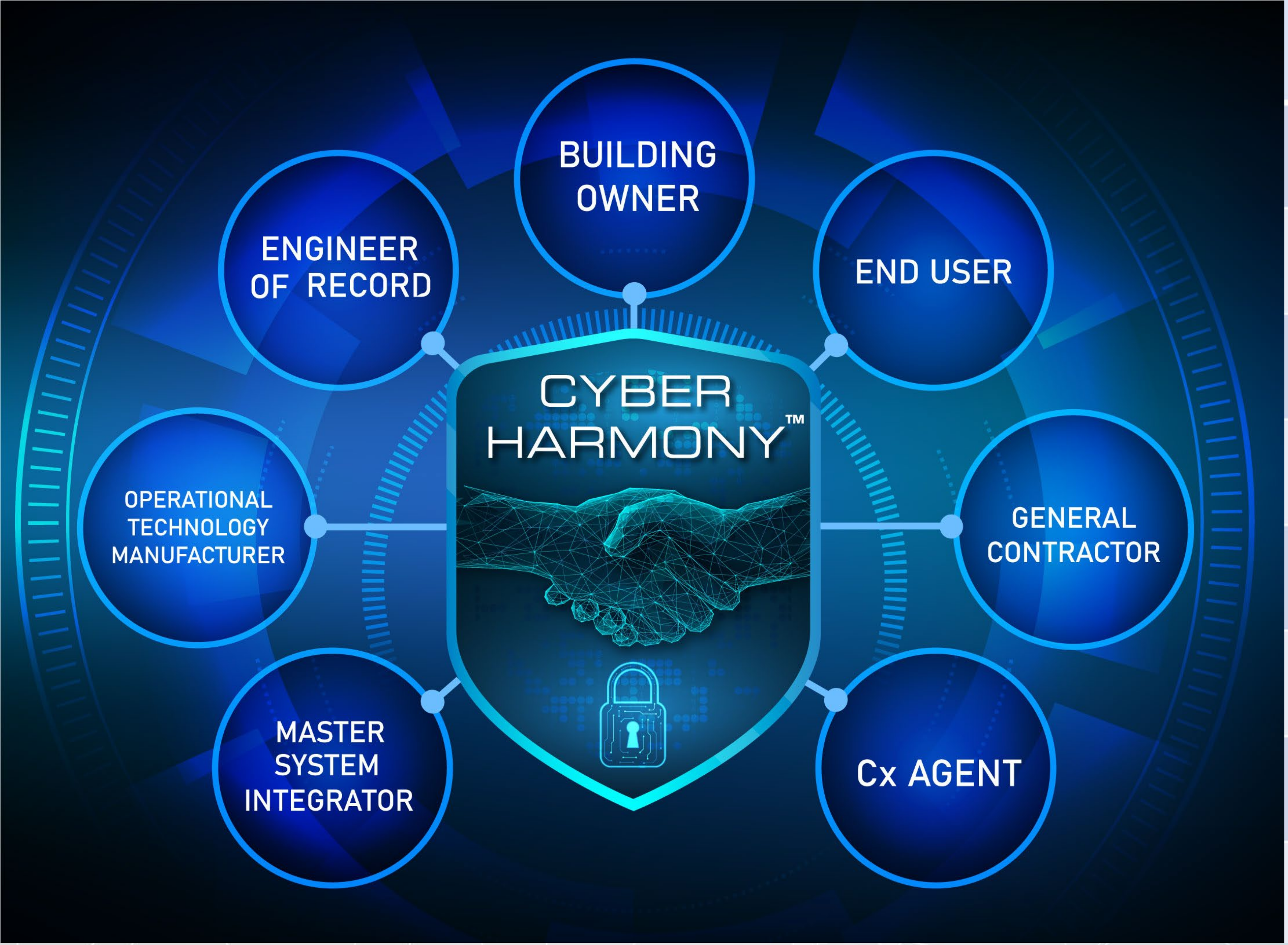
TRIDIUM

NS2024

APRIL 15 - 17 | ANAHEIM, CA

Cyber Fluency for the OT Environment

Panel



OPR DOCUMENTS

IT/OT TEAMS

OT PRODUCTS

PROTOCALS

BEST PRACTICES

SPECIFICATIONS

DRAWINGS

IT/OT POLICIES

Cx PROCEDURES

Secure-by-Design Solution for Critical Facilities

You Can't Say that Nobody Saw this Coming!

Sam Esmail

A visionary or a scary storyteller?

Cyber attacks can have an impact on our daily lives

Leave the World Behind (2023) – Netflix

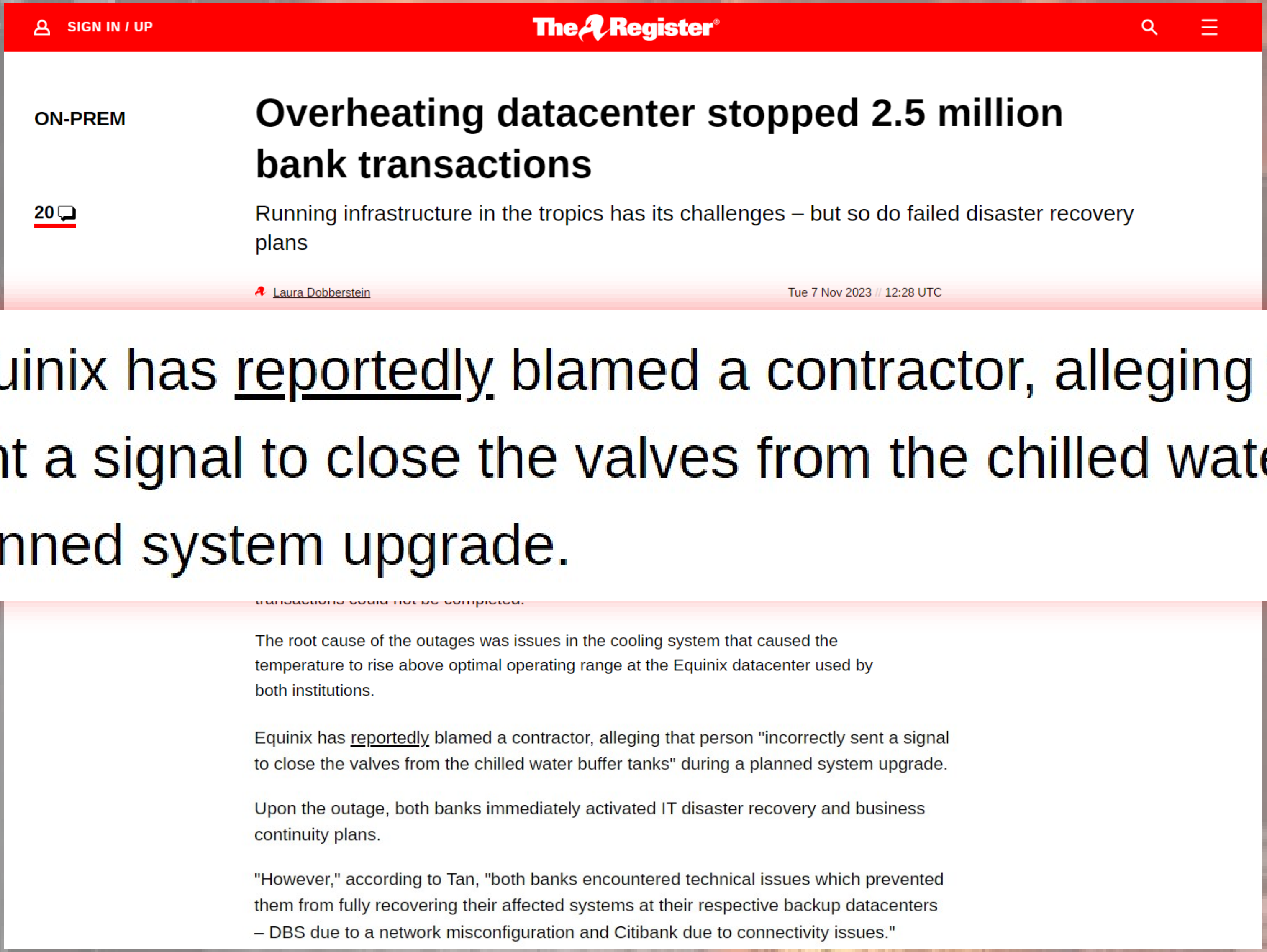
42M views

OT Networks are Good Entry Points for Creating Damage

Mr Robot (2015-2019) – USA Network

17M views

From Fiction to Reality : Overheated Data Center



ON-PREM

Overheating datacenter stopped 2.5 million bank transactions

20

Running infrastructure in the tropics has its challenges – but so do failed disaster recovery plans

Laura Dobberstein Tue 7 Nov 2023 // 12:28 UTC

> Equinix has reportedly blamed a contractor, alleging that person "incorrectly sent a signal to close the valves from the chilled water buffer tanks" during a planned system upgrade.

transactions could not be completed.

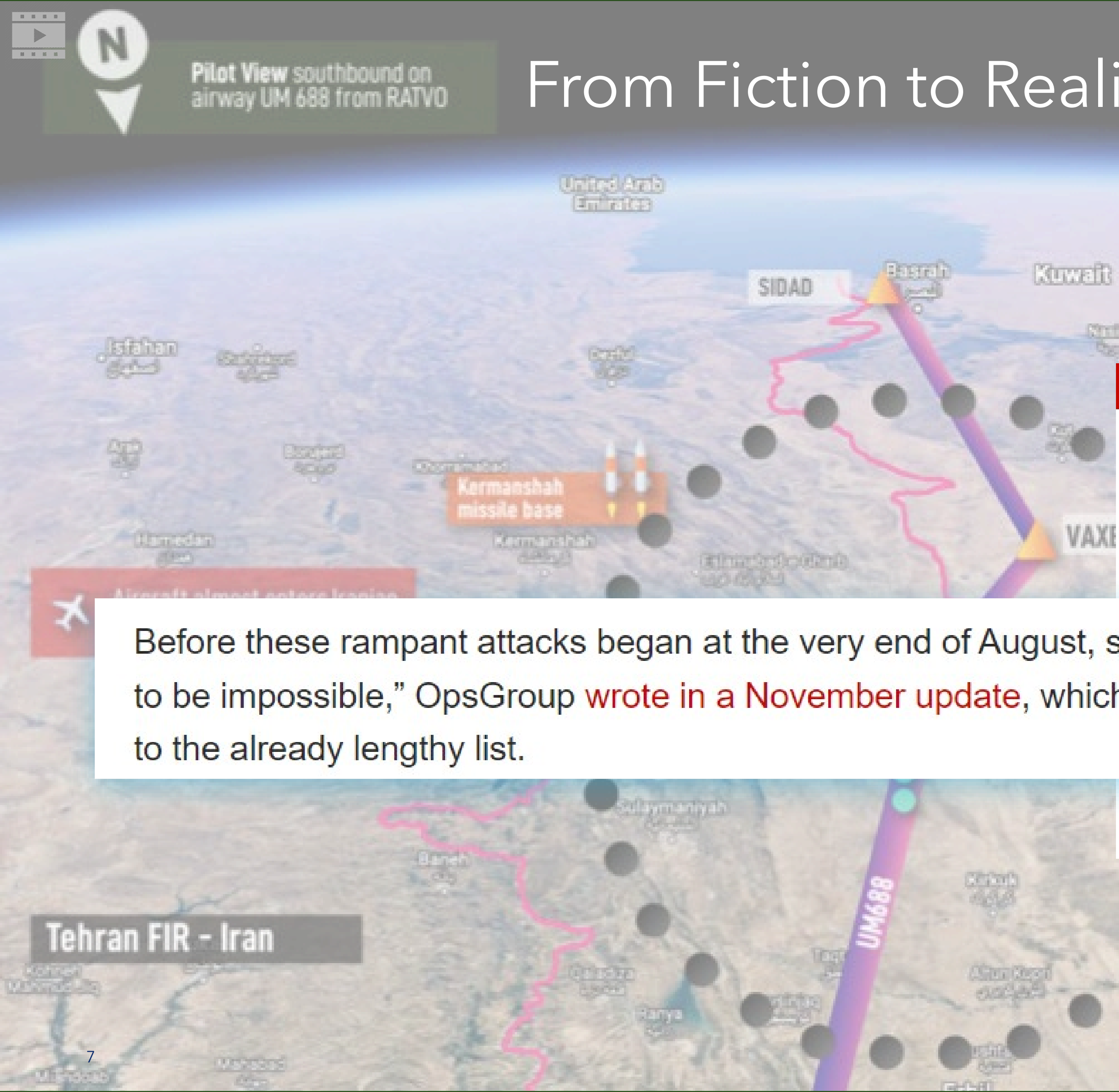
The root cause of the outages was issues in the cooling system that caused the temperature to rise above optimal operating range at the Equinix datacenter used by both institutions.

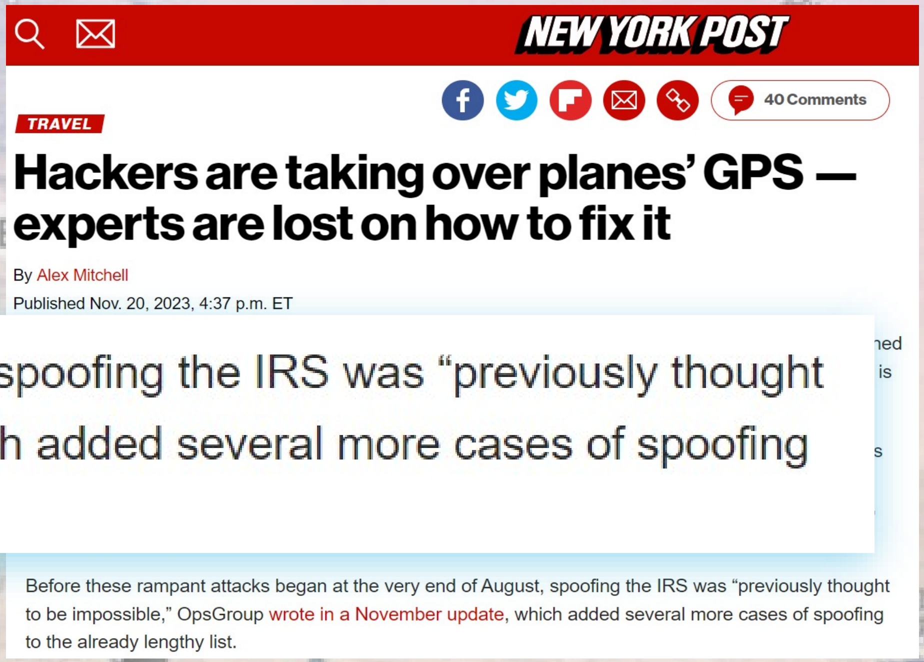
Equinix has reportedly blamed a contractor, alleging that person "incorrectly sent a signal to close the valves from the chilled water buffer tanks" during a planned system upgrade.

Upon the outage, both banks immediately activated IT disaster recovery and business continuity plans.

"However," according to Tan, "both banks encountered technical issues which prevented them from fully recovering their affected systems at their respective backup datacenters – DBS due to a network misconfiguration and Citibank due to connectivity issues."

From Fiction to Reality : GPS Spoofing





NEW YORK POST

40 Comments

TRAVEL

Hackers are taking over planes' GPS — experts are lost on how to fix it

By Alex Mitchell

Published Nov. 20, 2023, 4:37 p.m. ET

Before these rampant attacks began at the very end of August, spoofing the IRS was "previously thought to be impossible," OpsGroup wrote in a November update, which added several more cases of spoofing to the already lengthy list.

Before these rampant attacks began at the very end of August, spoofing the IRS was "previously thought to be impossible," OpsGroup wrote in a November update, which added several more cases of spoofing to the already lengthy list.

Adapting to a Less Secure World

Geopolitical tension

- ✓ Ukraine, Israel, Taiwan,…
- ✓ Sino-American Duopoly
  - – Extended BRIC (Saudi Arabia, Iran)
  - – Reindustrialization in OECD countries

Digitalization of Crime

- ✓ Corruption, or disruption of systems
- ✓ Fraud or identify theft
- ✓ Information warfare

Human Health & Safety

From cyber financial to cyber physical

A shift from white-collar crime to state-sponsored attacks on critical infrastructures, with many potential casualties.

Cyber-Security Standards

- ✓ NIST CSF & ISA/IEC 62443
- ✓ Secure-by-Design
- ✓ European Cyber Resilience Act

Why is Cyber Security becoming a priority?

+37%

IoT Malware Attack
(2023 vs 2022)

8T$

Worldwide Cybercrime Cost
(2023)

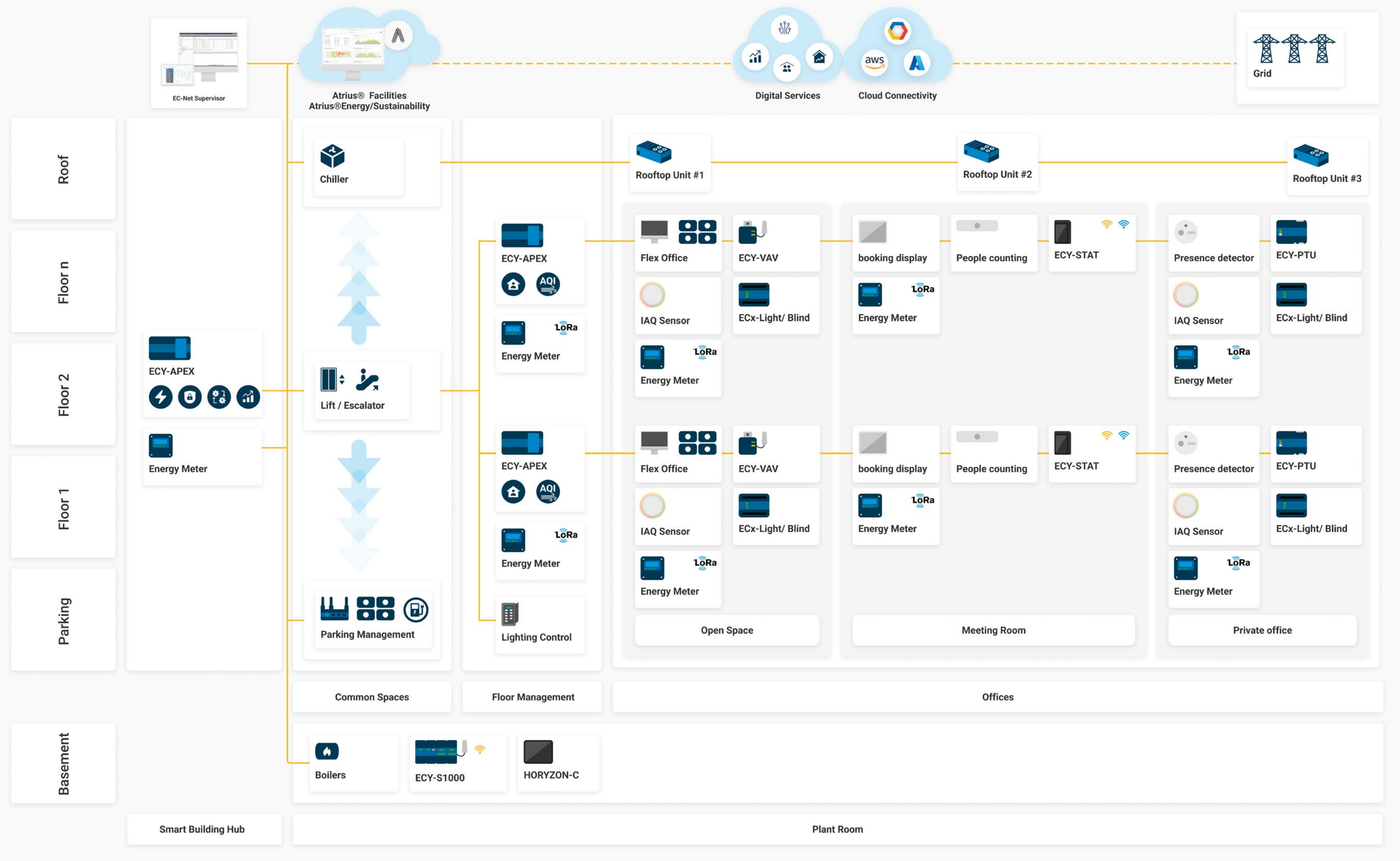
10B$

US Government Budget
Allocated to Cybersecurity
(2023)

Smart Building – An Ever-Expanding Attack Surface

Cyber Security is opening new bids and opportunities

- ADR / Virtual Power Plant
- Equipment Optimisation
- ESG / Energy Reporting
- Space Optimization
- Comfort Optimization



Targeted Markets

First and foremost, *critical infrastructures* where *any interruption in service has major repercussions*

- ✓ **Healthcare**
  Ransomware attacks impacted more than 289 hospitals in 2022. Hospitals are lucrative targets because their data is valuable & they have a higher rate of paying ransoms.

- ✓ **Datacenters**
  DC attacks are particularly dangerous because a single breech can many companies. Recent trends show hackers are concentrating on gaining access through OT networks because of softer security standards.

- ✓ **Corporate Campuses**
  Large institutions are vulnerable to attack because of the size of their networks and the number of people working on the network. Personal information, trade secrets, and financial data from large corporations is lucrative for hackers.

- ✓ **Secure Federal Government Facilities (for the USA)**
  The number of attacks targeting the US government increased 95% in the 2nd half of 2022 compared the same time period in 2021.
  - ✓ 3-Letter Agencies
  - ✓ US Overseas Embassy Facilities
  - ✓ High Security Military Base (Nuclear Facilities, Command and Control Facilities, etc.)

- ✓ **Transportation & Energy Infrastructure Control**

Securing IT network - A Mature, Tried-and-Tested Solution

In 2024, no serious company will connect a PC or any other IP device to its IT corporate network without having implemented a solution from at least the following 3 categories of IT security providers.

Digital Identity & Certificate Infrastructure (PKI)

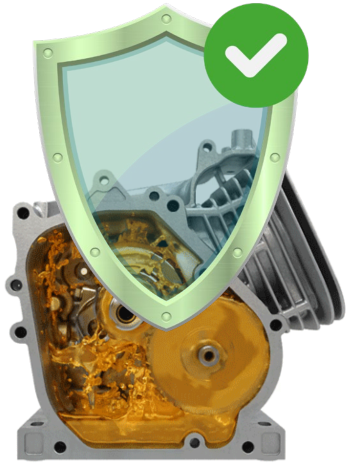
digicert®
ENTRUST
SECURING A WORLD IN MOTION
GlobalSign®
by GMO
COMODO

End Point Asset Management & Defense

McAfee™
TREND MICRO™
symantec.
CROWDSTRIKE
Bitdefender®
Microsoft

Network Visibility & Defense

CHECK POINT™
paloalto® NETWORKS
CISCO
FORTINET®



IT and OT Networks – Similarities, but Major Differences

Mainly PC with lot of resources

Often replaced (every 3-4 years)

Mainly one O.S.
Windows

Consistent install based
The latest version or the one before

Always up to date

IT

Embedded systems with limited resources

Can be 10+ years old

Lots of different O.S.
Linux, Android, QNX, …

Lot of different versions of the same O.S.

Almost never updated

OT

Securing OT Network - Traditional Solutions – Complex, Costly

Digital Identity & Certificate Infrastructure (PKI)

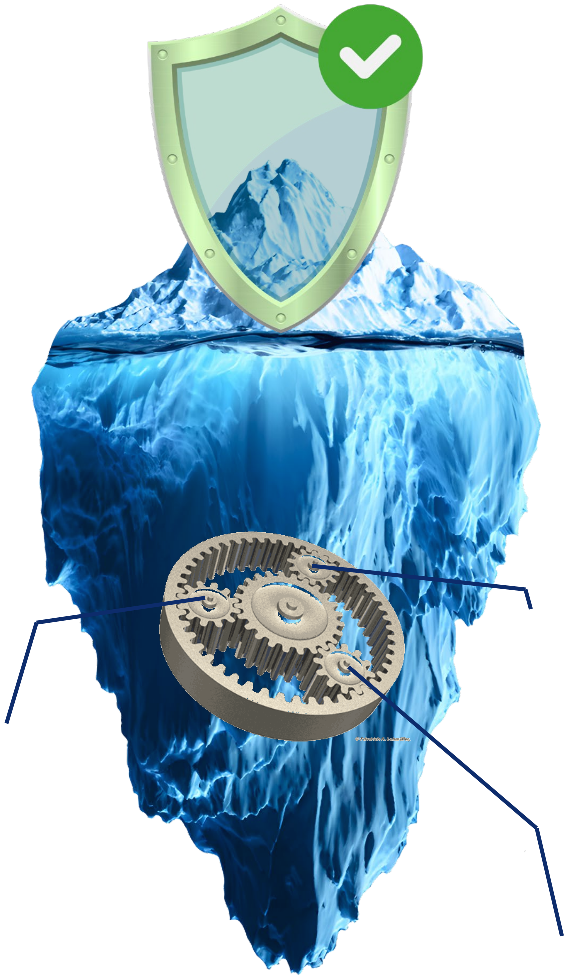
- ONCLAVE
- Veridify Security
- ENTRUST SECURING A WORLD IN MOTION
- Q-Net Security
- Venafi
- KEYFACTOR

End Point Asset Management & Defense

- Phosphorus
- VERVE
- txOne networks
- CROWDSTRIKE
- Shield-IoT

Network Visibility & Defense

- DRAGOS
- ARMIS.
- DARKTRACE
- CLAROTY
- tenable
- NOZOMI NETWORKS
- INDUSTRIAL DEFENDER®



Operational Overhead

Securing OT Network - Traditional Solutions – Complex, Costly and Risky

Digital Identity & Certificate Infrastructure (PKI)

ONCLAVE

Veridify Security

ENTRUST SECURING A WORLD IN MOTION

Q-Net Security

Venafi

KEYFACTOR

End Point Asset Management & Defense

Phosphorus

VERVE

txOne networks

CROWDSTRIKE

Shield-IoT

Network Visibility & Defense

DRAGOS

ARMIS.

DARKTRACE

CLAROTY

tenable

NOZOMI NETWORKS

INDUSTRIAL DEFENDER®

Complex Maintenance Over Time

Secure-by-Design

The software industry needs more secure products, not more security products. Software manufacturers should lead that transformation

SHIFTING THE BALANCE OF CYBERSECURITY RISK:

PRINCIPLES AND APPROACHES FOR SECURE BY DESIGN SOFTWARE

Reference document published by CISA
Last update October 16th 2023

Seamless integration reduces potential vulnerabilities and the risk of misconfigurations that could be exploited by malicious actors.

Pre-integrated cybersecurity solutions with BMS/HVAC vendor equipment offer better overall cybersecurity outcomes.

Australian Government
Australian Signals Directorate
ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC
Federal Office for Information Security
Communications Security Establishment
Centre de la sécurité des télécommunications
Canadian Centre for Cyber Security
Centre canadien pour la cybersécurité
National Cyber Security Centre
National Cyber Security Centre Ministry of Justice and Security
National Cyber Security Centre
CSIRTAmericas Network
NISC
CSA SINGAPORE
certnz
NSM NORWEGIAN NATIONAL CYBER SECURITY CENTRE
National Cyber and Information Security Agency
KISA KOREA INTERNET & SECURITY AGENCY
JPCERT CC

Approved by 13 countries

Left and Right of Boom

It's virtually impossible to guarantee 100% certainty that an unexpected hostile event won't occur, but concepts have been developed in military circles to limit the impact of such events and ensure a return to normal as quickly as possible once they have occurred.

Minimize Impact

Prevention Strategies

Intelligence Gathering

Left of the Boom (before)

Incident Response

Damage Control

Recovery Efforts

Right of the Boom (after)

Main Pillars to Secure OT Network

Based on NIST Cybersecurity Framework NIST 800-53

Identify

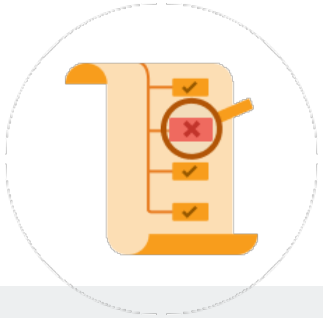
Define which equipment and operators are authorized

Protect

Encrypting communications
Create separate networks
Highly secure authentication method

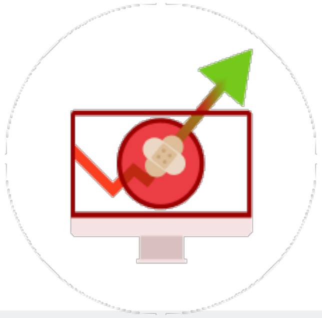
Detect

Recognize unidentified equipment and any unexpected or suspicious communication



Respond

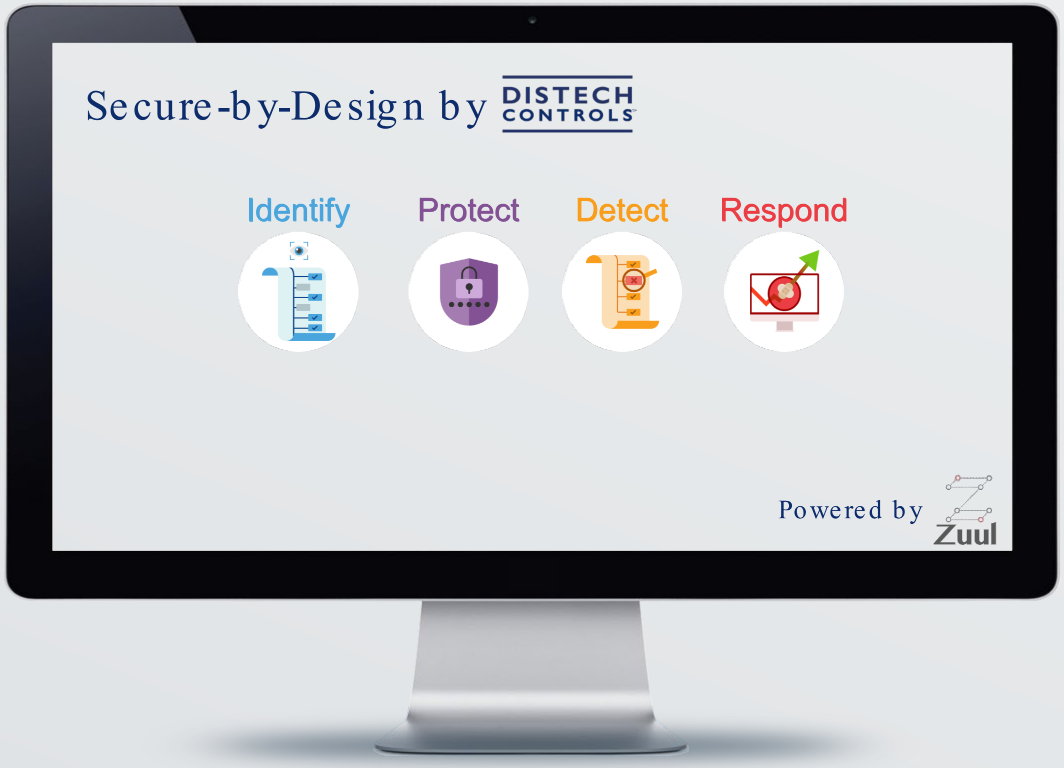
Analyze the problem
Remove the infection and return to a healthy situation
Improve protection to prevent the problem from recurring



Recover

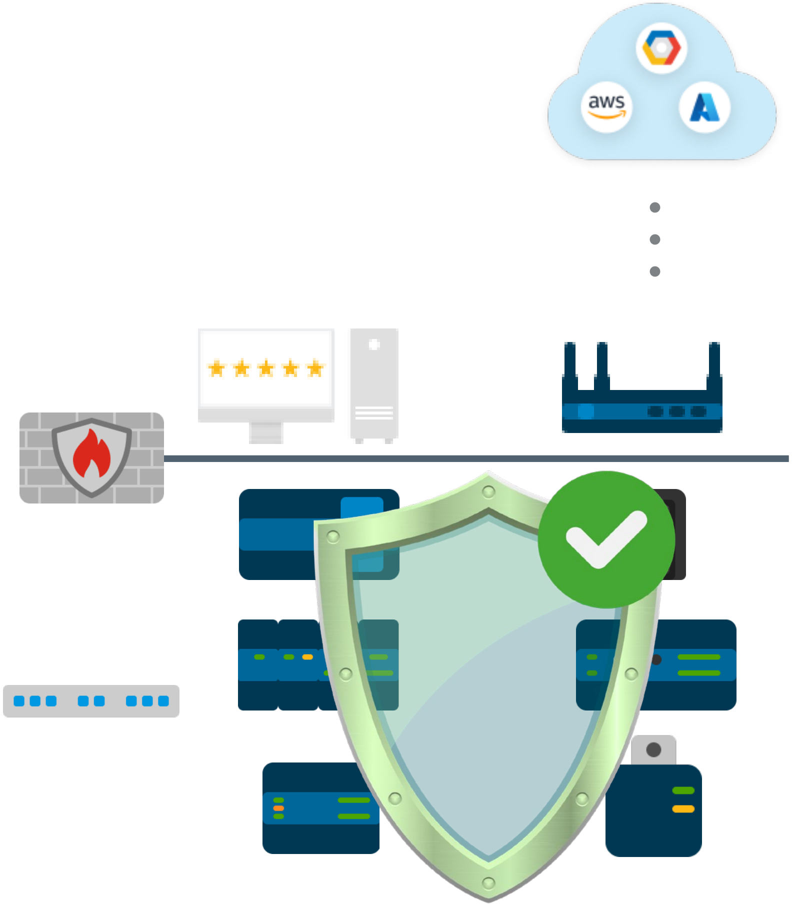
Develop and implement processes to maintain resiliency and business continuity

Secure-by-Design – Seamless Native Security



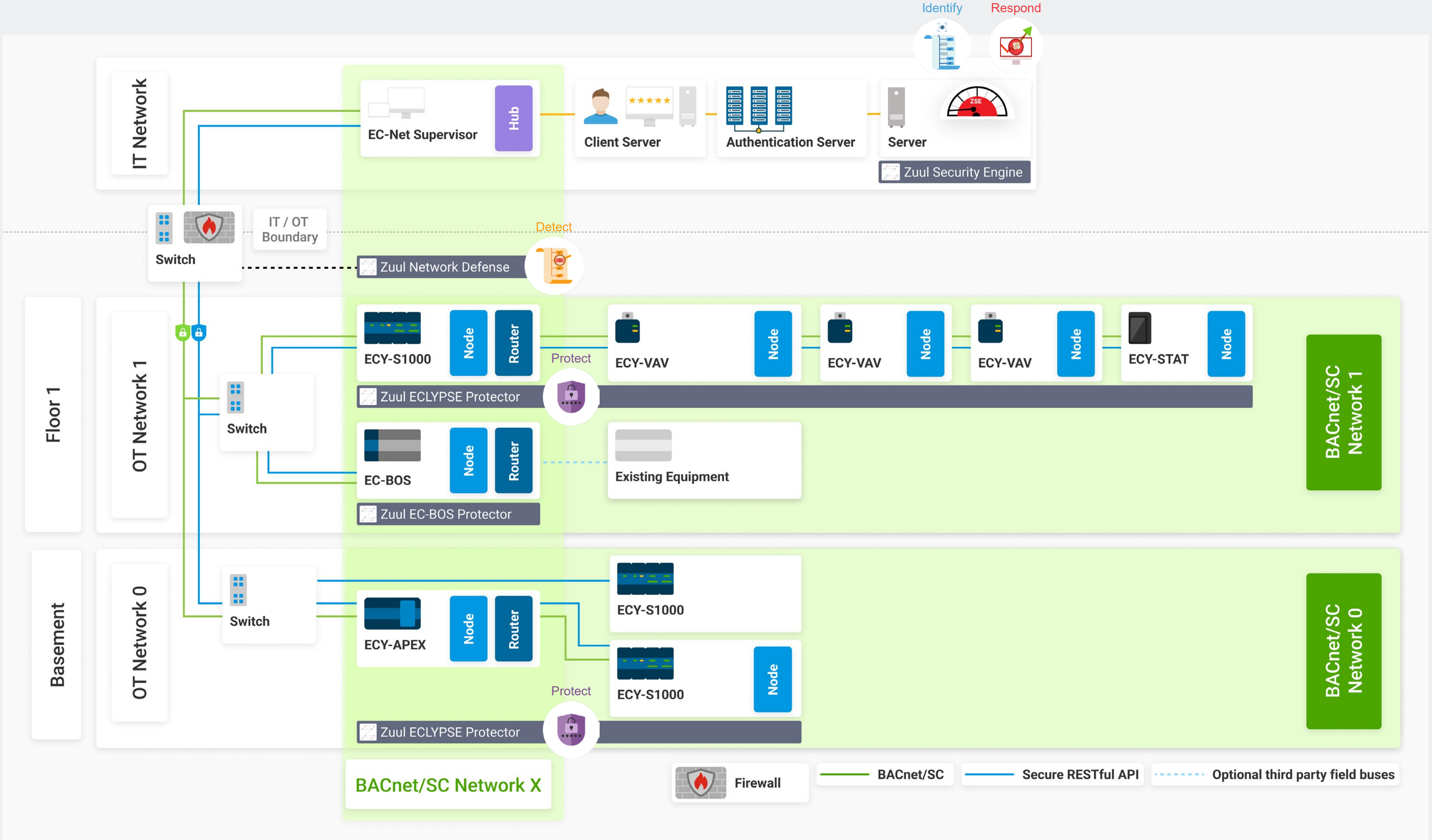
Secure-by-Design by DISTECH CONTROLS

Build-Secure, Deploy-Secure
On Prem or from the Cloud



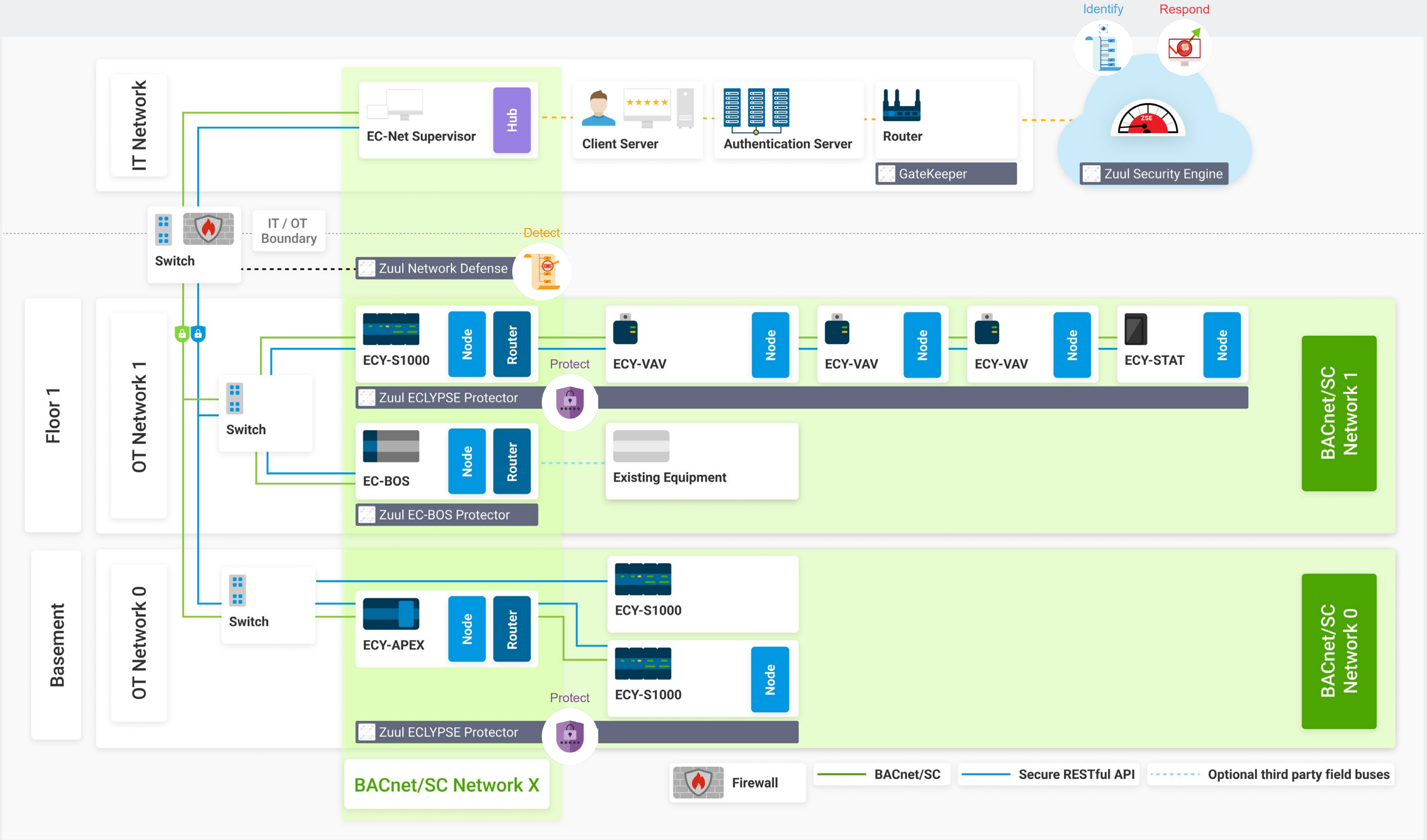
Securing critical assets that underpin the BMS

Secure-by-Design On-Prem Architecture



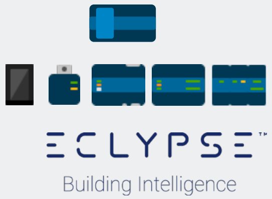
DISTECH CONTROLS

Secure-by-Design Cloud-based Architecture



DISTECH CONTROLS

Secure–by-Design – Distributed Software Components

	Capabilities	NIST CSF	Platform
Security Engine	Digital Identity / AAA Certificate Infrastructure Management	Identify Protect	
End Point Protection	End Point Asset Management & Defense	Identify Protect Detect	 Later
Network Defense	Network Visibility & Defense	Identify Detect Respond	Network Sensor Later

Benefits for Systems Integrators

✓Minimal Cyber Security Expertise

✓Built-in Cybersecurity

- Single source
- No risk of compatibility issues
- Tested and Validated in Highly Secure Environment

✓Easy deployment

- BACnet/SC (Digital Certificate Management)
- Cyber Security components

Questions?

If you have additional questions & we have run out of time, please reach out to any of our panelists outside of the room.