WHITE PAPER

A New Paradigm: OT Security and Data in the Cloud

Summary

Many industries have seen significant improvements in operational efficiency and reduced downtime by adopting advanced analytics and optimization algorithms that run on cloud services. Critical infrastructure operators have been slow to adopt this new technology, due to well-justified concerns over the security and regulatory compliance of external connections.

However, the potential benefits of OT-to-cloud connectivity grow more apparent each year, creating additional incentives for critical infrastructure operators and device manufacturers to support secure external network connections.

The adoption of hardware-enforced security technology to deliver data to the cloud can help the industry accelerate adoption of cloud services, without the need for complex network analysis, and while fully meeting all regional and federal regulatory requirements.

Equipment vendors are starting to explore the integration of this technology directly into their new designs, to enable advanced support and maintenance services that are driven by real-time machine data.

Is it safe to connect?

Conventional wisdom dictates that OT devices should not be connected to external networks, due to the potential consequences if a threat actor were to gain access to a sensor, programmable logic controller, SCADA device, or other OT asset. A successful cyber attack on an OT network, especially at the lowest network levels, can lead to damage far more serious than the financial losses that follow a typical security breach.

The need for rigorous security in the OT environment remains as strong as ever. However, new technological capabilities, together with changes in enterprise IT architecture, have forced a re-examination of the traditional approach to OT connectivity.

Rather than maintaining a simple “no connections” strategy, many organizations have begun to explore and implement technologies that keep OT devices safe from external threat vectors, while enabling—under strict control—connectivity to cloud services or other external networks.

Opportunities in the cloud

As the industrial internet of things continues to evolve and cloud providers add new capabilities, the case for sending OT data to the cloud has become compelling, even for the most security-conscious operations.

Cloud services provide an ideal platform for aggregating and analyzing operational data, especially for organizations with multiple facilities or business units that do not share a common IT infrastructure. With cloud connectivity, critical infrastructure organizations can improve the efficiency and resilience of their operations in ways that were not previously possible.

In addition, machine vendors to the industrial market are beginning to offer enhanced support and services that depend on connected equipment. In order to work, these services—which can include predictive maintenance, planned downtime, and data-driven failure analysis—depend on data flowing out of devices in the plant and back to the manufacturer’s cloud service, where the data can be monitored and analyzed.

Each year, new applications of cloud computing become available, and there are more benefits to be gained from centralized, real-time visibility into device status and performance. The question is how to achieve that visibility without exposing the connected devices to attack.

Hardware-enforced security

The answer is hardware-enforced security technology that allows data to travel out of the facility to the cloud, without providing a path back inside that could be exploited by threat actors. Data diodes and hardware-enforced protocol validation technology do exactly that.

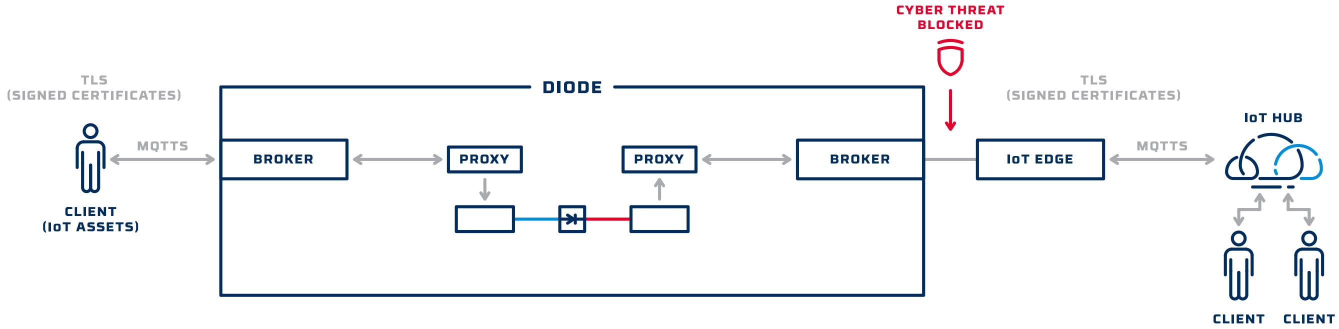
Inside an optical data diode, data follows a one-way path–through an optical transmitter, across a fiber optic cable, and into an optical receiver–that allows no possibility for data to travel in the opposite direction. Similarly, digital isolators use transformers to magnetically couple data across an isolation barrier in a one-way-only method.

No software-based firewall can provide the same level of assurance, which is why many organizations now require a hardware-based security for any use case that involves data from an OT device being sent to the cloud.

Protocol adaptability

To facilitate OT-to-cloud connectivity, security technology must be able to support a wide range of protocols. This includes protocols—such as MQTT or AMQP over TCP/IP—that are inherently two-way, even if the data flow is strictly one-way.

This can be achieved through the use of protocol adapters paired with data diodes. Data diodes provide secure, one-way data transfers, while proxies maintain simultaneous two-way communications on either side of the diodes.



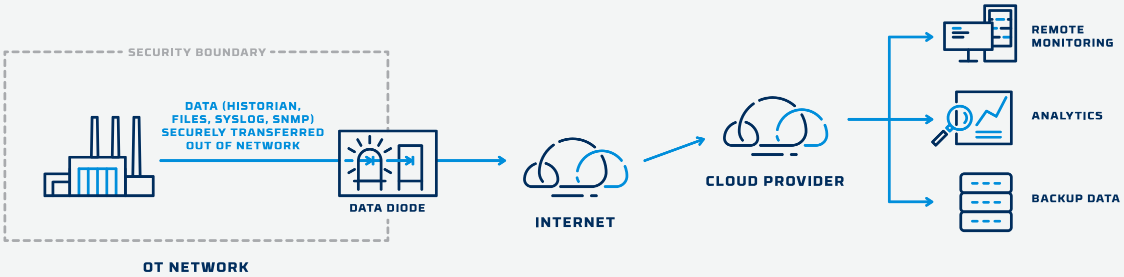
Hardware-enforced separation of source and destination networks ensures security for IoT assets, with no shared routing or device information between domains. Protocol validation that is implemented in hardware cannot be modified or disabled by malicious software. This approach can be used with or without cloud-based or external brokers.

Case study: Cloud-based monitoring and analytics

GE and Microsoft pioneered the use of cloud-based OT monitoring and analytics several years ago, using data diode technology from Owl Cyber Defense to protect the data.

In this implementation, gas turbines used for power generation are connected to the cloud, via a data diode that provides a deterministic one-way data flow from the turbine to an OSM console, which in turn is connected to a cloud-based analytics platform.

Data from the turbine can be used for performance optimization, maintenance scheduling, and other purposes, without exposing the device to external tampering, as there is no path back into the turbine that can be exploited by a threat actor.



With this type of OT-to-cloud data flow, protected by hardware-enforced security technology, critical infrastructure companies can optimize plant performance and device maintenance, thereby reducing operating expenses and delivering more value to customers.

On the horizon: embedded security technology

As the adoption of hardware-based security accelerates, a new technology will make it even easier for device manufacturers and asset owners to protect their OT devices while enabling outbound connections to the cloud.

Embedded cybersecurity technology–security hardware that is built directly into OT devices–offers an ideal solution for managing the growth of the IIoT and the need to share data securely.

Building security directly into industrial devices provides a range of benefits for operators, designers, and manufacturers of industrial and critical infrastructure controllers and safety systems. Recent innovations make it possible for hardware-based security to be built into modular platforms, such as sensors, programmable logic controllers, SCADA devices, and network switches. This technology provides highly secure, deterministic, data flow management between industrial equipment and external networks.

Embedded security modules provide maximum assurance for critical OT data, while reducing cost and administrative overhead. The first hardware-enforced embeddable security modules were introduced to the market in January 2021 and have already received significant interest from device manufacturers and OT operators.

The benefits of using OT data in the cloud are too numerous to ignore. With a new approach to security, based on hardware-enforced solutions, the energy industry will be able to harness the full potential of the cloud in 2021 and beyond.

OWL Cyber Defense

Owl Cyber Defense Solutions, LLC leads the world in data diode and cross domain network cybersecurity. With a constant focus on customers in the military, government, critical infrastructure, and commercial communities, Owl develops market-first, one-way data transfer products to meet a variety of operational needs, from entry level to enterprise.

For more information on Owl, or to schedule a demo, visit www.owlcyberdefense.com

@OwlCyberDefense

203-894-9342 | Sales@owlcyberdefense.com