DATA SHEET

Connect Securely to the AWS Cloud

With Data Diode-Based Secure Cloud Gateways

AT-A-GLANCE

- The AWS cloud offers a range of benefits however, data is trapped inside of OT networks due to cybersecurity concerns with air-gapped architectures
- Software-based solutions do not provide the security assurance required by critical infrastructure to connect to the cloud
- Hardware-enforced secure cloud gateways provide a secure one-way out data path to transfer data to the cloud without compromising cybersecurity
- Hardware-enforced secure cloud gateways support the DHS Seven Strategies to convert all connections possible to one-way out of secure networks
- Data can be securely shared from devices at low levels of the network directly to the AWS cloud

Data Is Trapped in Air-Gapped Networks

Critical infrastructure networks are generating more data than ever before. However, critical data is trapped inside of these networks due to cybersecurity concerns with introducing new threat vectors to an air-gapped architecture. While a traditional air gap provides the highest level of security, this architecture has prevented the exchange of mission critical data to the cloud. AWS cloud services provide an ideal platform for aggregating and analyzing operational data, but software-based solutions fail to protect critical infrastructure when connecting to the cloud, preventing organizations from taking advantage of these benefits. Critical infrastructure organizations need a more secure way to transfer critical data out of an air-gapped network to take advantage of the benefits of the cloud.

Release Data to the Cloud Securely

The Department of Homeland Security (DHS) advises to convert all connections possible to a one-way out only architecture, which cannot be achieved securely with software-based firewalls. The only way to achieve this architecture securely is through hardware-enforced data diode technology. Hardware-enforced data diode technology provides secure one-way transfers out of secure networks without compromising an air-gapped network architecture. Unlike software-based firewalls, data diodes prevent external routable access (ERA), eliminating new threat vectors from being introduced back into the secure network. Owl's data diode-based secure cloud gateway solutions provide critical infrastructure with a hardware-enforced, secure one-way path to the cloud without compromising the security of an air-gapped architecture.

Hardware-Enforced Cloud Secure Gateways

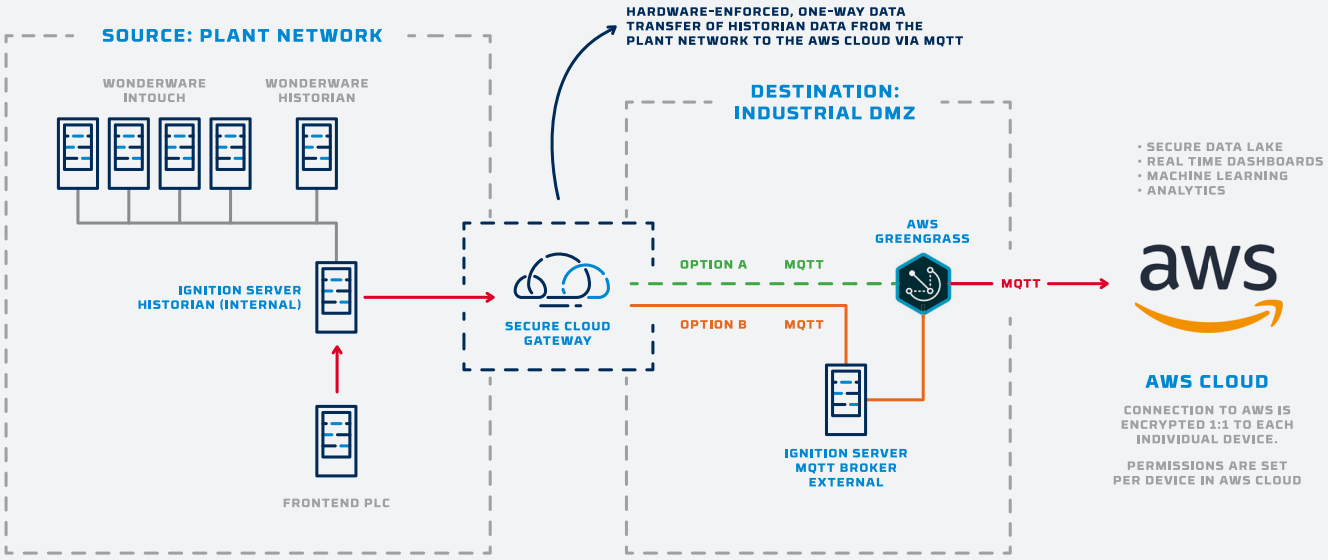
Owl's hardware-enforced data diode-based secure cloud gateway solutions securely transfer OT data one-way out of the network through cloud brokers, like Mosquitto, Chariott (Ignition), and Hive MQ, via industrial protocols, like MQTT and AMQP, to the cloud. The hardware-enforced nature of these solutions prevents external routable access back into the source network through these connections. Owl supports commonly-used industrial protocols and cloud brokers to achieve various cloud use case architectures. A large agricultural processing company deployed Owl's secure cloud gateway solutions to securely connect to the cloud and unlocked thirty years of an air-gapped network status.

USE CASE

USE CASE: CONNECT TO THE AWS CLOUD SECURELY THROUGH SECURE CLOUD GATEWAYS

A critical infrastructure organization needs to securely transfer Historian data from a plant network to the AWS cloud for monitoring and analytics, without introducing new risk to the plant network. Relying on a firewall is out of the question due to software-based solutions compromising the isolation of an air-gapped plant network. This organization deployed a hardware-enforced secure cloud gateway at the edge of the plant network to securely transfer operational plant data one-way out of the network to the AWS cloud.

The Historian data from the plant network can travel one-way from the internal Ignition server on the source side through the data diode via the MQTT protocol adapter to an external Ignition server on the destination side. From the external Ignition server, the data travels to AWS GreenGrass and then to the AWS Cloud for monitoring and analytics. The data can also travel through the data diode straight to AWS GreenGrass and then to the AWS Cloud. The hardware-enforced secure cloud gateway solution enables the organization to securely transfer OT data to the AWS Cloud without compromising the security of the plant network.



Supported Cloud Protocols & Brokers

Owl's hardware-enforced data diode-based secure cloud gateways support common industrial protocols and cloud brokers for secure cloud connections.

CLOUD PROTOCOLS

- MQTT
- AMQP
- File Transfer
- Modbus
- OPC
- Historian Replication (OPTS)

CLOUD BROKERS

- Mosquitto
- Chariott (Ignition)
- Hive MQ

Secure Cloud Gateway Solutions

OPDS-100D

OPDS-1000