Physical Cybersecurity: Using One-Way Data Diodes to Secure Asset Monitoring

Colin Dunn
Fend Incorporated

Tapan Patel
USACE ERDC-CERL

Agenda

- Data Diodes: Technology and Use Cases
- ESTCP Project Overview
- Questions and Answers

Agenda

- **Data Diodes: Technology and Use Cases**
- ESTCP Project Overview
- Questions and Answers


Critical infrastructure managers need real-time operational intelligence.
But ransomware and other cyber risks threaten the digital transformation of industrial management.

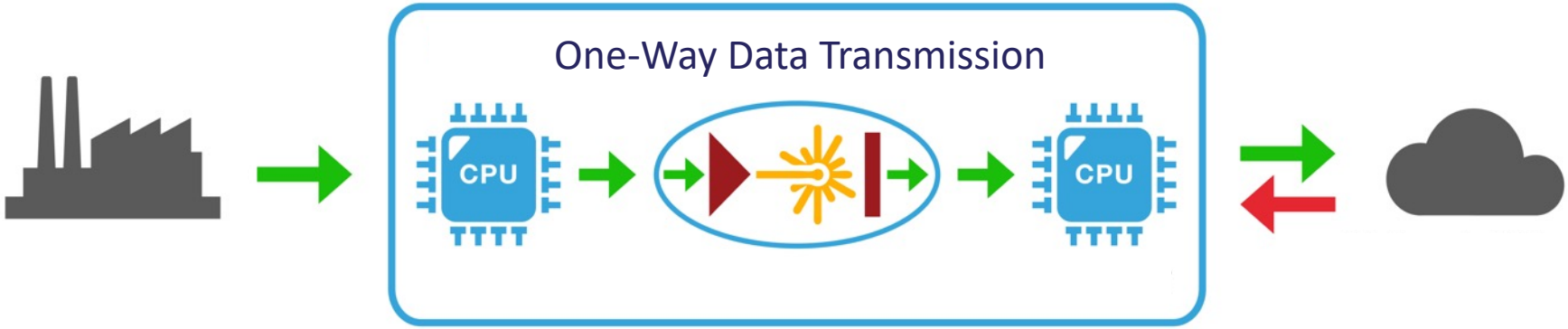
Data diodes get intelligence into your hands while physically blocking all outside cyberattacks.

Recommended Practice for Critical Infrastructure

On September 21st, the Cybersecurity & Infrastructure Security Agency (CISA) recommended the use of one-way communication diodes to:

- Protect control system boundaries
- Limit and control the flow of data between systems

DATA GOES OUT



NOTHING GETS IN

Operator Benefits

Improve Efficiency

Reduce Interruption

Increase Productivity

Protects Against Attackers

Steal Data

Inject Ransomware

Modify or Destroy Equipment

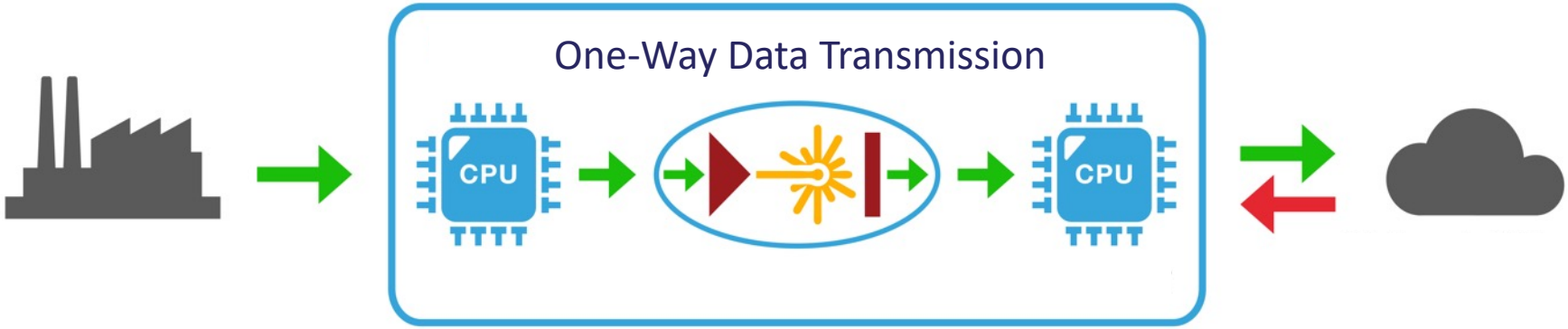
Firewalls

Software

Don’t Trust Software.

Trust Physics.

DATA GOES OUT



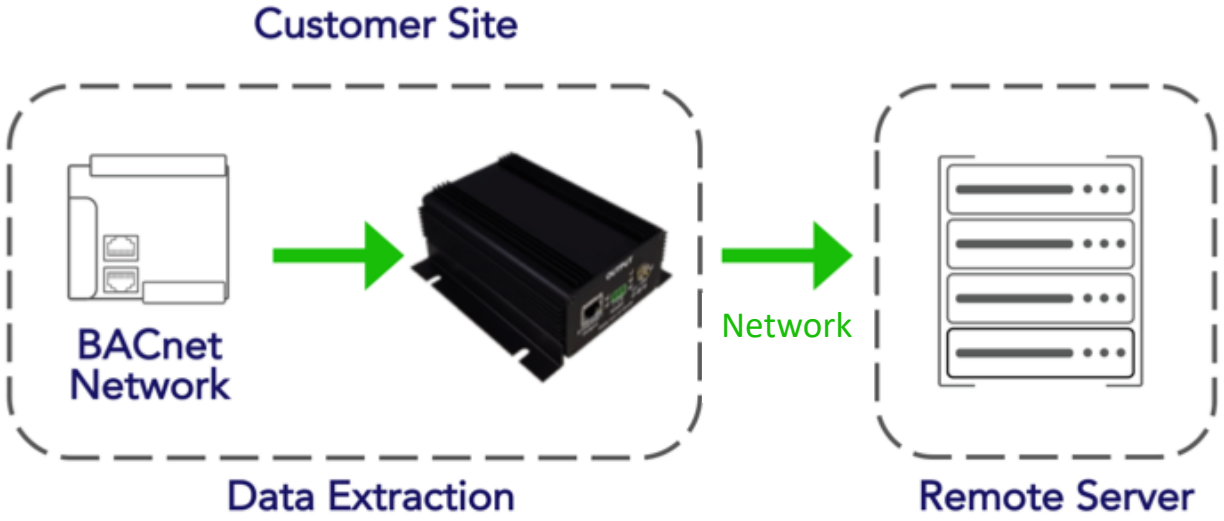
NOTHING GETS IN

Military
Transportation
Commercial Buildings

Data diodes have widespread IT and industrial uses.

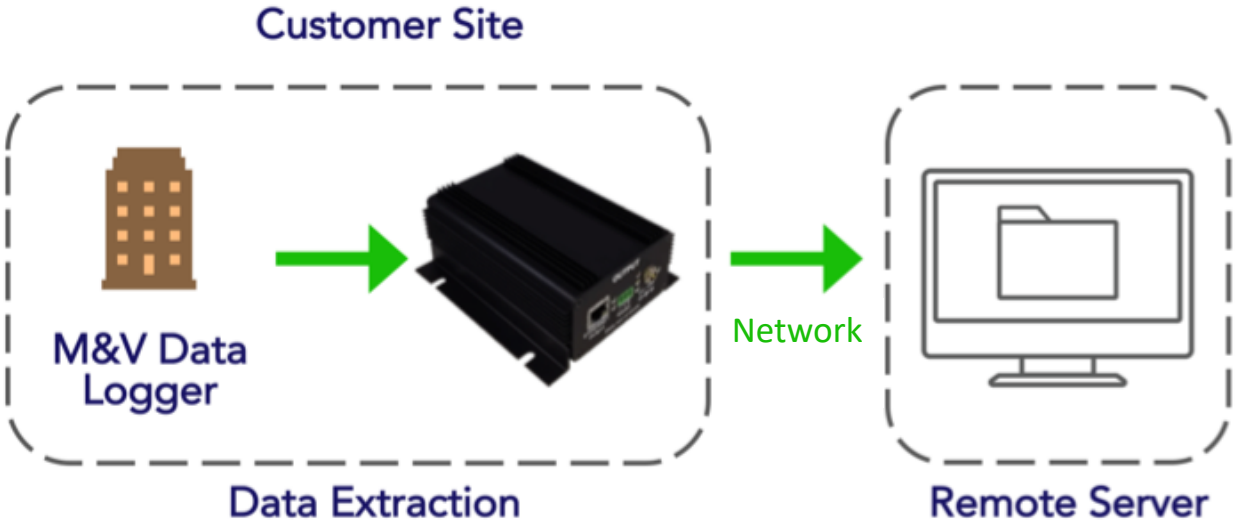
Utilities
Manufacturing

Example: Remote Monitoring



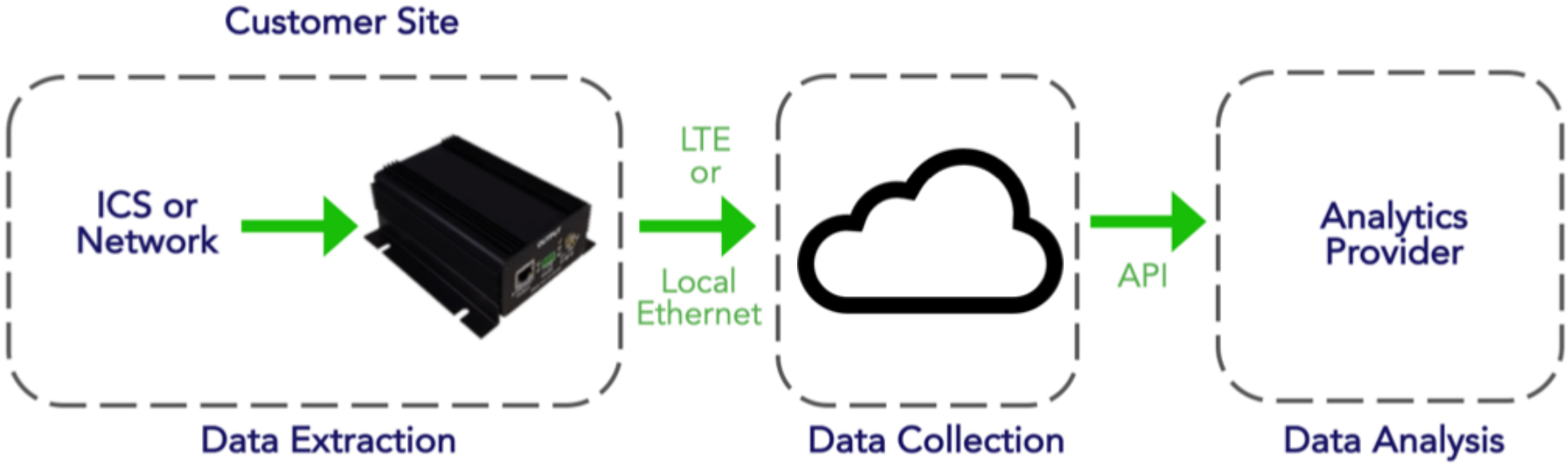
Stream industrial data

Example: Energy Savings Performance Contracts

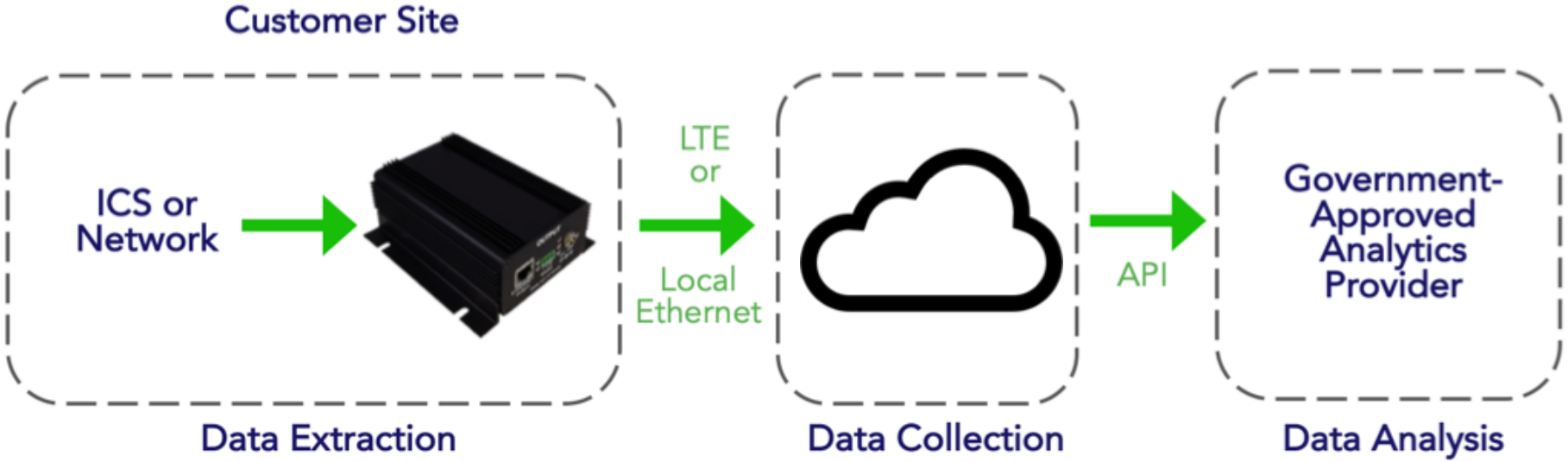


One-way file transfer

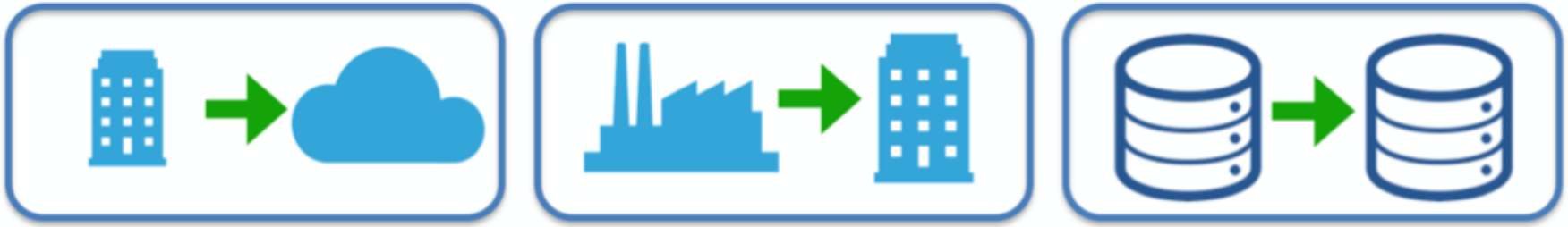
Example: Cloud-Based Analytics



Example: Government Applications



Data Diode Uses



Remote Monitoring

OT-IT Data Historian

Secure Database
Replication / Backup

Agenda

- Data Diodes: Technology and Use Cases
- **ESTCP Project Overview**
- Questions and Answers

Environmental Security Technology Certification Program (ESTCP)

- ESTCP Project EW19-5156 evaluated the use of next-generation, low-cost data diodes for secure data extraction from facility related control systems (FRCS)
- Awarded **"Project of the Year"** in the Installation Energy and Water category
- Key performers:

FEND®

ERDC
ENGINEER RESEARCH & DEVELOPMENT CENTER

CERL
CONSTRUCTION ENGINEERING RESEARCH LABORATORY

SERDP
DOD • EPA • DOE

ESTCP

Projects of the Year
2021

Test Design and Objectives

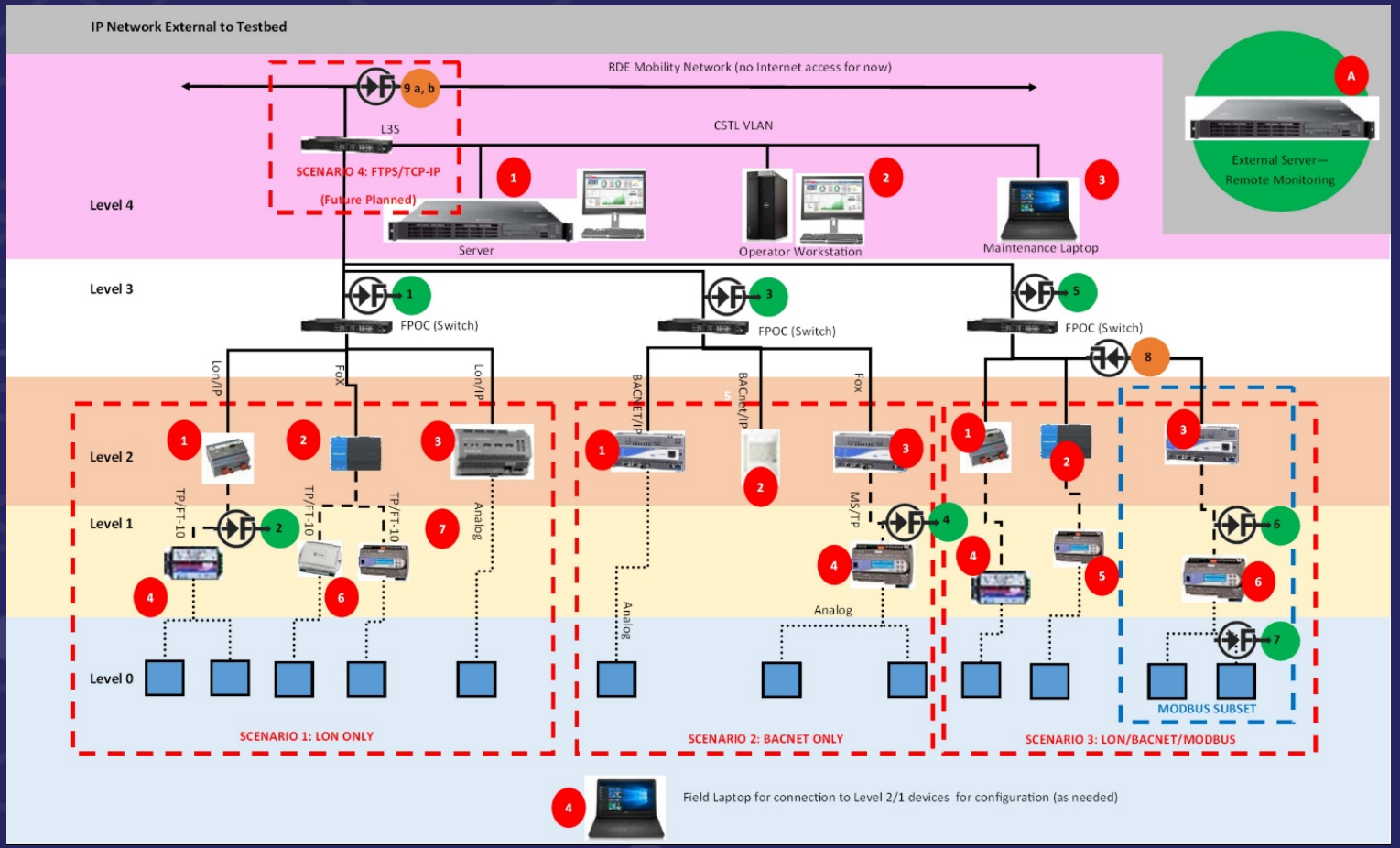
Objective	Test Method
Demonstrate that low cost data diodes provide physical isolation	Penetration tests by Army TSMO and NAVFAC CSTB teams
Show broad applicability across a variety of common DoD system types	Compatibility tests at CERL to transport data using common protocols (BACnet, Lon, Modbus, FTP)
Evaluate long-term device performance	Installation at operational buildings at CERL

Penetration Tests: TSMO and CSTB

Results: performed as expected

Compatibility Tests

<u>Results</u>
Transmits:
-Modbus
-BACnet
-LonTalk
-FTP



Long Term Tests

Results:

- Passed additional security tests
- Operated continuously
- Successfully transmitted FRCS data

Benefits to DoD Stakeholders

- Increased access to building performance data
- Compliance with cybersecurity requirements
- Integration of data from multiple disparate sources
- Improved operational efficiency: energy and manpower

Agenda

- Data Diodes: Technology and Use Cases
- ESTCP Project Overview
- **Questions and Answers**


Data diodes provide
physical cybersecurity.

Thank You

Colin Dunn
Fend Incorporated
571-970-1382
cdunn@fend.tech

Tapan Patel
USACE ERDC-CERL
217-373-3457
Tapan.C.Patel@usace.army.mil