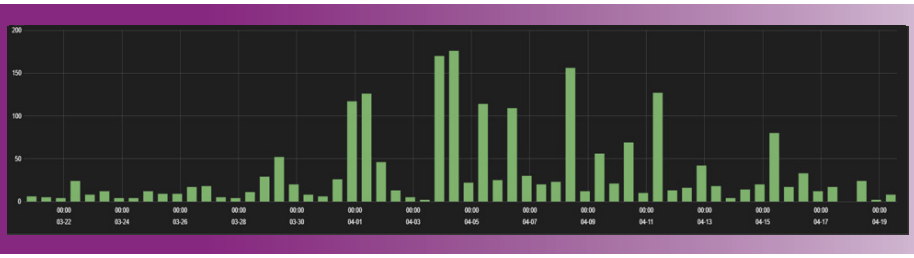
Earlier this year, ThreatLabZ analyzed certain threats that were targeting IoT devices. The team found that even though brute-force attacks that use default passwords are not new, they remain effective because default device passwords tend to go unchanged following installation. Often, the IoT malware payloads contain a list of known default username/password names, which, among other things, enables one infected IoT device to infect another.

In addition, the researchers saw variants of the Mirai botnet that seemed to be leveraging vulnerabilities present in IoT devices. These vulnerabilities are mostly in management frameworks and, by exploiting them, attackers are achieving remote code execution. This typically results in turning the infected device into a bot which, in turn, forms a bigger botnet army.

In some cases, we also saw cryptominers as the final payload delivered in the IoT campaigns. And we detected the RIFT botnet, which emerged in December 2018 and has in its arsenal up to 17 different exploits. To read more on these and other types of IoT malware, read the ThreatLabZ blog.

Figure 10 shows the distribution of malware families from enterprise traffic.

Fig 10
Transaction graph for industry control devices and networking devices



The top IoT malware families we saw during our study period include:

- **Mirai**
- **Gafgyt**
- **Hakai**
- **Rift**
- **Bushido**
- **Muhstik**

Top destination connected by IoT malware families

- **66%** connect to the United States
- **12%** connect to Canada
- **2.5%** connect to France
- **2.2%** connect to Greece
- **2%** connect to Russia

Conclusion

IoT devices have become commonplace in enterprises from all industries and in nearly every corner of the globe. These devices were designed to help improve efficiency and expand communications, and organizations continue to explore new ways to incorporate these devices into everyday operations. Of course, many of the devices are employee owned, and this is just one of the reasons they are a security concern.

The fact is that there has been almost no security built into the IoT hardware devices that have flooded the market in recent years, and there's typically no way to easily patch these devices. While many businesses have thought security for IoT devices unnecessary because nothing is stored on the devices, this isn't the case. The Mirai botnet attack illustrated how exposed companies can be as a result of their IoT devices. Even though companies hadn't thought of their IoT products as computers, Mirai showed that they essentially are, and very powerful botnets can be put together using IoT products as a result.

These devices continue to be an easy target for cyberattacks, but as the IoT footprint in the enterprise expands, there are some things that can be done to reduce the risk:

- Change default credentials to something more secure. As employees bring in devices, encourage them to be sure their passwords are strong, and their firmware is always up to date.
- Install IoT devices on isolated networks (to prevent lateral movement), with restrictions on inbound and outbound network traffic.
- Restrict access to the IoT device as much as possible from external networks. Block unnecessary ports from external access.
- Apply regular security and firmware updates to IoT devices, in addition to securing the network traffic.
- Finally, deploy a solution to gain visibility of the shadow IoT devices that are already sitting inside the network and ensure above safeguards.

Learn how Zscaler can help you protect IoT and all other internet-bound traffic.

Zscaler, Inc.
110 Rose Orchard Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com