CLEAR, CONCISE CYBER SECURITY SINCE 2003

TABLE OF CONTENTS

3 ABOUT US

4 OUR VALUES

5 OUR MISSION

6 OUR CERTIFICATIONS

7 INDUSTRIES

8 CUSTOMERS & PARTNERS

9 CROSS-DOMAIN SOLUTIONS

10 TRUSTEDFILTER™

12 OPDS-1000

14 OPDS-100D

16 SSUS

18 ReCon

20 V7 CARD KITS

22 XD GUARDIAN

24 SCOWT COMPACT

26 DiOTa

28 FPGA MODULES

29 XDE TITANIUM

30 XDE RADIUM

31 XDE COBALT

32 CROSS-DOMAIN INTEROPERABILITY

33 ENHANCING NETWORK SEURITY

34 MISSION CONTROL

35 CCTV OPERATIONS

36 WEARABLE DIODE

37 TELEMEDICINE

38 OFFSHORE TO ONSHORE

39 ENERGY INFRASTRUCTURE

40 SECURITY OPERATIONS CENTRE

41 INFORMATION CLASSES

42 SME BACKUP SAFEGUARD

43 MILITARY DATA IN THE FIELD

44 AIRPORT SECURITY

ABOUT US

4SECURE®

4Secure is home to a committed team of people who strive to deliver the very best for our customers, suppliers and peers. You'll get to know our experienced information security professionals by name, and they will provide innovative solutions that reflect the realities of your day-to-day. Think of us as a trusted partner who can guide you through the measures needed to counter and respond to the most sophisticated and targeted cyber security threats.

"We align with the old adage of being small enough to care, but big enough to deliver. This mantra is understood by our customers, and we are the preferred supplier for many large organisations," 4Secure Managing Director, Peter Hoinville.

Our size means we can be agile, adaptable and quick off the mark for our customers, which is exactly what you need in the event of a cyber security incident. Most importantly, our customers know who to speak to throughout the entire lifecycle of a project and can build genuine rapport.
4Secure is about people, reliability, flexibility, agility and the ability to deliver time and time again, whatever the scale and whatever the task.

OUR VALUES

As a company we remain committed to our core principle of being a security rather than IT company. We strive to deliver excellence across a vast array of business profiles and operational systems for government, defence and commercial sectors across the UK and Europe.

INTEGRITY

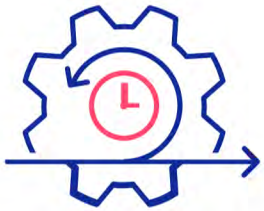
From our corporate strategy to our people, 4Secure has honesty and transparency at its heart. This means long lasting relationships with partners and customers alike.

ACCURACY

We conduct processes, data handling and record-keeping properly to ensure, as far as possible, that tasks are "right the first time". If we do make errors, we learn from our mistakes and refine our processes to avoid repetition.

#ONETEAM

We are small but mighty. We support and respect our colleagues and work collectively to achieve our and your goals. We embrace a healthy competitiveness and strive to push ourselves to all be better within our #OneTeam.



AGILITY

Being small allows us to move decisively and swiftly without compromising our integrity. Our processes are lean and reduce room for error or delay.

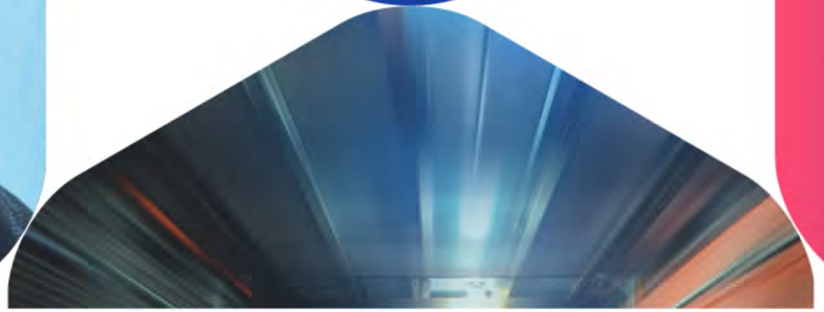
OUR MISSION, PURPOSE & VISION

Our vision is to cascade our knowledge and systems to the world, creating a space that is safe, secure and resilient no matter what the cyber threat landscape.

OUR PURPOSE

We live in a time with an increasing reliance on technology and fully connected digital worlds, which means an evolving cyber threat landscape. 4Secure exists to provide agile, effective and fully embedded cyber security expertise that maintains reliable IT systems and ensures business or mission continuity.

One-size-fits-all packages are not in the 4Secure repertoire. Our services are proportionate and conducted to suit the context of your business' requirements, threat level and risk appetite or tolerance level. We can proactively manage your cyber security efforts or work with an existing team to offer experienced knowledge and support at a moment's notice.



OUR MISSION

Since 2003, our seasoned cyber practitioners have focused on mitigating and eliminating the most serious cyber security threats for our clients. This means being at the end of the phone, responding quickly and curating meaningful relationships with each organisation on a case-by-case basis. This personal approach has led to many long-term relationships that we continue to nurture today.

OUR VISION

What will the digital world look like in 10, 20 or 30 years' time? At 4Secure, our long-term aspirations are to adapt and move with the cyber security landscape as it evolves, using all the knowledge we have today and shaping it to suit future threats and technologies. This means 4Secure will play an important role for our clients both now and in the coming decades as we keep pace with change.

OUR CERTIFICATIONS

CYBER ESSENTIALS PLUS

4Secure are Cyber Essentials Plus certified and are an IASME Cyber Essentials Scheme (CES) approved Certification Body (CB).

Having Cyber Essentials Plus offers a higher level of assurance to your organisations cyber security defences, through a range of internal and external tests of your network and computers.

IASME GOLD

The audited IASME Governance standard is IASME's highest level of certification and is an excellent alternative to ISO 27001 for small and medium sized organisations.

The standard includes all of the five Cyber Essentials technical topics and adds additional topics that mostly relate to people and processes, for example:

- Risk Assessment & Management
- Monitoring
- Change Management
- Training & Managing People
- Incident Response & Business Continuity

ISO 9001:2015

4Secure are ISO 9001:2015 accredited, demonstrating the adoption of a quality management system.

ISO 9001:2015 specifies requirements for a quality management system when an organization needs to demonstrate its ability to consistently provide products and services that meet customer and applicable statutory and regulatory requirements, and aims to enhance customer satisfaction through the effective application of the system.

JOSCAR SUPPLIER

By being a JOSCAR supplier, we are confident that we can continue to provide expert advice and demonstrate the effectiveness of compliance to our customers.

The JOSCAR Registration Mark is valued by some of the largest purchasers in the defence community and indicates that your organisation has gone through the process required to demonstrate its commitment and credentials to the industry.

INDUSTRIES

Our products and services have been deployed across a range of industries and are recommended by many of our customers. The US Department of Homeland Security has also listed Owl's products on the NATO Approved Information Assurance Catalogue.

Nuclear, fossil and hydro generation

Financial and banking

Telecommunications

Ministry of Defence

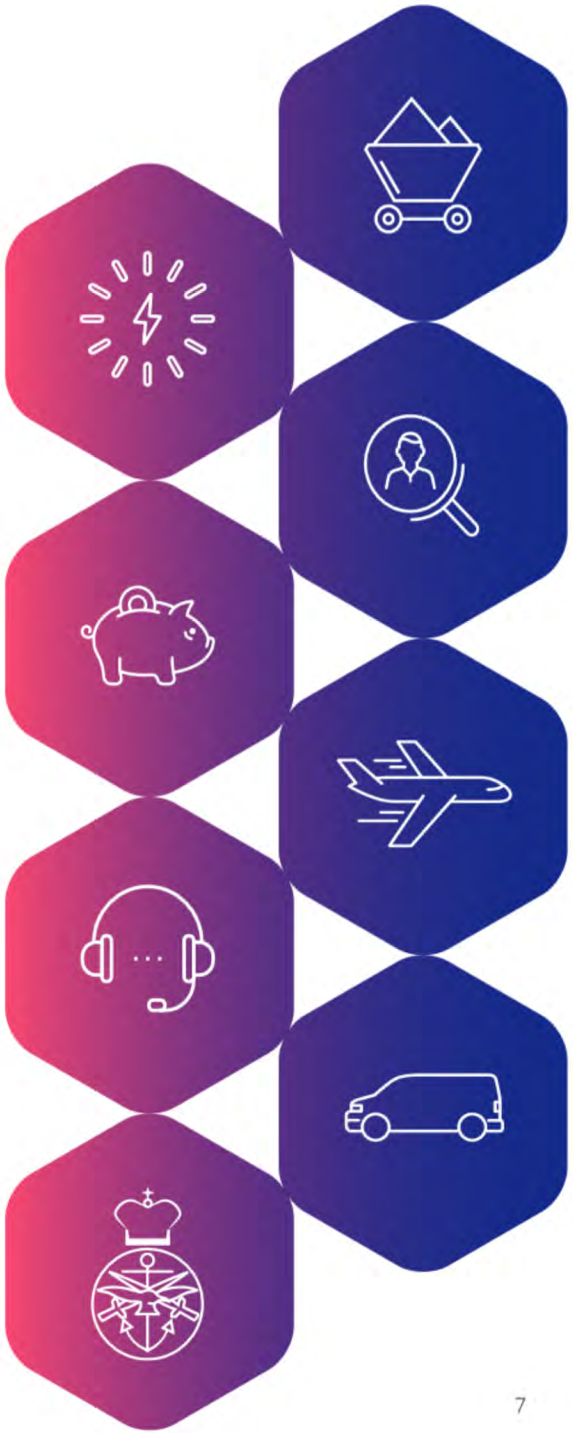
Oil, gas and mining industries

Security

Aerospace

Automotive & transport

DoD



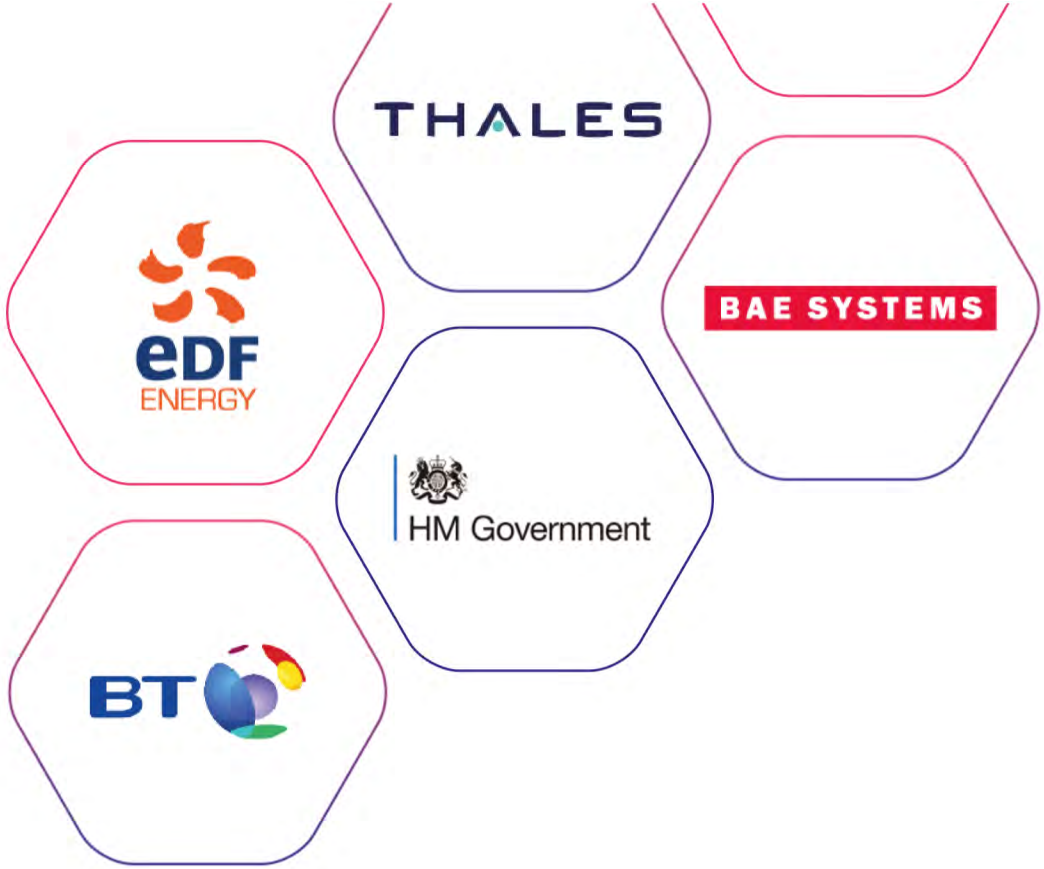
OVER 2,500 SECURITY SOLUTIONS DEPLOYED

OUR CUSTOMERS & PARTNERS

CUSTOMERS

4Secure manages a large client-base spanning across sectors such as government, defence, critical national infrastructure and enterprise.

With over 18 years of trading experience within government, defence and security, 4Secure is an agile and innovative cyber security company that is synonymous with delivering cross-domain solutions to enable data exchange across a broad spectrum of defence use cases.



PARTNERS

4Secure's exclusive partnership with Owl Cyber Defense provides a key element to the boundary security solutions deployed for our clients. Owl's hardware-based security combined with 4Secure's TrustedFilter™ Framework enables the deployment of reliable, robust and highly assured solutions for broad range of real world scenarios.

Owl Cyber Defence Technologies is recommended by many governmental and regulatory bodies worldwide as best practice in Industrial Control Systems (ICS) and Critical Infrastructure (CI) cyber security.

4Secure also work with partners such as 2iC and Panoptech to deliver enhanced network security for Government, Law Enforcement and Defence customers.

CROSS-DOMAIN SOLUTIONS

TRUSTED CROSS-DOMAIN SOLUTIONS IN MULTIPLE FORM FACTORS

Data diodes are hardware based, bound by the laws of physics and not susceptible to zero day vulnerabilities or any other hacks. These solutions are data and network agnostic, have been deployed across a range of industries and are recommended by the US Department of Homeland Security, as well as being listed on the NATO Approved Information Assurance Catalogue.

Being data agnostic we can move files, stream video, TCP/IP, UDP, database records, historians, sensor data, high-res images, system backups, personnel records and many other types of data; along with industrial protocols like Modbus and OPC. Our network independence allows us to work on unclassified, secret and top secret networks for government solutions and
IT and OT (Operations Technology) networks for our commercial and industrial customers.

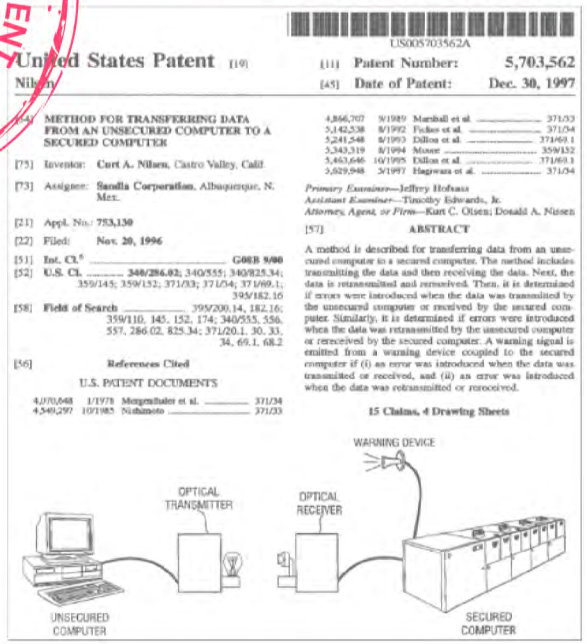
We offer all-in-one solutions in multiple form factors, from 1U rack mounted appliances to man portable USB devices and all in between. These form factors allow us to work across sectors and fit the individual needs within these. Our high bandwidth, enterprise solutions utilise commercial off the shelf (COTS) servers populated with our proprietary data diode cards.

Our technology is designed to be scalable; New software licences and modules allow end-users to increase bandwidth, add-on new interfaces and support new protocols within a live environment with minimal to no down time. Our technology protects the investment by organically growing to meet the project or mission requirements, and with a long mean time before failure rate, our technology not only meets long-term project requirements, our devices outlast most normal IT refresh rates, therefore reducing long term cyber security / IT costs.

OWL CYBER DEFENSE
RAISE THE BAR
READY
FLYING ABOVE THE BAR

UNITED STATES PATENT
DEC.30 1997
PATENT NUMBER 5,703,562
UNITED STATES PATENT

NEXT GEN CYBER SECURITY



US005703562A

United States Patent [19]
Nilsen

[11] Patent Number: 5,703,562
[45] Date of Patent: Dec. 30, 1997

[54] METHOD FOR TRANSFERRING DATA FROM AN UNSECURED COMPUTER TO A SECURED COMPUTER

[75] Inventor: Curt A. Nilsen, Castro Valley, Calif.

[73] Assignee: Sandia Corporation, Albuquerque, N. Mex.

[21] Appl. No.: 753,130

[22] Filed: Nov. 20, 1996

[51] Int. Cl.[6] G08B 9/00

[52] U.S. Cl. 340/286.02; 340/555; 340/825.34; 359/145; 359/152; 371/33; 371/34; 371/69.1; 395/182.16

[58] Field of Search 395/200.14, 182.16; 359/110, 145, 152, 174; 340/555, 556, 557, 286.02, 825.34; 371/20.1, 30, 33, 34, 69.1, 68.2

[56] References Cited

U.S. PATENT DOCUMENTS

4,970,648 1/1978 Morgenthaler et al. 371/34
4,540,297 10/1985 Nishimoto 371/33
4,866,707 9/1989 Marshall et al. 371/33
5,142,538 8/1992 Fickes et al. 371/34
5,241,548 8/1993 Dillon et al. 371/69.1
5,343,319 8/1994 Moser 359/152
5,463,646 10/1995 Dillon et al. 371/69.1
5,629,948 5/1997 Hagiwara et al. 371/34

Primary Examiner—Jeffrey Hofsass
Assistant Examiner—Timothy Edwards, Jr.
Attorney, Agent, or Firm—Kurt C. Olsen; Donald A. Nissen

[57] ABSTRACT

A method is described for transferring data from an unsecured computer to a secured computer. The method includes transmitting the data and then receiving the data. Next, the data is retransmitted and rereceived. Then, it is determined if errors were introduced when the data was transmitted by the unsecured computer or received by the secured computer. Similarly, it is determined if errors were introduced when the data was retransmitted by the unsecured computer or rereceived by the secured computer. A warning signal is emitted from a warning device coupled to the secured computer if (i) an error was introduced when the data was transmitted or received, and (ii) an error was introduced when the data was retransmitted or rereceived.

15 Claims, 4 Drawing Sheets

UNDERPINNED BY MATURE TECHNOLOGY

Established over 20 years ago, Owl's unique cyber security offering has stood the test of time against an ever evolving threat landscape. Owl's solution was developed from the ground up as a one-way transfer device and not a reverse-engineered two-way transfer product. Initially developed by Sandia National Laboratories to support the exacting security needs of the nuclear industry, Owl owns the exclusive rights and patent that was first granted in 1997.

50 PATENTS

This patent enables Owl to be incredibly flexible with the technology, offering solutions that can transfer terabytes of data, or devices small enough to fit in a pocket whilst enabling highly secure one-way transfer. Owl's patent adopts a simple methodology of having a send card containing only electronics capable of sending data and a receive card containing only electronics capable of receiving data; this hardware approach ensures that the cards cannot be compromised by way of software or electronic attack.

TRUSTED FILTER™

ADVANCED CONTENT FILTERING & PROTOCOL HANDLING

The ease of integration of the Owl product range is further enhanced by 4Secure's TrustedFilter™ framework. TrustedFilter™ augments SNTS by enabling advanced content filtering and protocol handling.

4Secure TrustedFilter™ is a compendium of software developed to enhance the outstanding security of Owl Data-Diode technology. TrustedFilter™ enables advanced content filtering and protocol handling, giving users the ability to streamline and augment cross domain data transfer and facilitate an end-to-end secure solution.

The advanced content filtering software has been developed over several years with easily extensible and configurable platform agnostic software modules that can be used onboard Owl OPDS products or as standalone tools in your data pipeline.

All of our applications come with 12 months software support and updates. Current components in the TrustedFilter™ framework include: 4SFT, 4MQT, 4XJS, 4MCT, 4BDT and 4TLS:

4SFT™

4Secure File Transfer (4SFT™) is a high performance file transfer application that runs as a service on external Windows and or Linux flanking operating systems and supports WSUS updates.

4SFT employs an easy to use GUI which facilitates simple and efficient setup of folder and file level replication, re-scans nominated directories every 30 milliseconds and uses file compression for unparalleled performance.

4MQT™

4Secure Message Queuing Telemetry Transport (4MQT™) is an Advanced Message Queuing Protocol (AMQP) and Message Queuing Telemetry Transport (MQTT) transfer utility that enables cross domain appliances to be seamlessly implemented into message queuing architecture, without impacting the connection aware producer-consumer environment.

4MQT™ delivers full fault-tolerant connectivity for the integration of AMQP and MQTT into a one way enforced cross-domain environment, scales with the enterprise and supports the full suite of queue and exchange types within a message queueing implementation.

NEED MULTIPLE APPLICATIONS?
Talk to us about our TrustedFilter™ Enterprise solution, which includes all software module applications.
(10% discount applied)

4XJS™

4Secure XML and JSON Streaming (4XJS™) application is a utility that enables XML and JSON files to be seamlessly transferred as a TCP stream across cross domain appliances, with full validation against a range of approved schema definition files. 4XJS™ is simple to configure, maintain and provides full audit logging for security management.

Enhanced options include:

Query String Filtering which allow scanners to check and filter HTTP POST data web form fields, URL query string fields, HTTP header fields and user defined restrictions on HTTP request methods.

TCP-XML Sec which facilitates signature verification and stripping on signed XML payloads prior to further schema validation. Messages can also have their signature information removed, prior to cross-domain transfer.

4TLS™

4Secure Transport Layer Security (4TLS™) is an application that enable HTTPS connections to function over a one way diode. This is achieved by terminating the HTTPS connection on the sending network and re-establishing the HTTPS connection on the receiving network.

The application works in tandem with the Owl Cyber Defense's Secure Network Transfer Service (SNTS), which facilitates communication across the network boundary. Additionally, if required allows for additional scanning and validation to be performed on the content by other applications.

4BDT™

4Secure Bidirectional Diode Tunnel (4BDT™) application is designed to facilitate full duplex TCP connections between specific host / port combinations across high and low security network domains, by splitting the directional traffic and redirecting it via diodes configured in opposing directions.

4MCT™

4Secure Multi Channel File Transfer (4MCT™) utility is a parallel file transfer application that has been designed to make use of the Owl Version 7 data diode card sets channelisation feature.

The application works in tandem with Owl Cyber Defense's Secure Network Transfer Service (SNTS) and only concerns itself with receiving, equally dividing, transmitting in parallel and ultimately concatenating the file in order to achieve and take advantage of the highest stable speeds achievable through the 10 Gbps diodes.

OPDS-1000

EAL 4+ CERTIFIED, NO ITAR RESTRICTIONS

COMPATIBILITY

Supporting multiple protocols, data types, and data streams the OPDS-1000 includes support for:

- TCP, UDP (multicast/unicast/broadcast)
- Secure Network Transfer (SNTS)
- Remote File Transfer (RFTS)
- Email (SMTP)
- FTP
- SNMP, Syslog

CONFIGURATIONS

Optimised for more demanding industrial control applications, it supports three configurations:

- SC - Standard capacity (26 Mbps)
- MC - Mid capacity (155 Mbps)
- HC - High capacity (1,000 Mbps)

INDUSTRIES

The OPDS-1000 is commonly found in the following industries:

- CNI
- Government
- Defence
- Security
- Enterprise

TrustedFilter® File Transfer Applications

The following file transfer applications can be integrated with the OPDS-1000:

- 4BDT
- 4SFT
- 4TLS
- 4XJS
- 4MQT

OPDS-1000

THE OWL SOLUTION

The Owl Perimeter Defense Solution (OPDS) OPDS-1000 is a multi-purpose, all in one, 1U rack-mountable cybersecurity solution designed to create a defensive cyber perimeter around plants. Optimised for more demanding industrial control applications, the OPDS-1000 supports software interfaces (connectors) to a broad range of applications that generate business-critical data (sensor information, data points, database historians, Syslog messages, alarms, etc.). That data is securely transferred to the business network and used for remote monitoring, production planning, and other management tasks.

The OPDS-1000 is EAL certified, has undergone shock and vibration testing and provides several physical security features to resist tampering. In addition, licensable bandwidth tiers allow customers to purchase only the bandwidth they need with the knowledge that they can increase bandwidth at any time by moving up to the next tier.

MULTI PURPOSE DATA DIODE

The OPDS-1000 is a highly integrated, all-in-one, 1U, rack-mountable data diode that provides secure, high-speed data transfers. Supporting multiple protocols, data types, and data streams at a time, the OPDS-1000 includes support for TCP, UDP (multicast/unicast/broadcast), Secure Network Transfer (SNTS), Remote File Transfer (RFTS), email (SMTP), FTP, SNMP, and Syslog. The OPDS-1000 additionally supports AMQP, MQTT, HTTP, IEC 104, SFTP protocol adapters, OPC UA, OPC Transfer Service, Pi Transfer, Virtual Screen View, and Modbus application connectors.

EASILY DEPLOYABLE

Designed to protect the industrial control systems found at refineries, substations, plants, pumping stations, manufacturing facilities, etc., the OPDS-1000 ensures cyber protection of digital assets within the plant and deterministic one-way only transfer of operational data to end-users outside of the plant.

Technical Specifications

OPERATING CONDITIONS

- 0°C to 43.33°C
- 5% to 90% humidity non-condensing

POWER SUPPLY

- Input: 75-230 VAC,
- Estimated Normal operating Usage 10-16 W/side

STORAGE

- -40°C to 70°C
- 5% to 90% humidity non-condensing

VIBRATION

- Vibration: (IEC 60255-21-1)
- Vibration 1g(10-500Hz) (operational)
- Vibration 2g(10-500Hz) (operational and non-operational)

NETWORK CONNECTIVITY

- Ethernet connections for network traffic and remote administration
- Physical connectors: 8P8C (RJ45)

SHOCK

- (IEC 60255-21-2) / Shock 10g 11ms (operational)
- Shock 10g 11ms (operational)
- Shock 30g 11ms (operational and non-operational)

COOLING SYSTEM

- Conductive cooling through enclosure side walls with high life expectancy/low noise fans

ISO

- Manufactured using ISO 9001:2015 certified quality program

CHASSIS

- Black anodised aluminium with locking top

CHASSIS SIZE

- 16.5"W x 1.75"H x 13"D
- 4.91cm x 4.5cm x 33cm

UNIT WEIGHT

- 3.6kg

DEVICE LIFESPAN

- 14+ years

MOUNTING SYSTEM

- (1U) Rackmount, tabletop

OPDS-100D

THE OWL SOLUTION

The OPDS-100D is a one-way data transfer solution built on patented data diode technology and designed specifically for OT networks. It features a compact, vertical form factor with a DIN rail mounting system.

The OPDS-100D is typically deployed at the edge of an OT network and contains the proprietary Owl data diode technology that only physically allows data to flow in one direction. As a result, data generated within a plant, substation, refinery, pump station or any other critical infrastructure facility is transferred across network boundaries to remote users for monitoring, performance, production and maintenance activities.

SINGLE DEVICE, MULTIPLE MISSIONS

The OPDS-100D is an extremely low SWaP, single-device data diode solution designed for DIN rail environments commonly found in the OT networks of industrial facilities and other critical infrastructure. With the power to support multiple functions simultaneously, the OPDS-100D can transfer files & images, stream video, send email alerts, transfer SNMP traps & Syslog messages, and support remote HMI screens. No competing product on the market offers the same range of capabilities in a single, easily deployable device.

REMOTE MONITORING, DIN RAIL FORM FACTOR

Critical infrastructure operators (power generation, T&D, substations, oil & gas, utilities, telecom, etc.) are taking decisive steps to protect the digital equipment in their operational technology (OT) networks against cyber attacks and threats. Owl Perimeter Defense Solutions (OPDS) are being used to segment OT networks and protect the SCADA equipment and PLCs operating on them to stave off these threats. Deployed at the edge of an OT network, the OPDS products allow data that is necessary for business operations and resiliency to flow out of the OT network to end-users while simultaneously protecting the OT network from any inbound attacks.

Technical Specifications

OPERATING CONDITIONS

- -40°C to 60°C
- 5% to 90% humidity non-condensing

POWER SUPPLY

- Input: 9-36V DC
- Estimated normal operating usage: 10-15W per side
- Max 20W per side
- Optional AC power brick with barrel connector (not included)

STORAGE

- -40°C to 70°C
- 5% to 90% humidity non-condensing

VIBRATION

- Vibration: (IEC 60255-21-1)
- Vibration 1g (10-500Hz) (Operational)
- Vibration 2g (10-500Hz) (Operational and Non-Operational)

SHOCK

- Shock: (IEC 60255-21-2)
- Shock 10g 11ms (Operational)
- Shock 30g 11ms (Operational and Non-Operational)

NETWORK CONNECTIVITY

- Separate Ethernet connections for network traffic and remote administration
- Physical connectors: 8P8C (RJ45)
- Supports 10BASE-T, 100BASE-TX, 1000BASE-T

COOLING SYSTEM

- Conductive cooling through enclosure side walls supplemented by adaptive active cooling based on system temperature control

ISO

- Manufactured using ISO9001:2015 certified quality programprogram

CHASSIS SIZE

- 2.75”W × 6.132”H × 5.5”D
- 6.99cm × 15.58cm × 13.97cm

UNIT WEIGHT

- 1.36 kg

DEVICE LIFESPAN

- 11 Years

MOUNTING SYSTEMS

- DIN Rail (1”) Mount, tabletop

OPDS-100D

EAL 2 CERTIFIED, NO ITAR RESTRICTIONS

COMPATIBILITY

The OPDS-100D supports a wide range of data formats and transport layer protocols from a host of different sources on the OT network:

- TCP, UDP (multicast/unicast/broadcast)
- Secure Network Transfer (SNTS)
- Remote File Transfer (RFTS)
- Email (SMTP)
- FTP
- SNMP, Syslog, SIEM

CONFIGURATIONS

Optimised for more demanding industrial control applications, it supports three configurations:

- SC - Standard capacity (10 Mbps)
- MC - Mid capacity (26 Mbps)
- HC - High capacity (104 Mbps)

INDUSTRIES

The OPDS-100D is commonly found in the following industries:

- SME
- CNI
- Government
- Defence
- Security

TrustedFilter™ File Transfer Applications

The following file transfer applications can be integrated with the OPDS-100D:

- 4BDT
- 4SFT
- 4TLS
- 4XJS
- 4MQT

SSUS

EAL 4+ CERTIFIED, NO ITAR RESTRICTIONS

COMPATIBILITY

Supporting multiple protocols, data types, and data streams at a time, the SSUS includes support for:

- File Extension Check
- ASCII Scan Check
- Malware Scanning
- Single File or Entire Directory

ARCHITECTURE

With an easy-to-use graphical user interface for both Send and Receive sides of the diode, SSUS dramatically simplifies the process of vetting incoming software updates and other files into a secured network. SSUS also includes a comprehensive logging suite, capturing a detailed history of all actions, files, and transfers performed on the platform.

INDUSTRIES

The SSUS is commonly found in the following industries:

- CNI
- Government
- Defence
- Security
- Enterprise
- Finance

TrustedFilter® File Transfer Applications

The following file transfer applications can be integrated with SSUS:

- 4BDT
- 4SFT
- 4TLS
- 4XJS
- 4MQT

SSUS

THE OWL SOLUTION

The Owl Secure Software Update Solution (SSUS) is a data diode-based cybersecurity solution that follows the "Seven Steps to Effectively Defend Industrial Control Systems by providing a highly secure method to validate, scan, and transfer software patch and executable files into secured or isolated networks. SSUS individually validates executable and non-executable files against a manifest of pre-configured hash numbers provided by the software provider or vendor. Files that do not have a matching hash are quarantined.

For additional security and information assurance, SSUS provides enhanced controls to enable content inspection, file type/extension checks, antivirus, and ASCII scanning. SSUS also permits the implementation of two-person authentication approval and release process. These comprehensive security features allow organizations to establish a security policy that explicitly prohibits the use of portable media devices to transfer data between security levels and only allows low-to-high and peer to peer transfers.

SAFELY IMPORTING SOFTWARE UPDATES INTO CLOSED NETWORKS

Just like any other network, secured or isolated networks (plants, oil rigs, substations) contain computers, servers, control systems, databases, etc., that require software updates on a recurring basis. In order to update these devices, software updates are typically downloaded from the vendor's website to a local server, copied onto a portable media device (e.g. a USB drive) and hand-carried into the secure network for installation.

According to the DHS, FBI, and NSA, this method is not a good choice. In the process of downloading, saving, copying to portable media and uploading on the secure network, the source file could be intentionally attacked, or the portable media device itself could be compromised with malware lurking. In the process of downloading, saving, copying to portable media and uploading on the secure network, the source file could be unwittingly manipulated.

Technical Specifications

OPERATING CONDITIONS

- 0°C to 43.33°C
- 5% to 90% humidity non-condensing

SYSTEM FEATURES

- TPM v2.0

POWER SUPPLY

- Input: 75-230 VAC
- Estimated normal operating usage 10-16W per side
- Max 20W per side

STORAGE

- -40°C to 70°C
- 5% to 90% humidity non-condensing

VIBRATION

- Vibration: (IEC 60255-21-1)
- Vibration 1g (10-500Hz) (Operational and Non-Operational)
- Vibration 2g (10-500Hz) (Operational and Non-Operational)

SHOCK

- Shock: (IEC 60255-21-2)
- Shock 10g 11ms (Operational)
- Shock 30g 11ms (Operational and Non-Operational)

ISO

- Manufactured using ISO9001:2015 certified quality programprogram

MOUNTING SYSTEM

- (1U) Rackmount, tabletop

CHASSIS SIZE

- 16.5"W x 1.75"H x 13"D
- 4.91cm x 4.5cm x33cm

UNIT WEIGHT

- 3.6 kg

DEVICE LIFESPAN

- 11+ Years

ReCon

THE OWL SOLUTION

Digital transformation creates both opportunity and risk for today's data-driven organisations. They are challenged with navigating the convergence of OT and IT systems, the emergence of the IoT and IIoT, and limiting or reducing the attack surfaces of their networks. As this digital transformation evolves and more networks and devices are connected, security concerns will only continue to grow.

To address this pressing need for security, hardware-enforced data diodes have been proven time and again to protect the OT networks; however, in some cases, organizations need to secure bidirectional communications that cannot be one-way.

The ReCon solution was designed to combine the same proven security benefits of a hardware-enforced data diode cybersecurity solution with the ability to provide secure round trip, bidirectional communication. ReCon enables organisations to maintain secure two-way connections between networks while reducing their attack surface with much higher security assurance than traditional firewalls.

BI-DIRECTIONAL PATHWAY IN ONE DEVICE

ReCon follows the Department of Homeland Security's (DHS) guidance for securing applications that cannot be one-way. Housed within a 1U standard rack-mountable enclosure, the solution is available in mid and high capacity models to better align with customer's security and budgetary requirements.

- Fixed destination IP address - Ensures that communication can only be directed to a single destination IP address
- Secure remote command and control - Enables secure remote command and control with less risk than firewall-based security
- Restricted session initiation - TCP/IP connection can only be initiated from the trusted source side network. Destination side cannot initiate communication into the device.

Technical Specifications

POWER SUPPLY

- Input: 100-240V AC auto-ranging, min. 30W per side (fused at 1A at IEC connector)
- Output: 5V at 5A - EU & UK power cables on request

STORAGE

- -40°C to 70°C
- 5% to 90% humidity non-condensing

VIBRATION

- Vibration: (IEC 60255-21-1)
- Vibration 1g(10-500Hz) (operational)
- Vibration 2g(10-500Hz) (operational and non-operational)

MOUNTING SIZE

- (1U) Rackmount, tabletop

NETWORK CONNECTIVITY

- Ethernet connections for network traffic and remote administration
- Physical connectors: 8P8C (RJ45)

SHOCK

- (IEC 60255-21-2) / Shock 10g 11ms (operational)
- Shock 30g 11ms (operational and non-operational)

COOLING SYSTEM

- Conductive cooling through enclosure side walls with high life expectancy/low noise fans

APPROVALS

- FCC Class B compliance
  CE Mark
  CB Certificate: 72130592
  UL 60950-1:2007 R12.11
  CAN/CSA-C22.2 No.60950-1-07+A1:2011
- International Common Criteria Certification - EAL Certified
- VCCI

ISO

- Manufactured using ISO 9001:2015 certified quality program

CHASSIS SIZE

- 16.5" W x 1.75" H x 13" D
- 41.91 cm x 4.5 cm x 33 cm

UNIT WEIGHT

- 3.96 Kg

DEVICE LIFESPAN

- 14+ years

LOCAL ADMINISTRATION

- VGA connector for monitor
- USB connectors for keyboard and mouse

ReCon

EAL 2 CERTIFIED, NO ITAR RESTRICTIONS

COMPATIBILITY

ReCon provides basic protocol support for secure bi-directional communicaton:

- FTPS
- TCP/IP
- DNP3
- Ethernet/IP
- IEC-104
- ICCP
- MS SQL Database Replication

CONFIGURATIONS

Optimised for more demanding industrial control to 104Mbps.

A hardware-based cybersecurity solution utilising two independent data diodes. Housed within a 1U standard rack-mountable enclosure, each one-way path within ReCon is completely independent from the other, creating a complete bi-directional pathway in one device.

INDUSTRIES

The ReCon is commonly found in the following industries:

- CNI
- Government
- Defence
- Security
- Enterprise

TrustedFilter® File Transfer Applications

The following file transfer applications can be integrated with the ReCon:

- 4TLS
- 4SFT
- 4MQT
- 4XJS

V7 CARD KITS

EAL 4+ CERTIFIED, NO ITAR RESTRICTIONS

COMPATIBILITY

Supporting multiple protocols, data types, and data streams at a time, the v7 includes support for:

- TCP, UDP (multicast/unicast/broadcast)
- Secure Network Transfer (SNTS)
- Remote File Transfer (RFTS)
- Email (SMTP)
- FTP
- SNMP, Syslog

CONFIGURATION

Optimised for more demanding industrial control applications, the v7 card kit supports three configurations:

- SC - Standard capacity (300 Mbps)
- MC - Mid capacity (1 Gbps)
- HC - High capacity (10 Mbps)

INDUSTRIES

The v7 card kits are commonly found in the following industries:

- CNI
- Government
- Defence
- Security
- Enterprise

TrustedFilter® File Transfer Applications

The following file transfer applications can be integrated with the v7 card kits:

- 4BDT
- 4SFT
- 4TLS
- 4XJS
- 4MCT
- 4MQT

V7 CARD KITS

THE OWL SOLUTION

The Owl v7 Communication Card Kit family represents the pinnacle of performance in data diode technology.

Each supports a different configuration capacity, and these three unique Card Kits comprise the fastest and most versatile data diode solutions available on the market. All v7 Card Kits come equipped with an Owl application-specific Transfer Software Application to transfer any variety of data types and sizes and can be configured with up to 32 discrete data transfer channels. In addition, Owl v7 Card Kits have been Common Criteria certified at EAL4+.

ADVANCED, CUSTOMISABLE DATA DIODE SOLUTIONS

Each individual card is installed on a separate host server in a PCI Express slot. They communicate in a single direction over a fibre optic cable via the asynchronous transfer mode (ATM) protocol. ATM serves two purposes – the first is to "break" the protocol of the original transfer for additional security, the second is to facilitate a high bandwidth, low latency one-way transfer using a protocol specifically designed for it.

Each card is colour-coded: Blue for send and red for receive. The send card resides in a designated send server (blue) on the source network and only has electronic components, including an LED, for transmitting the information. The receive card resides in a designated receive server (red) on the destination network and only has electronic components, including a photodetector, for receiving information. The hardware design of these cards physically enforces deterministic, one-way only data transfers.

TRANSFER SOFTWARE APPLICATIONS

Owl Data Transfer Applications are the software that serves as the protocol proxy component of an Owl Communication Card Kit, interfacing with the source and destination networks. They are designed to either support a specific, individual protocol (i.e. UDP or file transfer only) or multiple protocols/formats simultaneously.

Customers can select the appropriate Data Transfer Application(s) of data that needs to be transferred (UDP/IP, TCP/IP, raw Ethernet packets, files, directories), the protocols being used and whether or not data scanning is required.

Technical Specifications

OPERATING SYSTEMS

- RHEL®

SOFTWARE

- Owl Secure Transfer System Drivers
- Send/Receive Installation Software
- Owl Transfer Applications for: Files, Directories, TCP/IP, UDP, Syslog, SNMP Trads

CONNECTION

- Fibre Optic Multi-Mode/ Simple Mode
- LG-LC Cable
- Seamless 10/100/1000/10G Integration

COMPATIBILITY

- PCI Express (PCI SIG Compliant)
- Dell PowerEdge, Sunfire & Sun Blade, HP
- Proliant (For other platforms, contact Sales)

XD GUARDIAN

THE OWL SOLUTION

XD Guardian™ is a dual-guard, quad-diode cross-domain appliance that combines flexibility with low cost and high performance. The functional equivalent of Owl's XD Bridge™ product, XD Guardian is the only exportable product that has been assessed against the U.S. government's most rigorous requirements for cross-domain solutions.

XD Guardian supports both hardware-enforced unidirectional and bidirectional transfer modes ensuring fast, effective, and secure data transfer between systems of differing security levels.

With its standard 1U rack-mountable configuration and minimal administration requirements, XD Guardian can be easily deployed in enterprise applications or remote or isolated environments.
Structured data filters are available for both file transfer and streaming protocols.

XD Guardian brings certified cross domain security to every industry, around the world:

- Coalition military operations
- Foreign governments and defence
- Commercial, industrial, and utility orgs

MEETS RIGOROUS STANDARDS

The XD Guardian has undergone rigorous testing to meet U.S. government security standards and is also Raise-the-Bar (RTB) phase one compliant as listed on the NCDSMO Baseline (formerly UCDSMO Baseline).

Technical Specifications

PORTS (PER SIDE)

- 10 / 100 / 1000 Ethernet (data transfer) 10 / 100 Ethernet (management) ST Fiber – 1 transmit, 1 receive Kanguru USB sticks (Active on boot only) USB 2.0 (keyboard) VGA (video) Tubular pin lock (key load lock)

POWER SUPPLY

- 100-240 VAC, 5.5-2.5A, 47-63Hz

STORAGE TEMPERATURE

- -40°F to 158°F / -40°C to 70°C

OPERATIONAL TEMPERATURE

- 14°F to 122°F / -10°C to 50°C

MOUNTING SIZE

- (1U) Rackmount, tabletop

HUMIDITY

- Maximum 90% non-condensing relative humidity

DIMENSIONS

- 18.875" x 26" x 1.75"
- 47.94cm x 66.04cm x 4.445cm

WEIGHT

- 18.5 lbs/ 8.39kgs

ALTITUDE (UNPRESSURISED)

- 4,600m (15,000ft)

POWER

- 70W @ idle, 170W maximum

COOLING

- 580 BTU max and 240 BTU typical

PROTOCOL SUPPORT

- FTP, SFTP, FTP/S, TCP, UDP Unicast, Multicast, Broadcast

XD GUARDIAN

EAL CERTIFIED, NO ITAR RESTRICTIONS

COMPATIBILITY

Supporting multiple protocols, data types, and data streams at a time, the XD Guardian includes support for:

- XML, MS Office, PDF
- UDP data streams
- ISR Sensor Data Streams
- Unclassfied Data Feeds (NWS, FAA)

CONFIGURATIONS

Optimised for more demanding industrial control applications, the XD Guardian supports up to 1Gbps.

The product's design supports rapid development of data-filtering capabilities, including custom security policies and filters.

INDUSTRIES

The XD Guardian is commonly found in the following industries:

- CNI
- Government
- Defence
- Security
- Enterprise

SCOWT COMPACT

EAL 2 CERTIFIED, NO ITAR RESTRICTIONS

COMPATIBILITY

Scowt provides basic protocol support for secure bi-directional communicaton:

- TCP, UDP (multicast/unicast/broadcast)
- Secure Network Transfer (SNTS)
- Remote File Transfer (RFTS)

CONFIGURATIONS

Ruggedised for harsh environments and configured with the Owl 010 card set.

The Scowt Compact has a maximum throughput of up to 104Mbps.

INDUSTRIES

The Scowt is commonly found in the following industries:

- Defence
- Security

TrustedFilter™ File Transfer Applications

The following file transfer applications can be integrated with the Scowt:

- 4BDT
- 4SFT
- 4TLS
- 4XJS
- 4MQT

SCOWT COMPACT

THE OWL SOLUTION

The Owl Cyber Defense Solutions (Owl) Scowt-Compact is a ruggedised solution for airborne, ground, and naval assets and forward-operating bases and remote command stations that need to transmit, stream, and receive data at different security levels on protected networks. In Defense, Intelligence, and other sensitive Government operations, data streaming and file transfer dataflows are crucial components of any successful mission or organisation. Whether the dataflows are for collecting sensor output and information reports, or the dissemination of command and control, alerts, and tips - the dataflows must be protected.

SINGLE DEVICE, MULTIPLE MISSIONS

The Scowt-Compact can be tailored to meet the dataflow needs of a range of cross-domain missions. The device's metal housing and MIL 804 connectors allow for ruggedisation and ease of use, whether it be a small forward-operating base with a need to transmit logistics data or an MRAP with sensors that collects RF transmission data to send to a command centre for analysis. Data remains secure as it is sent from systems and sensors that are collecting and transmitting different types of information such as video streams, position data, vehicle status, and even dismounted soldier health.

REMOTE MONITORING, DIN RAIL FORM FACTOR

Scowt-Compact combines the Raise-the-Bar (RTB)-ready ruggedised hardware platform and Owl's Multi-Protocol Platform (MPP) Cross Domain Solution (CDS) software platform. Owl's CDS-MPP software is designed to address RTB's One-Way Transfer (OWT) design patterns. The Owl Scowt-Compact hardware platform is conduction-cooled, and frame or shelf mounted. This configuration is a reduced size, weight, and power (SWaP) dual-processing node, separated by Owl's patented hardware-enforced one-way transfer diode, that support dataflow bandwidth up to 104 Mbps for UDP and TCP content streaming and file transfers.

Technical Specifications

POWER SUPPLY

- Input: 100-240V AC auto-ranging, min. 30W per side (fused at 1A at IEC connector)
- Output: 5V at 5A - EU & UK power cables on request

STORAGE

- -40°C to 70°C
- 5% to 90% humidity non-condensing

VIBRATION

- Vibration: (IEC 60255-21-1)
- Vibration 1g(10-500Hz) (operational)
- Vibration 2g(10-500Hz) (operational and non-operational)

MOUNTING SIZE

- (1U) Rackmount, tabletop

NETWORK CONNECTIVITY

- Ethernet connections for network traffic and remote administration
- Physical connectors: 8P8C (RJ45)

SHOCK

- (IEC 60255-21-2) / Shock 10g 11ms (operational)
- Shock 30g 11ms (operational and non-operational)

COOLING SYSTEM

- Conductive cooling through enclosure side walls with high life expectancy/low noise fans

APPROVALS

- FCC Class B compliance
  CE Mark
  CB Certificate: 72130592
  UL 60950-1:2007 R12.11
  CAN/CSA-C22.2 No.60950-1-07+A1:2011
- International Common Criteria Certification - EAL Certified
- VCCI

ISO

- Manufactured using ISO 9001:2015 certified quality program

CHASSIS SIZE

- 16.5" W x 1.75" H x 13" D
- 41.91 cm x 4.5 cm x 33 cm

UNIT WEIGHT

- 3.96 Kg

DEVICE LIFESPAN

- 14+ years

LOCAL ADMINISTRATION

- VGA connector for monitor
- USB connectors for keyboard and mouse

DiOTa

THE OWL SOLUTION

DiOTa is a single-purpose data diode built on a hardened Linux operating system that physically only allows data to flow in one direction for the highest level of security. DiOTa can be deployed on a tabletop or DIN rail mount with a compact form factor, typically at the edge of operational technology (OT) networks or in front of other sensitive systems or IIoT devices.

Data generated within a substation, plant, pump station, refinery, or any other facility, system, or device is transferred across network boundaries to external users or the cloud for performance, safety, production, and maintenance monitoring and analytics. DiOTa is designed for OT micro-segmentation applications and network boundaries, on-site and remote locations in scalable deployments.

BUILT FOR CRITICAL INFRASTRUCTURE

DiOTa features an extremely low size, weight, power, and cost (SWaP-C) profile and meets the low-throughput requirements of most industrial and critical infrastructure applications. In addition, the device supports a single transfer protocol at a time - admins can select from TCP, UDP (Unicast/Multicast), files and directories, Modbus, OPC DA/A&E, SNMP Traps (TCP, UDP), or Syslog, and reconfigure as needed.

With a 10-year mean time before failure (MTBF) lifespan, DiOTa is built to last in critical infrastructure environments and meet the same refresh cycles as most industrial control systems.

DESIGNED FOR SIMPLICITY

With the Quick Start Guide (provided with the device) and the user interface setup wizard and help guides, no expertise is required to get DiOTa set up and configured in minutes. In addition, DiOTa is built to only transfer data one way to the destination you set, and once configured, is designed to operate with little to no maintenance or upkeep for the life of the device. There is simply no other solution available that combines this level of security at a lower total cost of ownership or higher ease of use.

Technical Specifications

POWER SUPPLY

- Input: 100-240V AC auto-ranging, min. 30W per side (fused at 1A at IEC connector)
- Output: 5V at 5A - EU & UK power cables on request

STORAGE

- -40°C to 70°C
- 5% to 90% humidity non-condensing

VIBRATION

- Vibration: (IEC 60255-21-1)
- Vibration 1g(10-500Hz) (operational)
- Vibration 2g(10-500Hz) (operational and non-operational)

MOUNTING SIZE

- (1U) Rackmount, tabletop

NETWORK CONNECTIVITY

- Ethernet connections for network traffic and remote administration
- Physical connectors: 8P8C (RJ45)

SHOCK

- (IEC 60255-21-2) / Shock 10g 11ms (operational)
- Shock 30g 11ms (operational and non-operational)

COOLING SYSTEM

- Conductive cooling through enclosure side walls with high life expectancy/low noise fans

APPROVALS

- FCC Class B compliance
  CE Mark
  CB Certificate: 72130592
  UL 60950-1:2007 R12.11
  CAN/CSA-C22.2 No.60950-1-07+A1:2011
- International Common Criteria Certification - EAL Certified
- VCCI

ISO

- Manufactured using ISO 9001:2015 certified quality program

CHASSIS SIZE

- 16.5" W x 1.75" H x 13" D
- 41.91 cm x 4.5 cm x 33 cm

UNIT WEIGHT

- 3.96 Kg

DEVICE LIFESPAN

- 14+ years

LOCAL ADMINISTRATION

- VGA connector for monitor
- USB connectors for keyboard and mouse

DiOTa

EAL 2 CERTIFIED, NO ITAR RESTRICTIONS

COMPATIBILITY

DiOTa provides basic protocol support for secure bi-directional communicaton:

- TCP, UDP (Unicast, Multicast)
- File Transfer, Modbus (2 PLCs/640 registers)
- OPC DA/A&E
- SNMP Traps (TCP, UDP)
- Syslog

CONFIGURATIONS

Optimised for low size, weight, power and cost with throughput up l to 5Mbps.

DiOTa also has two power supply options, including an AC power brick with a barrel connector or a DC power phoenix connector with a DIN rail clip included.

INDUSTRIES

The DiOTa is commonly found in the following industries:

- SME
- CNI
- Government
- Defence
- Security

TrustedFilter® File Transfer Applications

The following file transfer applications can be integrated with the DiOTa:

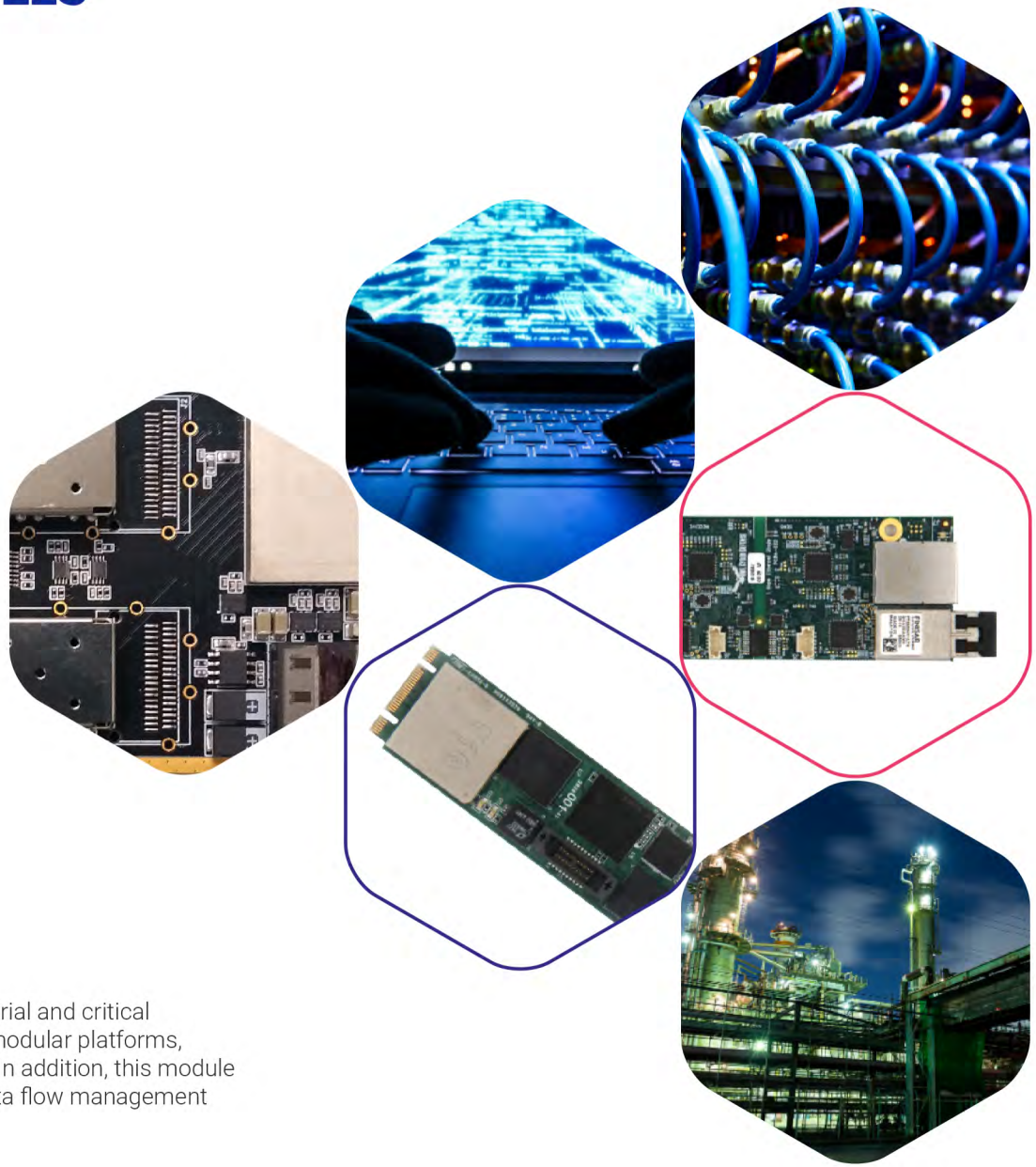
- 4MQT
- 4SFT

EMBEDDED FPGA-BASED MODULES

DEFENDING OPERATIONAL TECHNOLOGY

Industrial network owners are seeking alternatives to complex, maintenance-intensive industrial firewalls. Industrial device manufacturers that embed more secure, cost effective cybersecurity solutions into industrial network devices position themselves to increase market value by meeting industrial network owners' expectations for enhanced security. In addition, embedding cybersecurity into industrial devices helps industrial network owners confidently eliminate, or curtail, stand-alone industrial firewall devices with a more secure and unified approach. This migration away from stand-alone to embedded cybersecurity creates a compelling business case by delivering a more significant percentage of the overall network spend to industrial device manufacturers. Because of this, Owl is decomposing our technology and making it available as individual modules for industrial device manufacturers.

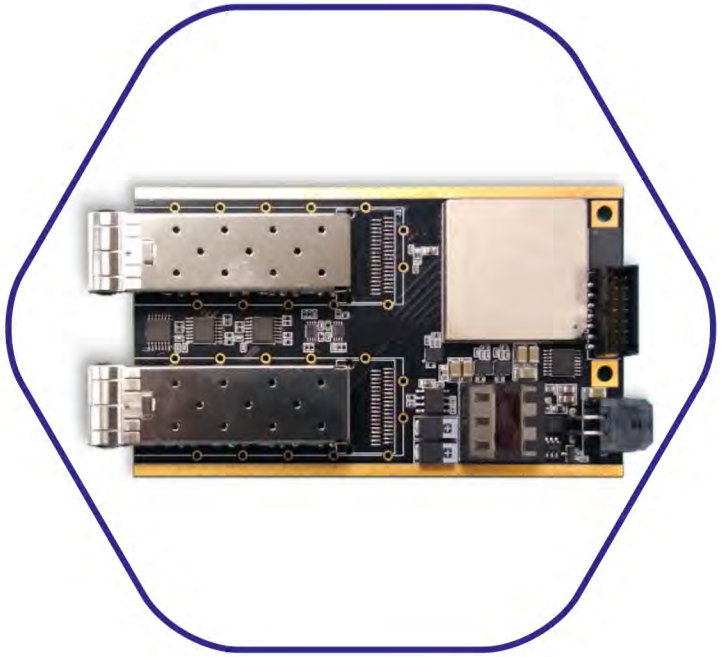
Owl is breaking new ground by providing a low SWaP-c (size, weight, power, and cost) cybersecurity module that can be designed into industrial control systems, providing hardware-enforced data evaluation and control without exposing industrial devices to new threat vectors. This module reduces operators' need for additional cybersecurity solutions and the overhead associated with maintaining them, thereby reducing their Capex and Opex costs.



EMBEDDED MODULES

For operators, designers, and manufacturers of advanced, connected, industrial and critical infrastructure controllers and safety systems, this module can be built into modular platforms, such as controllers, SCADA devices, safety systems, and network switches. In addition, this module provides a deterministic, one-way data transfer that provides very secure data flow management between equipment and external networks.

XDE TITANIUM



KEY FEATURES

- High throughput maximum of 40 Gbps
- SFP adapters for data input and output - supports 1GbE to 40 GbE over copper or optical media
- Hardware-based protocol validation and flow-control that is impervious to software-based threats
- Line-rate protocol inspection that is resilient against DDoS attacks
- Verification and authentication of common industrial protocols that operate over an IP network
- The admin port is segmented from network traffic for configurations and software updates

THE OWL SOLUTION

This technology is a miniaturised, hardware-based cybersecurity module that is incorporated into an IP-based controller or network appliance for manufacturing and critical infrastructure applications. This module incorporates advanced FPGA-based protocol validation and firewall rule enforcement, with the benefit of hardware-controlled flows. XDE Titanium can be configured to enforce strict one-way traffic or allow two-way traffic, with strict protocol validation and enforcement. Supporting a throughput maximum of 40 Gbps, XDE Titanium is resilient against DDoS attacks with line-rate protocol inspection while providing high-speed, secure data transfers.

Technical Specifications

POWER SUPPLY

- Power, configuration, and data inputs/outputs are all through a single edge connector

NETWORK CONNECTIVITY

- SGMII network connection in/out

BOARD DIMENSIONS

- Printed Circuit Board (PCB) Dimensions: 101.6mm × 57.1mm × 6.3mm

SUPPORTED PROTOCOLS

- UDP (Unicast, Multicast) and common industrial protocols

OPERATING CONDITIONS*

- -40°C to + 70°C

DEVICE LIFESPAN

- 14 years

THROUGHPUT

- Maximum of 40 Gbps

XDE RADIUM

KEY FEATURES

- High throughput maximum of 1 Gbps
- One-way UDP (Unicast & Multicast) and TCP/IP (in development) support
- Optical isolation, with a single fiber optic cable, or digital isolation
- Protocol break – no routable information is passed between source and destination networks
- Extended operating temperature range (-40°C to +70 °C)
- Low power consumption – no new software or computation resources needed
- Standard CAT 5/6 ethernet interface (in/out)

THE OWL SOLUTION

This technology is a single-board cybersecurity module that can be incorporated into the design of industrial devices, where safety and assurance are critical. This hardware module provides high-assurance, hardware-enforced, one-way data transfers from trusted to untrusted networks without requiring new software or computation resources. With a standard ethernet interface and a high-throughput maximum of 1 Gbps, XDE Radium performs one-way, UDP (Unicast & Multicast) and TCP/IP (in development) data transfers, preventing external access to industrial devices.

Technical Specifications

POWER SUPPLY

- Separate power sources on the source and destination sides of the module for security

NETWORK CONNECTIVITY

- Single CAT 5/6 input and single CAT 5/6 output

BOARD DIMENSIONS

- 101.6mm × 38.1mm

SUPPORTED PROTOCOLS

- UDP (Unicast, Multicast) & TCP/IP (in development)

OPERATING CONDITIONS

- -40°C to + 70°C

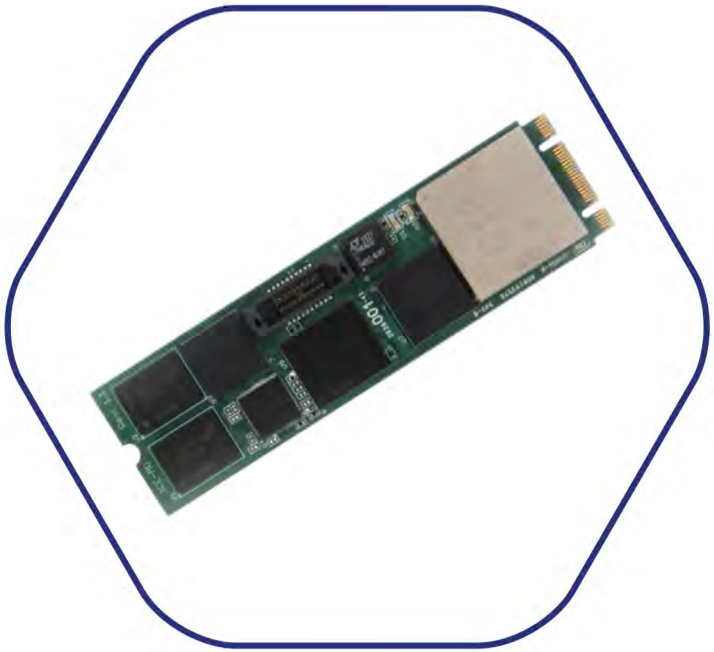
DEVICE LIFESPAN

- 14 years

THROUGHPUT

- Maximum of 1 Gbps

XDE COBALT



KEY FEATURES

- High throughput maximum of 1 Gbps
- One-way UDP (Unicast & Multicast) and TCP/IP (in development) support
- Optical isolation, with a single fiber optic cable, or digital isolation
- Protocol break – no routable information is passed between source and destination networks
- Extended operating temperature range (-40°C to +70 °C)
- Low power consumption – no new software or computation resources needed
- Standard CAT 5/6 ethernet interface (in/out)

THE OWL SOLUTION

This technology is a miniaturised, hardware-based cybersecurity module incorporated into industrial devices, including PLC modules, engineering workstation servers, and network gateways. This module combines advanced FPGA-based protocol validation and firewall rule enforcement with the benefit of hardware-controlled flows. XDE Cobalt can be configured to enforce strict one-way traffic or allow two-way traffic, with strict protocol validation and enforcement. Supporting a throughput maximum of 1 Gbps, XDE Cobalt is resilient against DDoS attacks with line-rate protocol inspection while providing secure data transfers.

Technical Specifications

POWER SUPPLY

- Power, configuration, and data inputs/outputs are all through a single edge connector

NETWORK CONNECTIVITY

- 1x 1Gb 60 pin male edge connector

BOARD DIMENSIONS

- 22mm × 80mm Standard M.2 module dimensions

SUPPORTED PROTOCOLS

- UDP (Unicast, Multicast) and common industrial protocols

OPERATING CONDITIONS

- -40°C to + 70°C

DEVICE LIFESPAN

- 14 years

THROUGHPUT

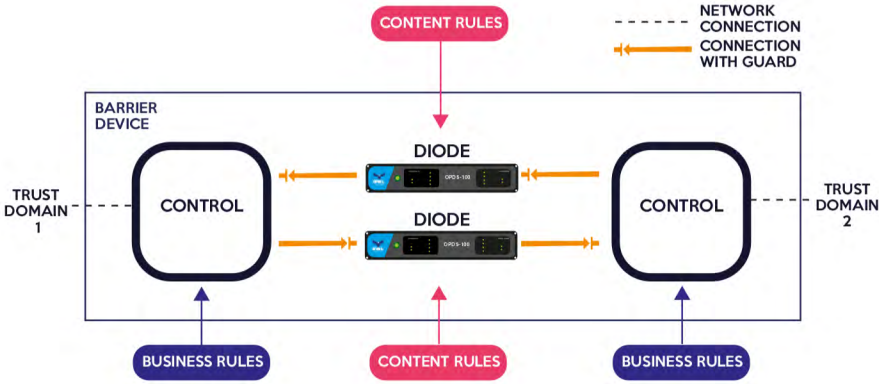
- Maximum of 1 Gbps

TACTICAL CROSS-DOMAIN INTEROPERABILITY

2iC

Over a number of years 2iC and 4Secure have worked on small form factor tactical "guards" and are working together to address a rapidly growing market. 2iC brings interoperability expertise and 4Secure brings security assurance and secure hardware expertise. Together there is formidable pedigree and knowledge.

The 2iC Assured Interoperability solution is the key missing piece needed to ensure the flexible coordination and two-way configurable-flow of information between different trust domains, separated by trust, ownership or nationality.



DSEI Innovation Challenge Winner 2013

Invented to provide a solution that is suitable for tactical use, rapid to deploy, quick to update and modify subsequently, whilst positioned right at the network edge (including soldier wearable).

Interoperability:

- OS EVA to GC2 Network
- OS BFT or CASE VAC to SC2
- Coalition to C2 Systems
- Provision of Common Operating Picture
- Full ODS Integration (Opensplice, RTI, Open DDS)

THE POWER OF JOINED-UP THINKING

2iC

WORKING TOGETHER TO ENHANCE NETWORK SECURITY

CLARITY

panoptech

DELIVERING SEAMLESS SECURITY SOLUTIONS

PANOPTECH

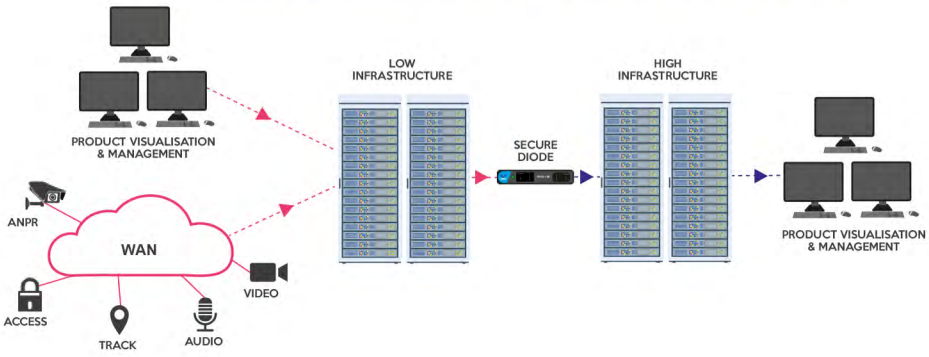
4Secure and Panoptech collaborate to deliver enhanced network security for Government, Law Enforcement and Defence customers. Security is fast becoming the foundation of any digital system and the level of security deployed is driven by the organisation or mission's need for availability, reliability and safety of systems, information and data.

This inherent need for connection and information sharing against a backdrop of budget cuts presents our customer daily challenges in delivering enhanced mission capability.

4Secure is partnered with Panoptech in delivering a range of high-security, low-cost, data diode based cross-domain security devices. Panoptech's customers are benefiting from better, more reliable technology with improved throughput, content inspection and the ability to scale with the project or mission. All of this capability is provided without any impact to existing classification levels of the data held on the system and a smooth system accreditation process thanks to the high assurance levels and pedigree of the technology.

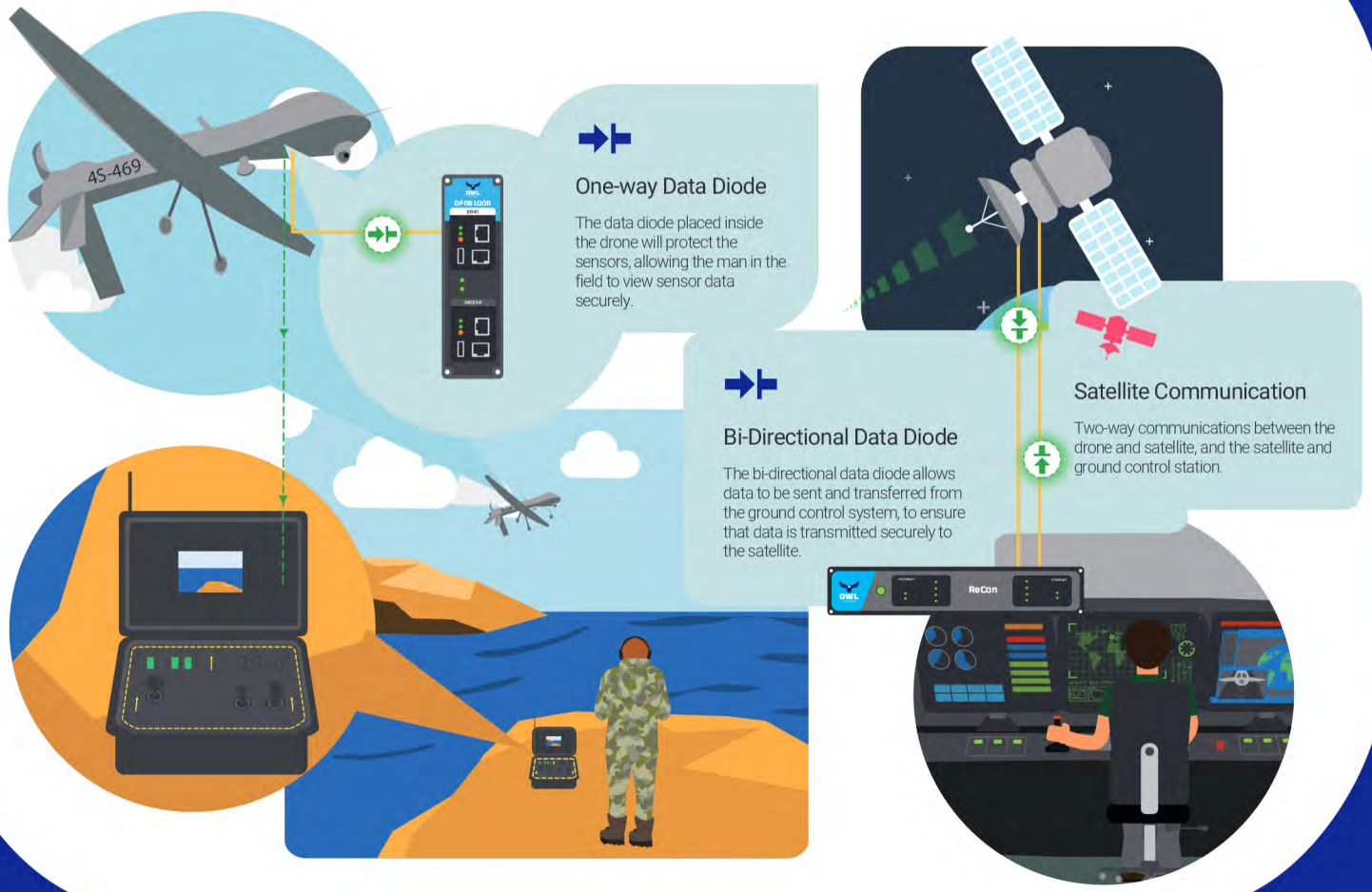
Following best-of-breed practices and our technical engineers experience, working within the industry for many years enables the solution to pass our customers' stringent tests and allows their own authority to approve the assurance of their systems. The ever challenging global climate and budget constraints ensure the latest variants of this technology will not only improve the capability of our customers, they will also enhance existing installations.

VIDEO THROUGH DIFFERENT NETWORK CLASSIFICATIONS



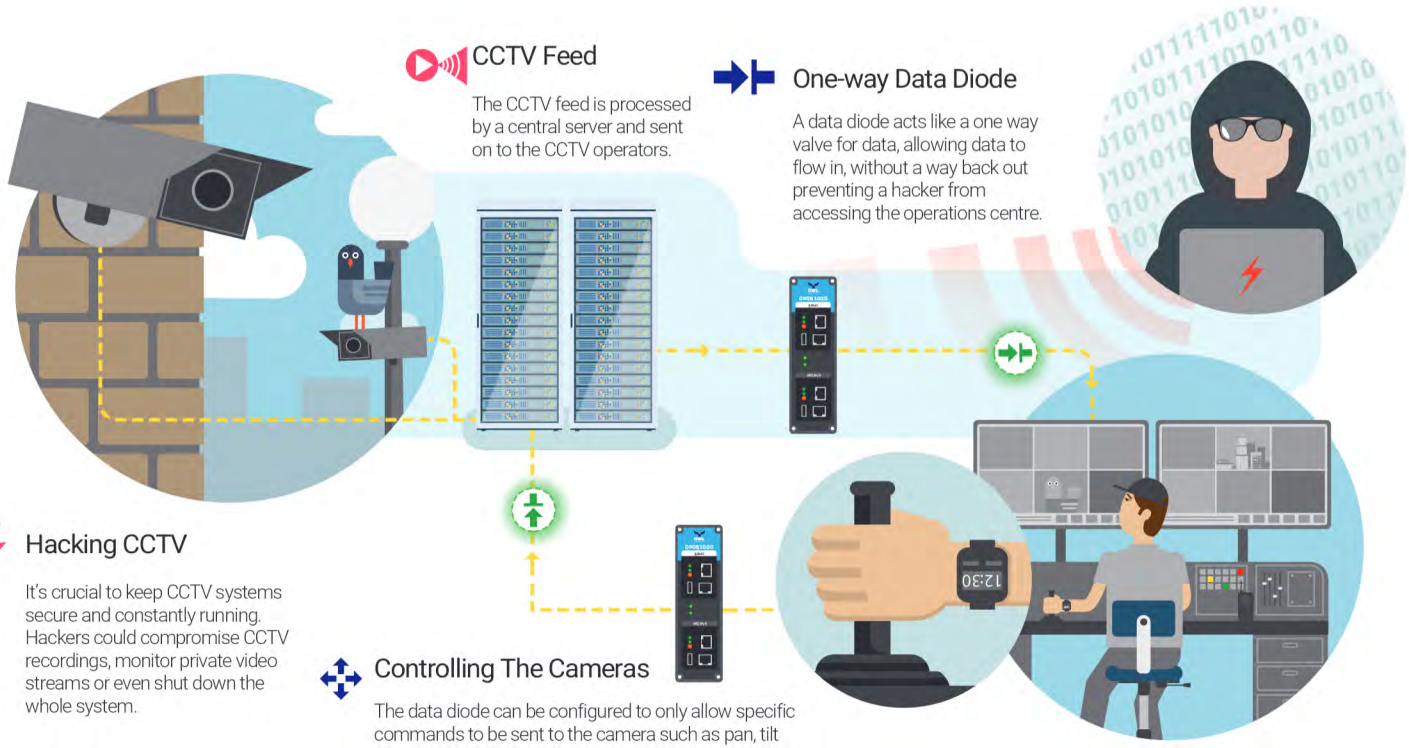
MISSION CONTROL

COMPATIBLE SOLUTIONS | DiOTa | OPDS 100D | OPDS-1000 | V7 CARD SET



CCTV OPERATIONS

COMPATIBLE SOLUTIONS | OPDS-100D | OPDS-1000 | ReCon



CCTV Feed

The CCTV feed is processed by a central server and sent on to the CCTV operators.

One-way Data Diode

A data diode acts like a one way valve for data, allowing data to flow in, without a way back out preventing a hacker from accessing the operations centre.

Hacking CCTV

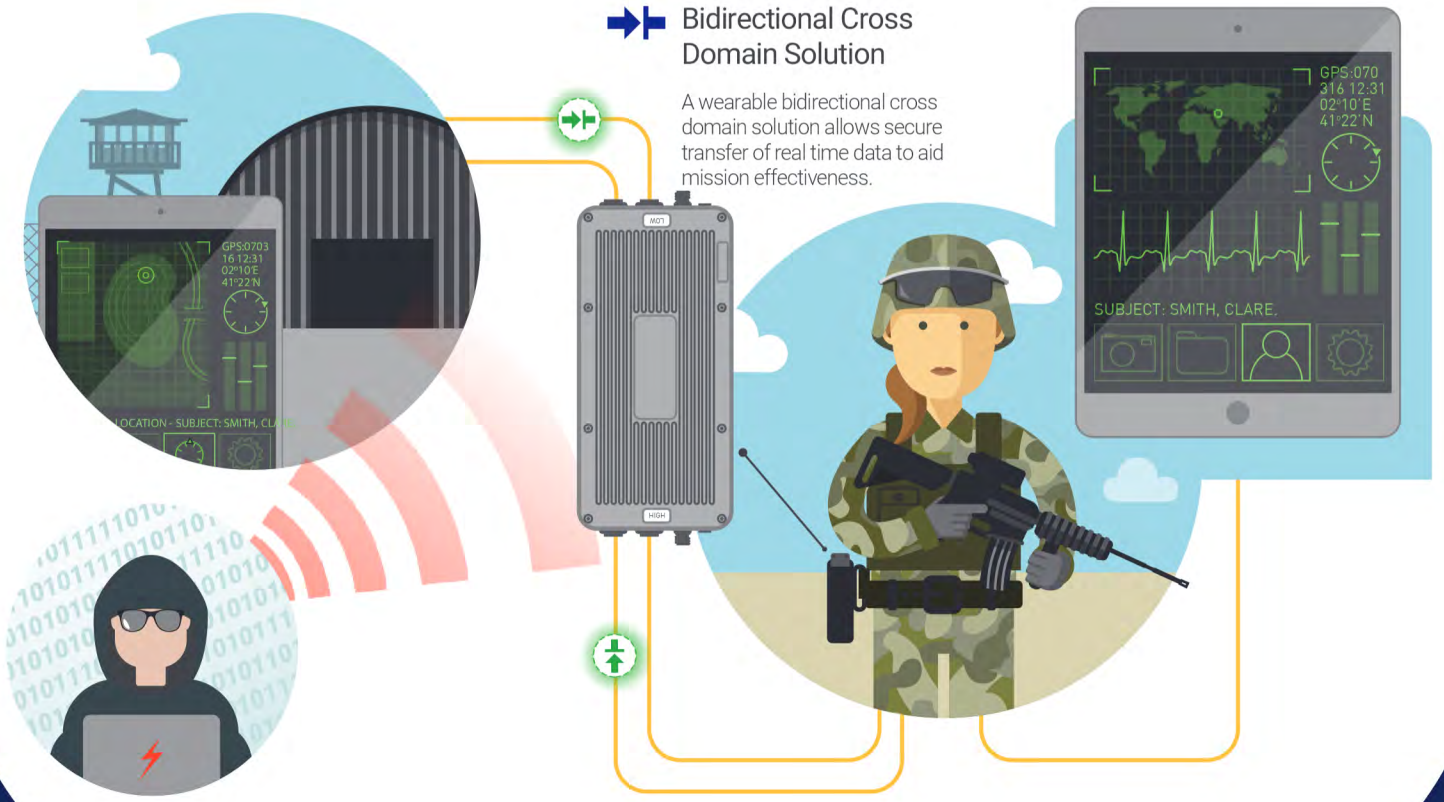
It's crucial to keep CCTV systems secure and constantly running. Hackers could compromise CCTV recordings, monitor private video streams or even shut down the whole system.

Controlling The Cameras

The data diode can be configured to only allow specific commands to be sent to the camera such as pan, tilt and zoom functions. Allowing the operator to control the camera without compromising security.

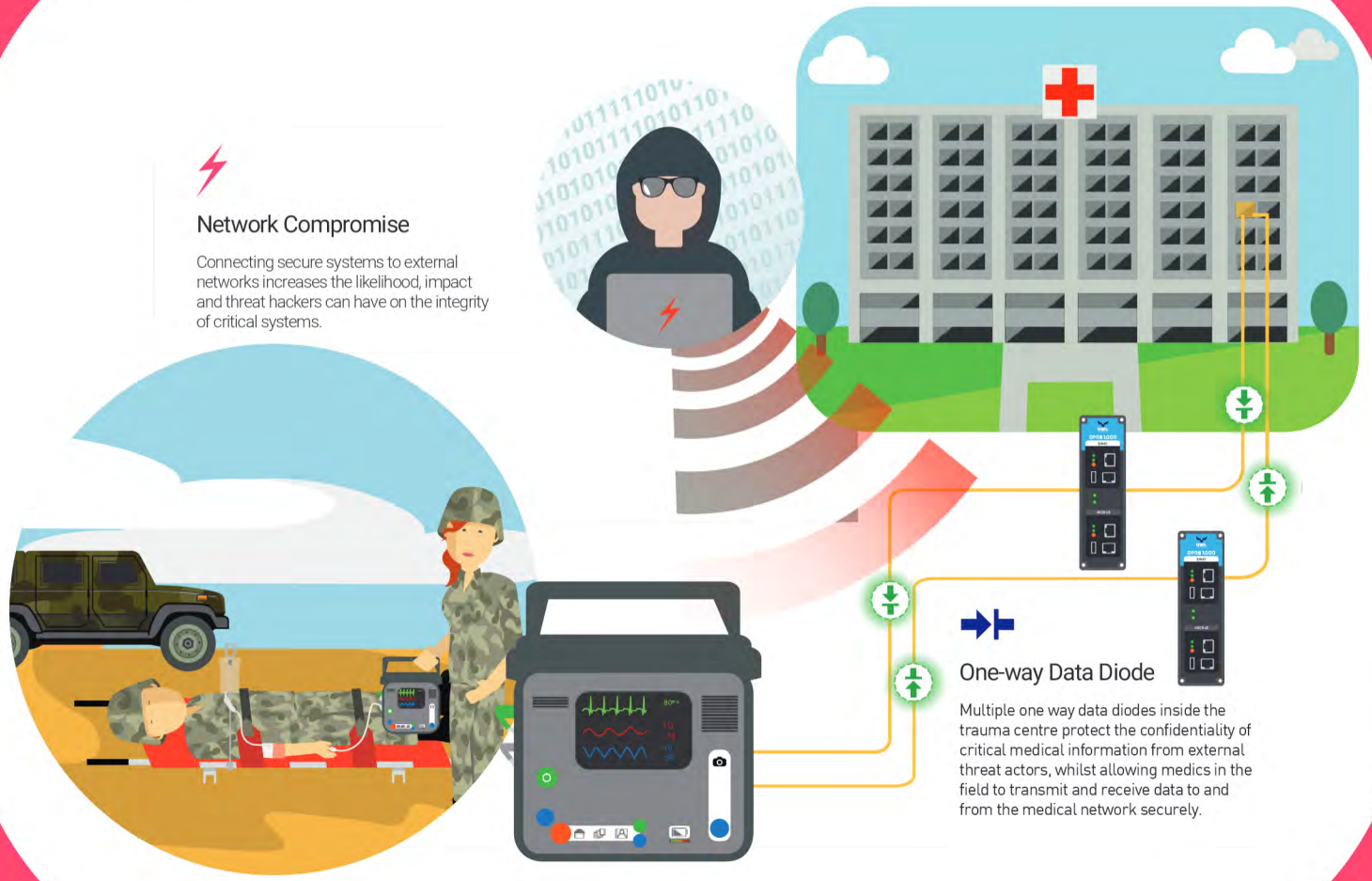
WEARABLE DIODE

COMPATIBLE SOLUTIONS | SCOWT | FPGA



TELEMEDICINE

COMPATIBLE SOLUTIONS | DiOTa | OPDS 100D | OPDS-1000 | ReCon | SCOWT | V7 CARD SET | FPGA



Network Compromise

Connecting secure systems to external networks increases the likelihood, impact and threat hackers can have on the integrity of critical systems.

One-way Data Diode

Multiple one way data diodes inside the trauma centre protect the confidentiality of critical medical information from external threat actors, whilst allowing medics in the field to transmit and receive data to and from the medical network securely.

OFFSHORE TO ONSHORE

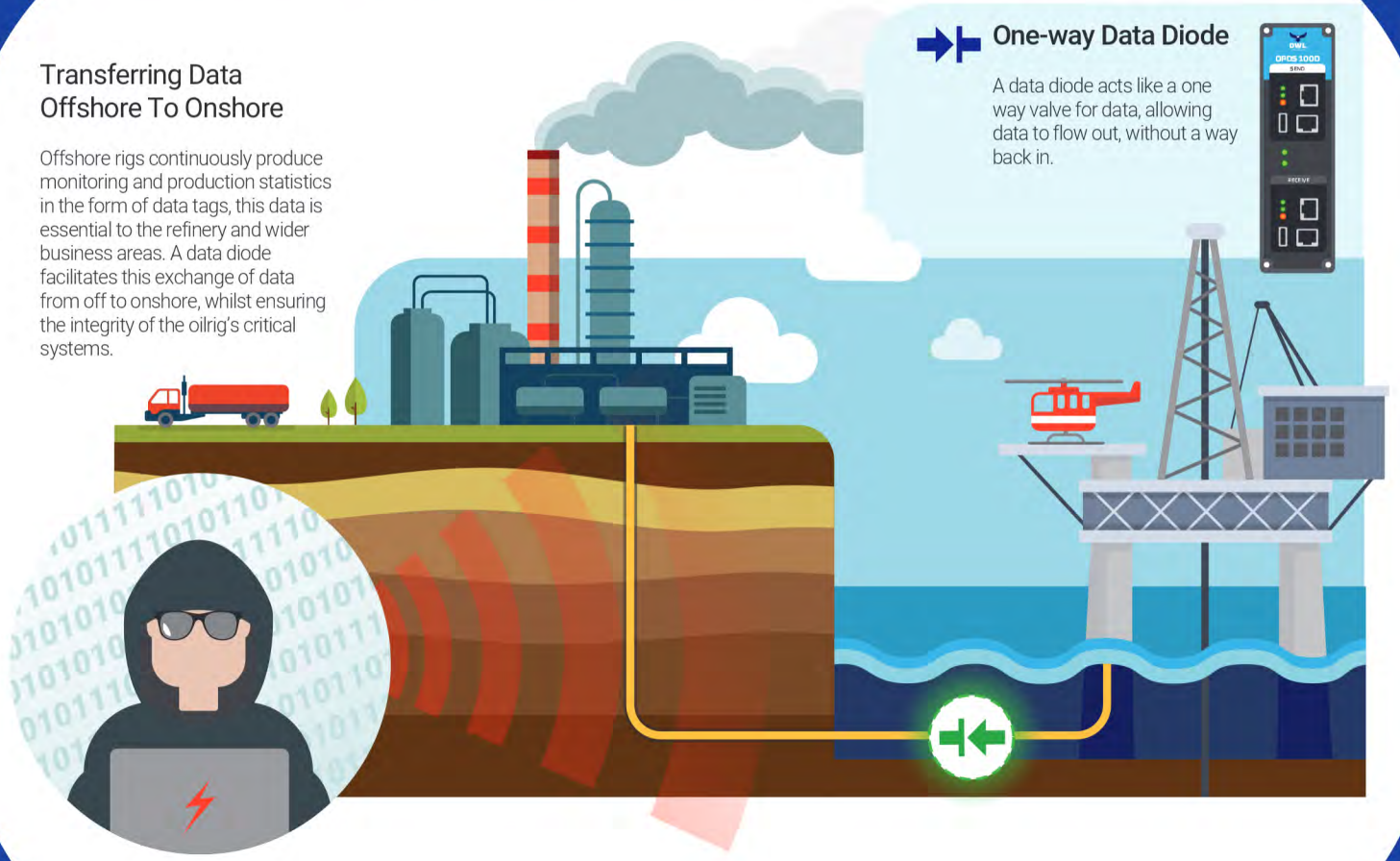
COMPATIBLE SOLUTIONS | OPDS 100D | OPDS-1000 | ReCon | SCOWT | V7 CARD SET | XD GUARDIAN

Transferring Data Offshore To Onshore

Offshore rigs continuously produce monitoring and production statistics in the form of data tags, this data is essential to the refinery and wider business areas. A data diode facilitates this exchange of data from off to onshore, whilst ensuring the integrity of the oilrig's critical systems.

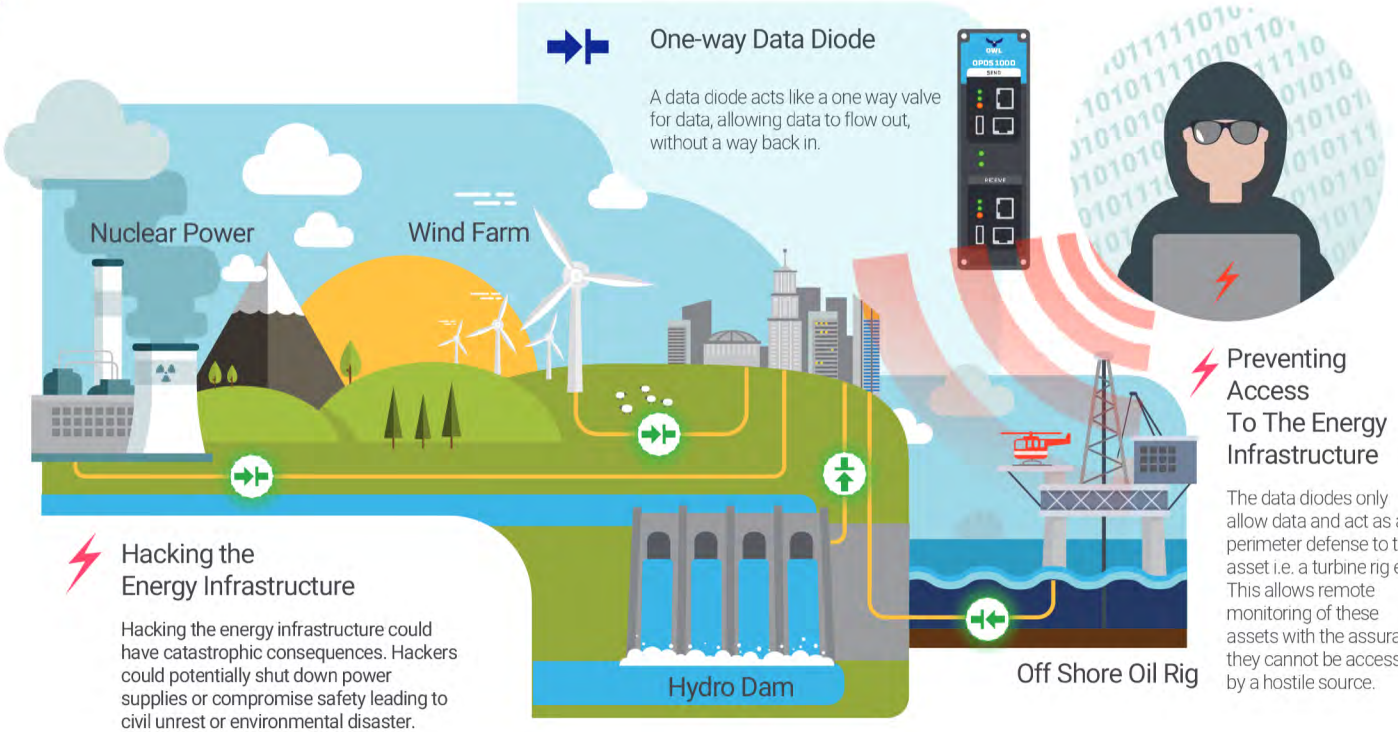
One-way Data Diode

A data diode acts like a one way valve for data, allowing data to flow out, without a way back in.



ENERGY INFRASTRUCTURE VULNERABILTY

COMPATIBLE SOLUTIONS | OPDS | OPDS 100D | OPDS-1000 | ReCon | SCOWT | V7 CARD SET | XD GUARDIAN



Hacking the Energy Infrastructure

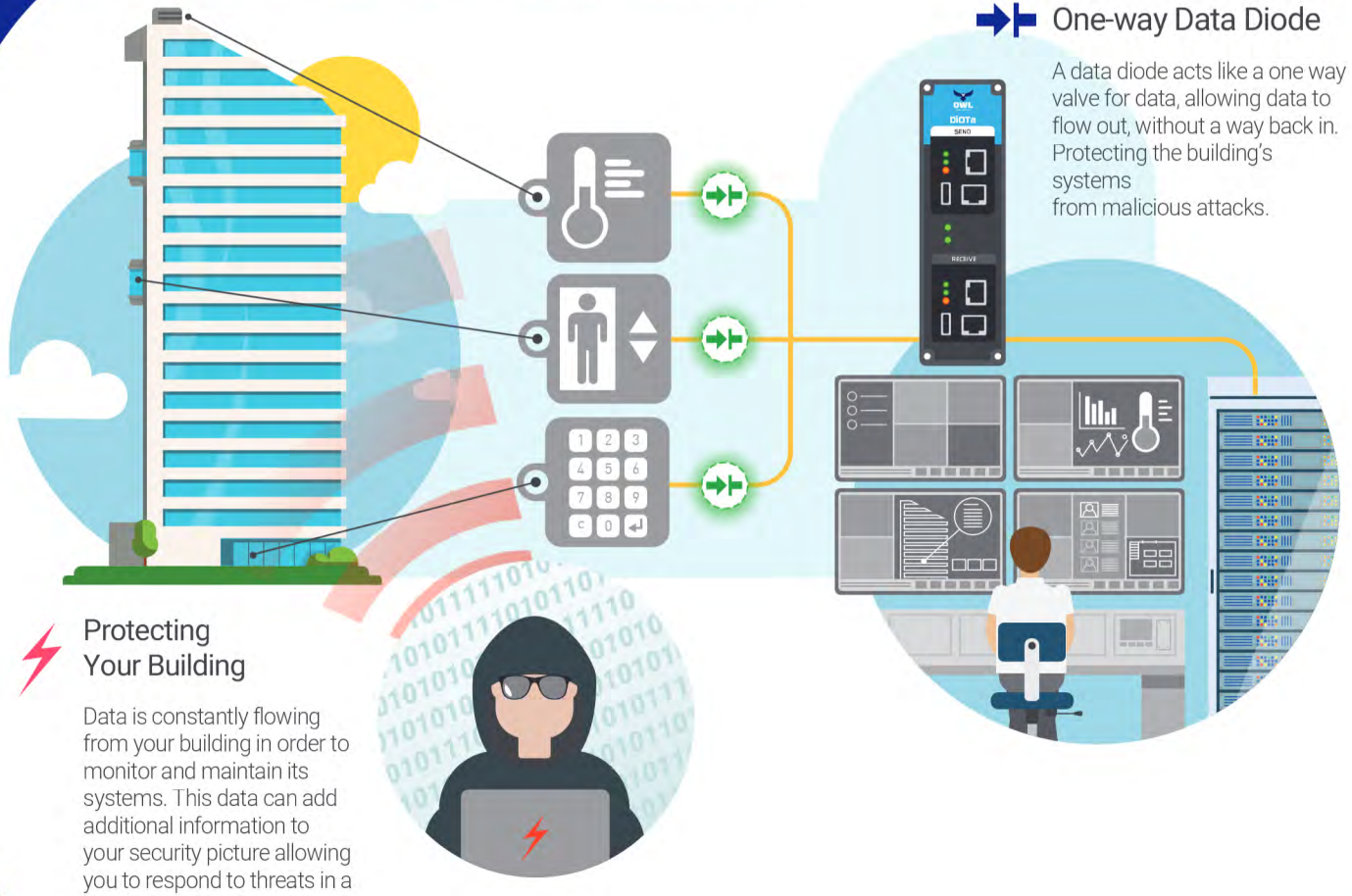
Hacking the energy infrastructure could have catastrophic consequences. Hackers could potentially shut down power supplies or compromise safety leading to civil unrest or environmental disaster.

Preventing Access To The Energy Infrastructure

The data diodes only allow data and act as a perimeter defense to that asset i.e. a turbine rig etc. This allows remote monitoring of these assets with the assurance they cannot be accessed by a hostile source.

SECURITY OPERATIONS CENTRE

COMPATIBLE SOLUTIONS | OPDS 100D | OPDS-1000 | ReCon | SCOWT | V7 CARD SET | XD GUARDIAN



One-way Data Diode

A data diode acts like a one way valve for data, allowing data to flow out, without a way back in. Protecting the building's systems from malicious attacks.

Protecting Your Building

Data is constantly flowing from your building in order to monitor and maintain its systems. This data can add additional information to your security picture allowing you to respond to threats in a timely manner.

INFORMATION CLASSES

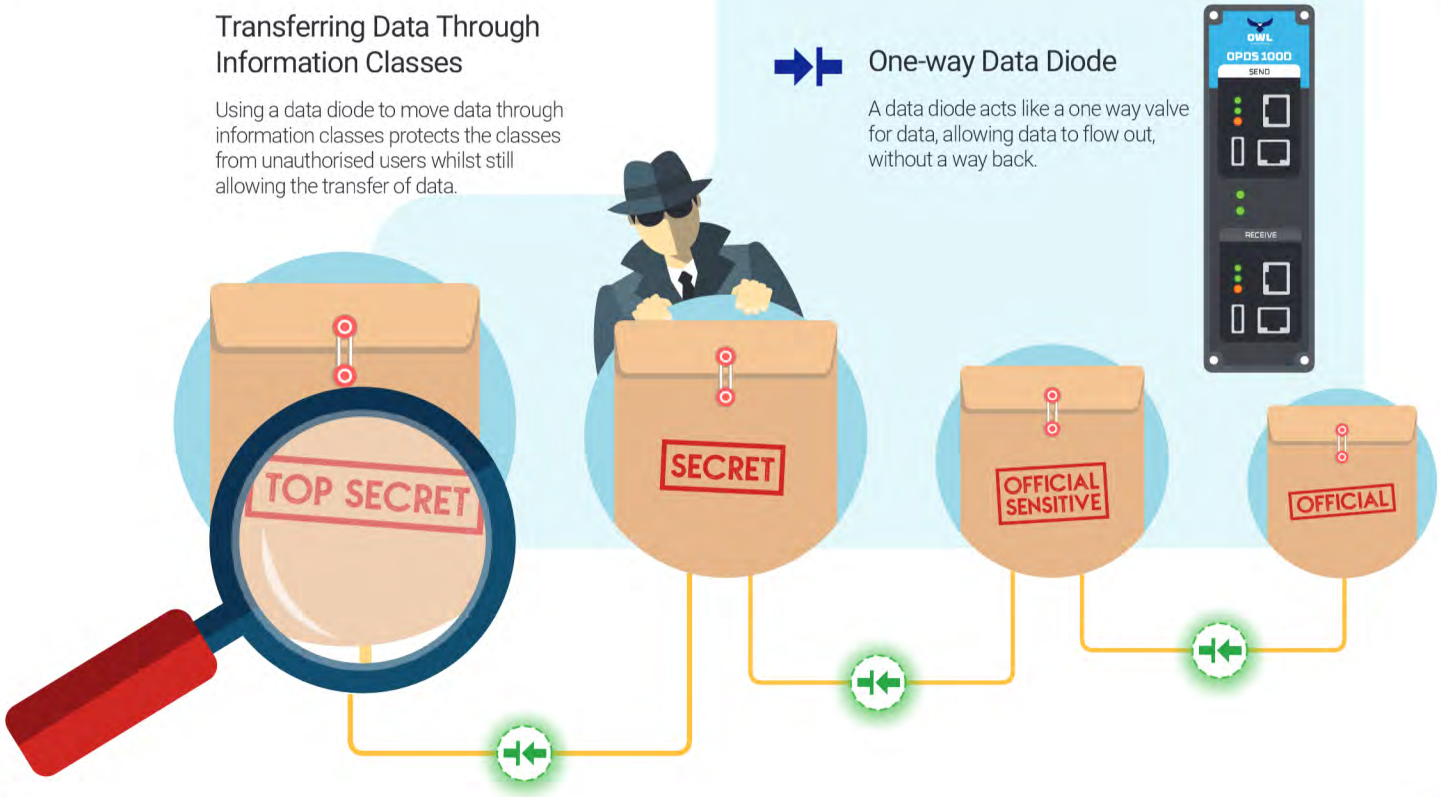
COMPATIBLE SOLUTIONS | DiODa | OPDS 100D | OPDS 1000 | XD GUARDIAN

Transferring Data Through Information Classes

Using a data diode to move data through information classes protects the classes from unauthorised users whilst still allowing the transfer of data.

One-way Data Diode

A data diode acts like a one way valve for data, allowing data to flow out, without a way back.



SME BACKUP SAFEGUARD

COMPATIBLE SOLUTIONS | DiOTa | OPDS 100D | OPDS-1000 | ReCon | SCOWT | V7 CARD SET

Hacking Your Business Computers

Any computer connected to the internet is vulnerable to hackers. A hacker could encrypt all the information on your computer making it impossible for you to retrieve without paying a ransom.

One-way Data Diode

A data diode acts like a one way valve for data, allowing data to flow in, without a way back out.

Data Screening

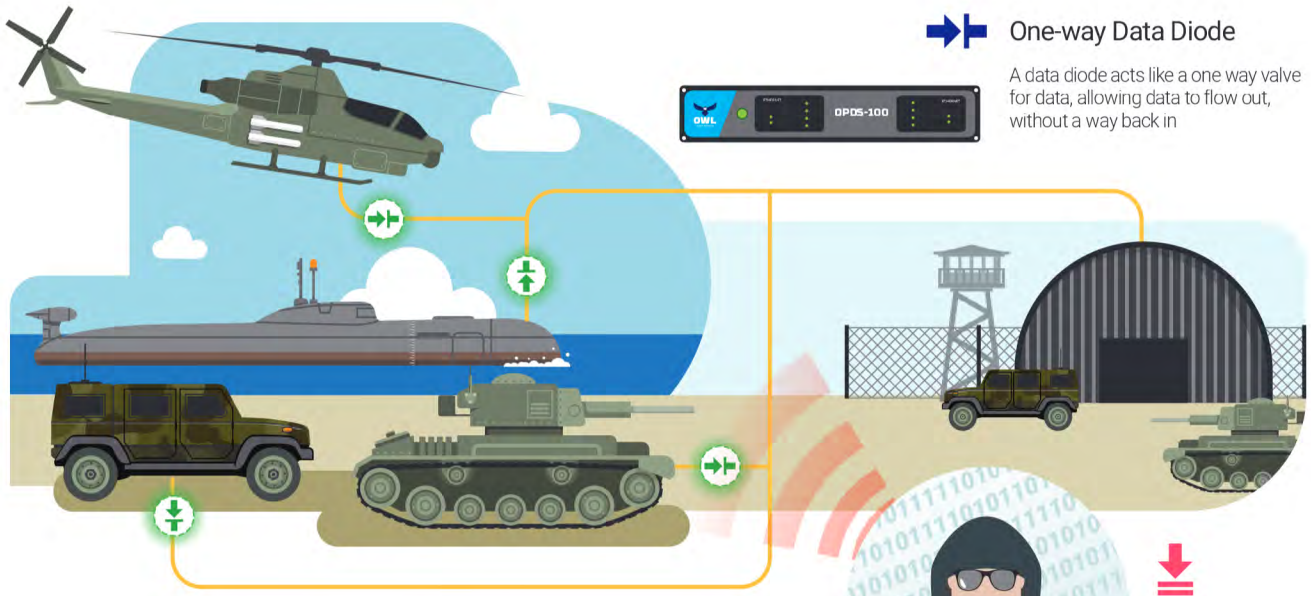
Your files are screened to make sure they don't contain viruses or malware.

Secure Backup

Your backup data is kept secure by the data diode. Allowing you to restore your computer systems and maintain business operation.

MILITARY DATA IN THE FIELD

COMPATIBLE SOLUTIONS | OPDS 100D | OPDS-1000 | ReCon | SCOWT | V7 CARD SET | FPGA | XD GUARDIAN



One-way Data Diode

A data diode acts like a one way valve for data, allowing data to flow out, without a way back in

Military Fleet Field Data

Vehicles on military operations are constantly collecting data in the field. This data is downloaded when the vehicles return to base.

Preventing Access To The Military Fleet

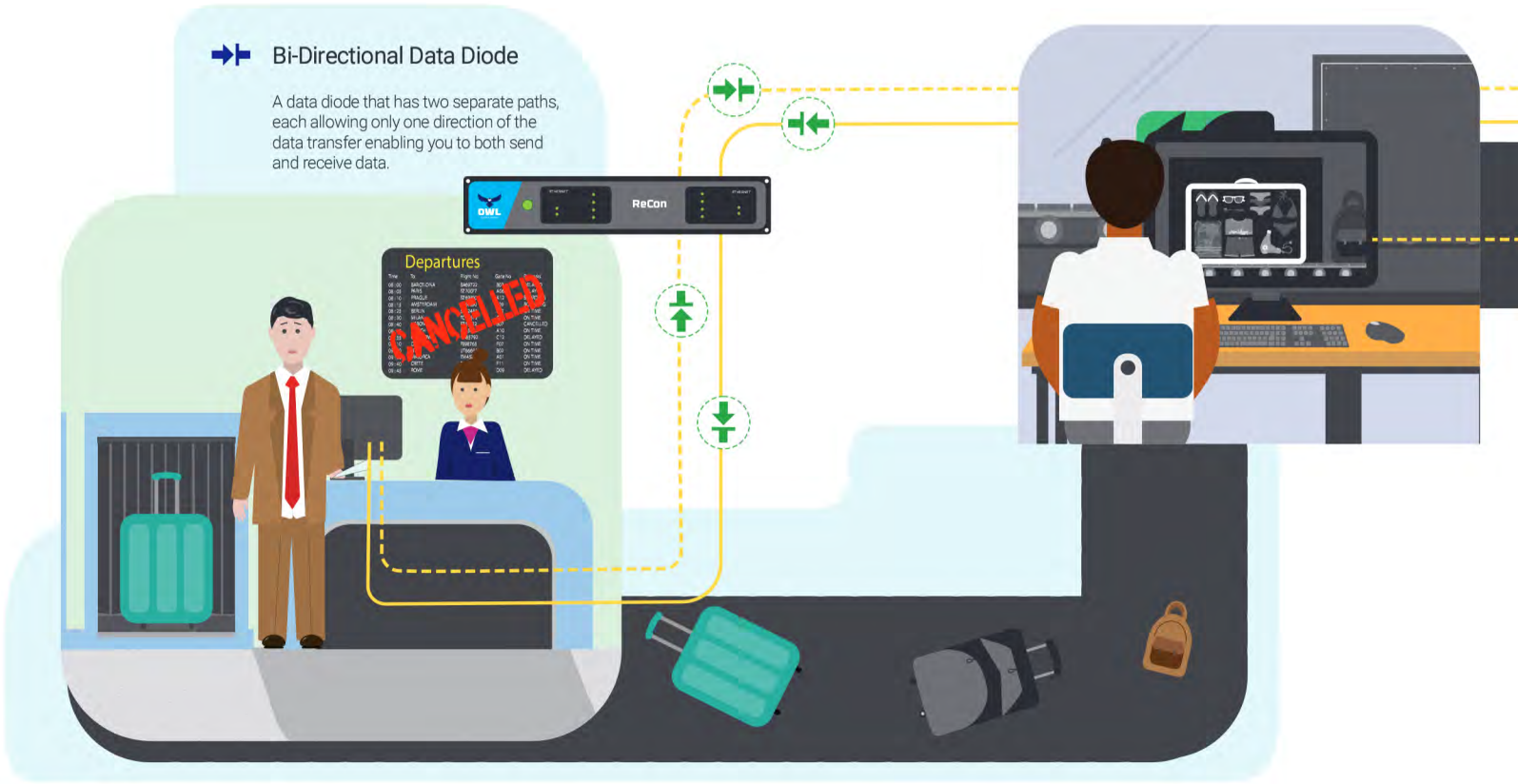
The data diode prevents the hacker from accessing the military vehicle's on board systems.

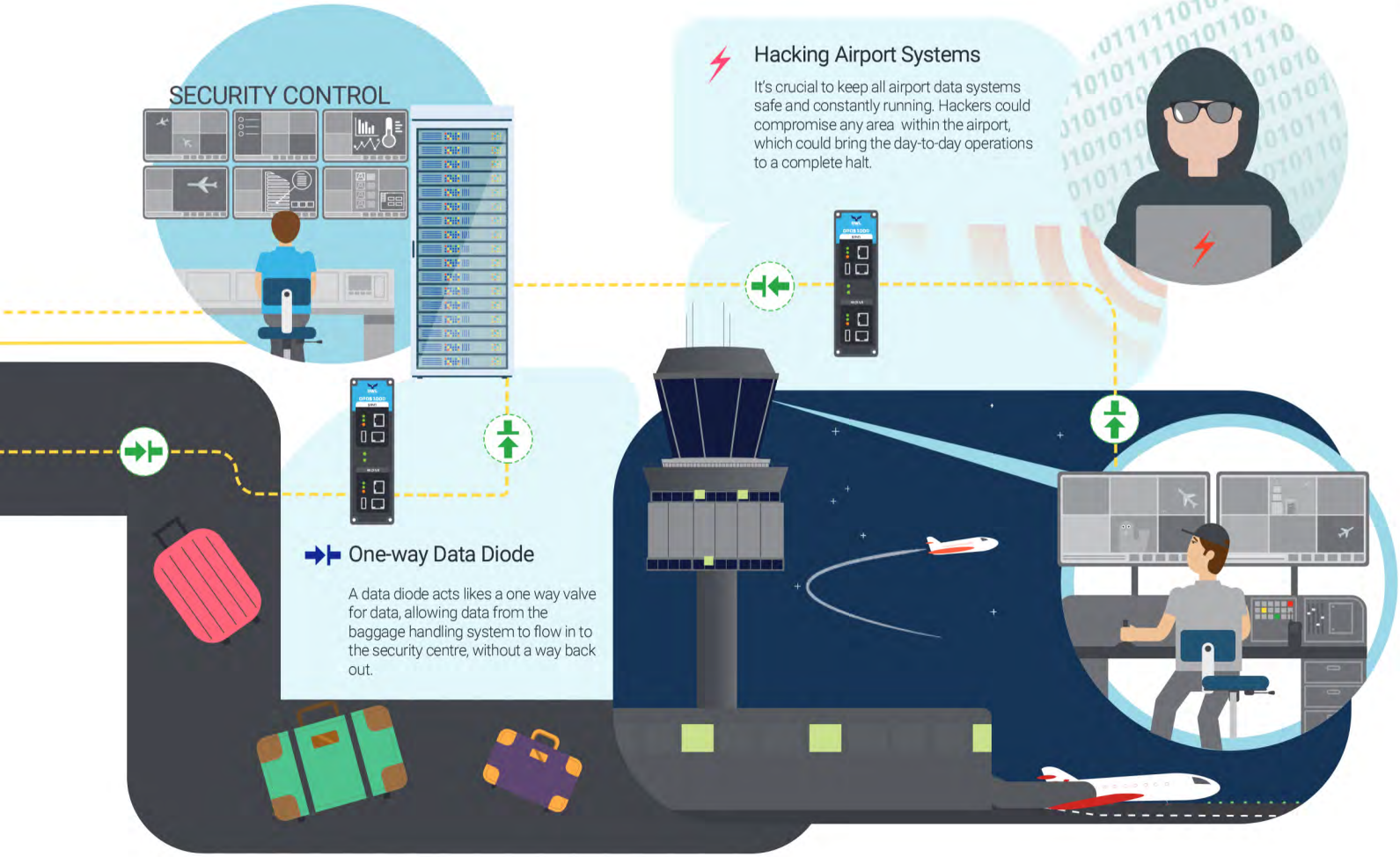
Download To Base

Data can be received instantly and checked for any viruses safe in the knowledge that the fleets on board systems are protected.

AIRPORT SECURITY

COMPATIBLE SOLUTIONS | ReCon | DiOTa | OPDS 100D | OPDS 1000 | XD GUARDIAN





Hacking Airport Systems

It's crucial to keep all airport data systems safe and constantly running. Hackers could compromise any area within the airport, which could bring the day-to-day operations to a complete halt.

One-way Data Diode

A data diode acts likes a one way valve for data, allowing data from the baggage handling system to flow in to the security centre, without a way back out.

4SECURE®

CONTACT US

ENQUIRIES@4-SECURE.COM

WWW.4-SECURE.COM

0800 043 0101