Aeris ConnectionLock: Restricting Device Communications to Select Destinations

PRODUCT SHEET

Gaining security for your IoT devices is a critical step for any deployment, large or small. Keeping your data secure can be business critical. Key to all this is the ability to restrict device communications only to select web destinations of your choosing.

Security Challenges in Today's IoT Deployments

Without any network restrictions in place, devices can send data to or receive data from any unintended destination. This increases the risk of the application data getting compromised, leading to data privacy violations. Such violations could be catastrophic for sensitive applications, such as remote patient monitoring or security systems.

In addition, this increases risk to customers by exposing applications and devices to open-ended attacks. For instance, massive botnet-powered distributed denial-of-service (DDoS) attacks have exploited vulnerabilities in tens of thousands of IoT devices (including video cameras, DVRs, etc.) and use them as a weapon to send a crippling amount of traffic to unsuspecting websites. One such vulnerability is that many IoT devices are shipped with easy-to-hack access credentials (username / passwords).

BENEFITS OF AERIS CONNECTIONLOCK™

Acts as an additional firewall within the Aeris IoT network.

Connect, send, receive only to/from pre-selected IP addresses or endpoints.

SIM cards cannot connect to other devices, thereby reducing security risks.

Solution implemented at the network level, so no added complexity or work for customer.

Furthermore, the SIM cards in customer devices that are fraudulently used for unintended applications (e.g., surfing the web) would result in significant data overage bills for the customers. For instance, restricted-access Tablets for IoT applications could be used to browse consumer internet websites (e.g., Facebook). As another example, in many places around the world, solar panel arrays are easily accessible. SIMs stolen from such field devices are used to browse the internet, leading to data overage charges.

Locking it Down

The Aeris Intelligent IoT Network is a dynamic, software-driven network that continuously evolves with new capabilities to support IoT deployments at scale. And gaining security with the Aeris solution is straightforward. In order to restrict data to and from devices, Aeris provides the ConnectionLock capability, which restricts data delivery only to designated IP addresses or endpoints. No additional action is needed from the customer side as ConnectionLock can be activated on all devices by the Aeris support teams during the onboarding process.

Customer Benefits

ConnectionLock acts as a software-based IoT firewall that is implemented as a core capability within the Aeris IoT network. This allows customer devices to connect (and send / receive data) securely to a set of pre-selected IP addresses or endpoints and prevent any fraudulent use by blocking access to any endpoint that has not been selected by the customer. As result, this significantly reduces the risk of customer application data getting compromised. Additionally, as the devices communicate to only selected endpoints, risk of devices being used for malicious open-ended attacks is significantly reduced.

Finally, in the event of theft or attempted misuse, ConnectionLock prevents access to unauthorized endpoints or IP addresses so that customer devices are not exposed to any data overage charges. If the SIM card gets stolen from the device, Aeris ConnectionLock ensures that the SIM card can connect to no other IP address or URL.

Customers don't need to implement any logic at the application level or in their business processes to receive the benefits of ConnectionLock. This Aeris solution is implemented at the network level so it doesn't add any complexity to the IoT device software. With this, manufacturers of connected devices can focus on bringing next-gen functionality to market and digital transformation to their businesses

Security and Support

The Aeris IoT network has been globally tested, is future proven, and can significantly enhance a business in multiple ways. When it comes to sending and receiving information, data connections are assessed according to the security rules that are configured for each device within the Aeris network. Any attempts by the devices to access unauthorized endpoints are blocked, keeping the sensitive application data from leaking out.

For more info, or to see a demo, contact Aeris

Visit www.aeris.com or follow us on Twitter @AerisM2M learn how we can inspire you to create new business models and to participate in the revolution of the Internet of Things.

United States Contact: **info@aeris.net** or **+1 408 557 1993**

Europe Contact: **eu_info@aeris.net** or **+44 118 315 0614**

India Contact: **india_info@aeris.net** or **+91 01206156100**

aeris