armis

BUYERS' GUIDE TO IOT SECURITY

The definitive guide for evaluating IoT security solutions.

The Internet of Things (IoT) age is here and thriving. Today there are over 8.4 billion devices connected, and that number will grow to 20 billion by 2020.[1] The IoT era not only brings new opportunities, but also presents an expanded attack surface, already being exploited by cyber criminals.

THE PROMISE OF THE IoT AGE

The promise of connected devices is they will help us conduct business, deliver healthcare, manage resources, faster and more efficiently. Today connected devices are business solutions such as smart devices, TVs, printers, business collaboration systems, HVAC systems, lighting systems, security systems, jet engine components, oil rig drills, manufacturing systems, medical devices and more. We are way beyond BYOD.

CONNECTIVITY FIRST, SECURITY SECOND

With the new IoT age, it is connectivity first – security second. This is true for manufacturers, consumers, and businesses alike. The focus is on getting the device, hooking it up, and establishing connectivity. From a user perspective, including businesses, security takes a back seat. Whether this is an employee bringing in a device, or new connected devices being installed by operations or facilities, IT and security are too often not aware or able to ask crucial architectural questions. McKinsey says security issues may represent the greatest obstacle to growth of the IoT.[2]

THE IoT SECURITY BLIND SPOT

These new devices bring three challenges to businesses:

1) Designed to Connect

IoT devices are designed to connect. In many cases, they are actively seeking connections, whether you want them to or not. Which means attackers can search, find, and attempt to connect to these devices anytime. And you won't even know about it.

2) They May Be Invisible

In many cases, IoT devices may not be connecting to the corporate wireless or wired network, as they should be. This effectively renders them, and the connections they make to unmanaged or rogue networks, invisible to businesses. In such a situation, traditional network access control and networking solutions cannot see the device or the connection. And in this case, you cannot manage what you cannot see.

3) They Are the New Attack Vector

With the Mirai attack in October of 2016, millions of IoT devices were easily and remotely compromised, creating the largest, and most coordinated IoT exploitation to date. It impacted companies globally, including Amazon.com, Airbnb, Netflix, and many others. The attack preyed on IP printers, cameras, DVRs, etc., and created a massive distributed denial of service (DDoS) attack. While we have seen this type of attack before, this signaled the vulnerability of the new IoT devices for business and showed how widespread an attack can be as a result. Today, we are watching the mysterious Hajime and Persirai botnets spreading through brute force attacks on IoT devices.

Businesses and security professionals find themselves blind when dealing with these new connected, unmanaged devices. This is the IoT security blind spot.

IOT DEVICES AND BEYOND

- Smartphones
- Tablets
- Smart TVs
- Smart Lighting Systems
- Smart HVAC Systems
- Security Cameras and Systems
- Wireless Keyboards
- Wireless Mouses
- Wireless Headsets
- DVRs
- Smart Cameras
- Medical Devices and Monitors
- MiFi-like Routers and Hotspots

THE TRADITIONAL APPROACHES WILL NOT WORK

The IoT security blind spot means cybercriminals have an expanded attack surface. This creates a new landscape where the traditional methods of security do not suffice. By 2020 fewer than 10% of all devices will be managed by traditional methods.[3] This means the exposure is real today.

In fact, IDC has stated that 90% of IT networks will have an IoT-based security breach within two years.[4]

The challenge is that you cannot put an agent on most of these devices, so they are defenseless in the new age. For those devices that have user IDs or passwords, too many have default credentials that are never changed or simple easily-exploited log ins. Not to mention, the user interfaces are seriously lacking to make security practical.

These are the challenges with the current approaches:

∘ **Endpoint Protection** – This won't work because most devices cannot host an agent. So it is a non-starter.

∘ **Firmware Updates** – Many IoT devices do not have a simple method for automated firmware updates.

∘ **Mobile Data Management (MDM)** – These devices might be smartphones or other mobile devices. However, as we have seen, MDM solutions are costly and require administration as well as compliance. The challenge is that MDM solutions still won't address a large volume of devices brought in by visitors, contractors, delivery people, and others.

∘ **Network Solutions** – These typically only see the unmanaged or IoT device when it is connected to the network. Devices that are off the network with a wireless connection to a rogue or shadow network are invisible. They are unstoppable via current network access controls.

∘ **802.1x** – This will not address devices that cannot have certificates (e.g. a printer). Even if 802.1x solutions whitelist IoT devices, they do not address situations where a 3rd party device is masquerading as a privileged device. Or worse, they are blind to an infected or compromised device that still has access privileges. We have seen both of these situations with customers.

REAL SCENARIOS - REAL CONSEQUENCES

COMPROMISED DEVICES
Privileged devices that are exploited and out of the kill chain

° Tablet streaming video from the board room to an unknown outside location

° Employee smartphone connecting to and scanning multiple corporate networks

° Security cameras and routers on the network that are compromised and part of
 a botnet

UNMANAGED DEVICES
40% of devices are not seen by businesses

° Amazon Echo discovered connected to managed network in the CEO's office,
  continuously listening and transmitting

° Smart TV with exploitable vulnerability compromising devices that connect to it

° Printer with an open hotspot that allows hackers to circumvent network access control

UNCONTROLLED NETWORKS
Corporate devices connecting to uncontrolled networks

° Outside network is bridged to corporate LAN via corporate desktop

° Credentials being stolen due to corporate laptop connected to a rogue network

° Open network exploited by malicious devices in order to attack corporate devices
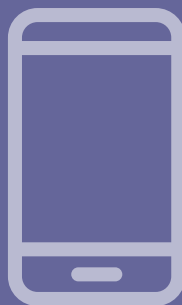
5 THINGS AN IOT SECURITY SOLUTION MUST DO

To be effective, an IoT security solution needs to be able to find a device in question device, understand its behavior, and proactively take action to protect the organization.

Here are 5 things an IoT security solution needs:

1) Should Have an Agentless Option
As we said above, you cannot put an agent on most IoT devices. Smart TVs, watches, projectors, printers, HVAC and even medical devices were not designed for an agent. And you cannot put an agent on every smartphone, tablet or device coming into your organization. How can you put an agent on the device the delivery person brings in to scan package deliveries?

Cybercriminals are always looking for the easiest way to gain access to your organization. As we have seen with the Mirai, Hajime, and Persirai botnets, IoT devices are the new targets. An agentless solution is critical because it is the only way to protect against attacks targeted at these devices.

2) See the Devices
In our IoT Security Assessment, we find that organizations are not aware of 40% of the devices in their environment.

You must be able to see the devices in your environment. As obvious as it sounds, this is not possible for traditional networking and network access solutions. Devices that are off the approved or managed networks, but connected to a rogue or shadow network, are invisible. This means these rogue networks are unstoppable via current network access controls. They are, in fact, out of the kill chain.

To be effective, an IoT security solution needs to see devices that may be "off" the approved or managed network. And not just devices: businesses need to see any network in their environment — unmanaged, rogue, or shadow networks included.

3) Identify and Track The Devices
Businesses must have deep insight into the devices, (managed or unmanaged), in and around their environment. It is important that you are able to:

◦ Profile and fingerprint any device

◦ Determine the state of that device
  ◦ Attack surface posture
  ◦ PCI/HIPAA compliance
  ◦ Jailbroken status
  ◦ Vulnerability history
  ◦ Number of wireless protocols
  ◦ User authentication
  ◦ Manufacturer reputation

◦ Track the device behavior and connections

◦ Provide historical record of the device behavior

◦ Associate devices with approved users

Only with this kind of data, can you assess the policy compliance or posture of a specific device.

4) Control The Connections

When addressing an IoT Security blind spot, visibility is critical. But visibility alone is not enough. Businesses need to take action, and disconnect questionable devices:

- Stop corporate devices from connecting to unmanaged, unapproved, or rogue networks

- Stop unmanaged or compromised devices from connecting to corporate or approved networks

- Reduce security admin workload by setting up policies for notification for critical alerts

You should be able to manually stop a device from connecting, as well as automatically disconnect devices and networks, in accordance with policies. Lastly, the solution should compile data and learn from devices and their interactions.

5) Frictionless Integration

No solution can help you if it is too complex or slow to deploy. So it is critical that an IoT security solution integrate in a fast and frictionless manner with your current infrastructure and environment. There are two components to consider:

○ First, it should integrate with and leverage your existing networking solutions, such as Cisco, Juniper, Brocade, Aruba, etc. This brings extended visibility and control across your existing environment.

○ Second, it should integrate with your existing security solutions, such as firewall solutions like Palo Alto Networks or Checkpoint and others. Strong integrations develop data and insights for deeper analytics and threat mitigation. No single solution can do it all, and you increase your protection when solutions work together.

SUMMARY

From the advent of the PC, to the internet, to mobile devices, to the cloud, history is a clear guide for us. With every technological advance and device, there are new security risks. Those new security risks are real, especially with the advent of these new IoT devices. Designed to connect in an ever-increasing wireless world, IoT devices are not built with security in mind. Cyber criminals are already exploiting that fact.

Now is the time for businesses and security professionals to include IoT security as a part of their comprehensive cyber-security strategy. Compliance and internal audits are identifying IoT devices as a point of vulnerability. Businesses need to be able to see and control any IoT devices in their environment.

The IoT age can deliver on the promise of efficiency and better insights — but only if it is safe.

ABOUT ARMIS

Armis eliminates the IoT security blind spot, protecting enterprises from the threat of unmanaged or rogue devices and networks. Midsize to large enterprises trust Armis' agentless IoT security platform to see and control any device or network. Headquartered in Palo Alto, California, Armis is a privately held company funded by Sequoia Capital with additional offices in Tel Aviv.

For more information, visit armis.com.

Sources:
[1] Source: Gartner, February 2017
[2] Source: McKinsey, May 2017
[3] Source: Gartner BI Intelligence
[4] Source: IDC FutureScape: Worldwide Internet of Things 2015 Predictions (December 2014)