OWL Cyber Defense

BROCHURE

Critical Infrastructure Frequently Asked Questions

1. Is the Owl data diode a firewall or is it different than a firewall?

Answer – Owl data diode solutions are similar in some ways to firewalls (or "industrial firewalls"), and perform many of the same security duties, but are inherently different because they are hardware-enforced, rather than software-enforced. Firewalls rely on software-based mechanisms, including rules, policy, and filters to control access, while data diodes rely on an immutable hardware-based mechanism that is enforced by the laws of physics and cannot be modified through software.

2. Does the data diode replace a firewall?

Answer – Not necessarily. Owl data diodes can work directly with existing firewalls as part of a strong "defense-in-depth" strategy, with layers of security tools working together for additional security. However, if it is determined the firewalls are no longer needed or do not provide any additional security, they can be removed.

3. How is the diode designed to be one way?

Answer – Owl data diodes are actually comprised of two communication cards that work as a pair. The communication cards are designed so that they work "in series," one sending data to the other. The first card is the "send" card and only has electronic components that allow it to send data, it has no way to "listen" or receive data. The second card, the "receive" card, only has electronic components that allow it to receive data and has no way to transmit data. In this way data can only flow in one direction and physically can't go backwards. This hardware design prevents any software-based cyberattacks.

4. Is a one-way flow of data too restrictive for normal business operation?

Answer – While data diodes aren't the ideal security solution for every situation, they can be used in more use cases than people probably think, and as companies start to increase the number of segments created within their networks, the use of data diodes will only continue to grow. Many organizations already try to create one-way transfers out of secure OT networks with firewalls; data diodes create true one-way paths. Some customers use multiple paths for transfer of information into and out of networks, with the addition of defense-in-depth techniques like deep packet inspection, authentication and white-listing to enable the uploading of software patches and the transfer of demand orders. U.S. government agencies and the Dept. of Defense have been running hundreds of different programs and projects successfully for over 20 years using data diode technology to secure the transfer of information between different networks, segments, groups and enclaves.

5. Can the data diode remain active even if other systems within the facility need to be isolated (disconnected) because of an incident?

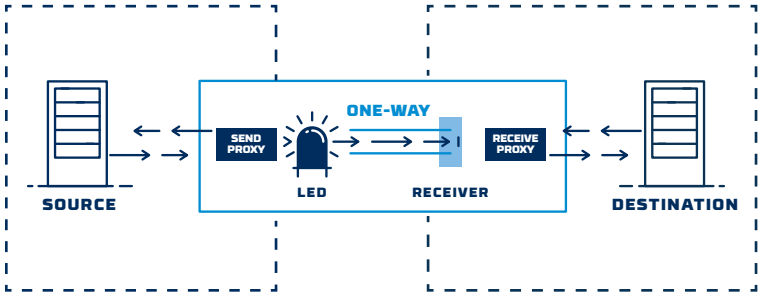
Answer – Yes, because the physical attributes of a data diode block 100% of any external access attempts against the network, the data diode can always remain operational without the need to be turned off or disconnected, sending reporting info to external end-users outside the security perimeter.

6. Don't you need two-way, bi-directional communication to establish communication between network endpoints?

Answer – Owl data diode solutions use proxies on both the send and receive sides to satisfy the transport layer (i.e. TCP connection) requirements by responding with the appropriate protocol messages (acks, nacks, etc.) to the endpoints on both source and destination networks. After the send side proxy terminates the TCP session, the payload is extracted from the packets and transported across the diode. On the receive side, a new TCP session is initiated, and the packets are sent to the destination endpoint. In this way, the source (OT) side remains invisible to the external networks and endpoints but data is able to flow from the OT network to the IT network.

7. How does TCP acknowledgement work with one-way transfers?

Answer – Each side of the data diode has a TCP proxy which interfaces with the endpoint on its respective network segment. The originating (source) TCP endpoint communicates with the proxy on the send side of the data diode, which terminates the source side TCP session and provides acknowledgements back to the TCP endpoint. Once the payload has traversed the data diode, the proxy on the receive side of the data diode communicates with the TCP endpoint on the destination network. The receive side proxy initiates the connection to the final destination and starts a new TCP/IP session. No TCP/IP session information is transferred across the diode.



8. How does the source network know the destination received the data?

Answer – With one-way communication, the question needs to be asked a different way. The source can't ask the destination if the data was received, the destination needs to be able to determine, on its own, if it received all the data. Owl data diodes provide an internal validation mechanism to achieve this. The source side calculates a running hash code value that is inserted in each packet so that the destination can verify if any transmit problems exist.

9. How is data integrity maintained without two-way communication?

Answer – Hashing and CRC (cyclic redundancy check) calculations are performed to ensure integrity of files. In addition, sequence numbers are assigned to each data packet that traverses the data diode so that the receive side will know if any packets are missing or out of sequence. Owl also uses the AAL5 (ATM Adaption Layer 5) standard for segmenting and reassembling packets which includes CRC on each packet.

10. When data is being replicated, how does the source application receive confirmation of the transfer?

Answer – Owl data diodes support several different methods of confirming the receipt of data from the source application(s). Both standards-based (OPC, Modbus, DNP3, IEC 104, etc.) and vendor specific protocols (OSIsoft, Rockwell, Schneider, etc.) are supported, as well as applications for transferring replicated data to the data diode. The send side of the data diode acts as the endpoint to the source application and provides confirmation to the application that the data is replicated (to the data diode). As the send side transport layer proxy (e.g. UDP, TCP, file) acknowledges the receipt of the data packets, the data payload is transferred across the data diode and strict policies/algorithms are used to ensure the destination application receives the data.

11. When a file is being transferred, what mechanism is used to make sure the whole file is transferred?

Answer – Before a file is transferred across the data diode, the system can automatically perform a hashing or CRC calculation on the file. The value derived from this calculation is part of the EOF (end of file) notification sent across to the receive side of the data diode. After the file is transferred, the same calculation is performed, and the results are compared to ensure the file was fully and correctly transferred. Any anomalies are logged. However, due to the extremely low latency and the very high reliability of Owl data diodes, if a solution is operating within bandwidth specifications, there is no reason for there to be any loss of data.

12. If a file fails to transfer, how can it be retransmitted?

Answer – Typically customers designate a folder/directory where the data diode checks for files to transfer. If there is an issue with a file transfer, it can be resubmitted to the directory and it will be automatically picked up and transferred. The frequency/interval that the data diode checks the directory is customer configurable.

13. What is the max throughput on both sides of the data diode?

Answer – Different models support different bandwidth ranges. For example, Owl DiOTa is designed for low-bandwidth, single protocol applications and supports up to 5 Mbps, but typical multifunctional models are capable of handling most throughput requirements (anywhere from 10 Mbps up to 1 Gbps). Higher-powered enterprise solutions are also available that support up 10 Gbps, or even greater throughput if used in parallel.

14. Is SABI and TSABI certifications required for Critical Infrastructure communication?

Answer – SABI and TSABI certifications are not mandated for any non-U.S. government applications.

15. Can you provide examples of OT domains where data diodes are deployed (DMZ/SCADA/EMS/ADMS, etc.)?

Answer – Data diodes can be deployed virtually anywhere from the edge of the facility network all the way down to individual devices. Typically, we see them deployed at DMZs between various levels of the network, to control data flows from one to the next. More recently, however, we've seen more installations at the micro-segmentation level and have recently released a line of embedded solutions designed to be installed within SCADA/ICS devices themselves.

16. Is there a use case where bidirectional data diodes would serve to eliminate ERC with an external customer for purposes of NERC-CIP compliance purposes?

Answer – This is one of the reasons that Owl created the ReCon bidirectional data diode solution. ReCon enables a secure, non-routable bidirectional command and control initiated only on the secure side of the network that meets the ERC requirements for eliminating persistent, routable bidirectional data connections. If a bidirectional data flow requirement cannot be met with ReCon, it is likely that the implementation would require a more sophisticated solution such as the XDI cross domain solution.

17. Are data diodes recommended by industry standards bodies or do they help meet any industry regulations or standards?

Answer – Data diodes are recommended for the security of industrial control systems by the U.S. Department of Homeland Security and the FBI1 and recognized by NERC and the NRC as a proven security method for electronic security perimeter defense. They are utilized in power stations and energy production facilities worldwide and can help meet a variety of standards and regulatory requirements such as NERC-CIP, ISA 62443, NIST SP 800-53 and 800-82, NRC Regulatory Guide 5.71, and more.

18. How does the data diode secure the "unpatchable"?

Answer – Because all data transfer to a protected domain, system, or device is eliminated by the data diode, there is no external digital method to access them, thus preventing any potential cyber attack which might exploit an unpatched weakness.

19. How do you protect the proxy server on the IT side of the data diode to protect from DOS attacks?

Answer – The deterministic nature of the one-way connection and the security of the operating system ensure that the device is completely locked down and does not even respond to ping messages from the destination side.

20. Do OT and IT remain in different domains? How does that work?

Answer – By definition, a data diode has a presence in two different networks/domains and acts as the boundary or demarcation point between the networks. Typically, the send side of the data diode is connected to the OT (trusted) network while the receive side is connected to the IT (untrusted) network. The data diode securely transfers data from the source to the destination while mitigating any attempts to penetrate the OT network.

21. If the routing information is pulled off the incoming packets, how does the data get to the destination?

Answer – Independent, deterministic routing tables are set up on both sides of Owl data diodes, based on each data flow that needs to be supported. When the data reaches the send side of the data diode, the first routing table is used to map the incoming data to a specific channel to cross the data diode. After the data crosses, the second routing table on the receive side is used to map the incoming channel to the final network address and the data is sent to the appropriate destination.

22. If you want to send data from the IT to an application on the OT network, do you need another path?

Answer – Yes, two independent paths can provide one-way out and/or one-way into the OT network. In addition, Owl has created a specialized solution (SSUS) designed to securely transfer files, software patches, and anti-virus updates into a secured network. These types of transfers are also performed extensively with specialized "cross domain solutions" across the Department of Defense and intelligence agency networks.

23. Does the data diode support encryption?

Answer – Yes, in two different ways:

- Encrypted data can be transferred across the data diode without any issues or special treatment
- Files identified for transfer can be encrypted by the data diode before being transferred

24. Can you store data in the DMZ?

Answer – Yes, depending on workflows, storage devices and policies. The data diode itself is not intended to act as a storage device; data is transferred between networks/segments/endpoints including storage points within a DMZ.

25. How is the network terminated on the data diode?

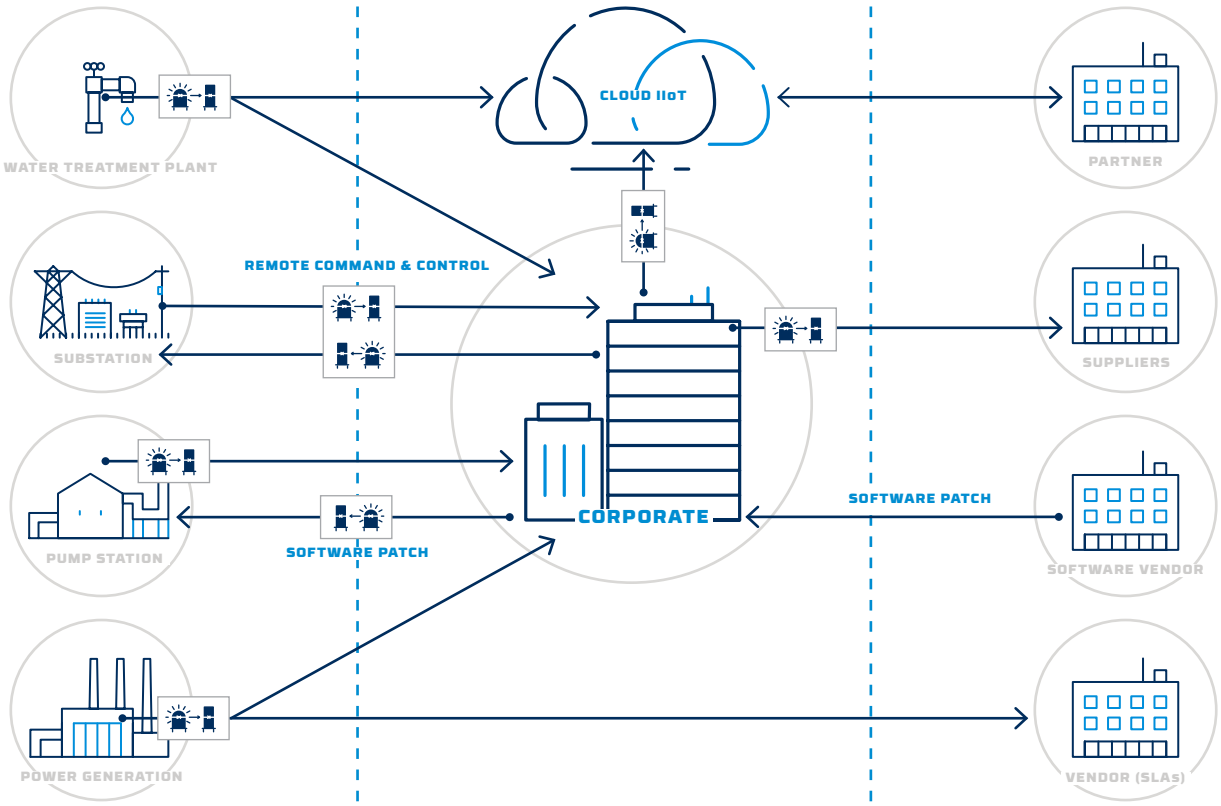
Answer – Each Owl solution has two Ethernet connections, one for the source network and one for the destination network, which are separated by the communication cards. A connection from the source network is established with the proxy on the send side of the data diode, which terminates that network session and initiates the isolated one-way transfer across to the receive side. On the receive side, the proxy accepts the data from the send side and initiates the connection with the destination network. In this way, each network connection is terminated at the point it reaches the data diode.

26. How is the data diode configured?

Answer – Each "half" (send/receive) of the data diode is configured independently in order to maintain the effective physical separation of the networks created by the device. A system administrator on the send side assigns incoming data flows to channels for transfer across the data diode and configures the source IP address/port and the protocol used (TCP/IP, UDP, etc.). Another system administrator on the receive side maps the incoming channels to source IP addresses/ports and defines the protocol to be used to transfer data to the destination point.

27. How do you connect two plants and send data between them?

Answer – At a basic level, each plant would have a data diode to send and receive data. However, as noted in the presentation, data workflows and policies need to be reviewed to ensure proper data flows to serve the business. Owl customers have deployed many different configurations that include consolidation of data from multiple plants into one plant, one-to-one data transfers, single direction data flows, redundant/failover configurations and multi-directional transfers. These configurations may require one or more data diodes to satisfy operational security requirements.



28. Who sets up the data flows and routing tables?

Answer – A system administrator from each domain that the data diode connects to is responsible for configuring their “side” of the data diode.

29. How do you ensure the data flow is not tampered with or redirected?

Answer – Owl data diodes feature separate network and admin ports, and the device must be taken offline in order to modify data flows. Owl also offers the flexibility to utilize an independent administrative network such that the data diode can be configured and maintained completely independently from the data transfer connection.

30. If you configure one side, do you have to configure the other side?

Answer – Yes, the data diode is intentionally designed to have each side be completely independent. If there was a way to configure both sides through a single admin channel then the diode would no longer be deterministically one-way, and there would be a “backdoor” between the two sides.

31. Is the remote HMI screen View-Only application?

Answer – Yes, Owl has an optional proprietary remote screen view software module. Two-way communication is not needed, the initial screen image and all changes are automatically pushed to the destination location. Command and control signaling cannot pass through the one-way data diode back into the OT network. However, if remote command and control is required, Owl does have a bidirectional solution (ReCon) that supports a secured connection over a single port, as recommended by the Department of Homeland Security.

32. How do data diodes prevent malware infections from spreading, e.g. to another plant?

Answer – Several features prevent the proliferation of malware from an infected network/segment:

- Owl data diodes only accepts data from a whitelisted source: Malware would need to spoof a valid source IP address, port, and protocol type in order to cross.
- Payload only transfer: Data is not transmitted in original packets across the data diode
- Protocol break: A different protocol is used to transfer the data payloads across the data diode
- Hashed and sequenced packets: Any "injected packets" would be identified and discarded
- Deterministic routing: If malware managed to cross the data diode it would have no control over where it goes, it is restricted to a predefined and configured address
- No return path: Malware cannot "phone home" through a data diode
- No external access: Malware cannot receive any remote commands through a data diode

33. What is the throughput or bandwidth of the data diode?

Answer – Different models support different bandwidth ranges. The DiOTa device is designed for low-bandwidth, single protocol applications and supports up to 3 Mbps. Owl's DIN rail compatible solution (OPDS-100D) supports up to 100 Mbps, while the 1U rackmount solution (OPDS-1000) supports upgradeable bandwidth from 26 Mbps up to 1000 Mbps. Higher-powered enterprise solutions are also available that support up 10 Gbps, or even greater bandwidth if used in parallel.

34. If I am transferring multiple data types, do I need multiple data diodes?

Answer – With the exception of DiOTa, all Owl data diode solutions can transfer multiple data types and multiple data flows simultaneously with multiple sources and destinations.

35. What is the latency of Owl data diode transfers?

Answer – It is measured in single digit milliseconds.

36. Can Owl data diodes transfer and/or replicate historian data?

Answer – Yes. Owl data diodes can replicate historian data out of the OT network in a one-way only transfer to any external network or the cloud. The one-way transfer ensures that the OT network remains isolated and protected from any potential cyberattacks.

37. If a historian is being replicated to a second location, is a second license required for the replicated historian?

Answer – Typically yes. Check with the historian provider for specific terms.

38. Are redundant solutions available?

Answer – Yes. There are a number of different possible solutions, including server-based configurations, failover configurations, redundant devices and support of 3rd party high availability configurations. In an Active Standby configuration, a second data diode can immediately and automatically take over the transfer of files if the primary fails for some reason. Upon the primary data diode returning to service, it automatically resumes the transfer of data.

39. When installing data diodes, does any software need to be installed on the source or destination servers/systems?

Answer – This depends on the type of data being transferred, the source of the data and how it is being accessed. Owl data diodes run on the Linux operating system; any data being transferred at a transport layer level (UDP, TCP, etc.) is handled natively by the Owl data diode. Data sources that have application specific requirements, require a file to be retrieved, or require support in a Windows environment may require the installation of a small application (i.e. client side of a client/server application).

40. Which industrial protocols are supported by Owl data diodes?

Answer – Owl data diode products natively support UDP, TCP/IP, SNMP, SMTP, NTP, SFTP, and FTP transfers, and a variety of other protocols and applications via optional software packages. Protocol adapters are available for Modbus, AMQP, MQTT, DNP3, IEC 104, HTTP(S), and OPC.

41. Is there a way to detect if people/viruses are trying to get into the network through the data diode?

Answer – Owl data diodes are locked down and don't even respond to ping messages – any attempts to ping the destination network go nowhere. The systems run on the Linux operating system and the audit logs (with corresponding Syslog messages) are available to the system administrators/ auditors to examine activities like failed login attempts. Owl data diodes also perform automatic internal audits that trigger alarm messages if the system has been modified.

42. Does Owl help with designing a solution using data diodes?

Answer – Yes, Owl sales engineers have extensive experience working with different data types (databases, historians, streaming video, files, etc.), sources, and protocols (SNMP, DNP3, IEC 104, OPC, Modbus, SMTP, etc.) and provide comprehensive pre and post-sales support to ensure the optimal solution is specified and successfully implemented.

43. Are Owl data diodes configured using a browser-based (web) interface?

Answer – It depends on the solution. Owl DiOTa features an intuitive browser-based interface, however for the majority of Owl solutions, a conscious decision was made to use a text-based menu system due for maximum security.

44. How can end-users on the IT network perform remote management of assets in the OT network?

Answer – Customers typically utilize the ReCon bidirectional solution for secure remote command and control of OT assets. Alternatively, users can deploy two one-way paths to maintain the integrity of the security perimeter.

45. Are upgradable bandwidth/throughput levels supported?

Answer – Yes. The OPDS-100D and OPDS-1000 support upgradable bandwidth licensing. Owl is the only provider that offers the ability to increase bandwidth as needed through a simple software license mechanism. Customers unsure their current or future bandwidth requirements can start at one level and then quickly and easily increase bandwidth by purchasing an upgrade license for a higher bandwidth level.

46. Does Owl have a sales office outside of the U.S?

Answer – Owl has direct sales presence in Europe and the Middle east, as well as a number of master distributor partners supporting sales and marketing activities globally. Please contact the Owl main office in the U.S. to be referred to the appropriate point of contact.

47. How are Owl products priced?

Answer – Owl offers a comprehensive line of products to meet a variety of budgets and requirements. Pricing is generally based on product bandwidth, although specialized products such as ReCon and SSUS are priced at a single tier. Owl sales engineers work with customers to determine the proper solution.

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 | Info@owlcyberdefense.com