Owl Computing Technologies, Inc.

ACSAC 2007 - CWID 2007 Data Diode Case Study

http://www.owlcti.com toll free 866.695.3387

Coalition Warrior Interoperability Demonstration (CWID) 2007

Case Studies in Data Diode Application

Scope of Presentation

- Coalition Warrior Interoperability Demonstration (CWID)
- Case Study: CWID07 Trial 3.27, “IIMS”
  - Dahlgren Naval Base (Virginia), USA
  - Emergency Response, Command & Control
  - One-way data transfer systems as core service
- Case Study: CWID07 Trial 1.56, “DualDiode”
  - Shirleys Bay (Ottawa), Canada
  - Intelligence Data Fusion, Streaming Video
- Case Study: “Virtual Trial” Enterprise Data Diode Deployment
- Summary

Coalition Warrior Interoperability Demonstration (CWID) – what is it?

- Global international exercise in info sharing

Government ←→ Government

Military ←→ Intelligence

Military ←→ Civil Emergency Response

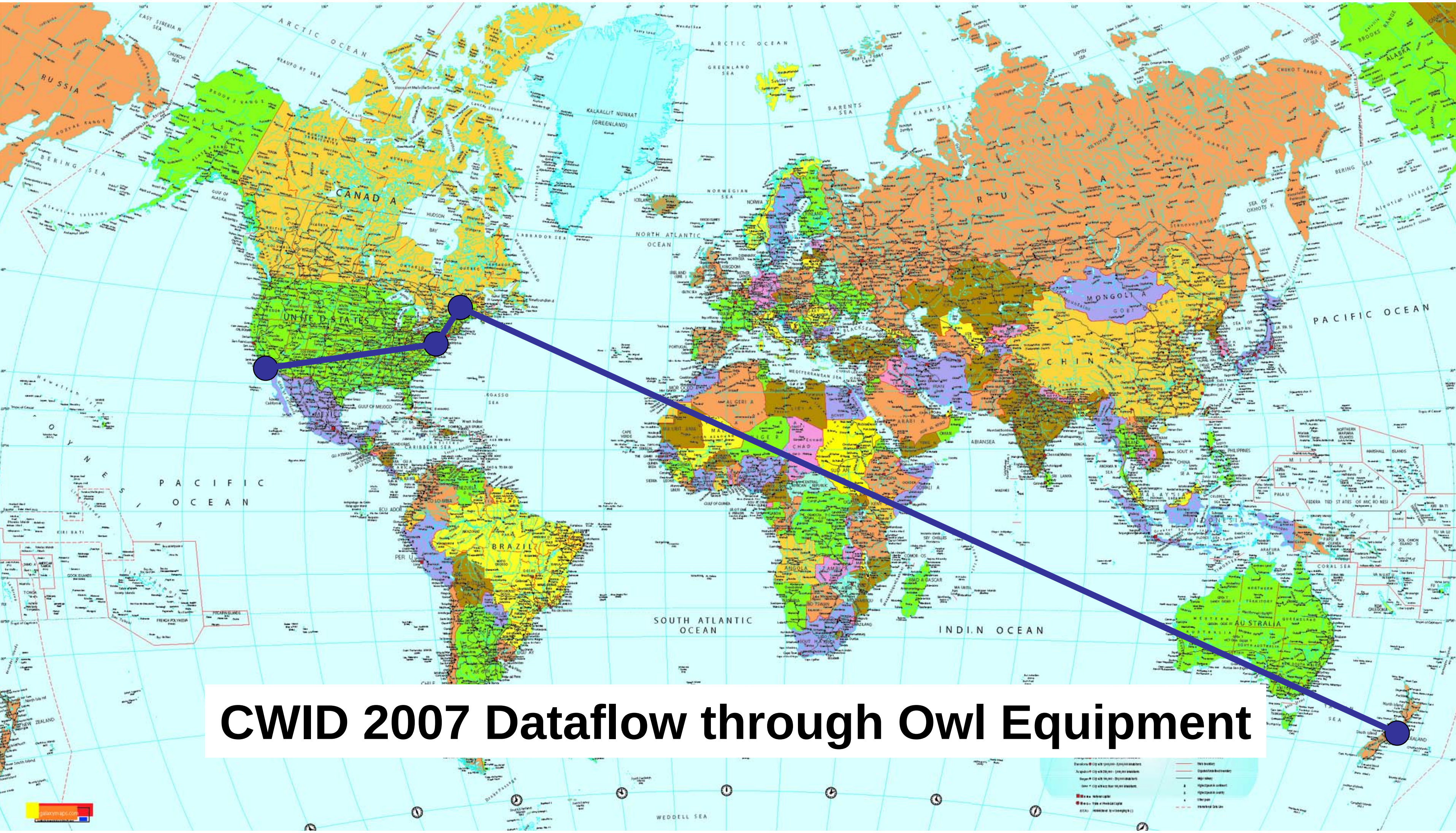
- Communications technology demonstration with formal assessment

What happens during CWID Trials?

- Simulated natural disasters
  - Earthquake, hurricane, disease pandemic
- Simulated man-made disasters
  - War, terrorism, environmental disaster
- ***Information flows between networks***

Who participates in CWID ?

- Governments
  - – US, Canada, UK, Australia, NZ, NATO
- Military, Intel, Civil Protection Agencies
- Commercial Defense Contractors (Cross Domain Solution Providers)



CWID 2007 Dataflow through Owl Equipment

CWID 2007 Timeline

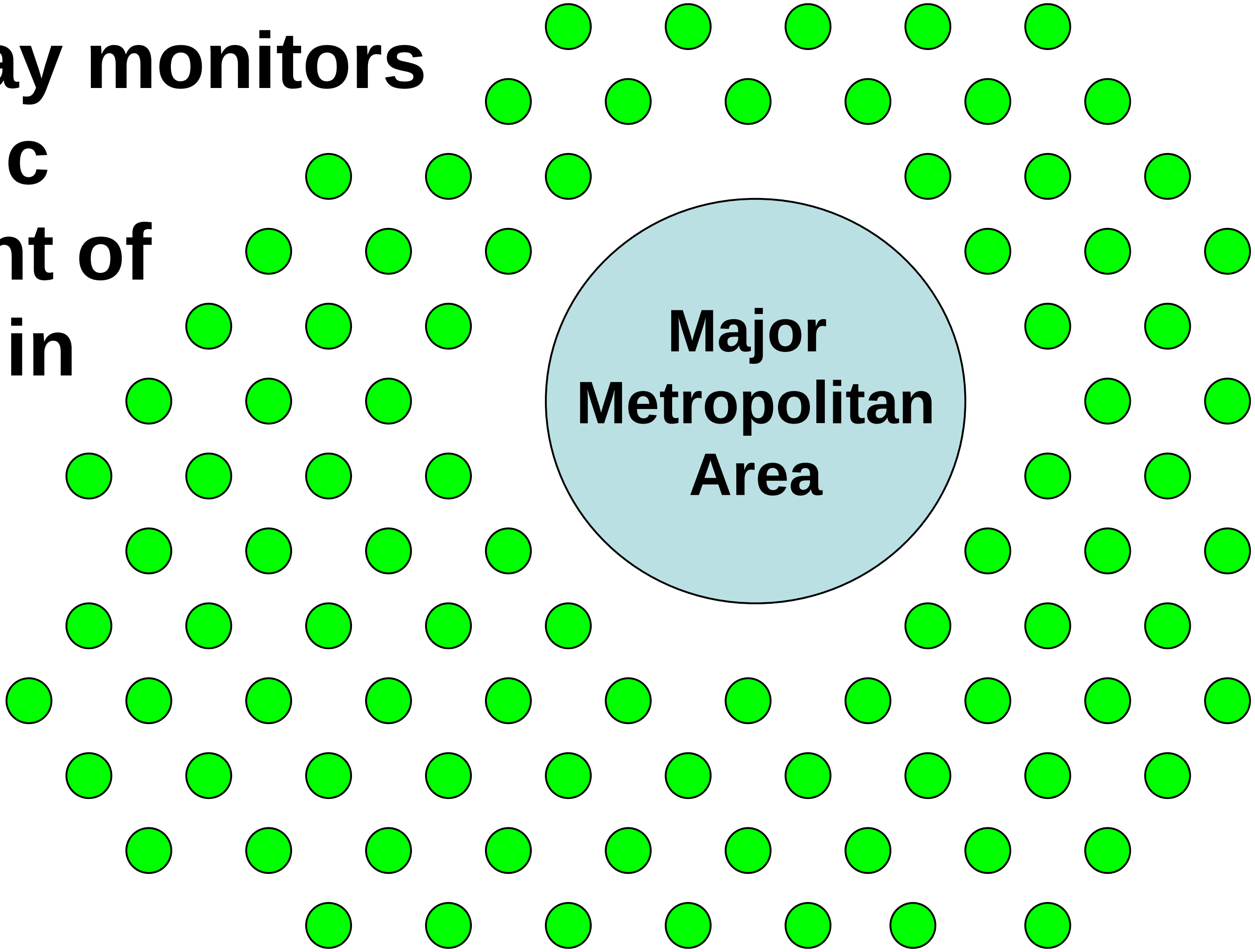
- Initial Planning Conference 13-17 Nov, 2006
- Mid Planning Conference 19 Jan – 2 Feb, 2007
- Final Planning Conference, 26-30 Mar, 2007
- Training for Role Players 4-8 Jun, 2007
- Execution 11-21 Jun, 2007

Case Study 1

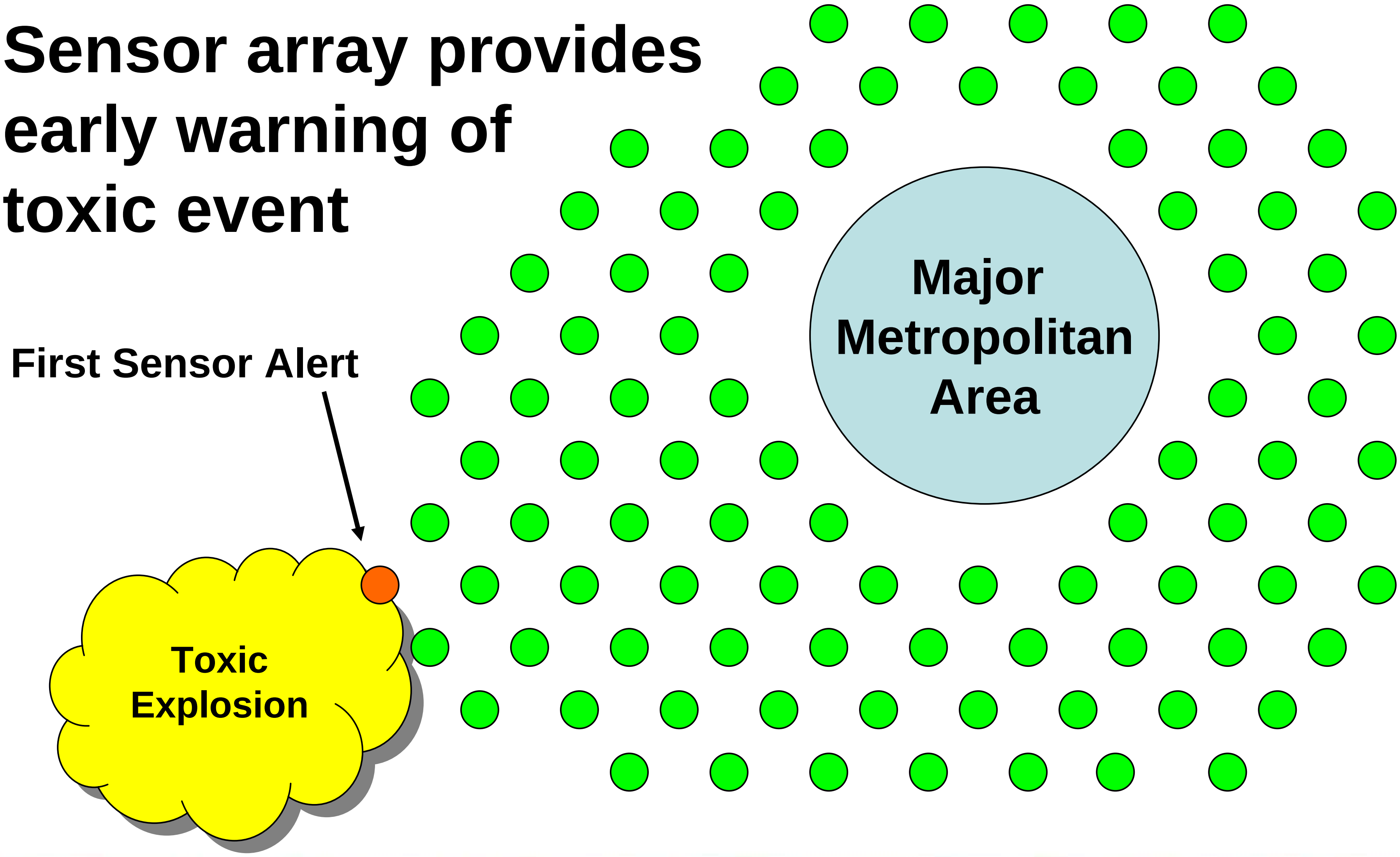
CWID 2007 Trial 3.27, IIMS, Dahlgren VA Integrated Information Management System

- Enhance preparedness for natural or man-made threats to homeland security.
- Early detection of threat or attack
  - biological, chemical, radiological
- Coordinate response to emergency or attack
  - local, state, federal organizations
- Sponsor: USAF, developer: US Army

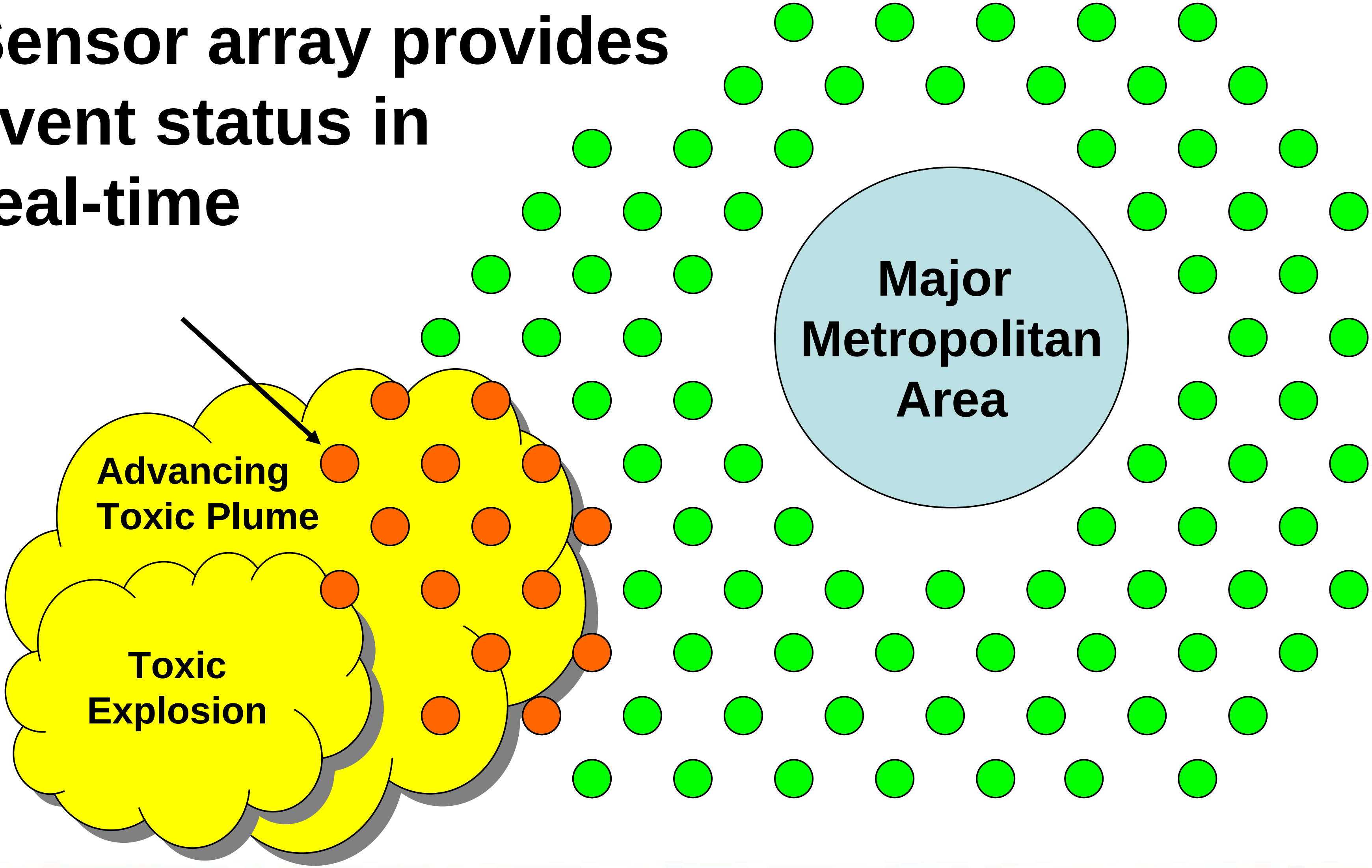
Sensor array monitors atmospheric environment of metro area in real-time



Sensor array provides early warning of toxic event

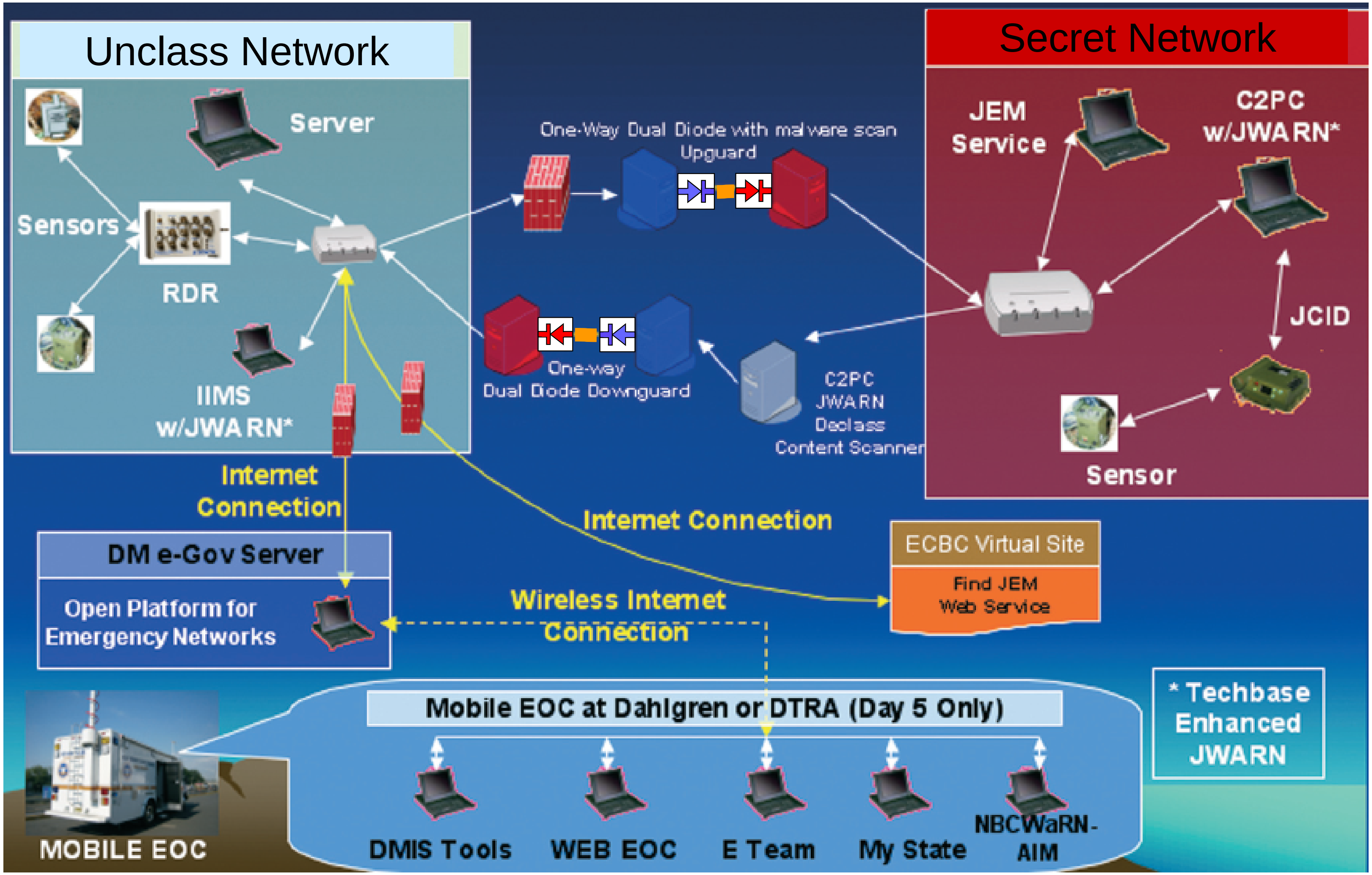


Sensor array provides event status in real-time



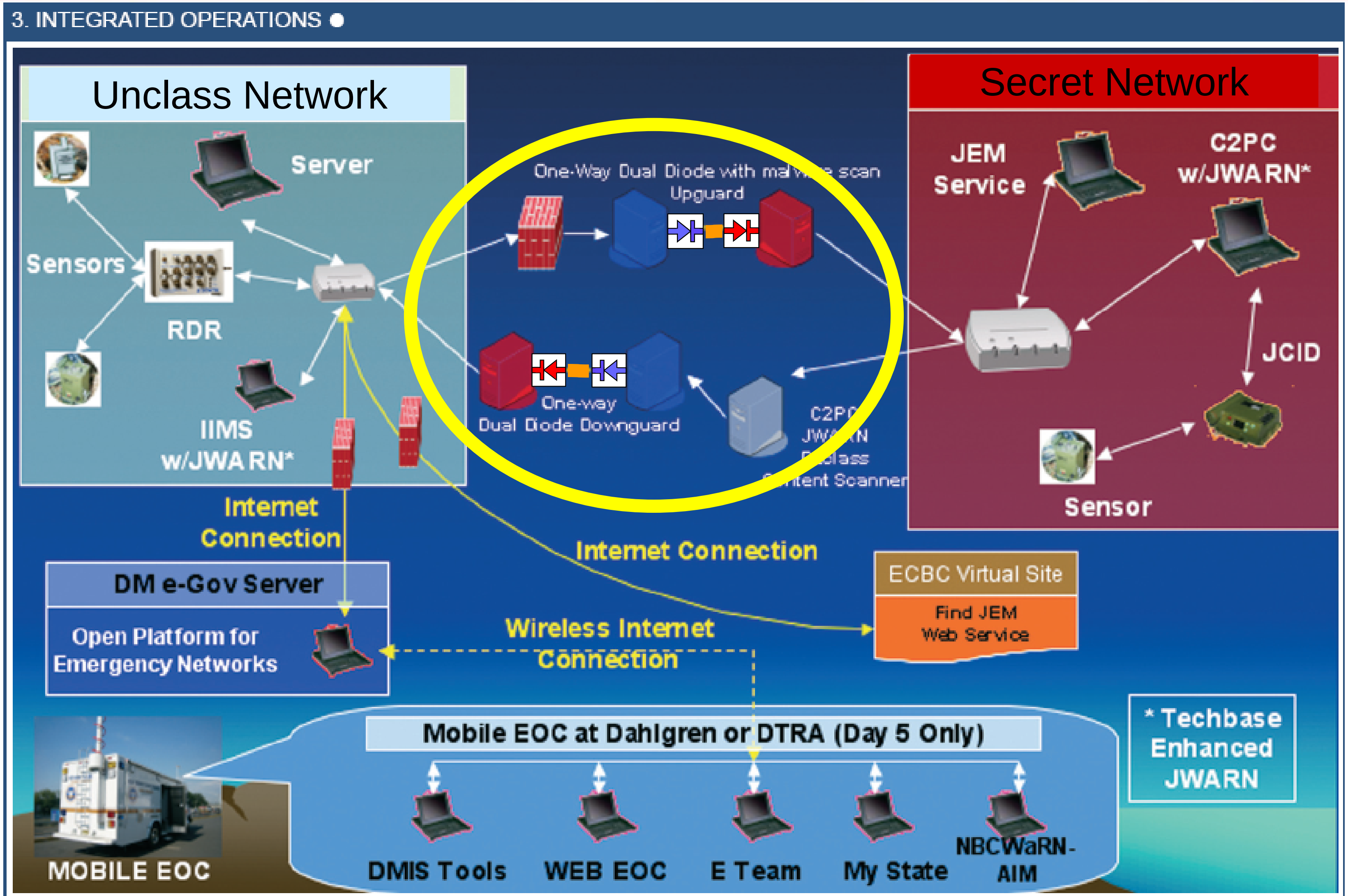
CWID 2007 Trial 3.27 – IIMS Architecture Details

3. INTEGRATED OPERATIONS ●


Unclass Network
Server
Sensors
RDR
IIMS w/JWARN*
Internet Connection
DM e-Gov Server
Open Platform for Emergency Networks
One-Way Dual Diode with malware scan Upguard
One-way Dual Diode Downguard
C2PC JWARN Declass Content Scanner
Internet Connection
Wireless Internet Connection
Secret Network
JEM Service
C2PC w/JWARN*
JCID
Sensor
ECBC Virtual Site
Find JEM Web Service
* Techbase Enhanced JWARN
Mobile EOC at Dahlgren or DTRA (Day 5 Only)
MOBILE EOC
DMIS Tools
WEB EOC
E Team
My State
NBCWaRN-AIM

IIMS IS CURRENTLY FIELDED IN:
- U.S. Pacific Command (USPACAF) in the Korean theater of operation, Osan Air Force Base
- U.S. Central Command (USCENTCOM) in the Southwest Asia theater of operation, Port of Ash Shuaybah, Kuwait

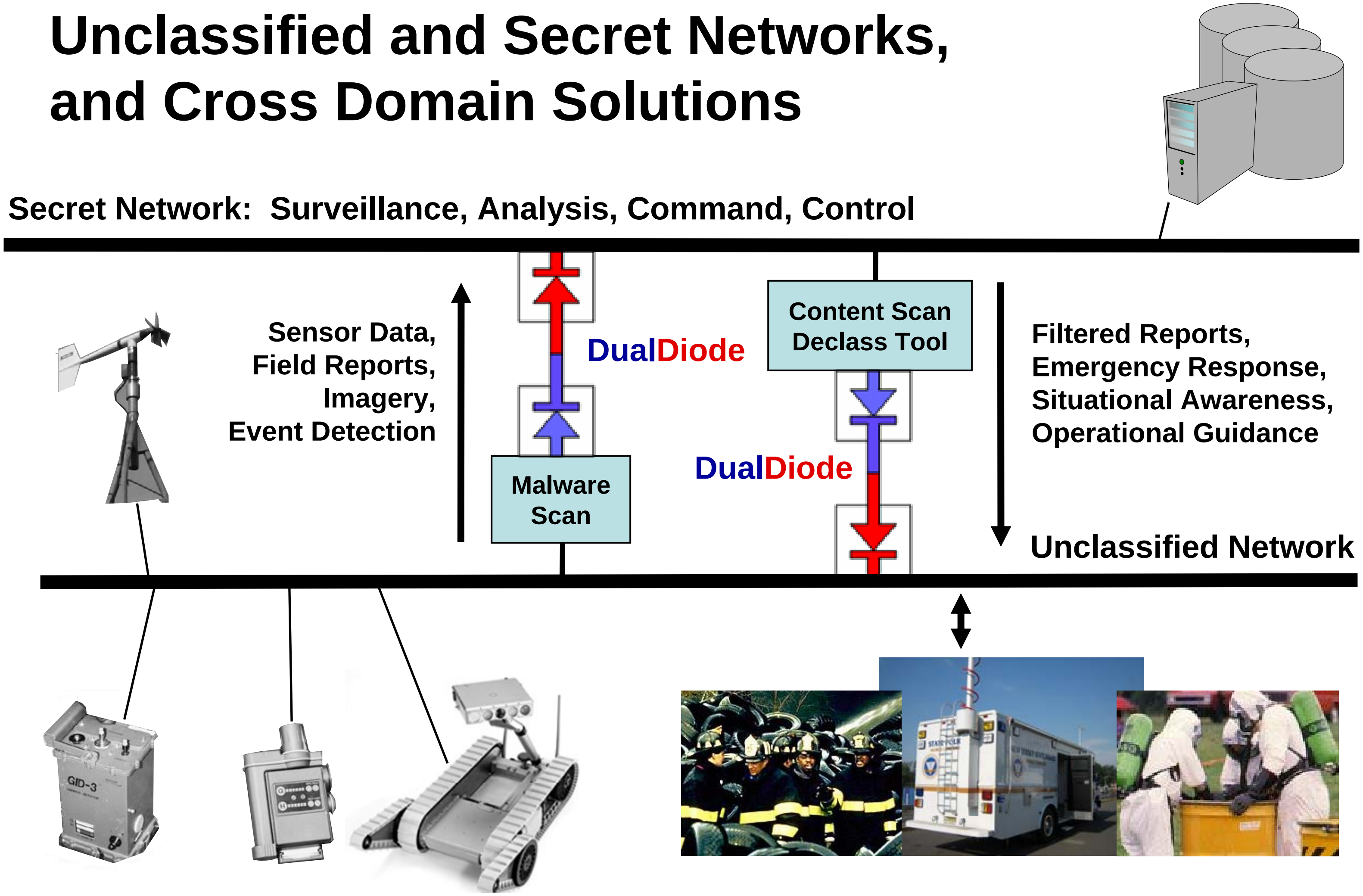
CWID 2007 Trial 3.27 – IIMS Architecture Details



IIMS IS CURRENTLY FIELDED IN:
- U.S. Pacific Command (USPACAF) in the Korean theater of operation, Osan Air Force Base
- U.S. Central Command (USCENTCOM) in the Southwest Asia theater of operation, Port of Ash Shuaybah, Kuwait

CWID Trial 3.27 IIMS, Simplified

Multi-Network Architecture includes Unclassified and Secret Networks, and Cross Domain Solutions



Secret Network: Surveillance, Analysis, Command, Control

Sensor Data,
Field Reports,
Imagery,
Event Detection

DualDiode

Malware Scan

Content Scan Declass Tool

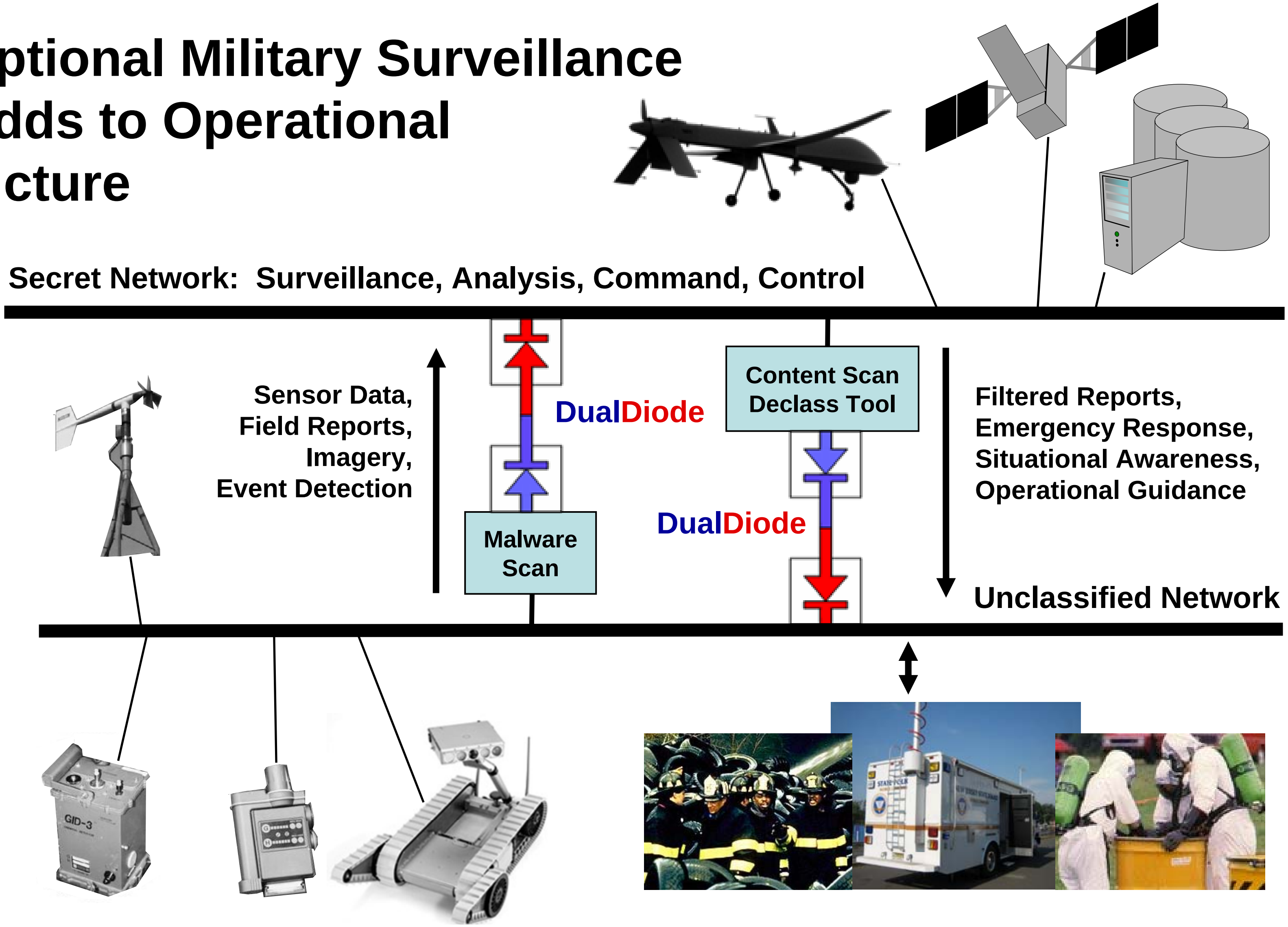
DualDiode

Filtered Reports,
Emergency Response,
Situational Awareness,
Operational Guidance

Unclassified Network

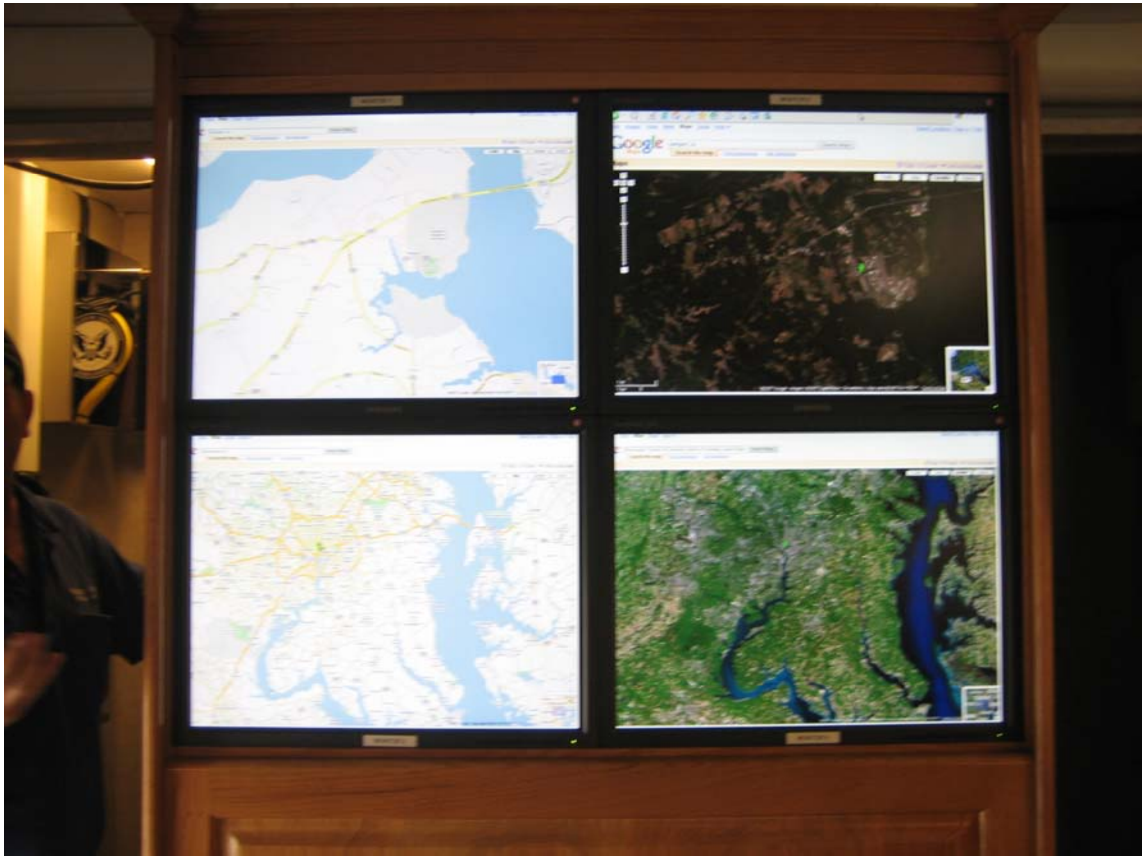
CWID Trial 3.27 IIMS, Simplified

Optional Military Surveillance Adds to Operational Picture



- **IIMS exchanges alerts with a civilian mobile Emergency Operation Center (EOC).**
- **EOC shares alerts with Federal, State, Local agencies through Open Platform Emergency Networks (OPEN).**
- **The EOC is provided by Rapid Response Institute of Monmouth University. The EOC also known as Joint Mobile Command and Training Center.**

Emergency Operation Center (EOC) info processing focuses on Geospatial situational awareness.



CWID Trial 3.27 IIMS - General Description

- Accumulate sensor data on low security networks.
- One-way Transfer data from low to high security networks for analysis, event detection.
- military surveillance data on secure network enhances situational awareness.
- One-way Transfer alerts, reports, directives from secure network to civilian networks for joint response.

Data Diode as Core Service

- Data flow is separated into two one-way transfer paths subject to different security protocols.

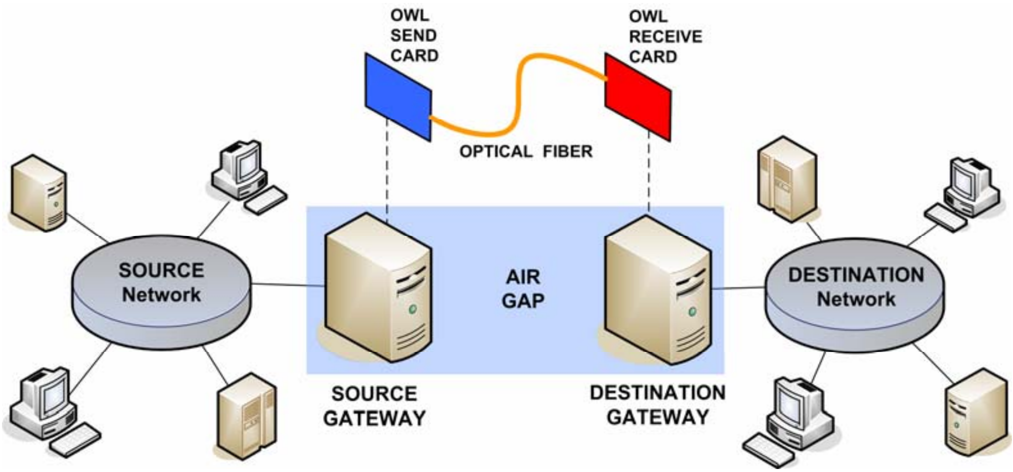
- Data flow from Unclass to Secret (low to high) requires malware scan before transfer.

- Data flow from Secret to Unclass (high to low) requires human-review, content scan before transfer.

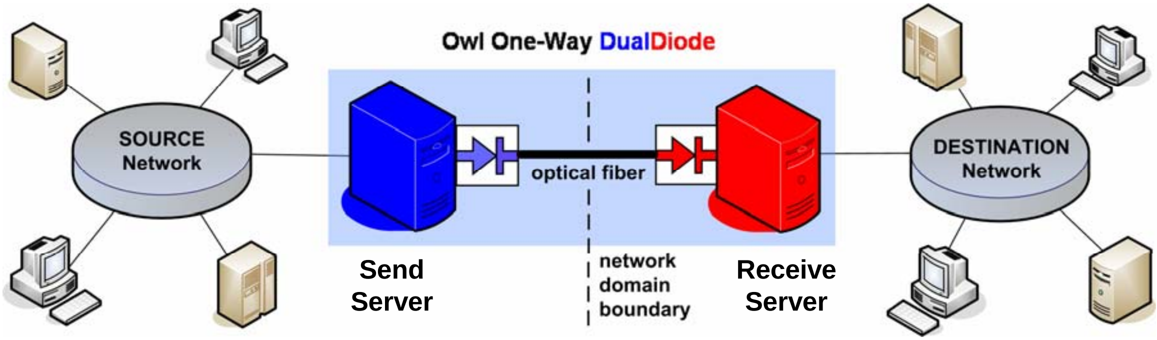
Why hardware-enforced one-way transfer?

- cannot be probed or hacked with software
- rigorous protocol break across domains
- From low to high, data transfer policy compliant with established data security models
- From high to low, data transfer always initiated (pushed) from trusted source.

DualDiode Specifics

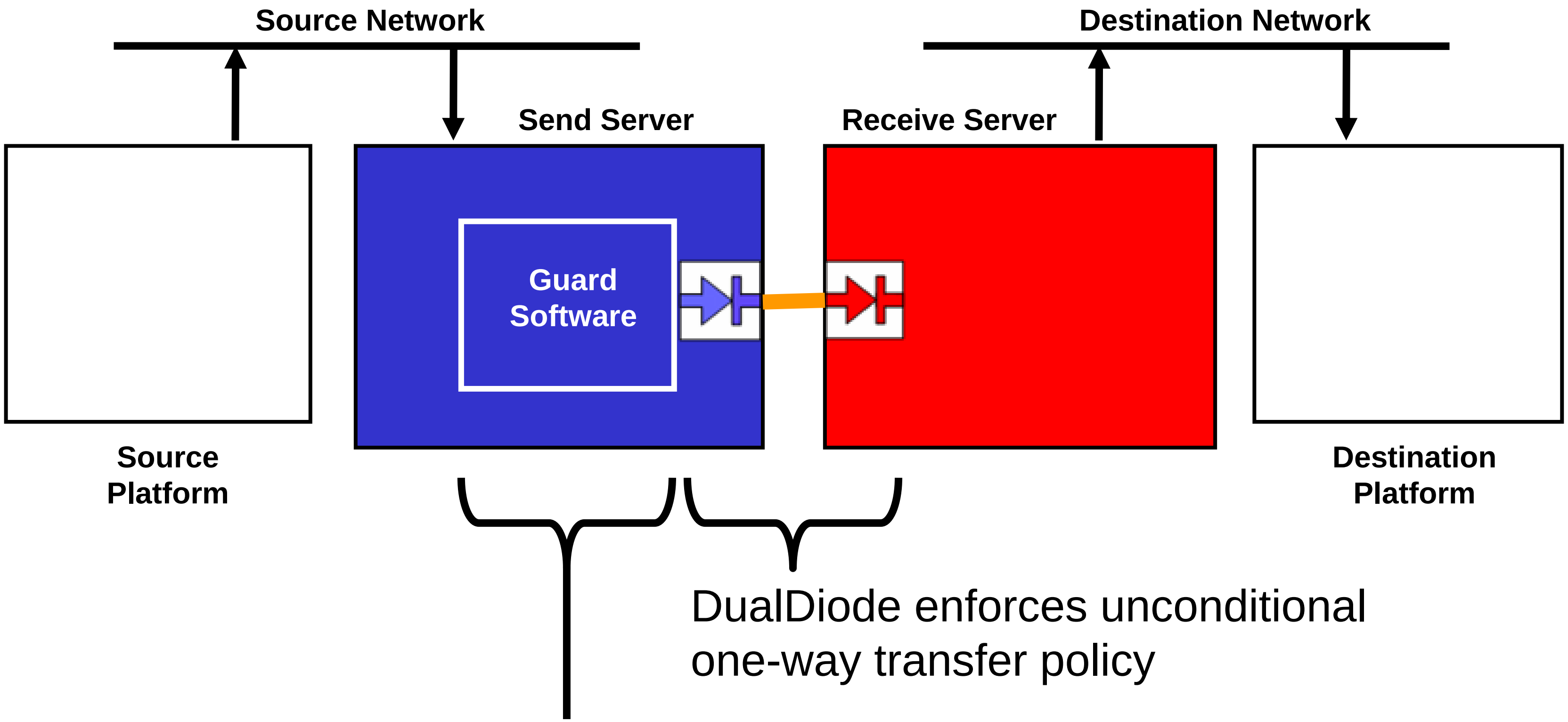


Send and Receive Owl Cards installed in host computer platforms…



…Create Send and Receive gateways for their respective networks.

What makes a One-Way Cross-Domain Solution

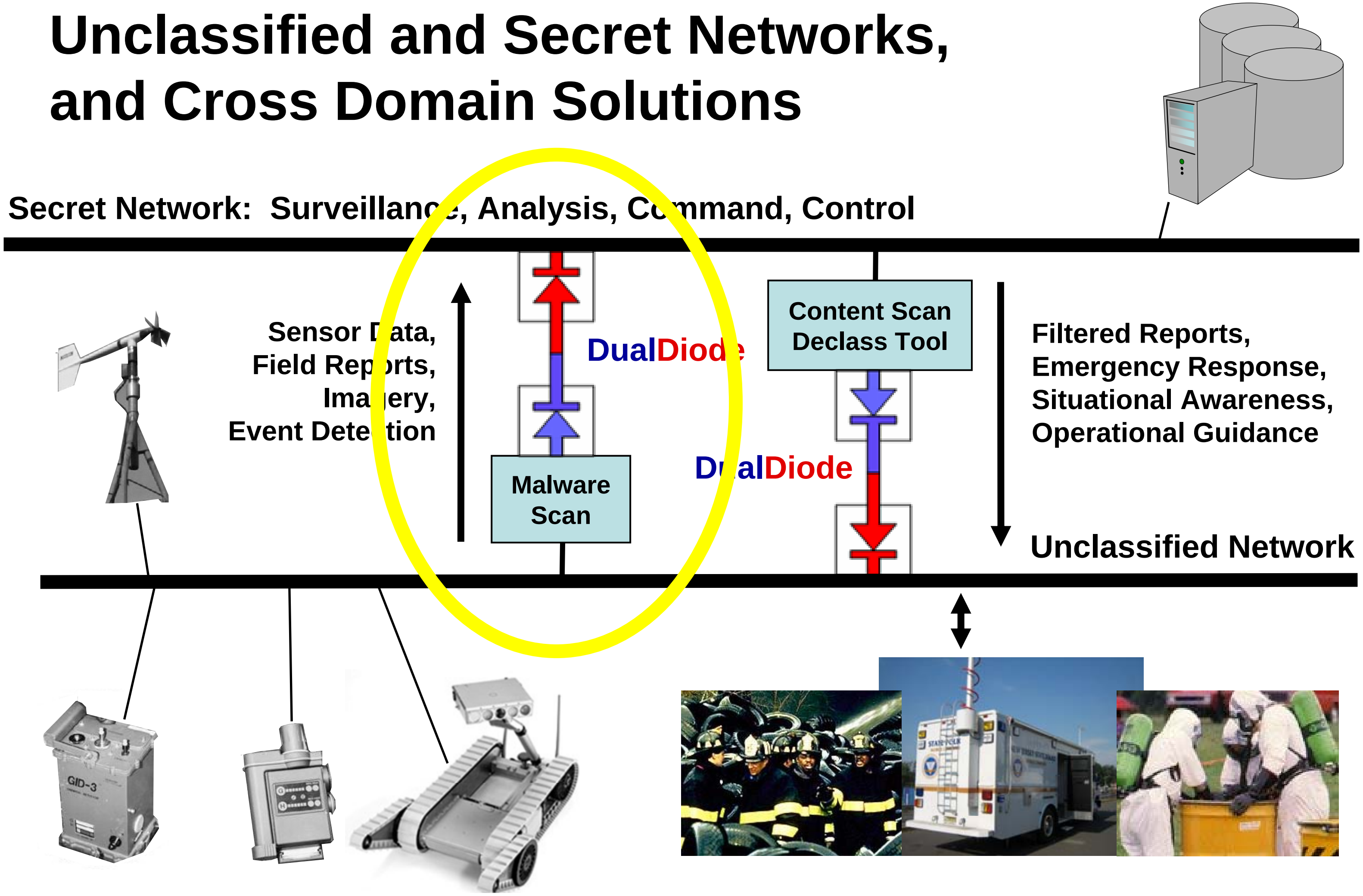


DualDiode enforces unconditional one-way transfer policy

Guard software enforces conditional forward data transfer policy

CWID Trial 3.27 IIMS, Simplified

Multi-Network Architecture includes Unclassified and Secret Networks, and Cross Domain Solutions



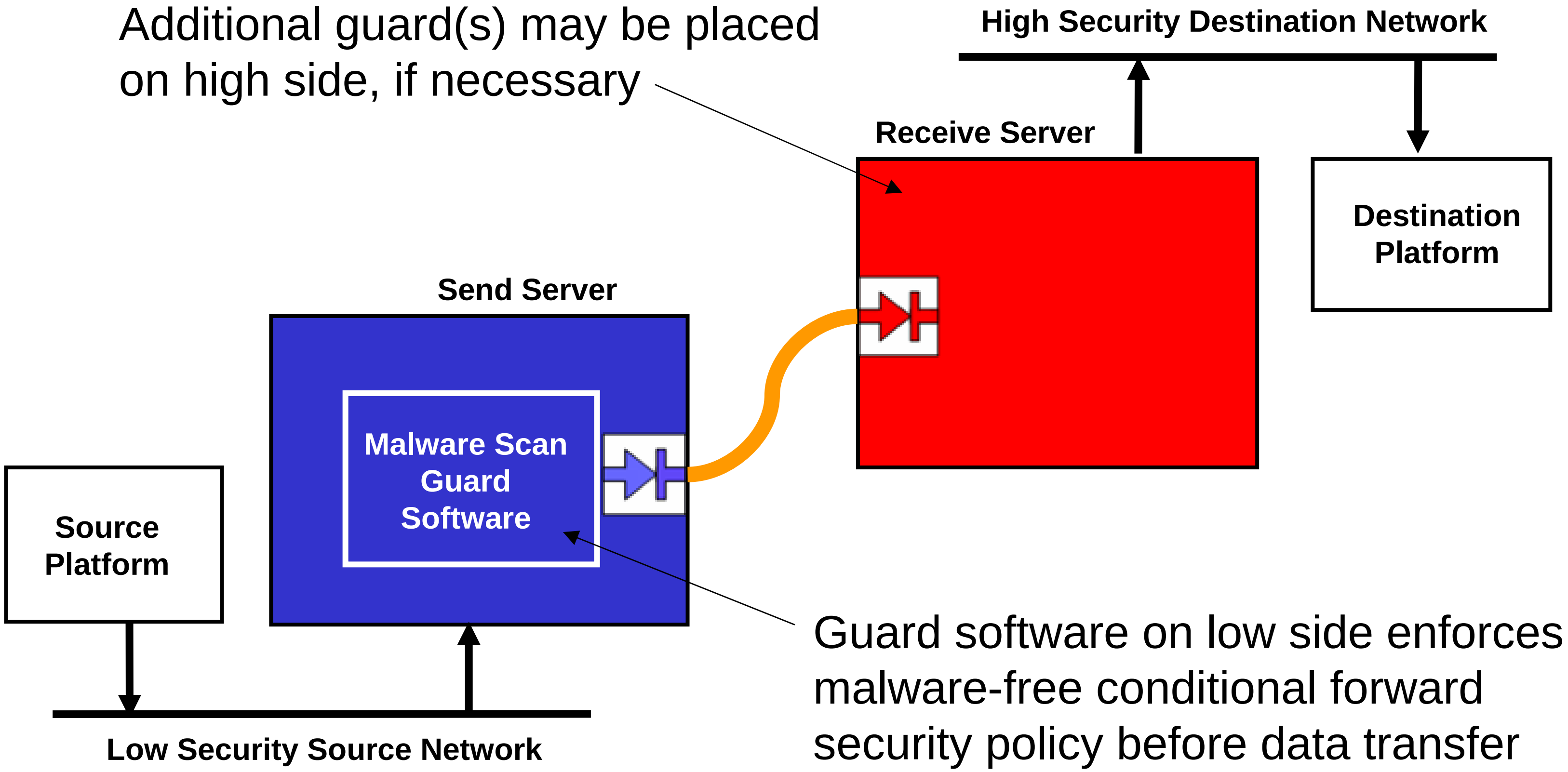
Secret Network: Surveillance, Analysis, Command, Control

Sensor Data,
Field Reports,
Imagery,
Event Detection

Filtered Reports,
Emergency Response,
Situational Awareness,
Operational Guidance

Unclassified Network

Low to High “Upguard” Cross-Domain Solution

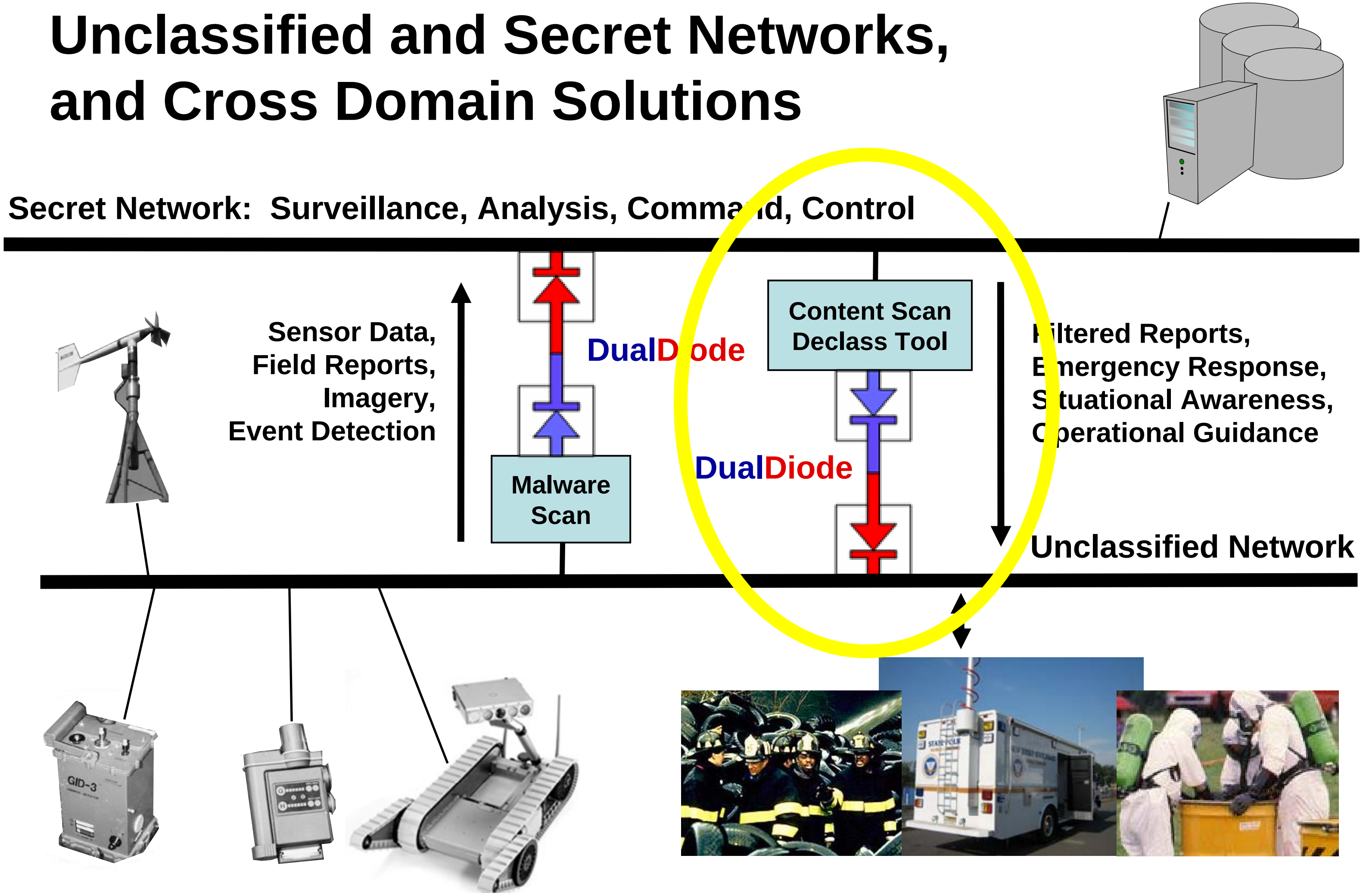

High Security Destination Network
Receive Server
Destination Platform
Send Server
Malware Scan Guard Software
Source Platform
Low Security Source Network

Additional guard(s) may be placed on high side, if necessary

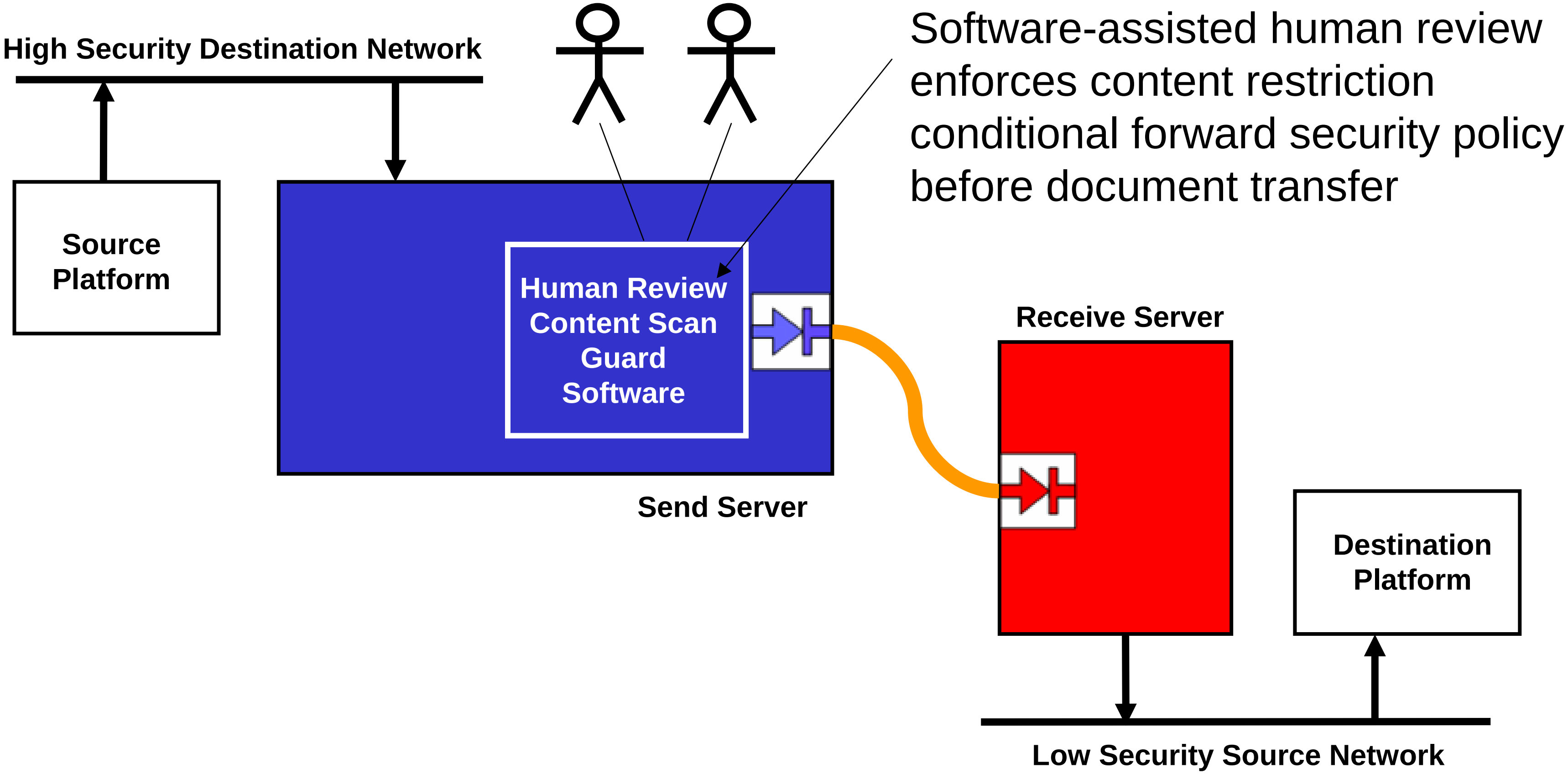
Guard software on low side enforces malware-free conditional forward security policy before data transfer using Symantec Scan Engine

CWID Trial 3.27 IIMS, Simplified

Multi-Network Architecture includes Unclassified and Secret Networks, and Cross Domain Solutions



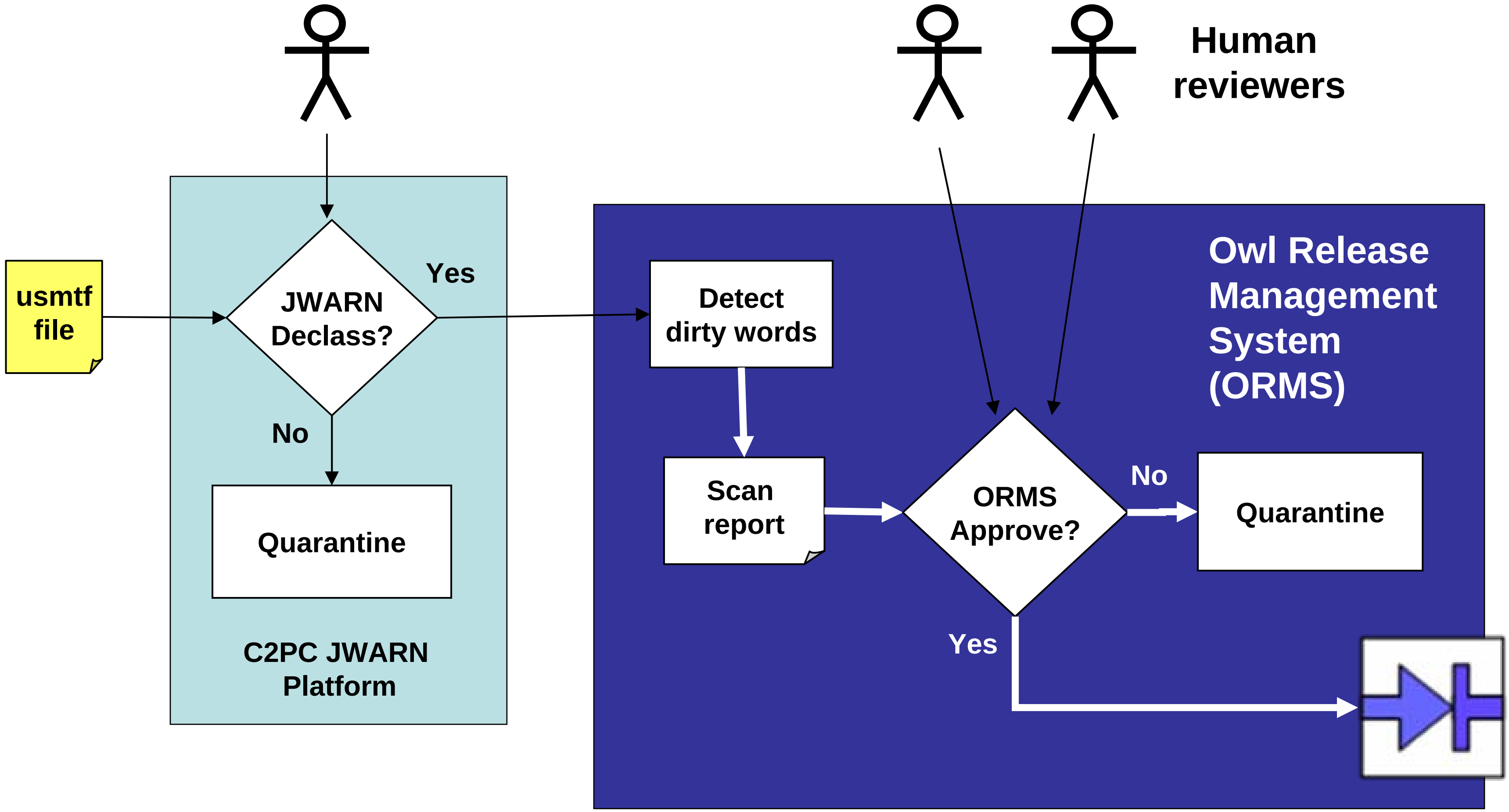
High to Low “Downguard” Cross-Domain Solution



Software-assisted human review enforces content restriction conditional forward security policy before document transfer

Trial 3.27 Downguard Details: JWARN, ORMS

Downguard Data Review Process Flowchart



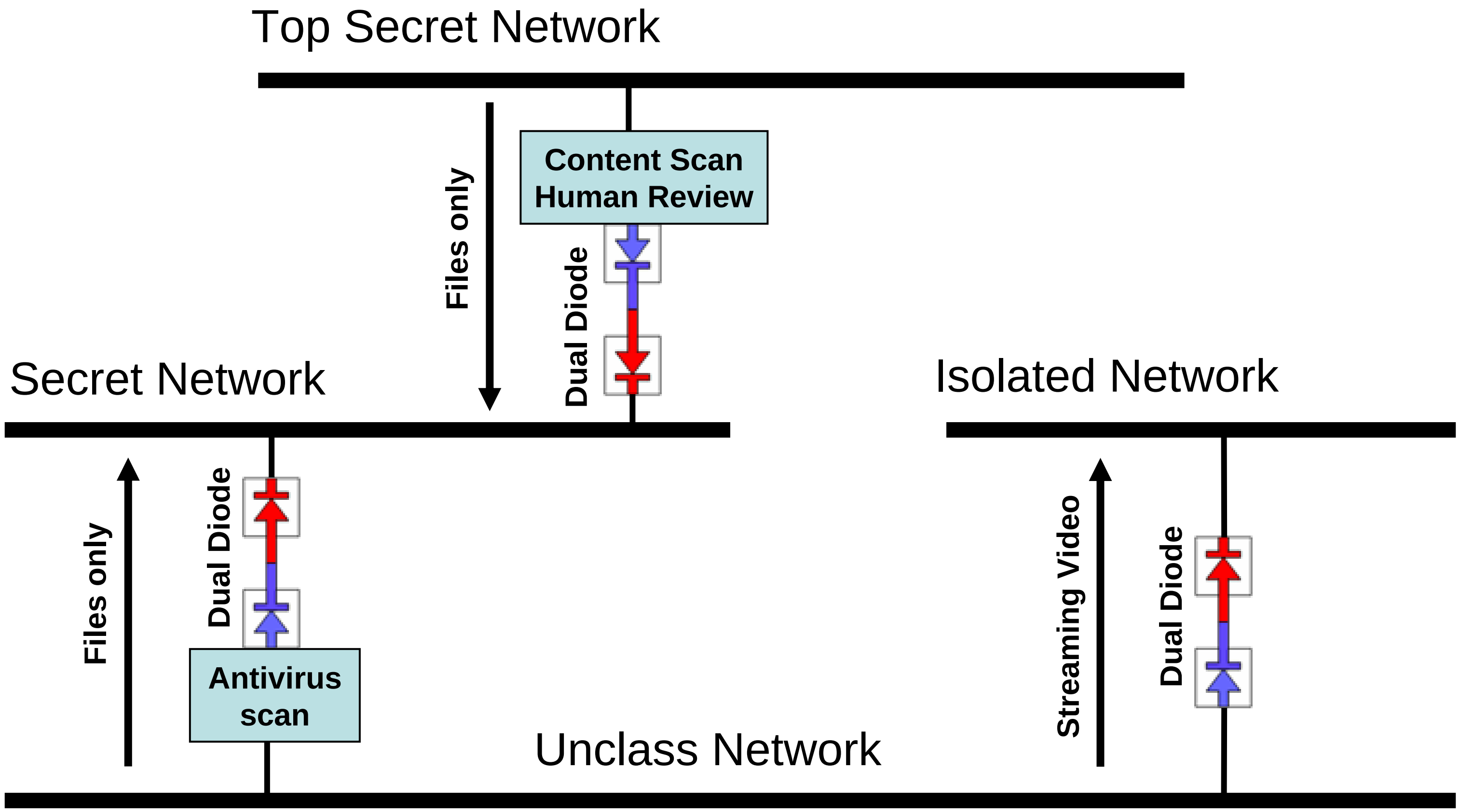
Case Study 1 Summary:

- **Upguard Data Diode file xfer**
  - malware scan

- **Downguard Data Diode text file xfer**
  - “dirty word” content scan
  - multi human review

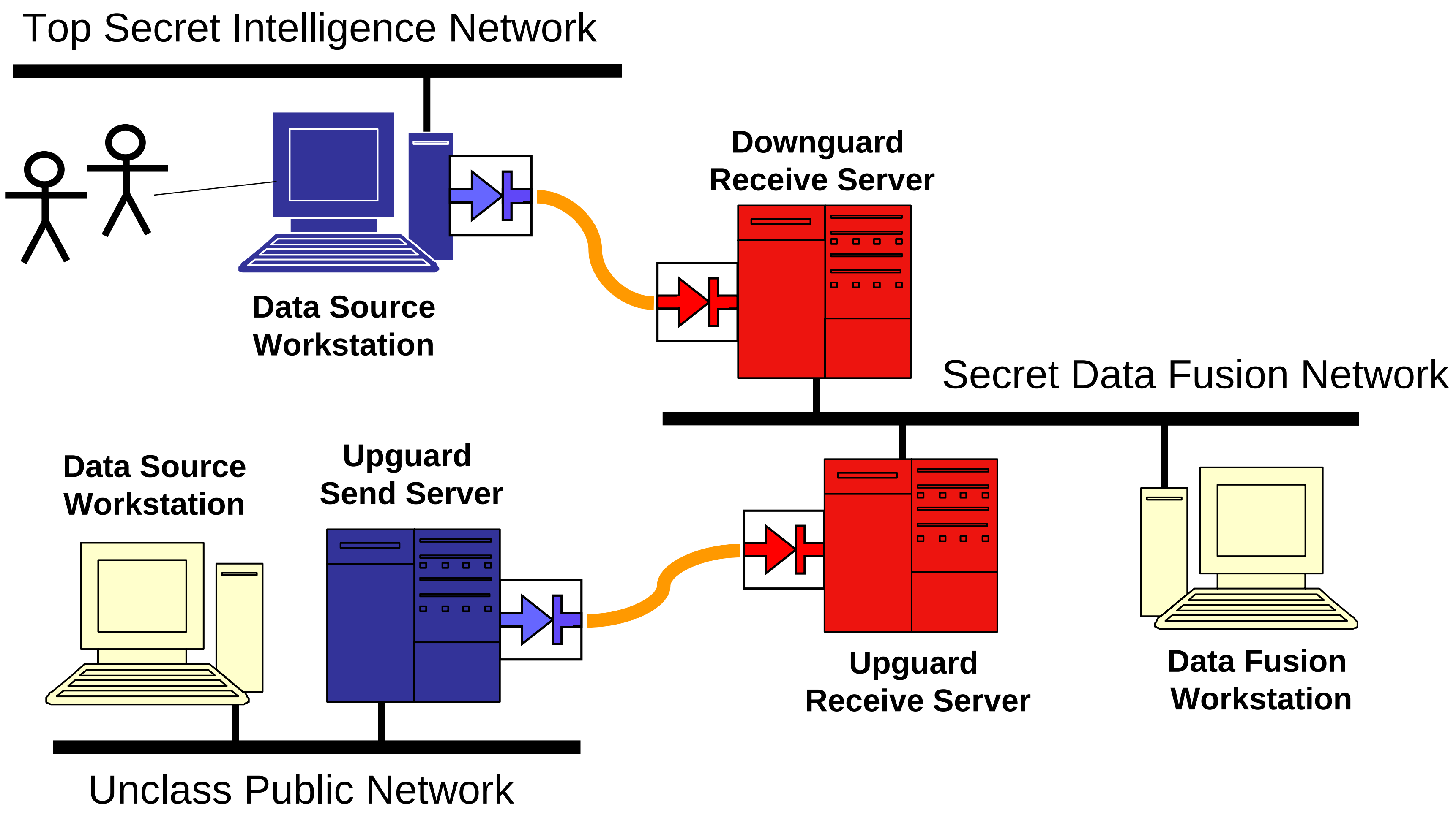
Case Study 2

CWID 2007 Trial 1.56 “DualDiode”, Shirleys Bay, Canada

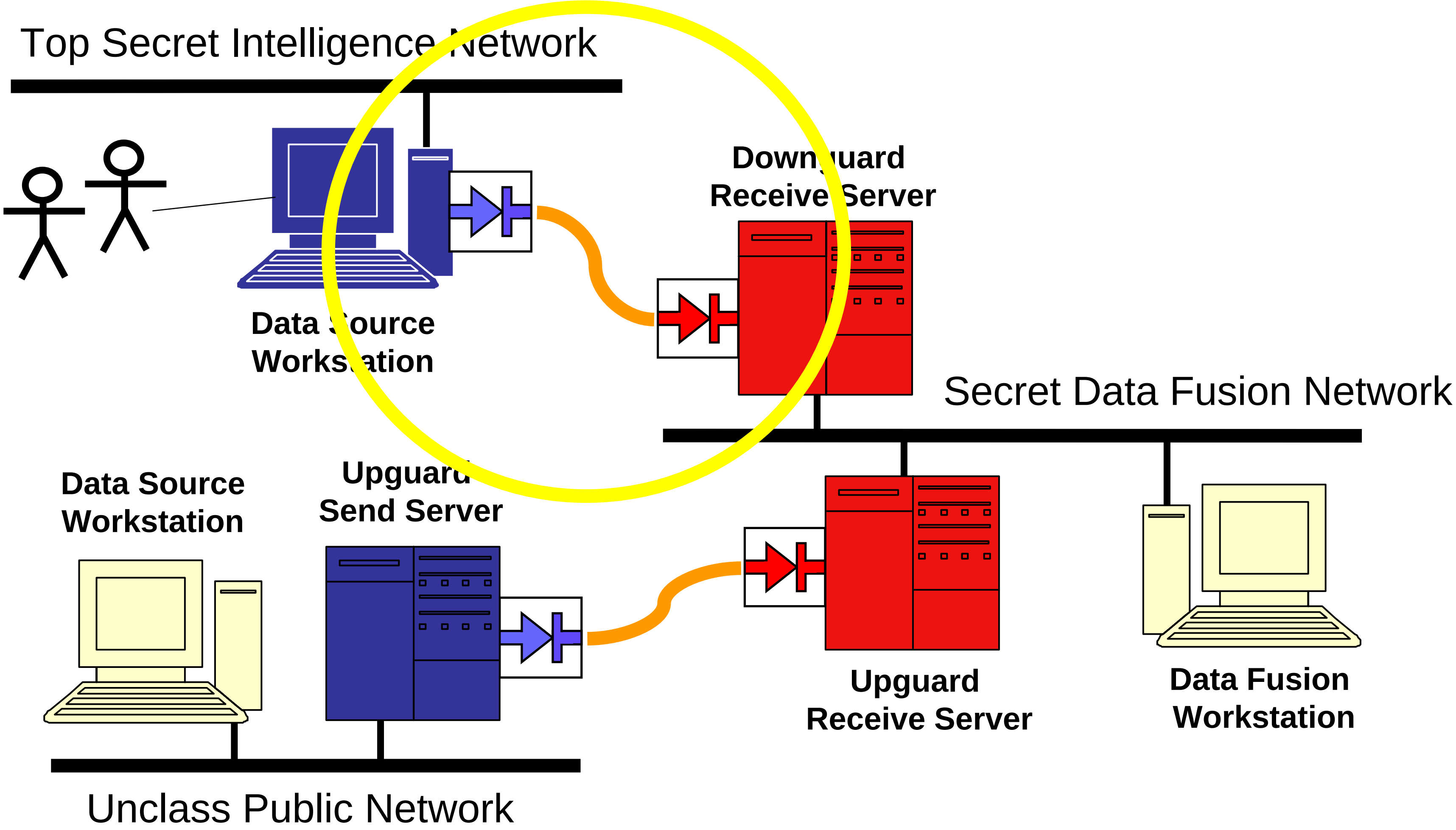


Data Fusion & Streaming Video

Trial 1.56 Data Fusion Demonstration

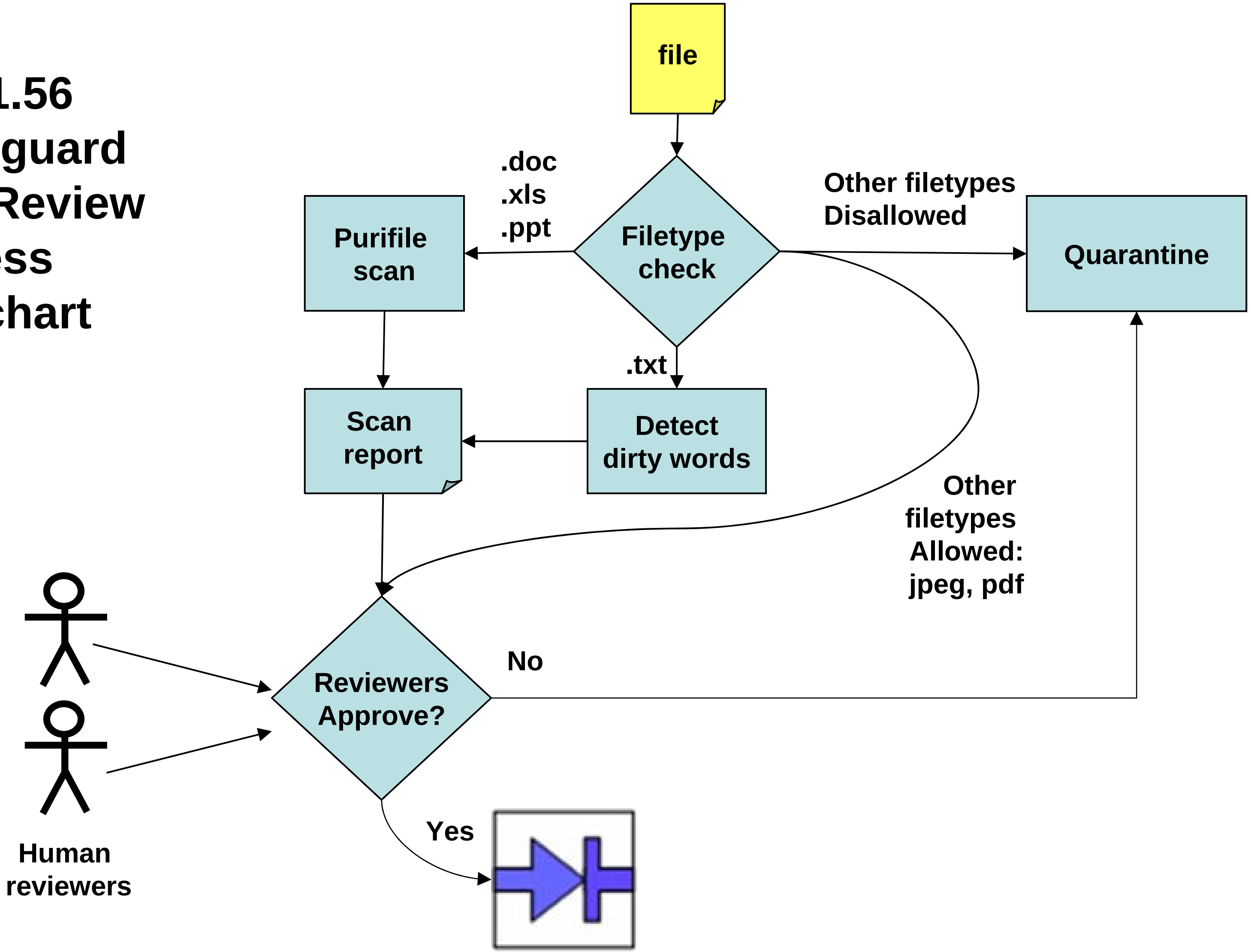


Trial 1.56 Data Fusion Demonstration



Owl Release Management System (ORMS)

Trial 1.56 Downguard Data Review Process Flowchart

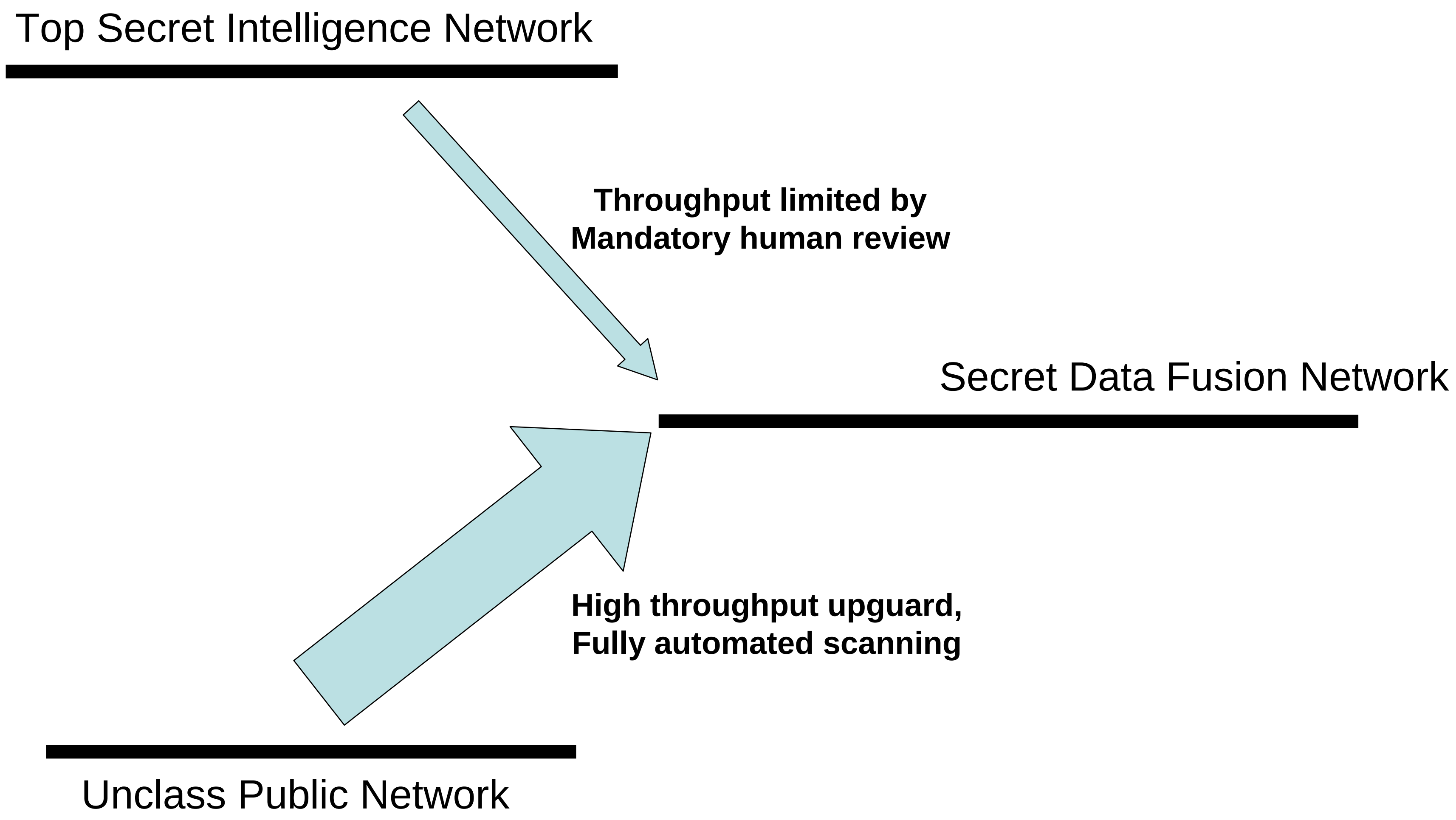


Trial 1.56 – Downguard Features

Owl Release Management System (ORMS) Features Multiple-human Review and Purifile™ Content Scanning:

- **Deep Content Scanning of Microsoft Office Filetypes .doc, .xls, .ppt**
- **Scan results rendered in human-readable report**
- **Detects improperly embedded info content not obvious to human reviewer. Examples include:**
  - **White text on white background**
  - **Image or text shrunk to line or point**

Trial 1.56 Data Fusion Throughput



Top Secret Intelligence Network

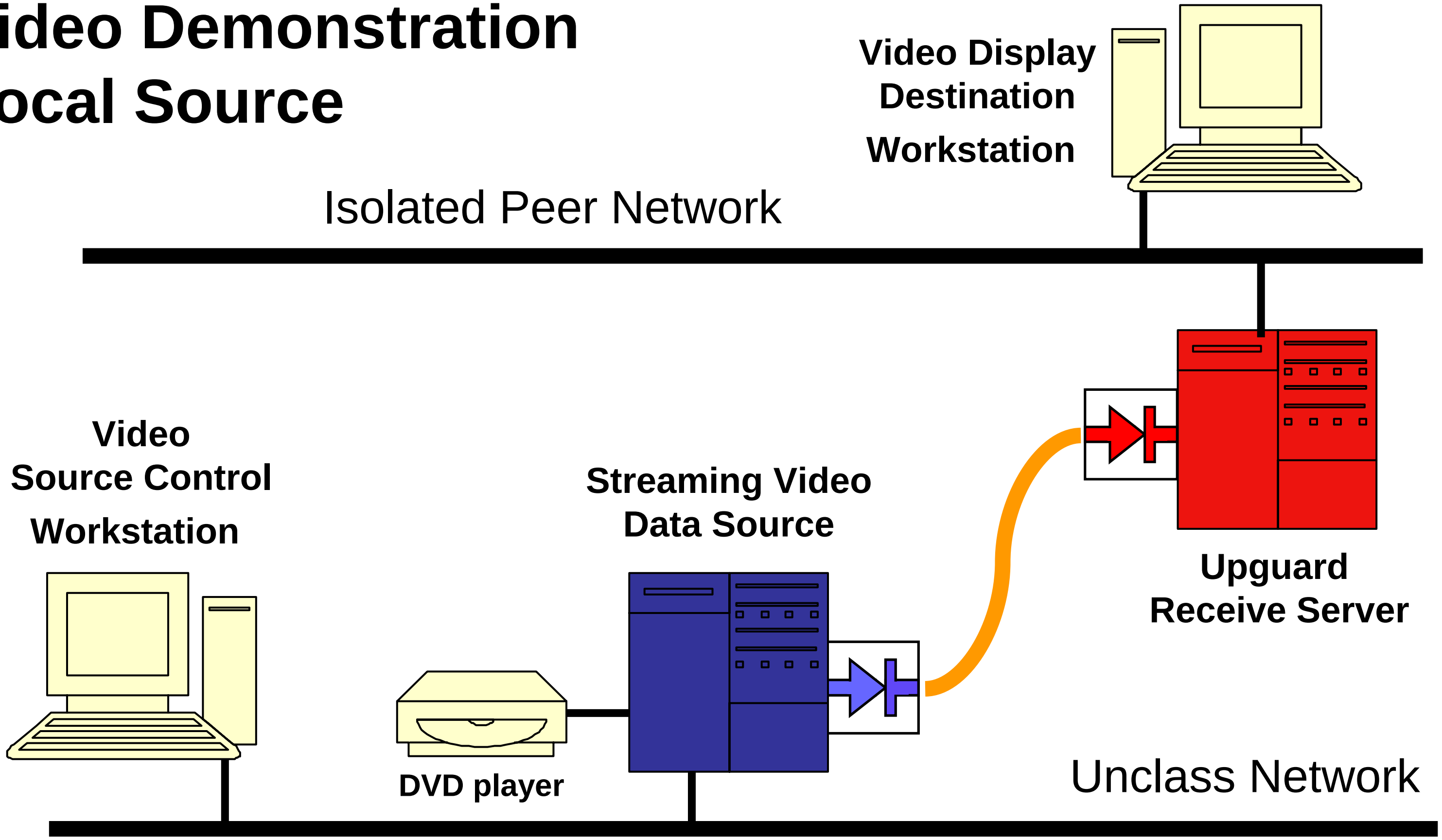
Throughput limited by
Mandatory human review

Secret Data Fusion Network

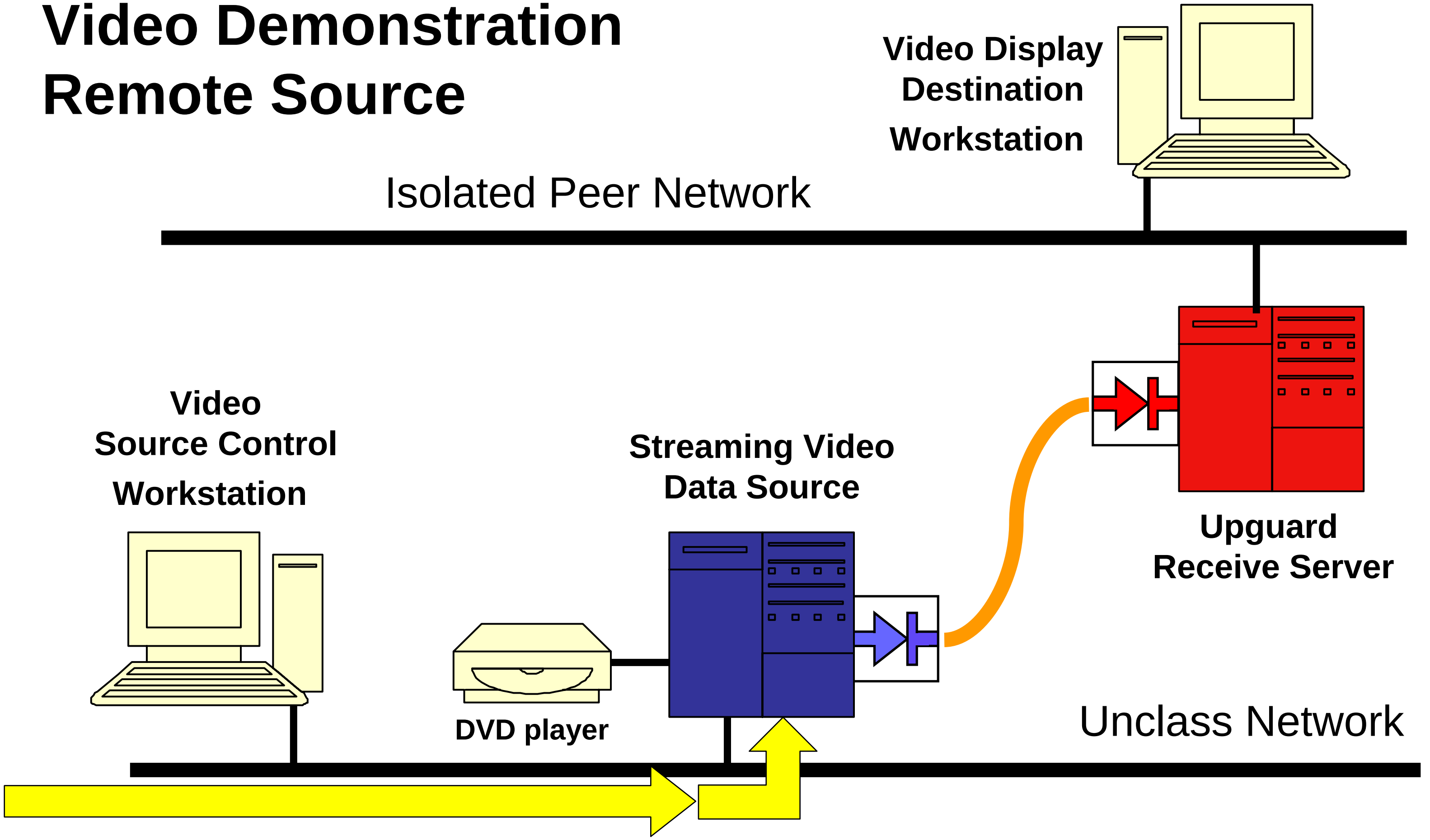
High throughput upguard,
Fully automated scanning

Unclass Public Network

Trial 1.56 Streaming Video Demonstration Local Source



Trial 1.56 Streaming Video Demonstration Remote Source



Case Study 2 Summary:

- Upguard Data Diode file xfer
  - malware scan
- Downguard Data Diode document xfer
  - deep content scan
  - multi human review
- Peer-to-peer streaming video
  - multiple concurrent streams

Case Study 3

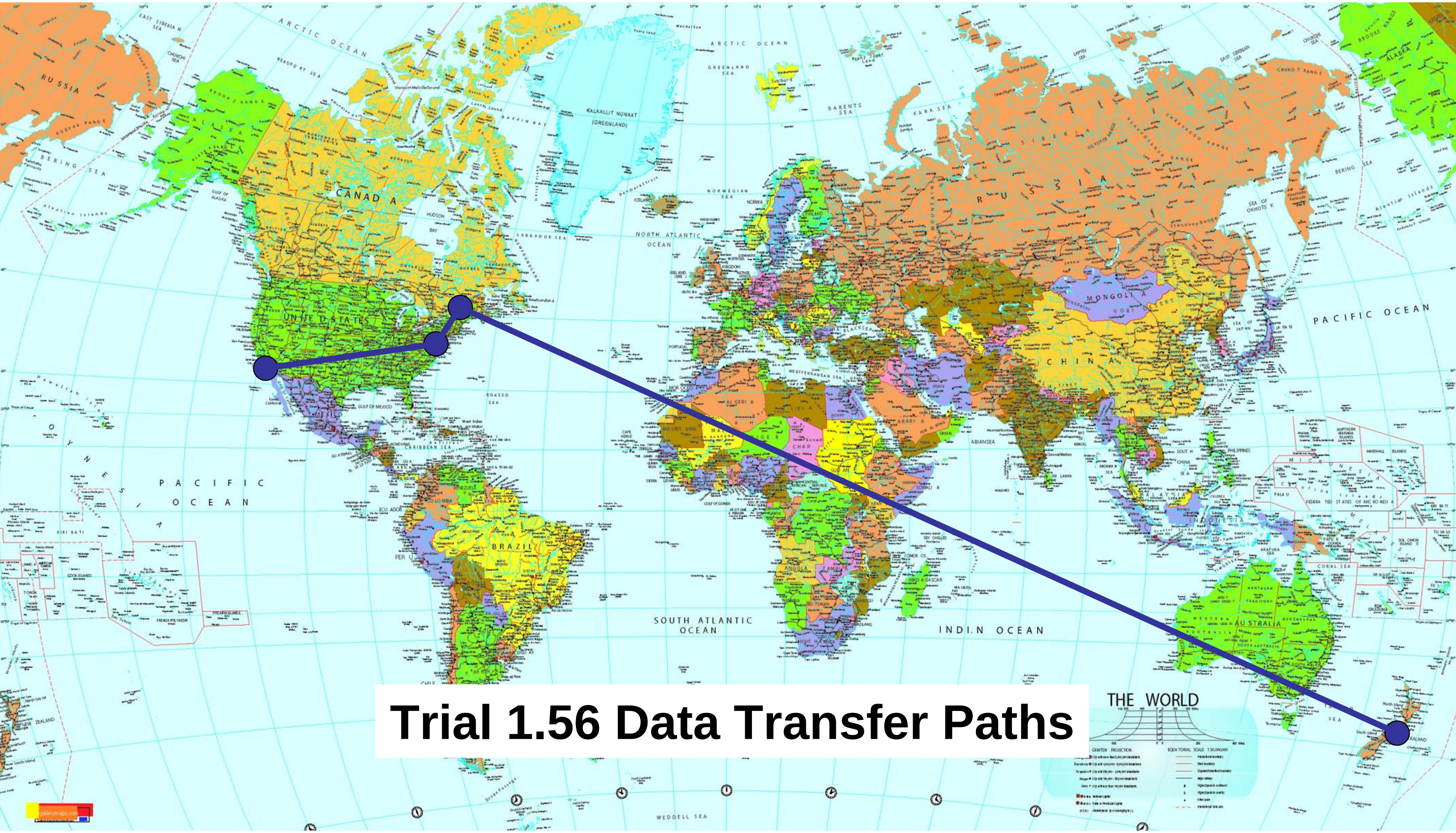
CWID Trial 1.56 includes three “virtual” trials that use Data Diode as an enterprise service:

Geolap (Shirleys Bay, Canada)
- Large GIS image files
- populated GIS directory structures

New Zealand
- Low bandwidth TCP file transfers (no FTP)

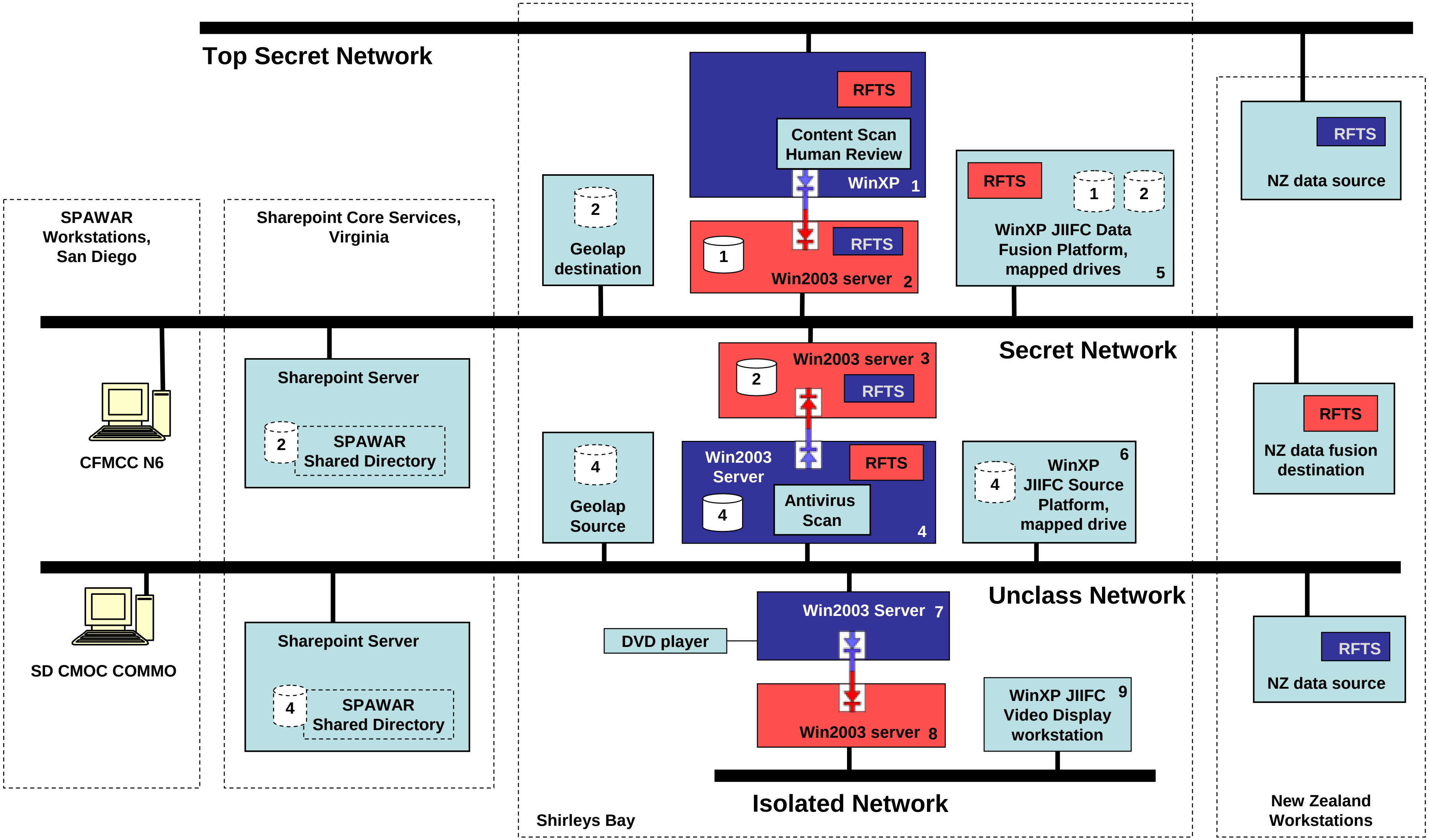
SPAWAR (US Navy, San Diego, CA)
- integration with Sharepoint web services

CWID Trial 1.56 Global Reach

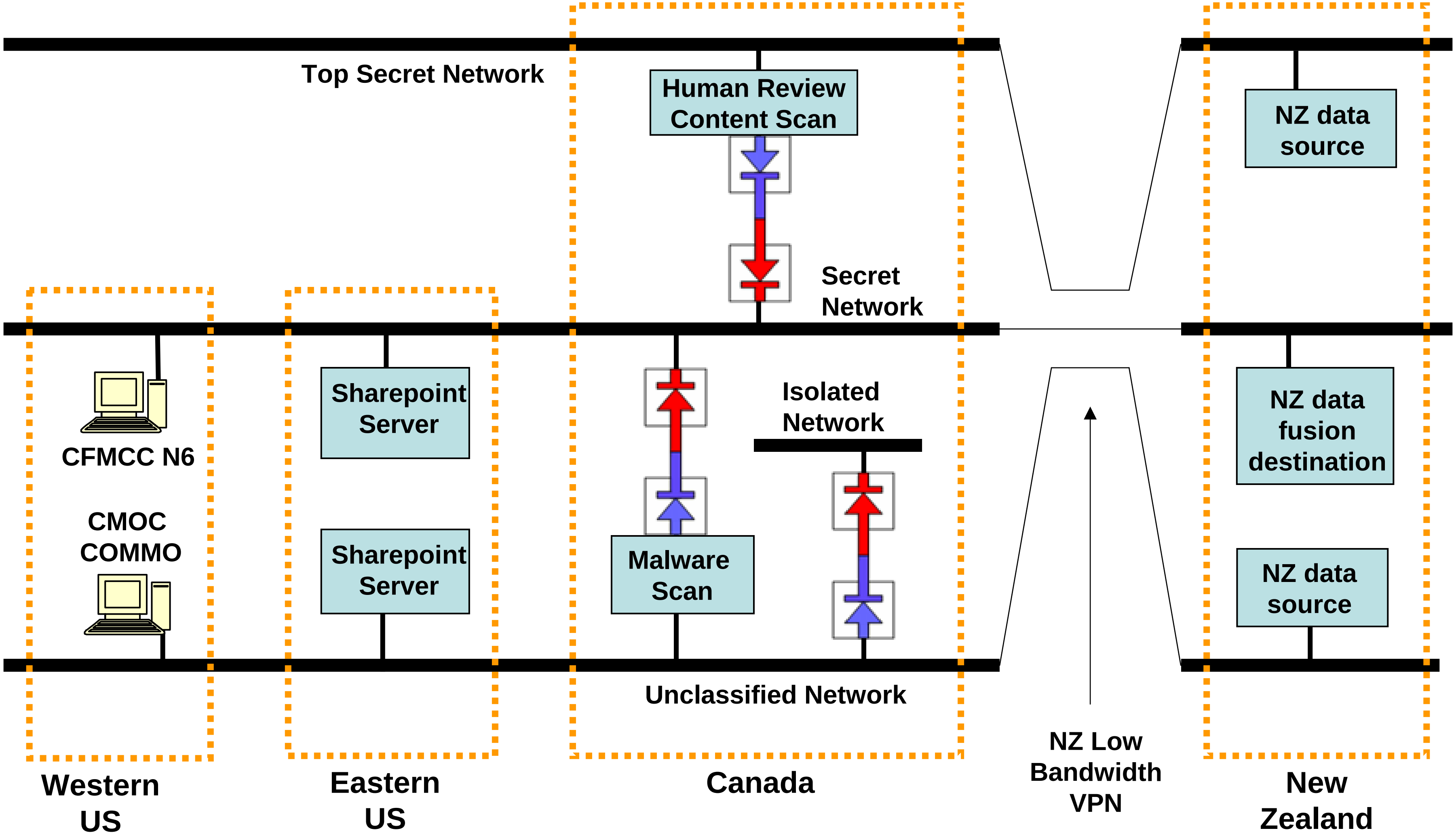


Trial 1.56 Data Transfer Paths

CWID Trial 1.56 Virtual Players, All

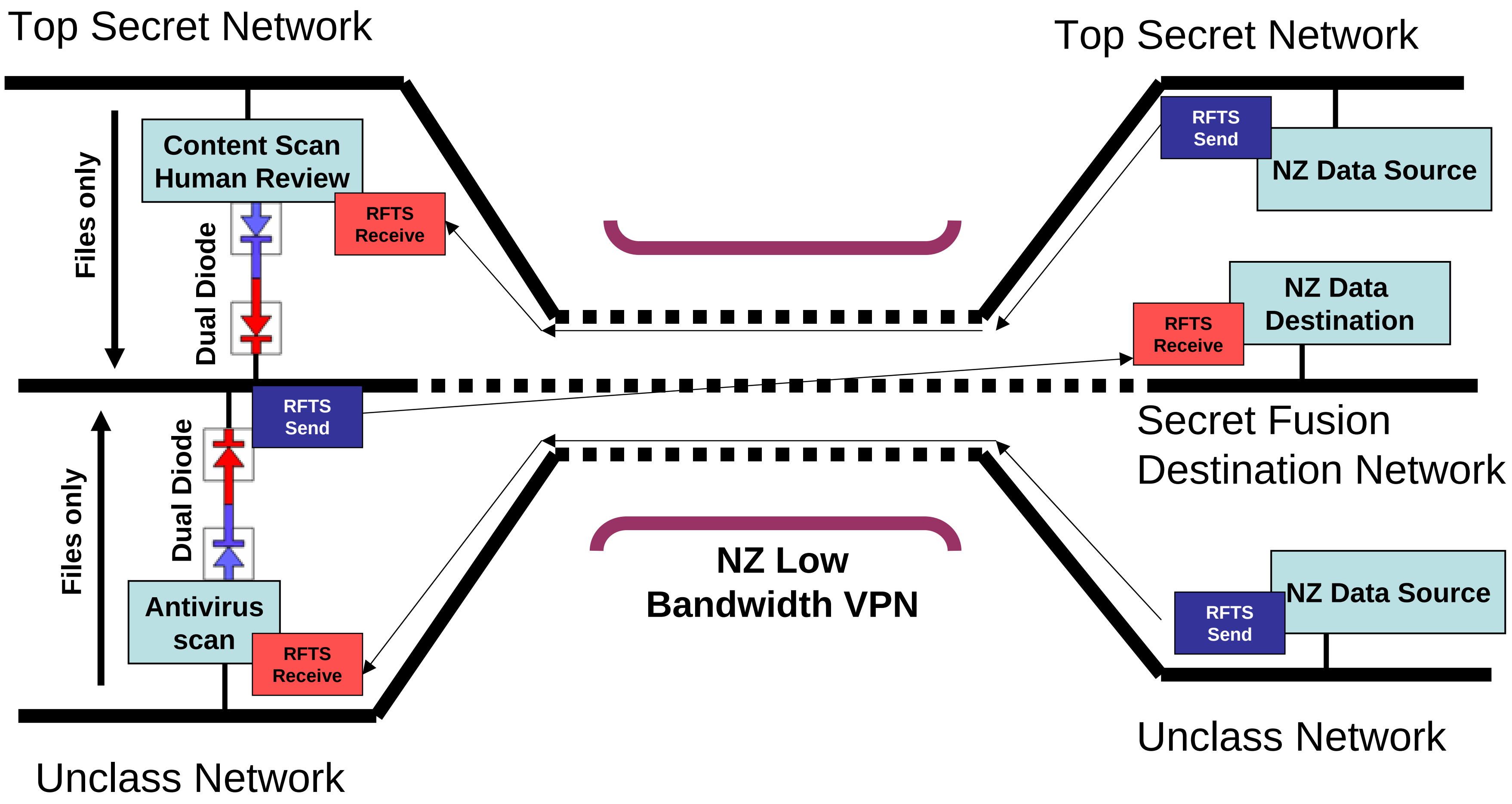


CWID Trial 1.56 Enterprise Deployment



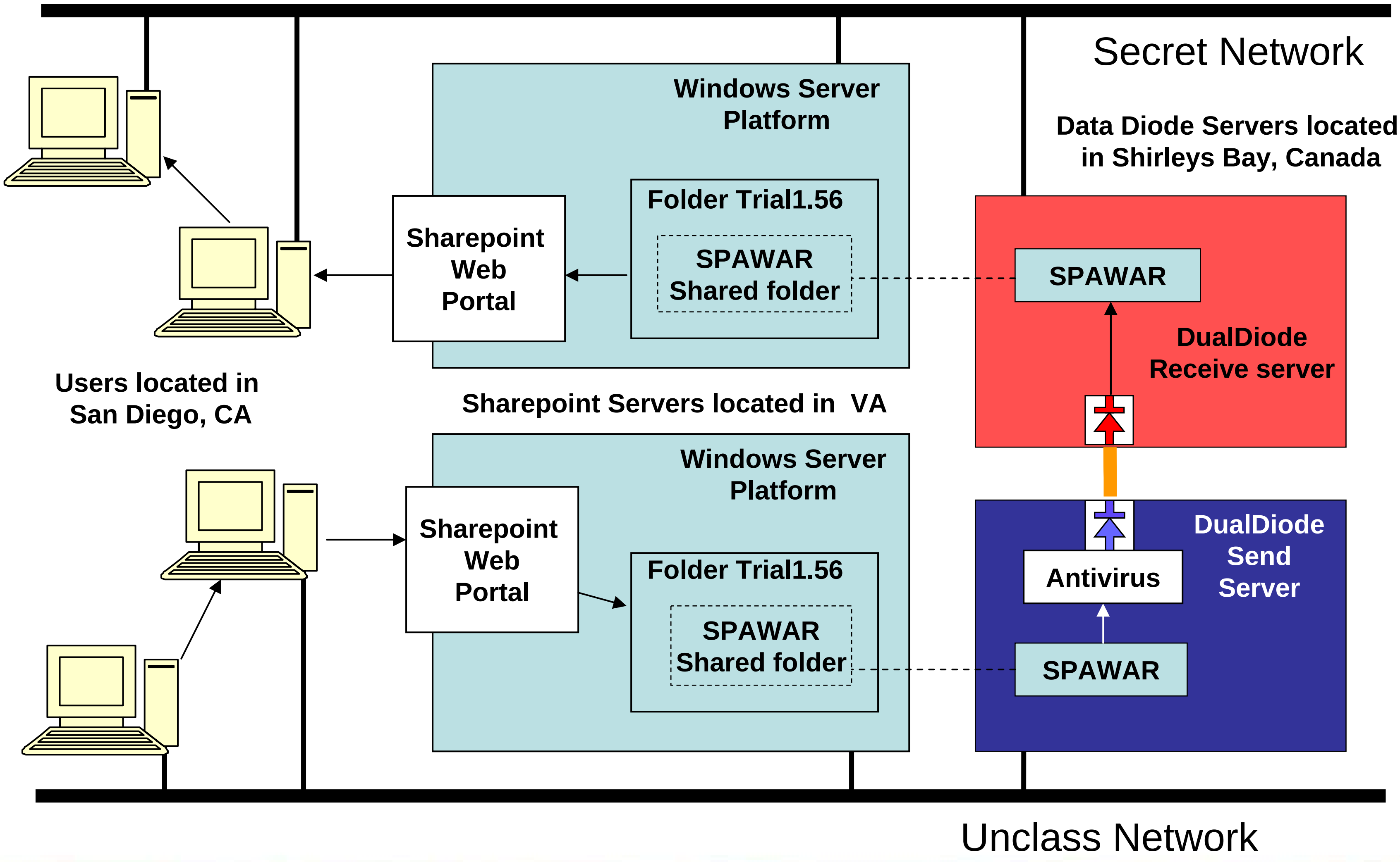
Virtual Trial 1.56 - New Zealand Detail

New Zealand Connectivity via TCP File Transfer – no FTP services



Virtual Trial 1.56, SPAWAR Detail

SPAWAR Role Player access to DualDiode via Sharepoint Web Portal



Case Study 3 Summary:

- **Enterprise Cross Domain Xfer Service**
- **Upguard file xfer**
  - **malware scan**
  - **TCP file xfer service (RFTS, no FTP)**
  - **Sharepoint web server GUI**
- **Downguard file xfer**
  - **content scan**
  - **multi human review**

CWID 2007 Results - Proven Success !

- Data Diode Cross Domain Connectivity
- Large files and directory structures
- 13 parallel MPEG video streams
- Low bandwidth VPN operation
- Sharepoint integration
- Easy to use
- 100% transfer success

Summary

Three CWID 2007 case studies were presented:

1. Trial 3.27 IIMS – Sensors, Command, Control
2. Trial 1.56 DualDiode - Data Fusion, Video Stream
3. Enterprise Scale Data Diode Deployment

Conclusions

- Data Diodes provide reliable real-time connectivity while maintaining high levels of network security.
- Data Diode capability may be scaled upward to provide Enterprise-Scale Cross Domain Solutions

SECURED BY OWL

owlcti.com

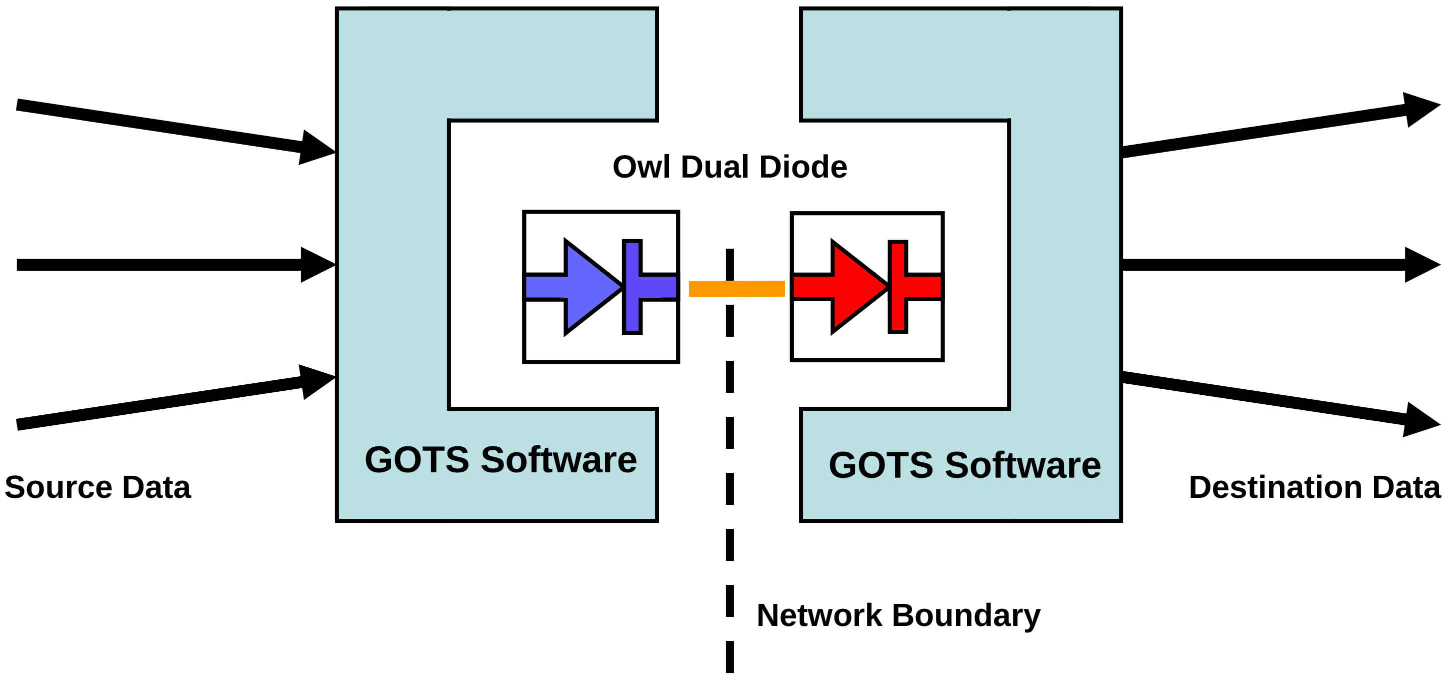
Thank You !

Any Questions ?

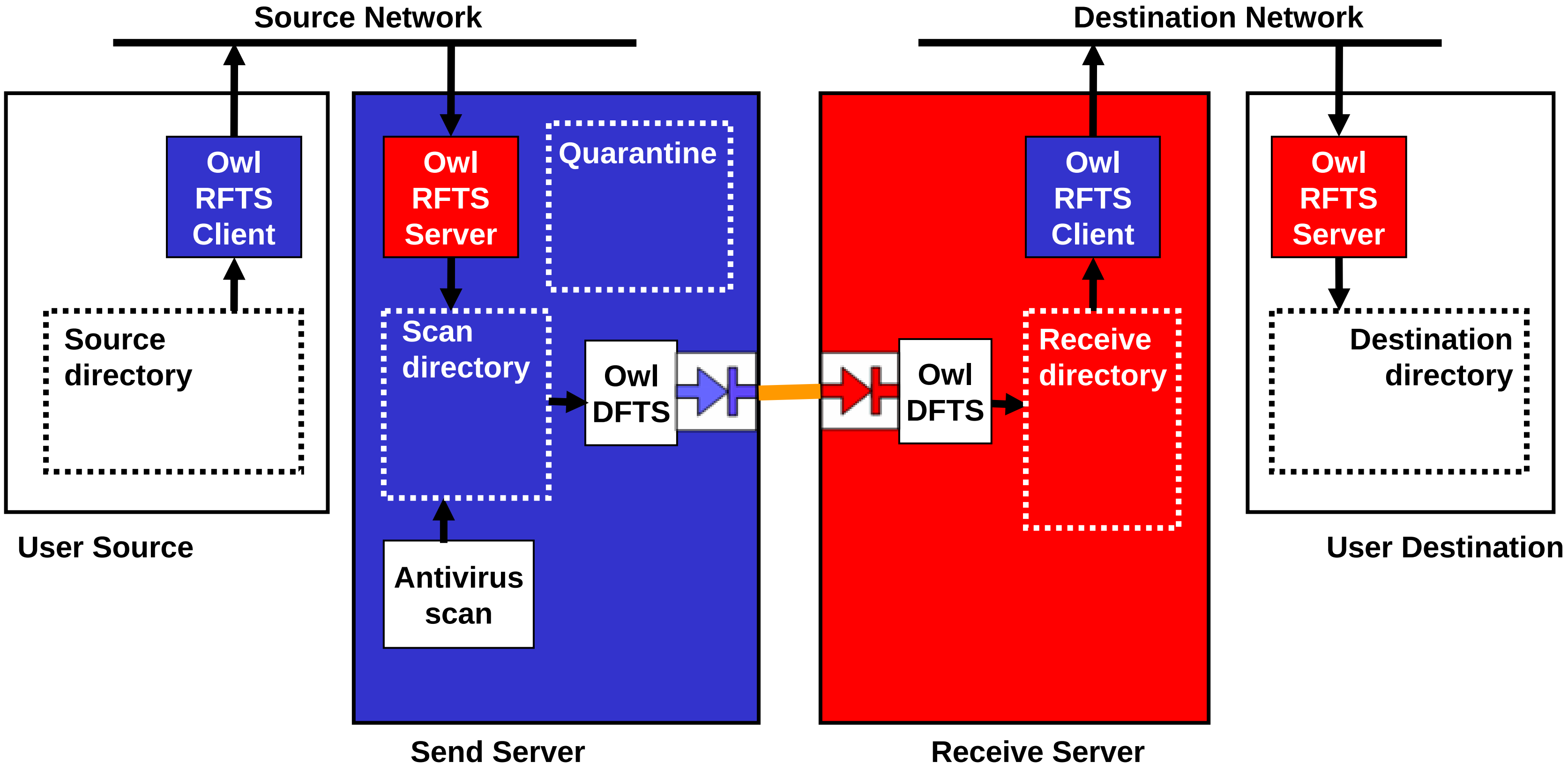
Special Notes on Cross Domain Solutions

- Unified Cross Domain Management Office (UCDMO) sets Cross-Domain security policies across DNI, DoD
- New data sharing paradigms based on Risk Management rather than data confidentiality
- UCDMO maintains a “baseline” list of approved Cross Domain Solutions
- The UCDMO baseline list includes TSABI-OWT, a Data Diode Cross Domain Solution

TSABI-OWT Product Graphic

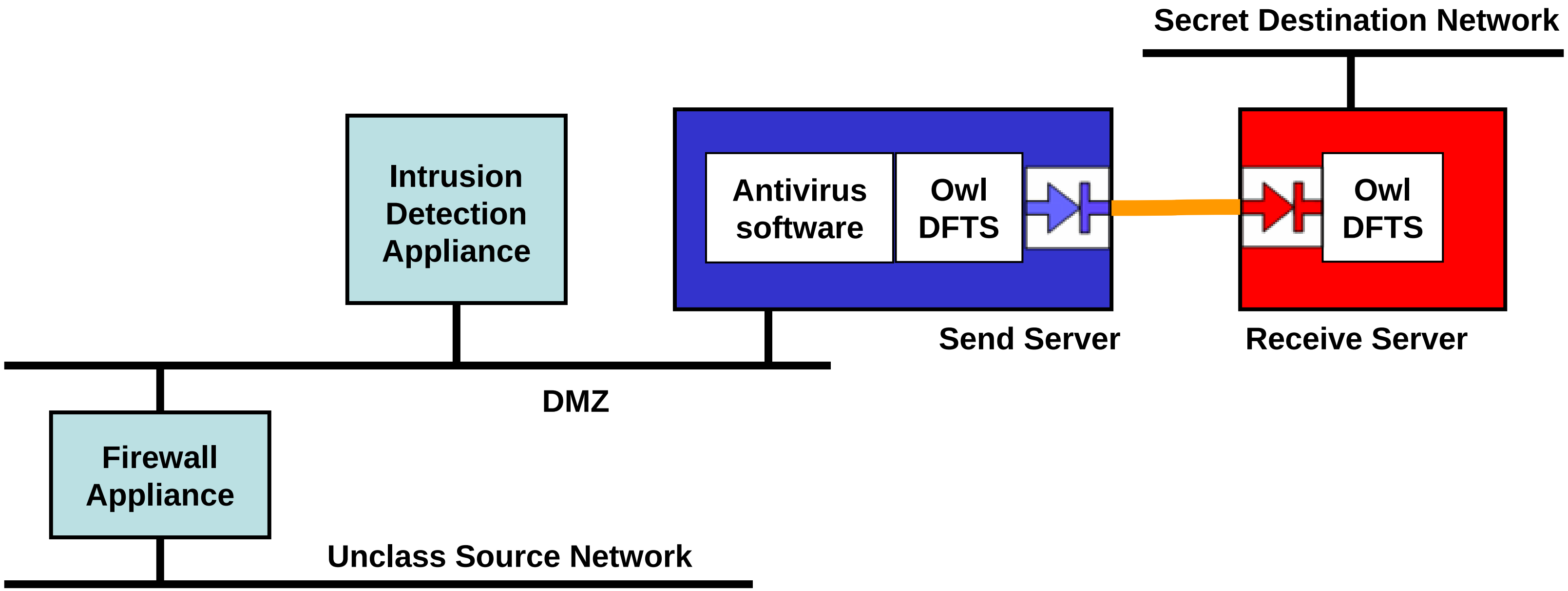


Cross-Domain Upguard File Transfer Solution



Antivirus scan is an example of a conditional forward data transfer policy in series with unconditional one-way transfer policy

Additional Security Requirements Satisfied by adding Security Appliances

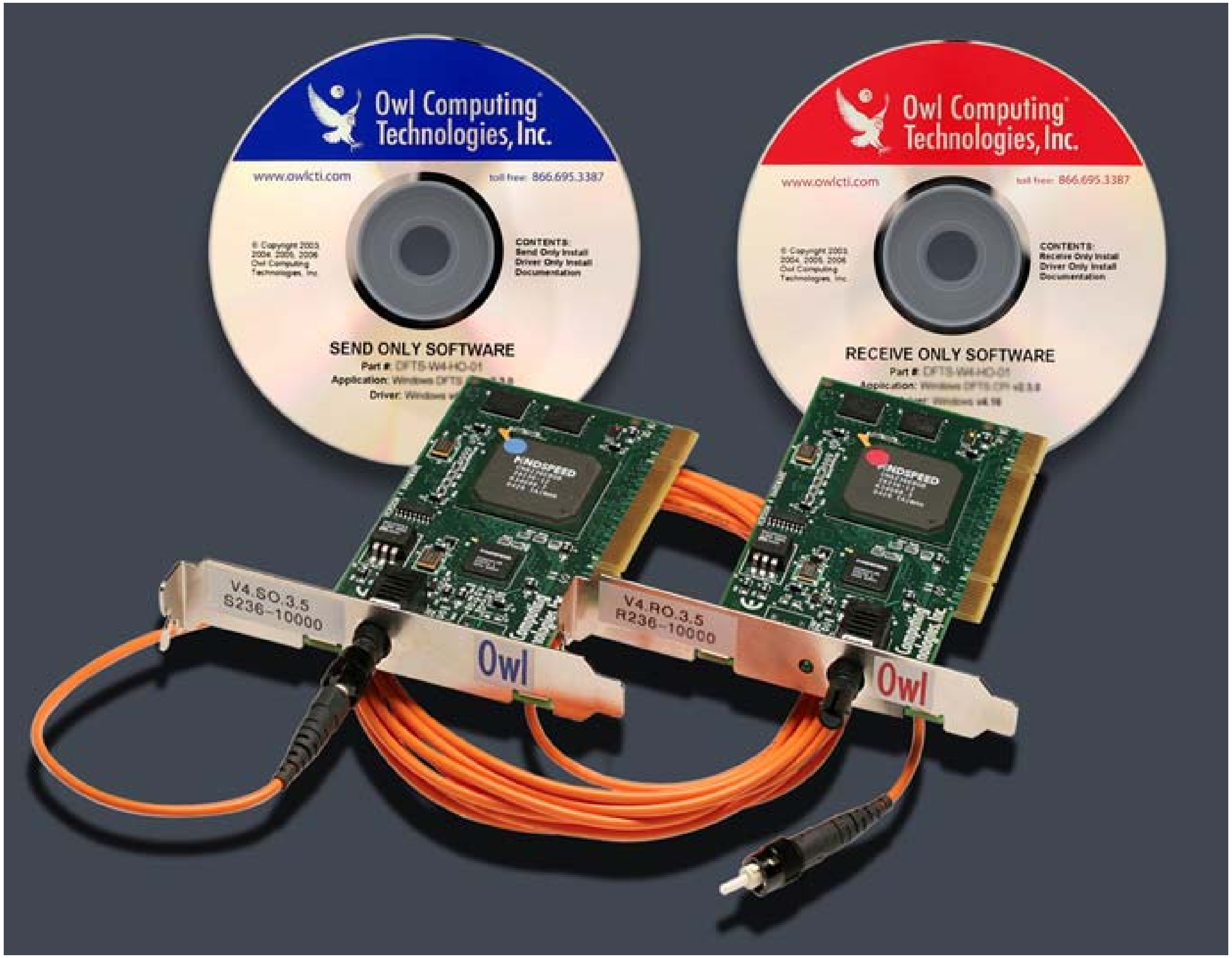


Owl Computing
Technologies, Inc.

www.owlcti.com

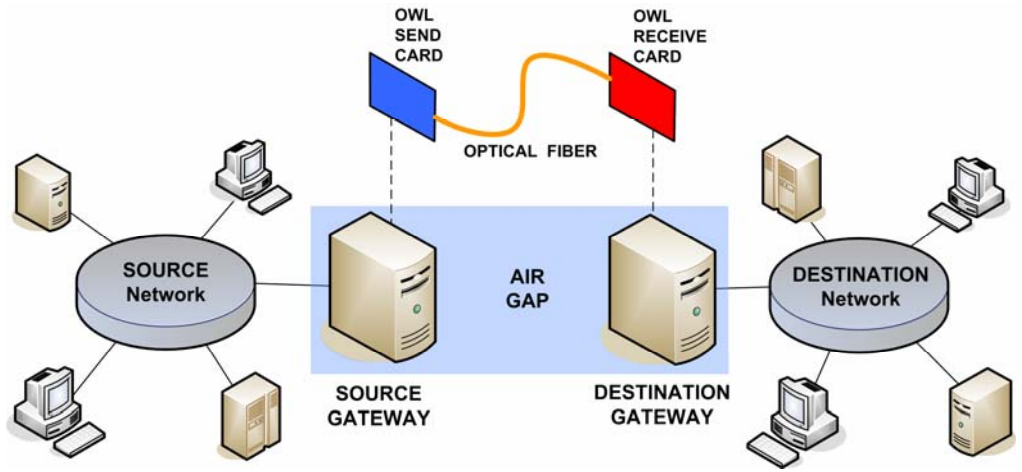
toll free 866.695.3387

DualDiode Technology

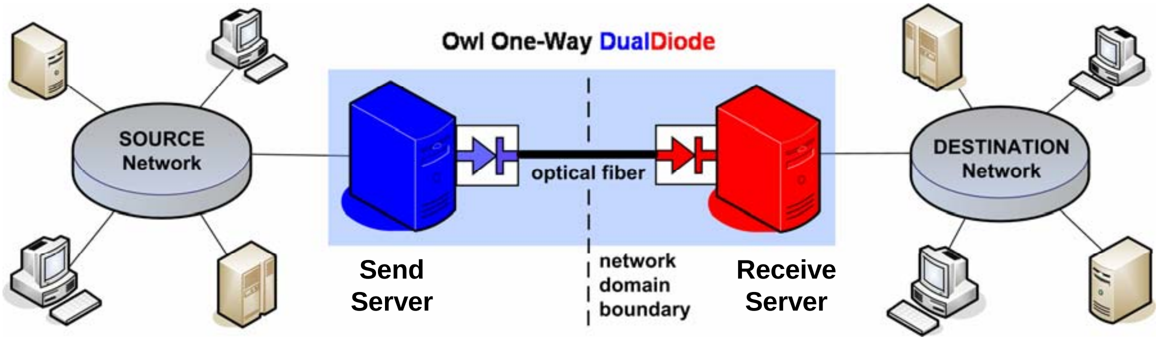

Owl Computing Technologies, Inc.
www.owlcti.com
toll free: 866.695.3387
CONTENTS: Send Only Install Driver Only Install Documentation
SEND ONLY SOFTWARE
RECEIVE ONLY SOFTWARE
CONTENTS: Receive Only Install Driver Only Install Documentation
V4.SO.3.5
S236-10000
V4.RO.3.5
R236-10000
Owl

Send Only & Receive Only NIC pair, 155 Mbps

DualDiode System Installation



Send and Receive Owl Cards installed in host computer platforms…



…Create Send and Receive gateways for their respective networks.