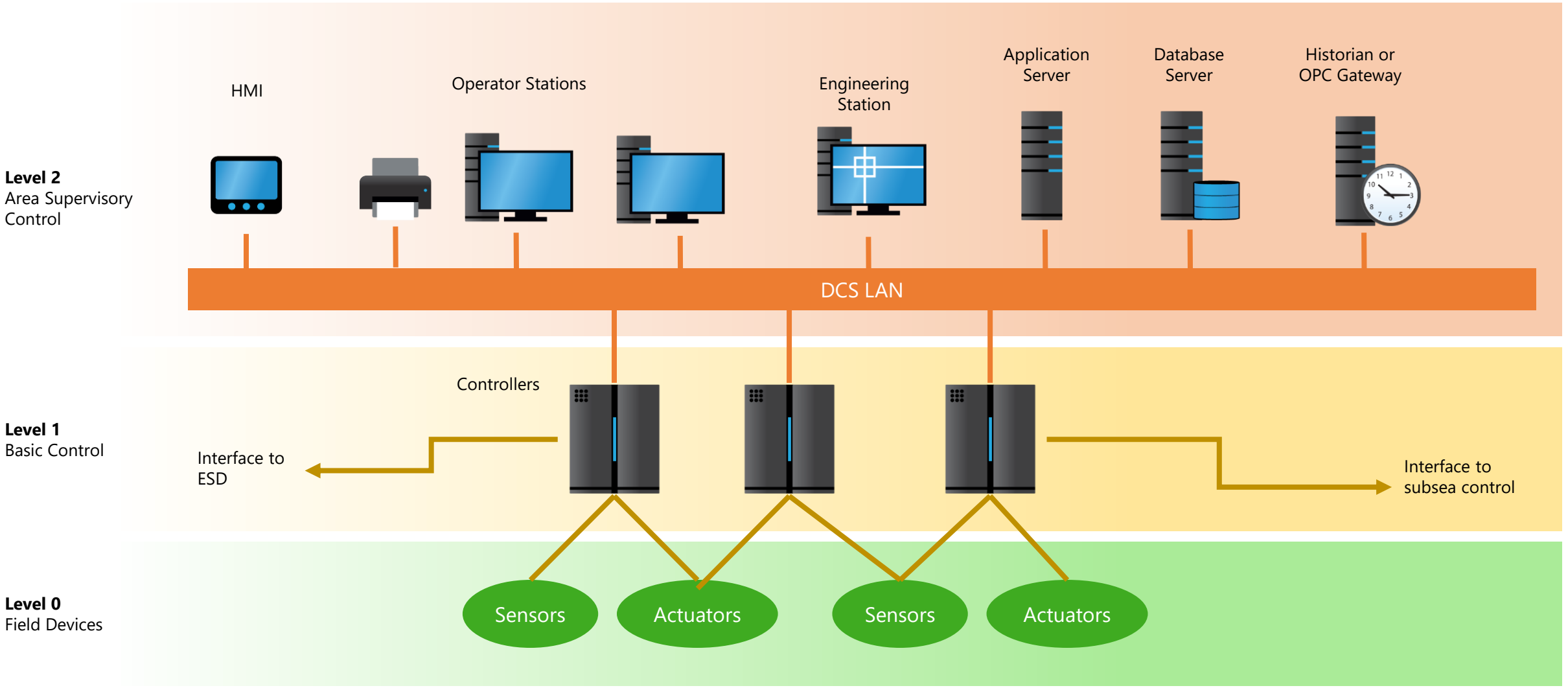
prosource.it
High Performance IT Solutions

# Creating a system of systems which securely enables digitalisation

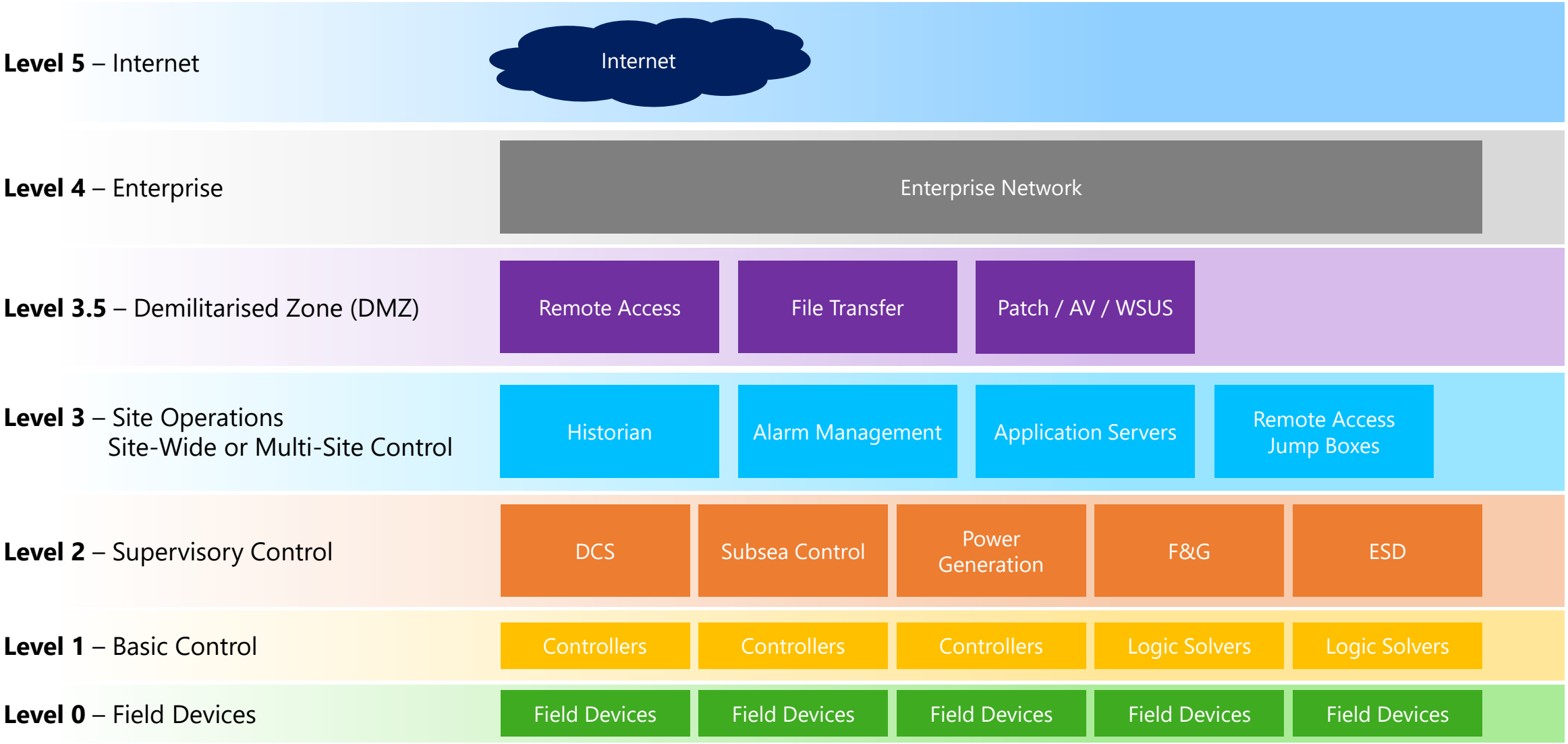
Rob Rothwell, OT Cybersecurity SME

# Assumptions and Definitions

# Purdue Model



# Purdue Model



# Securely building a system of systems

## A reference architecture for brownfield installations

# Why is a secure architecture important?

Standard way to access data from OT systems

Keep OT systems secure and safe

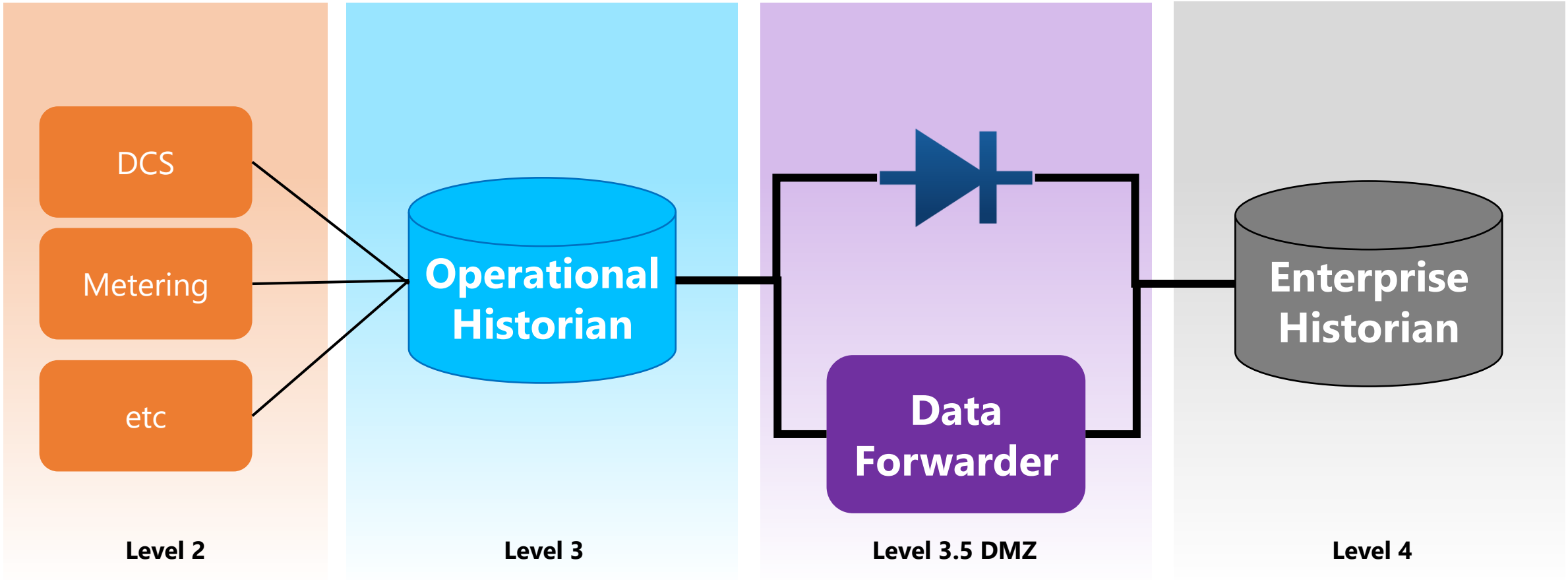
Vendors will offer a variety of options – good, bad and ugly

It is **your** data. Don't just give it away to vendors!

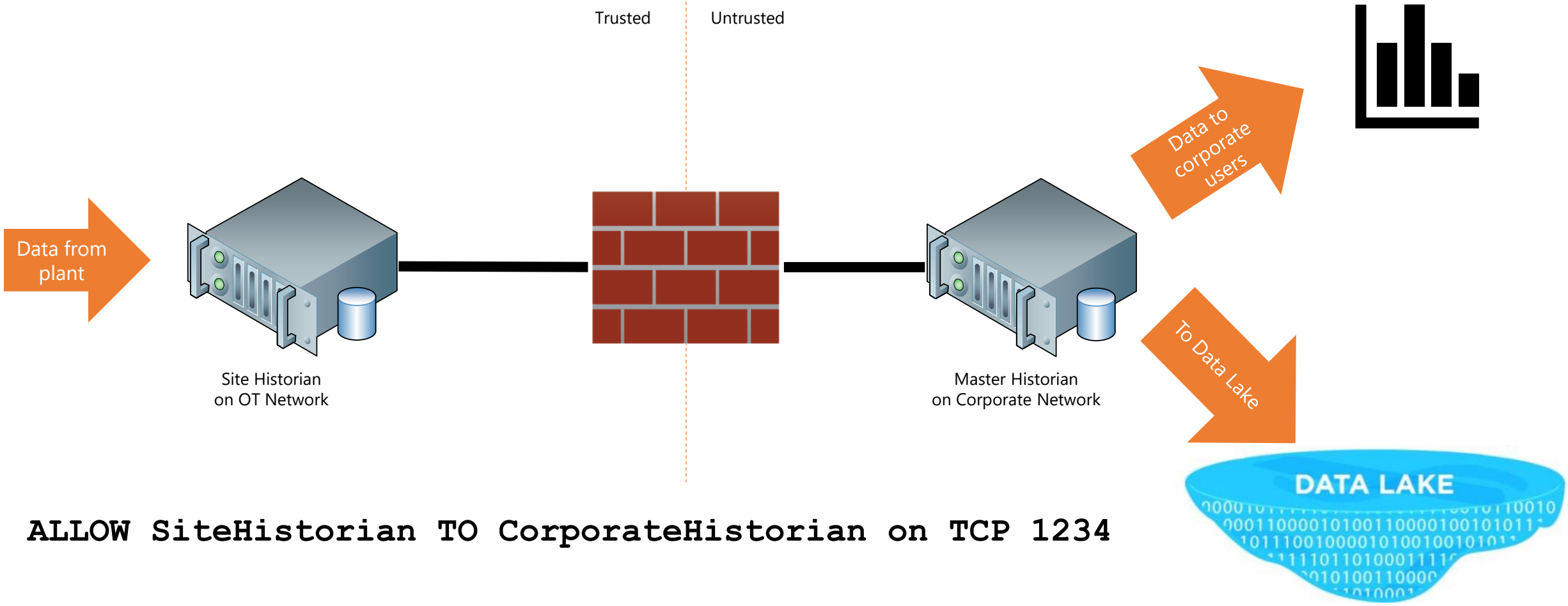

Historian
DCS
Metering
etc


MY OTHER COMPUTER IS YOUR DATABASE !

# Historian Architecture

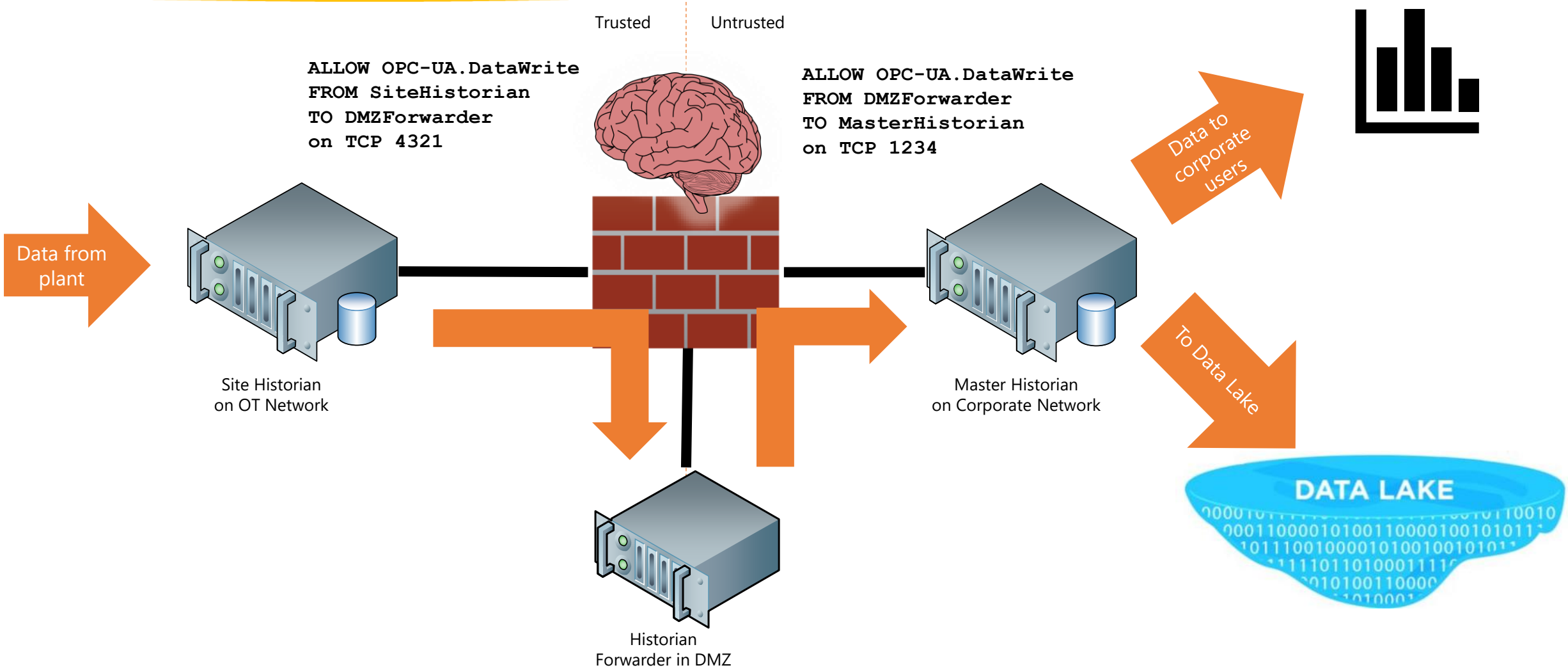


# Standard Firewall

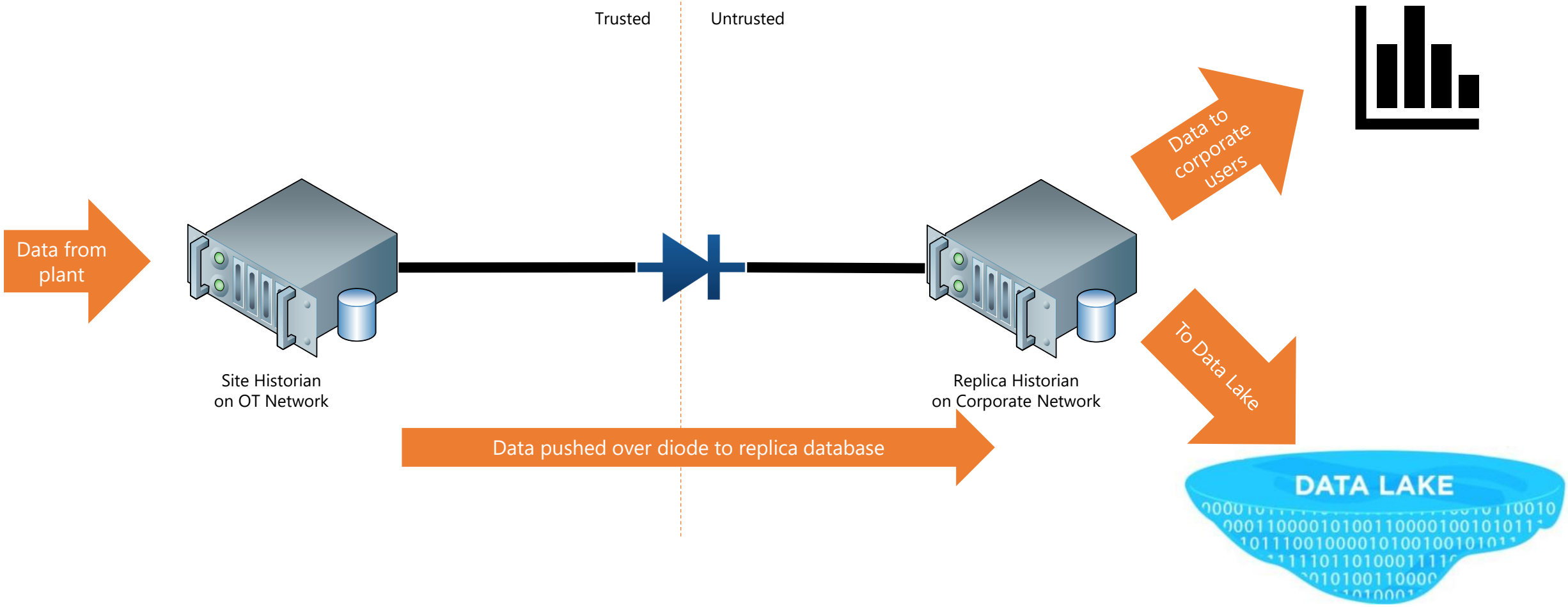



**ALLOW SiteHistorian TO CorporateHistorian on TCP 1234**

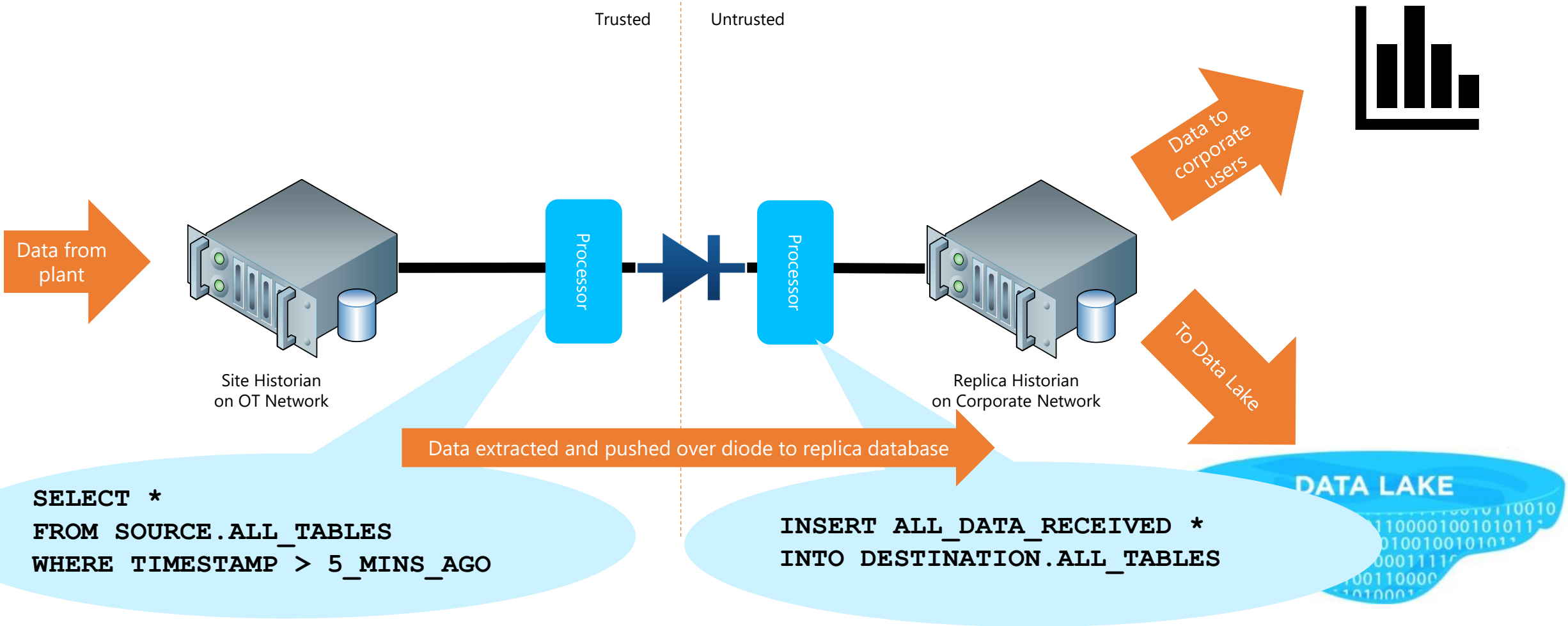
# Next Generation Firewall (NGFW) with DMZ



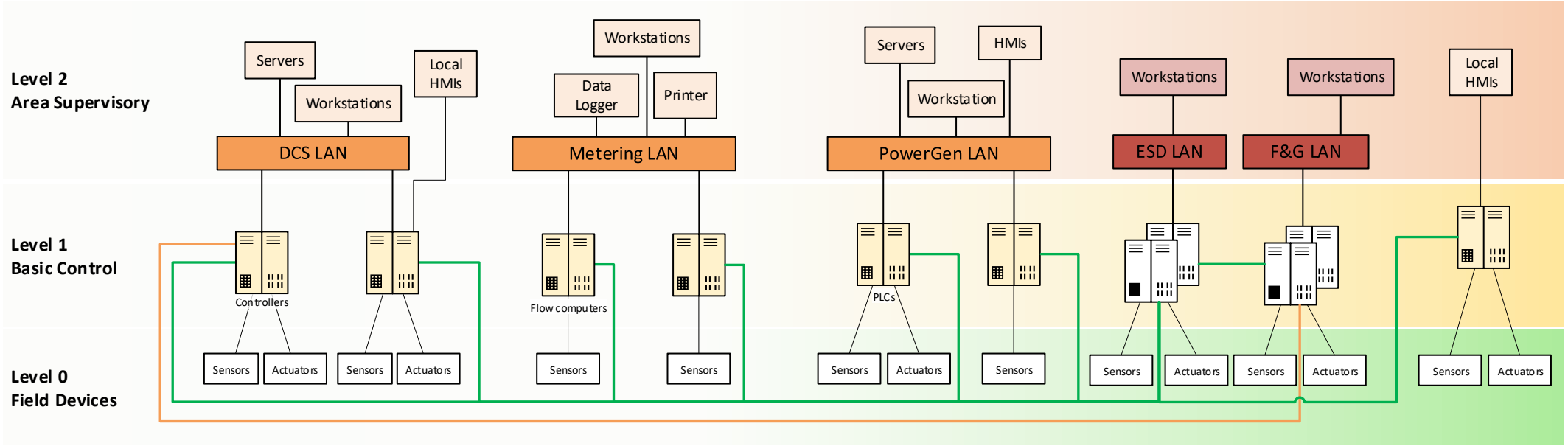
# Data Diode


Trusted
Untrusted
Data from plant
Site Historian on OT Network
Replica Historian on Corporate Network
Data to corporate users
To Data Lake
Data pushed over diode to replica database
DATA LAKE

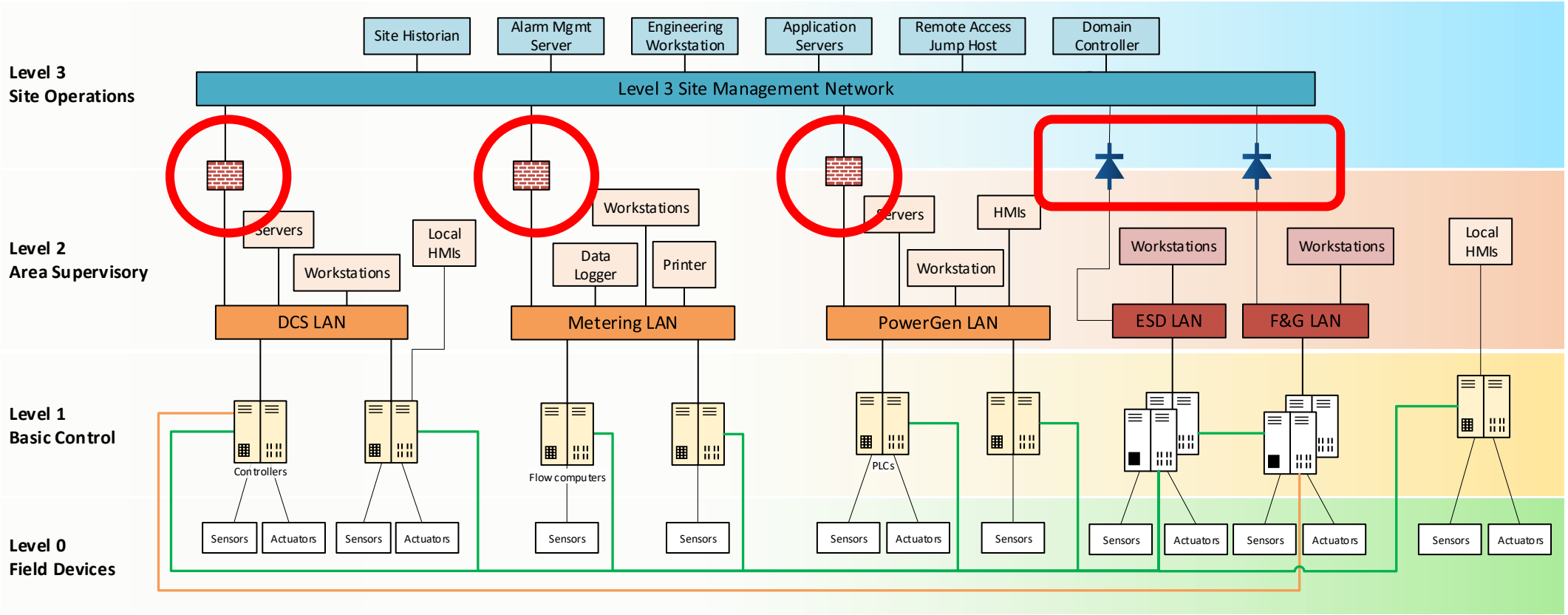
# Unidirectional Security Gateway



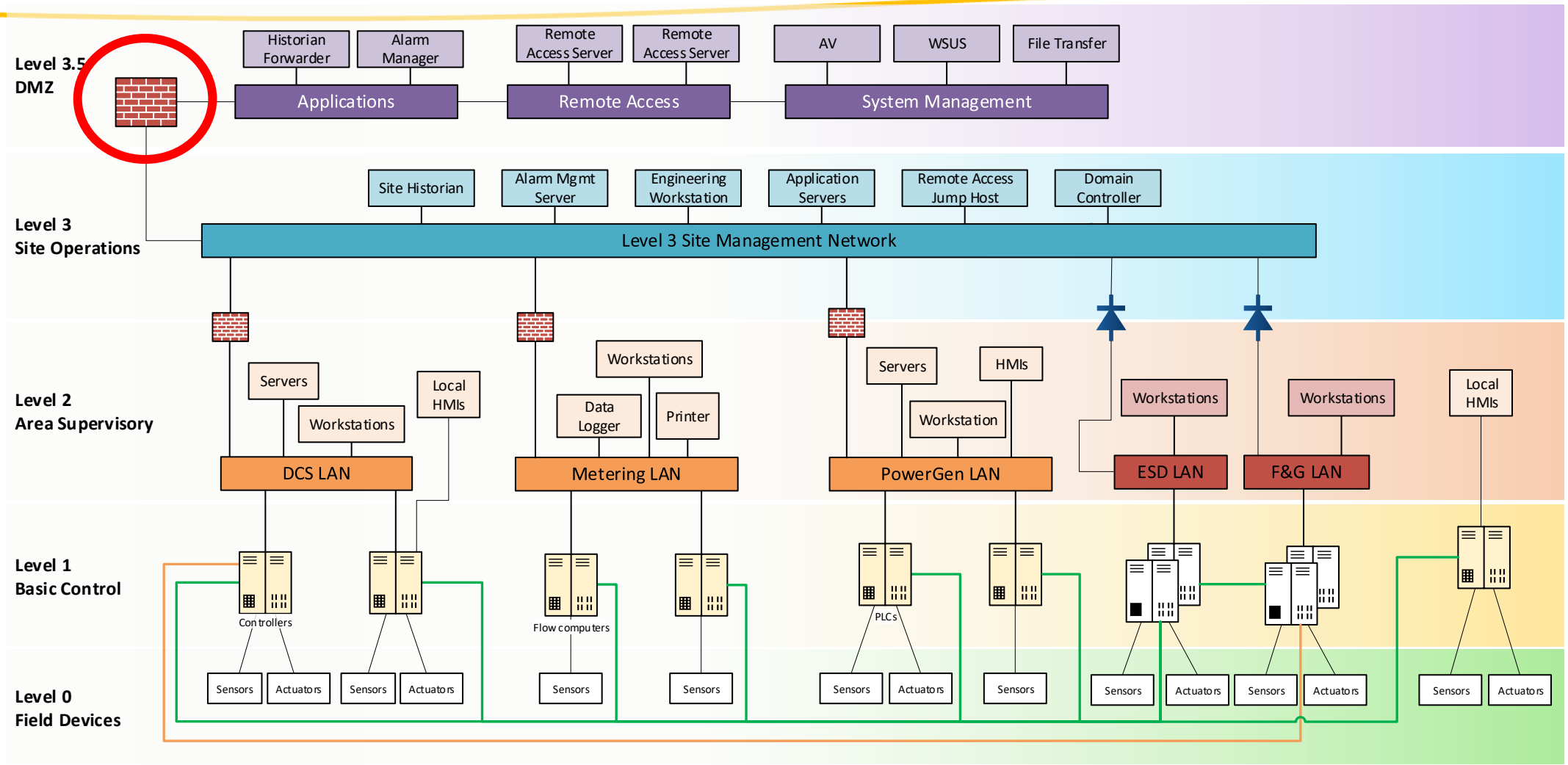
# Site Level Architecture

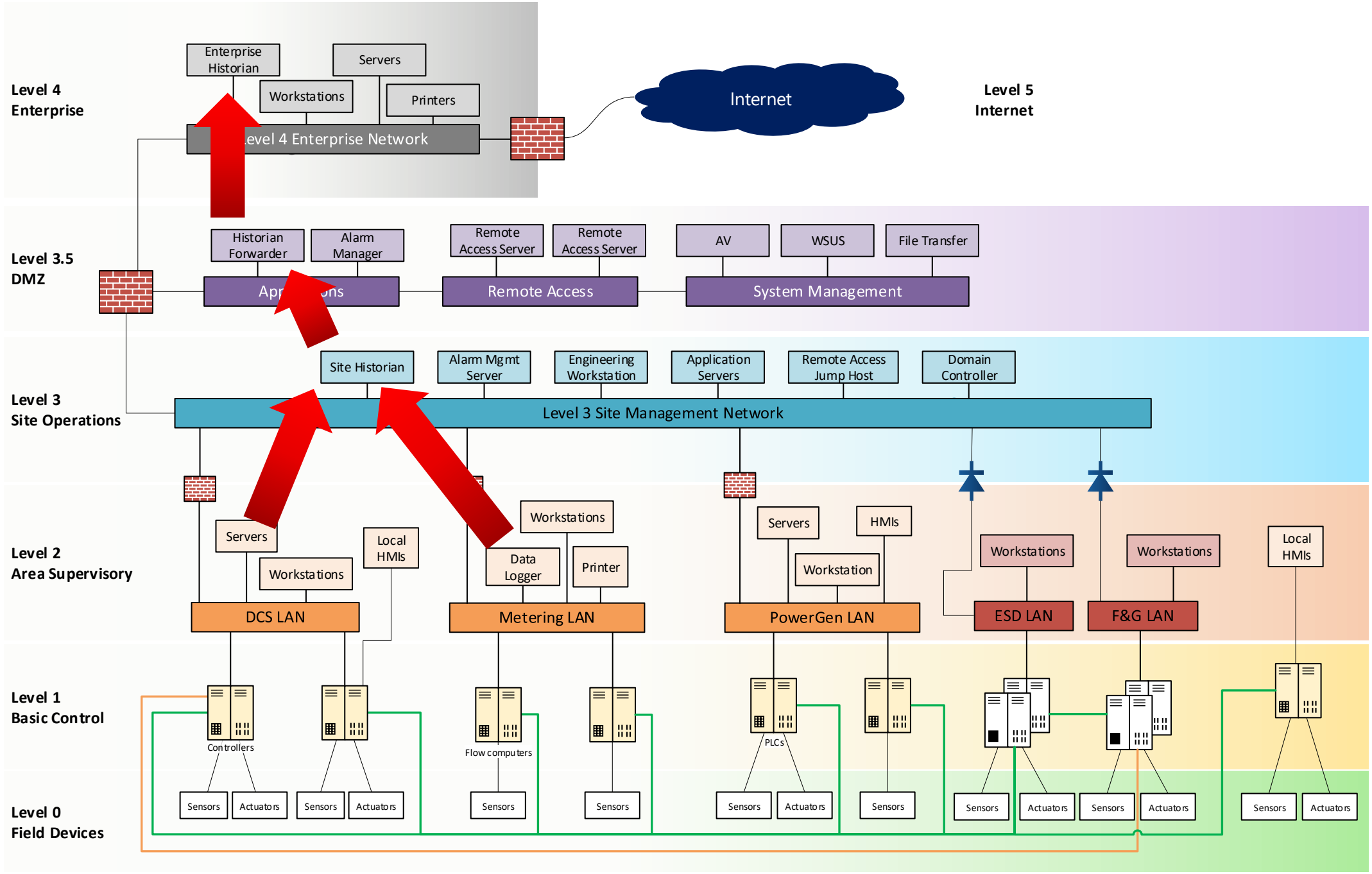


# Site Level Architecture



# Site Level Architecture

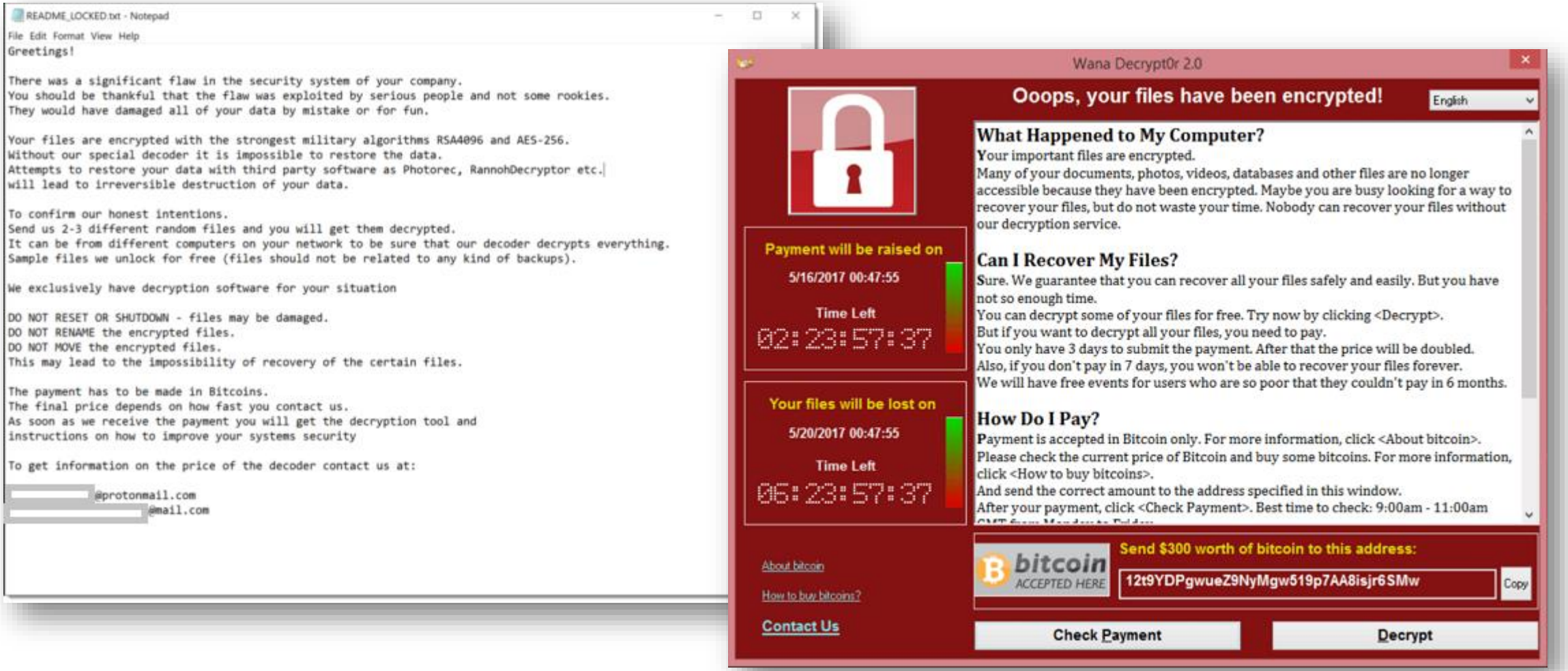



Level 4
Enterprise
Enterprise Historian
Servers
Workstations
Printers
Level 4 Enterprise Network
Internet
Level 5
Internet
Level 3.5
DMZ
Historian Forwarder
Alarm Manager
Remote Access Server
Remote Access Server
AV
WSUS
File Transfer
Remote Access
System Management
Level 3
Site Operations
Site Historian
Alarm Mgmt Server
Engineering Workstation
Application Servers
Remote Access Jump Host
Domain Controller
Level 3 Site Management Network
Level 2
Area Supervisory
Servers
Workstations
Local HMIs
DCS LAN
Workstations
Data Logger
Printer
Metering LAN
Servers
HMIs
Workstation
PowerGen LAN
Workstations
ESD LAN
Workstations
F&G LAN
Local HMIs
Level 1
Basic Control
Controllers
Flow computers
PLCs
Level 0
Field Devices
Sensors
Actuators

# How Good Architecture Defends Against ICS Attacks

Some examples of different malware attacking ICS

# Ransomware


README_LOCKED.txt - Notepad
File Edit Format View Help
Greetings!
There was a significant flaw in the security system of your company.
You should be thankful that the flaw was exploited by serious people and not some rookies.
They would have damaged all of your data by mistake or for fun.
Your files are encrypted with the strongest military algorithms RSA4096 and AES-256.
Without our special decoder it is impossible to restore the data.
Attempts to restore your data with third party software as Photorec, RannohDecryptor etc.
will lead to irreversible destruction of your data.
To confirm our honest intentions.
Send us 2-3 different random files and you will get them decrypted.
It can be from different computers on your network to be sure that our decoder decrypts everything.
Sample files we unlock for free (files should not be related to any kind of backups).
We exclusively have decryption software for your situation
DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME the encrypted files.
DO NOT MOVE the encrypted files.
This may lead to the impossibility of recovery of the certain files.
The payment has to be made in Bitcoins.
The final price depends on how fast you contact us.
As soon as we receive the payment you will get the decryption tool and
instructions on how to improve your systems security
To get information on the price of the decoder contact us at:
@protonmail.com
@mail.com
Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
Contact Us
Send $300 worth of bitcoin to this address:
bitcoin ACCEPTED HERE
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt

# TRITON / TRISIS

**XENOTIME**
SINCE 2014

**ADVERSARY:**
+ Unique tool development

**CAPABILITIES:**
+ TRISIS
+ Custom credential harvesting
+ Off-the-shelf tools

**VICTIM:**
+ Oil & Gas, Electric Utilities
+ Middle East, North America

**INFRASTRUCTURE:**
+ Virtual Private Server and compromised, legitimate infrastructure
+ European web hosting providers
+ Asian shipping company

**ICS IMPACT:**
+ Demonstrated capability to execute disruptive ICS attack, such as the 2017 TRISIS incident



U.S. DEPARTMENT OF THE TREASURY

For small businesses seeking direct relief from COVID-19, CLICK HERE to learn more about Paycheck Protectio

HOME > NEWS > PRESS RELEASES

PRESS RELEASES

## Treasury Sanctions Russian Government Research Institution Connected to the Triton Malware

October 23, 2020

**Washington** – Today, the Department of the Treasury's Office of Foreign Assets Control (OFAC) pursuant to Section 224 of the Countering America's Adversaries Through Sanctions Act (CAATS Russian government research institution that is connected to the destructive Triton malware. T malware — known also as TRISIS and HatMan in open source reporting — was designed specifi target and manipulate industrial safety systems. Such systems provide for the safe emergency industrial processes at critical infrastructure facilities in order to protect human life. The cyber behind the Triton malware have been referred to by the private cybersecurity industry as "the dangerous threat activity publicly known."

"The Russian Government continues to engage in dangerous cyber activities aimed at the Unite and our allies," said Secretary Steven T. Mnuchin. "This Administration will continue to aggressi the critical infrastructure of the United States from anyone attempting to disrupt it."

In recent years, the Triton malware has been deployed against U.S. partners in the Middle East, hackers behind the malware have been reportedly scanning and probing U.S. facilities. The dev and deployment of the Triton malware against our partners is particularly troubling given the R government's involvement in malicious and dangerous cyber-enabled activities. Previous exam Russia's reckless activities in cyberspace include, but are not limited to: the NotPetya cyber-att most destructive and costly cyber-attack in history; cyber intrusions against the U.S. energy gri potentially enable future offensive operations; the targeting of international organizations such Organization for the Prohibition of Chemical Weapons and the World Anti-Doping Agency; and disruptive cyber-attack against the country of Georgia.

**Triton Malware**

In August 2017, a petrochemical facility in the Middle East was the target of a cyber-attack invol

Computing /

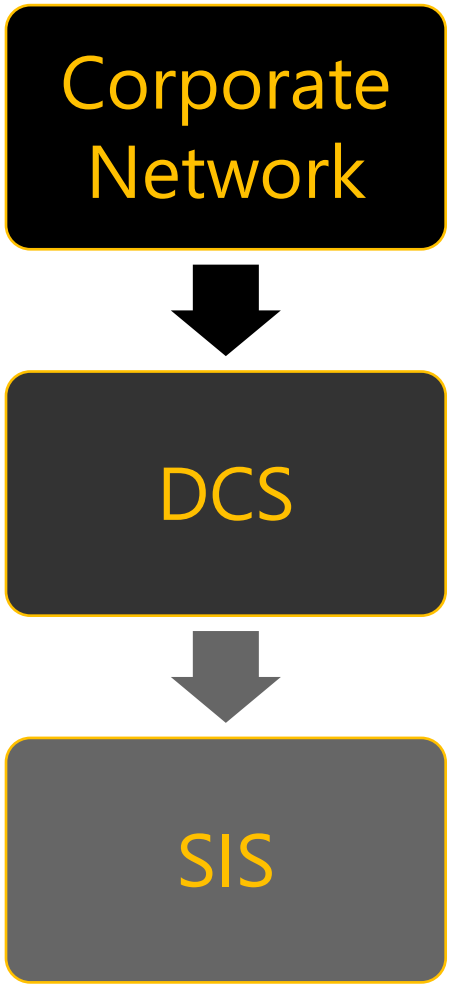
Triton
murd
it's sp

The rogue c
catastrophic
East, but the
North Ameri

by Martin Gil

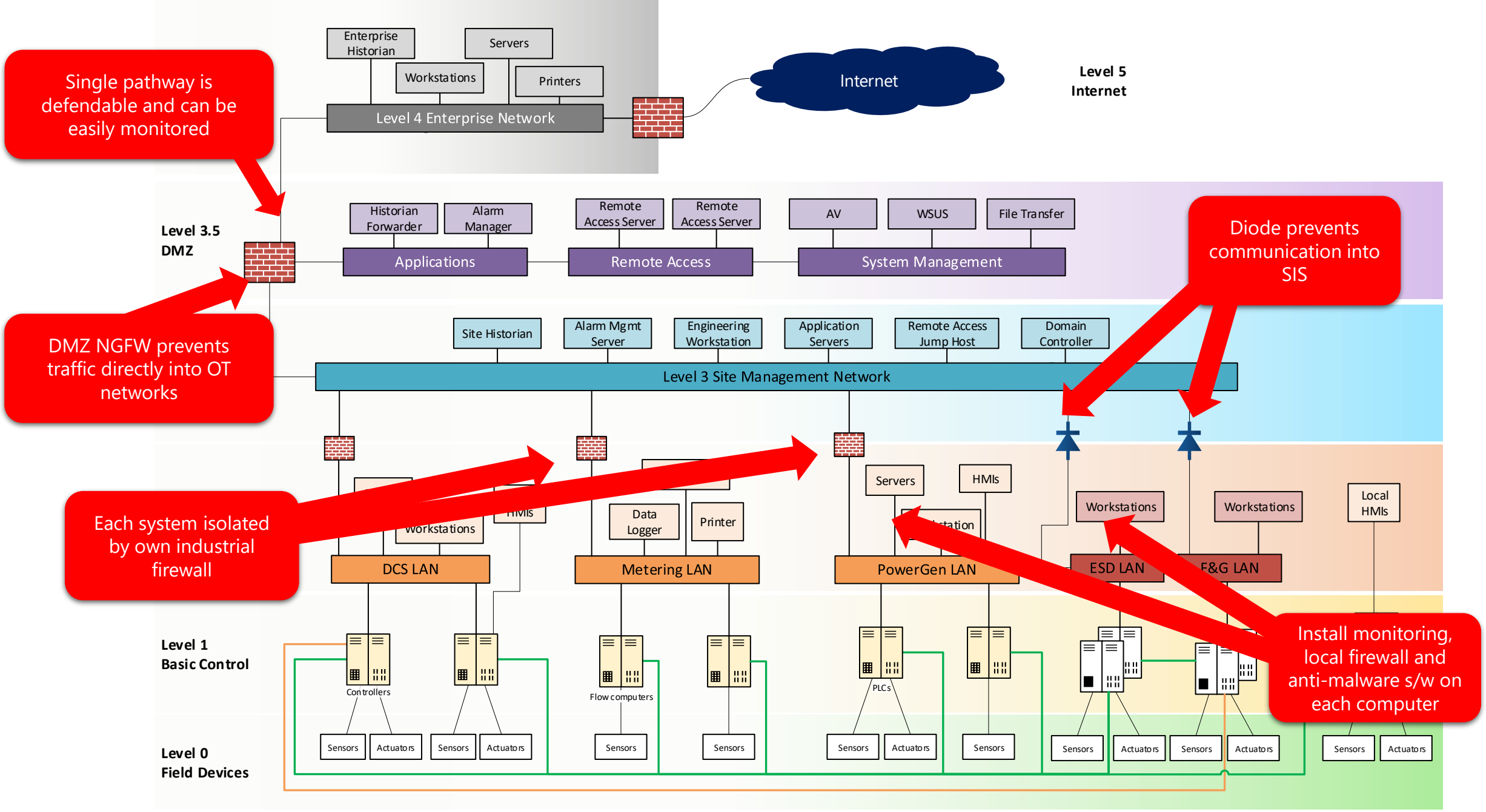
**As an experienced cyber first responder, Julian Gutmanis had been called** plenty of times before to help companies deal with the fallout from cyberattacks. But when the Australian security consultant was summoned to a petrochemical plant in Saudi Arabia in the summer of 2017, what he found made his blood run cold.

# TRITON / TRISIS





Credit for most of the analysis goes to Dragos and FireEye


Single pathway is defendable and can be easily monitored
DMZ NGFW prevents traffic directly into OT networks
Each system isolated by own industrial firewall
Diode prevents communication into SIS
Install monitoring, local firewall and anti-malware s/w on each computer
Enterprise Historian
Servers
Workstations
Printers
Level 4 Enterprise Network
Internet
Level 5
Internet
Level 3.5
DMZ
Historian Forwarder
Alarm Manager
Applications
Remote Access Server
Remote Access Server
Remote Access
AV
WSUS
File Transfer
System Management
Site Historian
Alarm Mgmt Server
Engineering Workstation
Application Servers
Remote Access Jump Host
Domain Controller
Level 3 Site Management Network
Workstations
HMIs
DCS LAN
Data Logger
Printer
Metering LAN
Servers
HMIs
PowerGen LAN
Workstations
ESD LAN
Workstations
F&G LAN
Local HMIs
Level 1
Basic Control
Controllers
Flow computers
PLCs
Level 0
Field Devices
Sensors
Actuators

# Thank You!

prosource.it
High Performance IT Solutions

## Questions?



Rob.Rothwell@prosource.it


https://www.linkedin.com/in/robrothwell


@rdrothwell


https://github.com/S3cur1tyH4ggis/ICS-Security-Products/