ROCKWELL AUTOMATION
FREQUENTLY ASKED QUESTIONS

Rockwell Automation Encompass™ Product Partner

OWL CYBER DEFENSE

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

Answer – *The Owl Perimeter Defense Solution (OPDS) is similar in some ways to a firewall but is inherently different because it is hardware based. The OPDS/EPDS data diode products include the security properties of a software firewall but the real difference is that it is hardware restricted not software controlled. Software firewalls rely on rules and filters to control access, Owl's data diode relies on a patented hardware design that cannot be modified and only allows data to flow in one direction without any return path or backdoor.*

2.Does the data diode replace a firewall?

Answer – *Data diodes can work directly with existing firewalls creating a strong Defense-in-Depth strategy. If at a future point it is determined the firewalls aren't needed they can be removed.*

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

Answer – *Our data diode is 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 "source" 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 destination 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 cyber-attacks.*

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

Answer – *While data diodes aren't recommended for every situation, there are many different use cases where they are used. And as companies start to increase the number of segments created within their networks, the use of data diodes will continue to grow. Many organizations already try to create one-way transfers today 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 17 years using data diode technology to secure the transfer of information between different 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, since the physical attributes of a data diode block 100% of any inbound attempts against the network, the data diode can always remain operational, sending reporting info to external end-users outside the security perimeter.*

6. Don't you need 2 way, bi-directional communication to establish communication between network endpoints?

Answer – *The OPDS uses proxies on both the source and destination 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 sides. After the source side proxy terminates the TCP session, the payload is extracted from the packets and transported across the diode. On the destination side, a new TCP session is initiated and the packets are sent to the destination end point. In this way, the source (OT) side remains invisible to the external networks and endpoints but data is able to flow from the OT to the IT.*

7.How does TCP acknowledge work with one-way?

Answer – *As described in the question above, each half or side of the data diode has a TCP proxy which interfaces with the TCP endpoint. The originating (source) TCP endpoint communicates with the proxy on the source side of the diode, terminating the source side TCP session and providing acknowledgements to the TCP endpoint. Once the payload has traversed the diode, the TCP proxy on the destination side of diode communicates with the TCP endpoint on the destination network. The Owl destination side proxy initiates the connection to the final destination, and starts the TCP/IP session. The source side TCP proxy provides acknowledgements that the diode has received the data and destination side proxy receives acknowledgements that the destination has received the data. 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 doesn't need to ask the destination, the destination needs to be able to determine, on its own, if it received all the data. With the Owl data diode, 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.*

However, it is important to remember that issues related to data loss basically don't exist. The Owl DualDiodes are high performance solutions with very high reliability. The ATM protocol being used for one-way transfer across the DualDiode is very reliable, it maintains a very high level of quality of service (QoS) and is moving data a very short distance so the normal network impacts (latency, congestion, packet loss, packet switching, etc.) are avoided. In addition, the DualDiodes are always deployed with more than ample bandwidth so that reliability and performance are maintained.

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

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

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

Answer – *The Owl data diode supports several different ways of acknowledging the receipt of data from the source application(s). We support both standards based (OPC, Modbus, etc.) and vendor specific protocols (OSIsoft, Rockwell, Schneider, etc.) and applications for transferring replicated data to the data diode. The source side of the diode acts as the endpoint to the source application and provides confirmation to the application that the data is replicated (to the diode).As the source side transport layer proxy (UDP,TCP, file) acknowledges the receipt of the data packets, the data payload is transferred across thediode 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 diode the customer has the option for the system to automatically perform a hashing or CRC calculation on the file. The value derived from the calculation is sent across the diode as part of the EOF (end of file) notification sent to the destination side of the diode. After the file is transferred the same calculation is performed and the results are compared to ensure the file was correctly and fully transferred. Any anomalies are documented. However due to the extremely low latency and the very high reliability the diode, if it is operating within bandwidth specifications, there is no reason for there to be a loss of any data.*

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

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

13. Are OT and IT different domains? How does that work?

Answer – *By definition a data diode has a presence in two different networks/domains with the boundary or demarcation point between the networks going right down the middle of the diode. Typically the source side of the diode is connected to the OT network while the destination side is connected to the IT network. The diode securely transfers data from the source to the destination while blocking any attempts to penetrate the OT network.*

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

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

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

Answer – *Yes, just like airport security, two independent paths that provide one-way in and one-way out. In addition we have a specific product configuration designed to securely transfer files, software patches and anti-virus updates into a network. We do these types of transfers extensively across the Department of Defense and Intelligence agency networks.*

16. Does the data diode support encryption?

Answer – *Yes, in two different ways:*

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

17. Can you store data in the DMZ?

Answer – *Yes, depending on your workflows, storage devices and policies. The data diode itself is not a storage device; we transfer data between networks/segments/endpoints including storage points within a DMZ.*

18. How is the network terminated on the Owl diode? Where are the cards in the diagram?

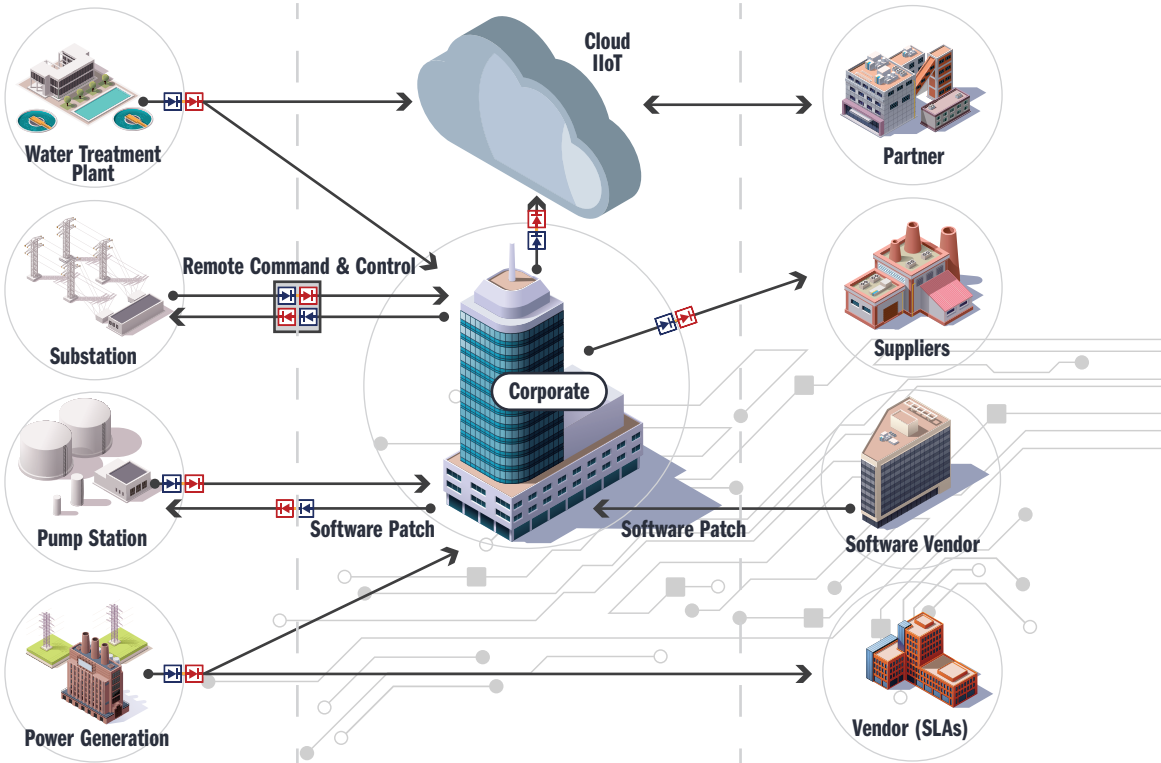
Answer – *Each Owl solution has two Ethernet connections, one for the source network and one for the destination network. The Ethernet connections are separated by the communication cards and help form the Defense In Depth strategy we deploy. The communication cards vary in capability and size to support different data rates and different form factor housings, for example the OPDS-100 1U appliance and the OPDS-100D (DIN rail) device.*

19. How is the data diode configured?

Answer – *Each "half" (source/destination) is configured independently in order to maintain the absolute one-way movement of information across the DualDiode. A system administrator on the source side assigns incoming data flows to channels for transfer across the DualDiode; this includes configuring the source IP address/port and the protocol being used (TCP/IP, UDP, etc.). A system administrator on the destination side maps the incoming channels to source IP addresses/ports and defines the protocol to be used to transfer data to the destination point.*

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

Answer – *At a basic level, each plant would have an OPDS 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. Our 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.*



21. 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.*

22. Are admin and data ports separate?

Answer – *Yes, we offer 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.*

23. 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.*

24. I understand how data diodes don't allow anything bad in to the OT network but how do they prevent a malware infection from spreading to another plant?

Answer – *Several features prevent this:*

- *Malware would need to spoof a valid source IP address, port and protocol type as the diode only accepts data from a white listed source*
- *Data is not transmitted in original packets across the diode, only the payload is transferred*
- *A different protocol is used to transfer the data payloads, creating a protocol break*
- *Packets are sequenced and any "injected packets" would be identified and discarded*
- *Static routing - Since the diode is split into two separately configured and administered "halves", if malware managed to cross the diode it has no control over where it goes, it is restricted to a predefined and configured address*
- *Malware cannot "phone home" through a data diode.*
- *Malware cannot receive any remote commands through a data diode*

25. Is the remote HMI screen (Virtualscreen View application) a view only application?

Answer – *Yes. 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 data diode back into the OT network. Owl does have a BiLateral solution that does support a single TCP connection over a single port as recommended by the Department of Homeland Security for remote command and control using data diode cybersecurity.*

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

Answer – *Different models support different bandwidth ranges. Our entry level model the OPDS-5D supports up to 5 Mbps, the OPDS-100D and OPDS-100 support between 10 Mbps and 100 Mbps, the OPDS-1000 supports up to 1000 Mbps per second and we have card kits that support up 10 Gbps.*

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

Answer – *No, the Owl OPDS data diodes can transfer multiple data types and multiple data flows simultaneously with multiple sources and destinations.*

28. What is the latency of the packets moving across the data diode?

Answer – *It is measured in single digit milliseconds.*

29. The diode allows me to transfer a Historian outside of the plant and leave the OT environment secure?

Answer – *Yes. The data is replicated out of the OT network in a one-way only direction, leaving the OT network safe from any network cyber-attacks while getting data to another part of the organization.*

30. If the historian is being replicated at corporate, is a second license required?

Answer – *Typically yes, but you need to check with your historian provider.*

31. Are redundant solutions available?

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

32. When installing the data diodes, does any software need to be installed on the servers that the data diode is either retrieving data from or sending data to?

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. Other data sources that have application specific requirements, need a file to be "picked up" or require support in a Windows environment may require a small application (i.e. client side of a client/server application) to be installed to support the collection of data before the data is sent to the data diode for transfer to the destination network.*

33. Is SNMP supported?

Answer – *Yes, the transfer of SNMP messages is a core capability of the Owl data diode products.*

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

Answer – *The Owl data diodes are normally "locked down" and don't even respond to "ping" messages. 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. The Owl data diodes also perform automatic internal audits that trigger alarm messages if the system has been modified.*

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

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

36. Who within an organization is usually responsible for implementing this technology?

Answer – *It varies across organizations. We have seen members of the cybersecurity team, OT engineers and IT engineers. Since the DualDiode typically sits between OT and IT (collecting data from the OT network and transferring it to the IT network) a good place to start is with the group that maintains the firewalls/DMZ that separates the OT network from the IT network.*

37. Is the DualDiode configured using a browser (web) based interface?

Answer – *No, a conscious decision was made to use a Linux, text based menu system due to the many vulnerabilities inherent in web servers and services.*

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

Answer – *Customers deploy two one-way paths to maintain the integrity of the security perimeter.*

39. Are variable bandwidth/throughput levels supported?

Answer – *Yes. The OPDS-100, OPDS-100D and OPDS-1000 support variable bandwidth licensing. Owl is the only provider that offers the ability to increase bandwidth as needed through a simple license mechanism. Customers unsure of exactly what their bandwidth requirements are going to be can start at one level and then increase throughput by purchasing a license for a higher bandwidth level as needed.*

40. Do you have a sales office outside of the U.S?

Answer – *We have a number of strategic partners supporting sales and marketing activities in different geographic regions globally. Please contact our main office in the U.S. and we can refer you to the appropriate partner.*

41. What is the pricing for the products?

Answer – *Pricing is based on throughput requirements. Owl offers a line of products that support different ranges of bandwidths. Our sales engineers work with customers to determine the proper solution.*

ABOUT OWL

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.