WATERFALL®
Stronger Than Firewalls

Safe OT Security Monitoring

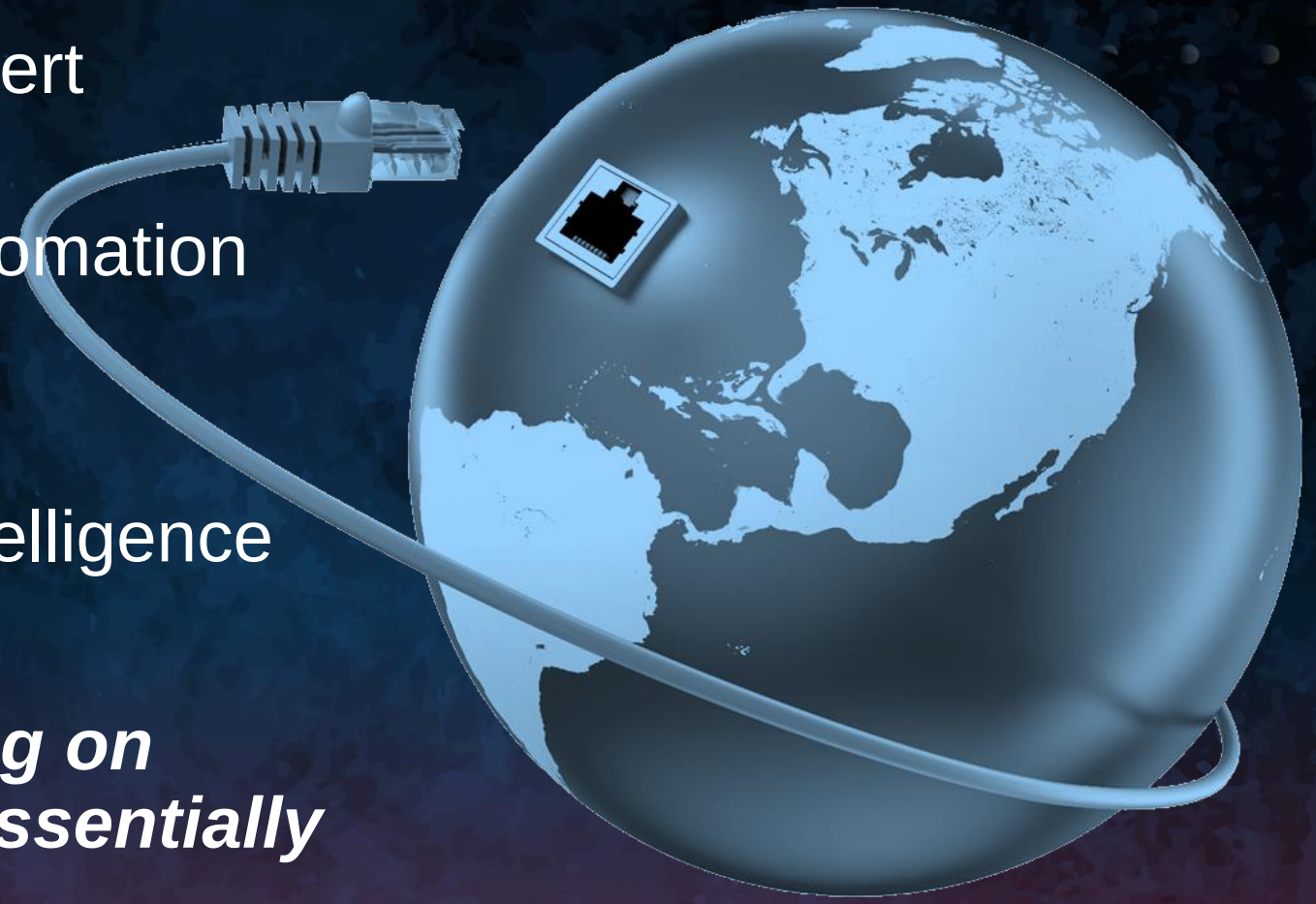
Andrew Ginter

VP Industrial Security, Waterfall Security Solutions

S4x20

MATURE CENTRAL MONITORING

- IDS – attacks in progress
- SIEM – log aggregation, alert management
- SOAR – orchestration, automation & response
- Cross-site correlations
- Integrated global threat intelligence



Central security monitoring on enterprise networks has essentially universal coverage

WATERFALL®
Stronger Than Firewalls

EXTENDING TO OT NETWORKS IS ESSENTIAL

OT NETWORKS ARE VITAL TO INDUSTRIAL ENTERPRISES
BUT MONITORING THROUGH FIREWALLS INTRODUCES RISKS

SYSLOG

SNMP TRAPS

SECURITY STATUS

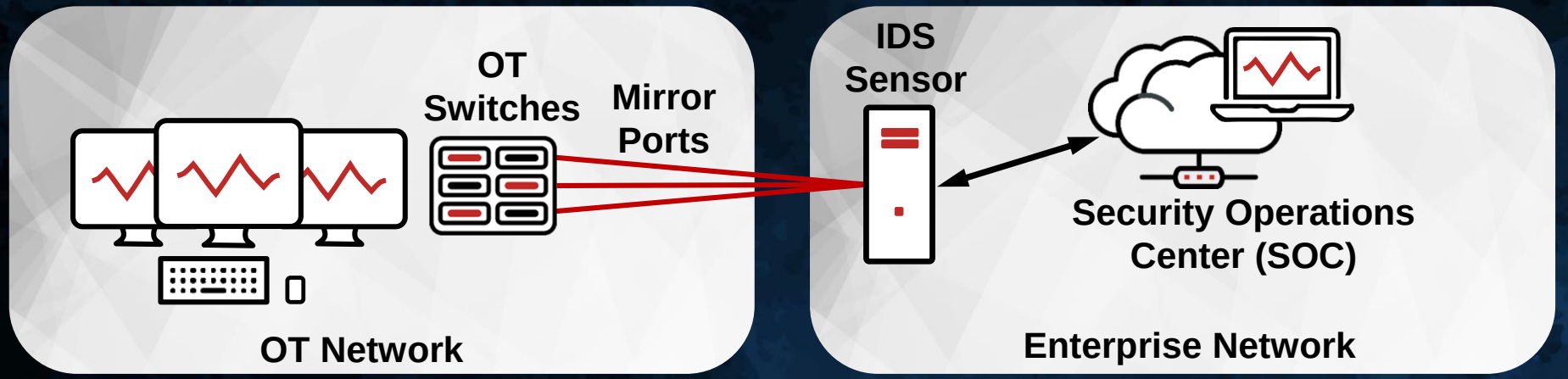
TROJAN

DOS ATTACK

TARGETED & NONTARGETED RANSOMWARE

WATERFALL®
Stronger Than Firewalls

OT IDS SENSORS?



IDS sensors should be deployed on IT networks - they need frequent updates and adjustments by central SOC analysts.

But – mirror ports are notorious for bi-directionality, and any claimed switch unidirectionality is only software-based, not physical

WATERFALL®
Stronger Than Firewalls

WATERFALL FOR INTRUSION DETECTION SYSTEMS (IDS)

Enables intrusion detection sensors to monitor OT networks without putting OT network at risk

1

COLLECT

Mirror port and SPAN traffic from protected industrial control system and operations technology networks

2

SENSE

Safely replicates traffic captures to a network intrusion detection sensor on the IT network for analysis

3

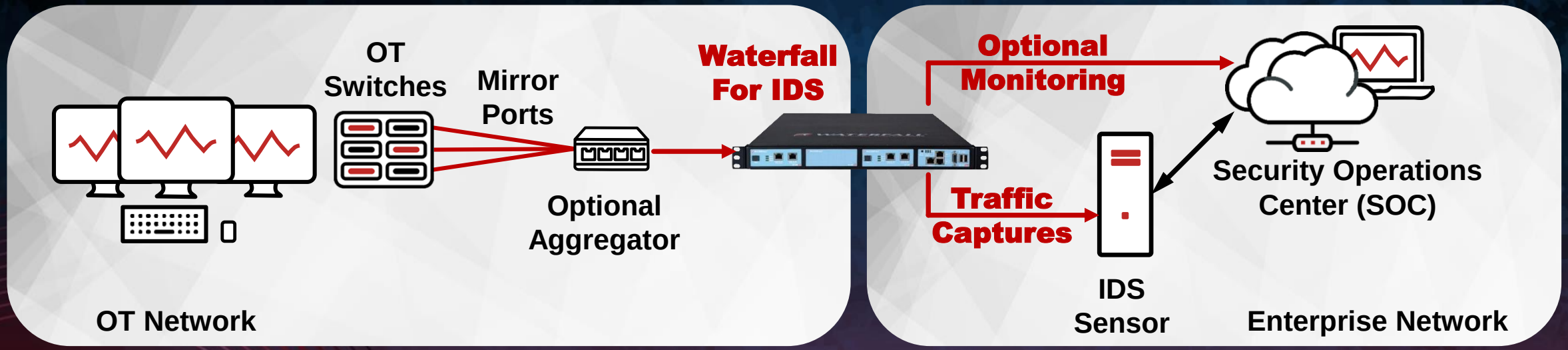
REPORT

Monitors, summarizes and reports monitored traffic for local analysis and to central SIEMs, SOCs and NOCs

WATERFALL®
Stronger Than Firewalls

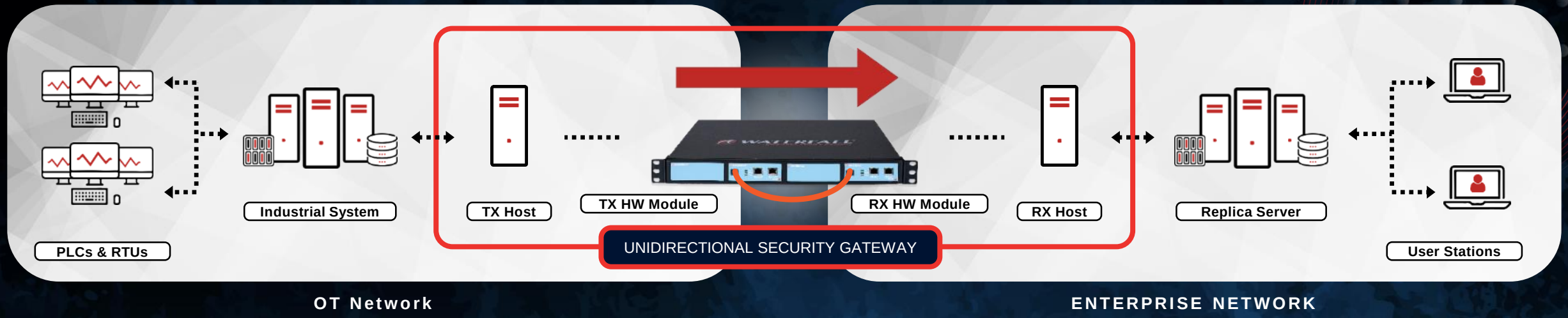
WATERFALL FOR IDS – HOW IT WORKS

- Gathers data from ICS/OT network mirror and SPAN ports, no hosts needed on ICS network
- Mirror/SPAN ports are replicated unidirectionally to an IDS sensor on an IT network, simplifying maintenance of the sensor for SOC analysts while preserving strong protection for the ICS network
- The Waterfall packet monitor delivers optional health, volume, summary and other information to a central SOC, SIEM or NOC via Syslog or SNMP traps



WATERFALL®
Stronger Than Firewalls

UNIDIRECTIONAL SECURITY GATEWAY



Unidirectional Security Gateways are a combination of hardware and software

- The hardware sends information in only one direction
- The software replicates servers & emulates devices from the OT network to the IT network
- No attack, no matter how sophisticated, can propagate back to the industrial network through the gateway

WATERFALL®
Stronger Than Firewalls

SAFE UNIDIRECTIONAL MONITORING

- UGWs emulate Syslog and SNMP devices to central/cloud SOCs
- They replicate log file servers and other security-relevant devices
- The replicate OPC servers, historians, RDBs and mirror ports
- All without the risks that firewalled SOC connectivity always introduces

WATERFALL®
Stronger Than Firewalls

STRATEGIC PARTNERSHIP

"FireEye, working with Waterfall Security, will be able to increase its scope of security functionality to better serve the needs of industrial customers."

Rich Stegina
Vice President at FireEye.

WATERFALL & FIREEYE

THE GOLD STANDARD FOR OT SECURITY MONITORING

➢CHALLENGE

Cloud-based, universal central monitoring of business and operational networks in real time, without risking any compromise of the operations network

➢SOLUTION

- ➢**Waterfall Unidirectional CloudConnect** – gathers industrial / security data, translates to cloud-friendly formats & sends the information reliably and securely across IT and Internet WANs
- ➢**FireEye Helix** – a SOAR platform that integrates security tools and applies threat intelligence, automation and case management allowing SOC analysts to respond efficiently to OT and IT threats

➢RESULT

Safe, universal coverage for central security monitoring and analysis for industrial enterprises

WATERFALL®
Stronger Than Firewalls

WATERFALL'S OT MONITORING PARTNERS

FIREEYE™

DRAGOS

splunk>

Indegy

FORESCOUT

CyberX

WATERFALL®
Stronger Than Firewalls

THIS IS THE GOLD STANDARD

… FOR OT SECURITY MONITORING

Intrusion detection for OT networks without risk

- The most secure and reliable way to monitor OT networks from a central IT / cloud SOC is via Unidirectional Gateways:
  - Physical protection for OT networks
  - OT IDS sensors can safely be deployed on IT networks for easy management
  - 1st law of SCADA security: nothing is secure – monitoring is vital

https://waterfall-security.com/gold-standard

WATERFALL®
Stronger Than Firewalls

THE OT SECURITY COMPANY

WATERFALL ENABLES

- SECURE AND RELIABLE OPERATIONS
- SAFE OT INTEGRATION WITH EXTERMAL ENVIRONMENTS
- ACCESS TO OPERATIONS DATA, OT SECURITY MONITORING
- DISCIPLINED REMOTE ACCESS AND REMOTE CONTROL

WATERFALL PREVENTS

- REMOTE CYBER ATTACKS ON INDUSTRIAL AND CRITICAL ENVIRONMENTS
- MALWARE AND RANSOMWARE FROM REACHING INTO CONTROL NETWORKS
- NATION-STATE LEVEL REMOTE ATTACKS AND PIVOTING ATTACKS
- PHISHING AND SOCIALLY ENGINEERED ATTACKS

WATERFALL®
Stronger Than Firewalls

INDUSTRIAL SECURITY PODCAST

GUESTS FROM ACROSS THE INDUSTRIAL SPACE

Vendors: issues, technology & approaches

Government agencies: programs & resources

Owners & **operators**: priorities & approaches

Other: recruiters, educators & more

https://waterfall-security.com/podcasts

WATERFALL®
Stronger Than Firewalls

SECURE OPERATIONS TECHNOLOGY

- IT-SEC = protect the information – CIA, AIC
- SEC-OT = protect physical operations *from* information – because all cyber attacks are information
- The world's most secure industrial sites ask different questions and so of course get different answers

Complementary copies are available – ask me

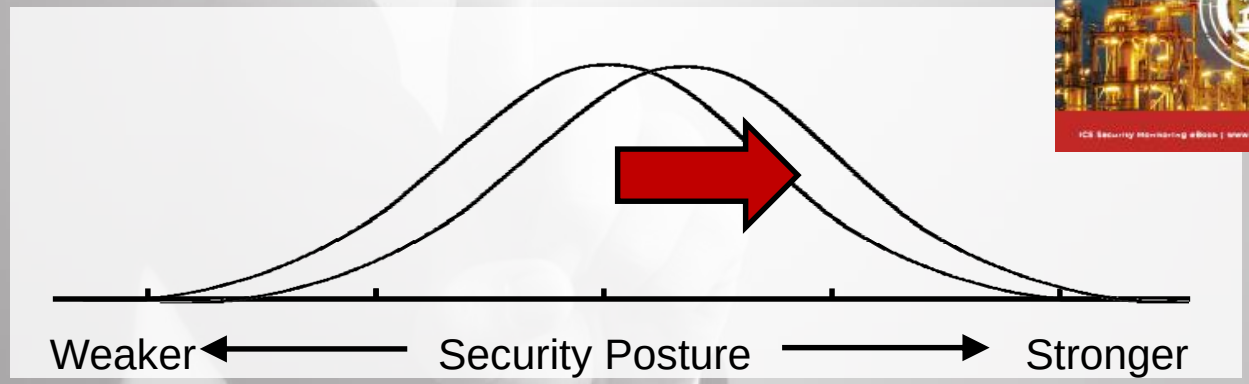
WATERFALL®
Stronger Than Firewalls

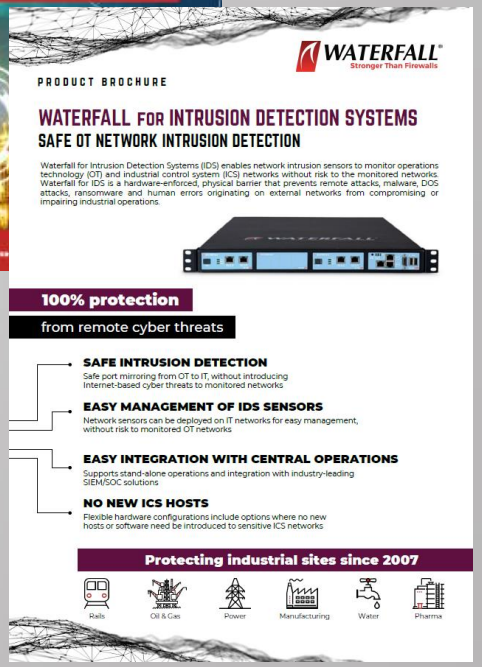
THE GOLD STANDARD

Attack capabilities only increase, so must our security posture

Safe, universal security monitoring without firewalled connectivity risks

Convenient, IT-based network intrusion detection





https://waterfall-security.com/gold-standard
https://waterfall-security.com/waterfall-for-ids

WATERFALL®
Stronger Than Firewalls