IT security newsletter

December 2018

keypoint

IoT security

Described as the next industrial and human lifestyle revolution, the Internet of Things (IoT) refers to the use of sensors and communication technology embedded into physical devices that enable them to be tracked and controlled over the Internet. In a business setting, IoT devices include industrial machines, smart energy grids, building automation, plus whatever personal IoT devices employees bring to work. IoT security is the act of securing IoT devices and the networks they're connected to.

What are the main challenges?

IoT devices were not built with security in mind. Usually there is no easy way to install security on the device itself. They even sometimes ship with pre-installed malware, which then infects any networks they are connected to. Some network security can't detect connected IoT devices - or don't have visibility on which devices are communicating through the network.

How can Keypoint address your requirements?

IoT security can only be accomplished with an integrated solution that delivers visibility, segmentation, and protection throughout the entire network infrastructure. \
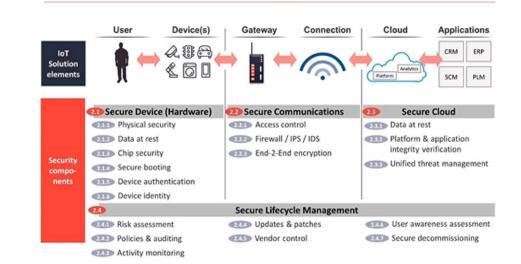
Learn

With complete network visibility, security solutions can authenticate and classify IoT devices, building risk profiles and assigning them to IoT device groups.

Segment

Once an enterprise understands its IoT attack surface, IoT devices can be segmented into policy-driven groups based on their risk profiles.

Protect

Policy-driven IoT groups and internal network segmentation enable monitoring, inspection and policy enforcement based on activity at various points within the infrastructure.

IoT Security happens on four different levels
Device, Communications, Cloud, and Lifecycle Management

Contact us:

Srikant Ranganathan
Senior Director
IT consulting
+973 1720 6827

Rayan Britto
Senior Manager
IT consulting
+973 1720 6834

Sagar Rao
Senior Consultant
IT consulting
+973 1720 6802