Webinar

February 25, 2021

Building the Confidence to Connect with Zero Trust Edge Security

ZEDEDA accenturesecurity Lanner

Today’s Speakers

ZEDEDA

Jason Shepherd

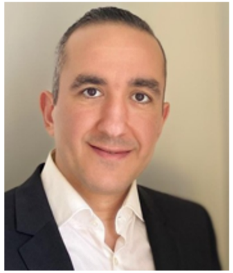
VP Ecosystem

accenturesecurity

Chris Shaunfield

Principal Director

Lanner



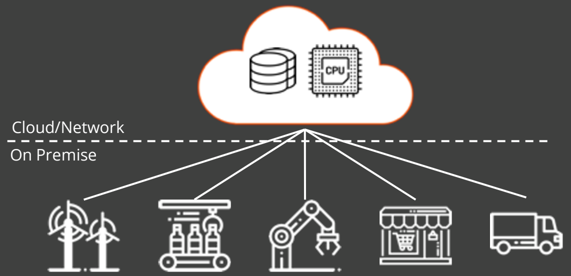
Ahmed Khalil

Americas Business Development Lead,
IoT Solutions

Evolution in a Connected World

Internet of Things

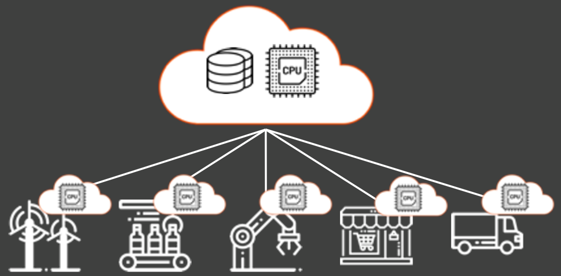
Past



- “Connect” Era
- Trusted Cloud Computing
- Big Data

Edge Computing

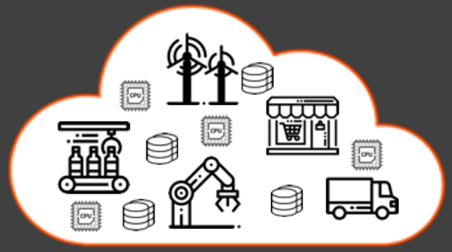
Now



- ”Compute” Era
- Cloud-Native “Everywhere”
- Artificial Intelligence

Trust Fabrics

Future

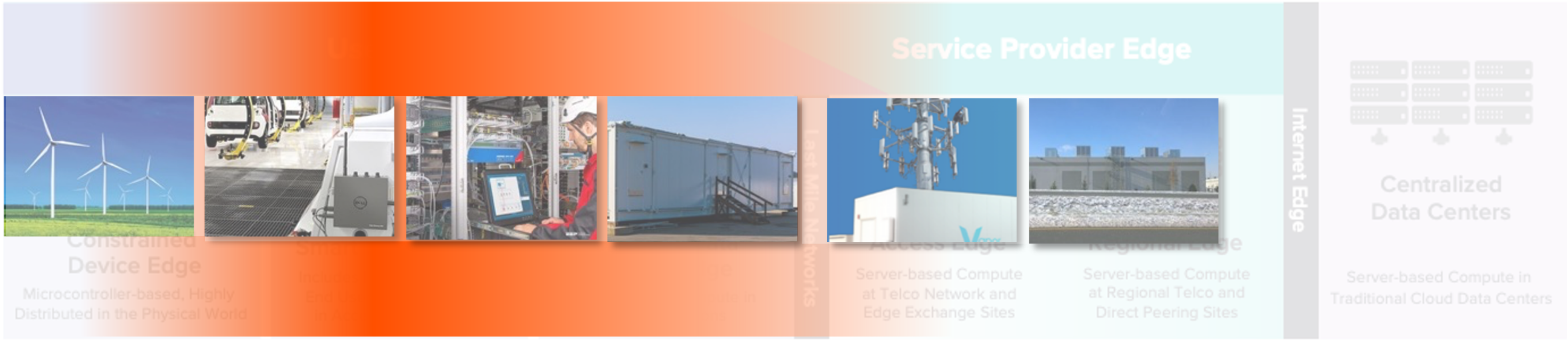


- “Confidence” Era
- Interconnected Ecosystems
- Ambient Computing

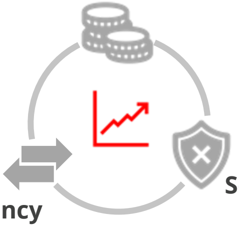
ZEDEDA

The Edge is the Last Cloud to Build

Field Devices/Assets/Users — **Distributed Edge** — **Cloud Edge** — **Centralized Cloud**


Service Provider Edge
Constrained Device Edge
Microcontroller-based, Highly Distributed in the Physical World
Last Mile Networks
Access Edge
Server-based Compute at Telco Network and Edge Exchange Sites
Regional Edge
Server-based Compute at Regional Telco and Direct Peering Sites
Internet Edge
Centralized Data Centers
Server-based Compute in Traditional Cloud Data Centers

Source: LF Edge June 2020 taxonomy white paper



Bandwidth Cost

Latency

Security / Privacy

IoT

AI

5G/CPE

Security

The Distributed Edge Solves Myriad Business Problems

Predictive Analytics

Wireline Analytics

Industrial Network Threat Detection

Smart Industrial Machines

AGV and Autonomous Drones

Tactical Edge

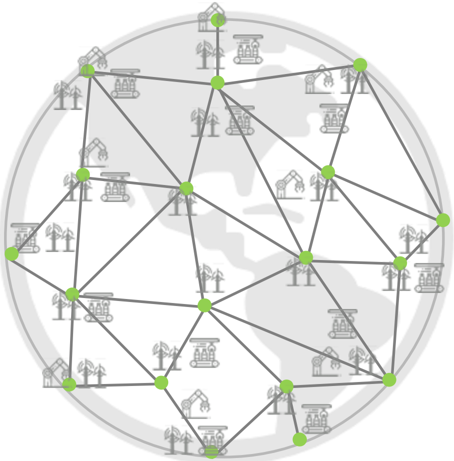
CLOUD
UAS/DRONE
COMMAND POST
TACTICAL VEHICLE
SQUIRE
DELL EMC

The Distributed Edge Has Unique Challenges

- **Diversity of hardware, software and skill sets**
  - New edge infrastructure deployed into legacy environments
  - Lack of autonomous and remote orchestration
  - Mix of skill sets (OT and IT) in the field

- **New security threat vectors**
  - Remote non-trustable networks
  - No physical or cyber security perimeter in the edge
  - No centralized pane of glass for visibility & remediation

- **Unprecedented scale of nodes**
  - Geographically-dispersed locations
  - High cost for field deployment and maintenance
  - DC solutions are resource-intensive and not priced for this scale



The Distributed Edge Needs Orchestration

Securing Industrial IoT and Distributed Edge Computing Solutions

Key Priorities

OT

Priorities

Availability
Integrity
Confidentiality

Top Concerns

Uptime and Safety

At Risk

Immediate loss of production and/or life

IT

Priorities

Confidentiality
Integrity
Availability

Top Concerns

Security, Governance and Compliance

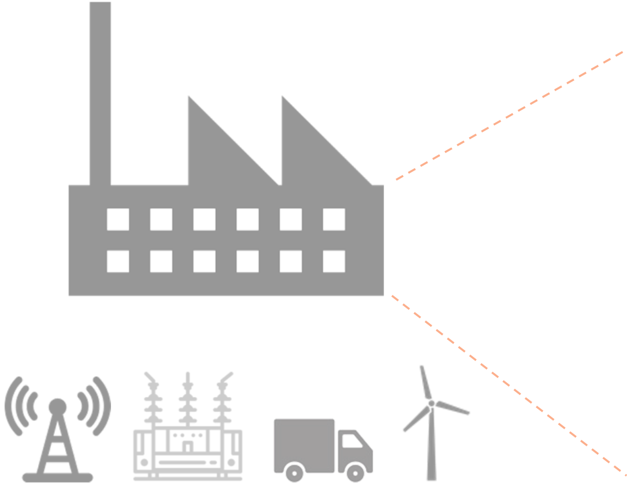
At Risk

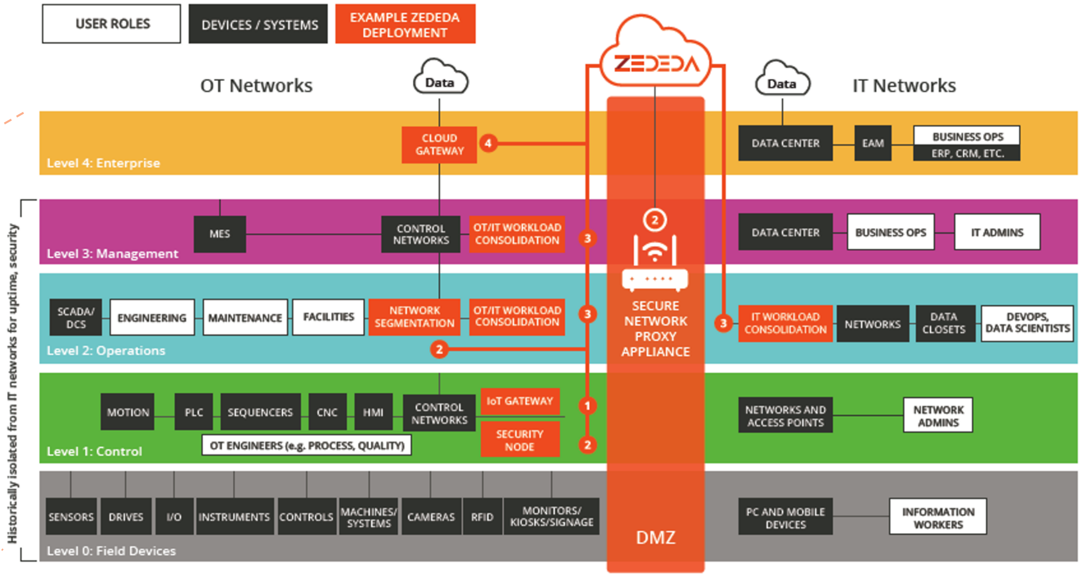
Data/IP loss, playing out over long periods of time and at great scale

Common Edge Deployment Patterns

Use Cases:

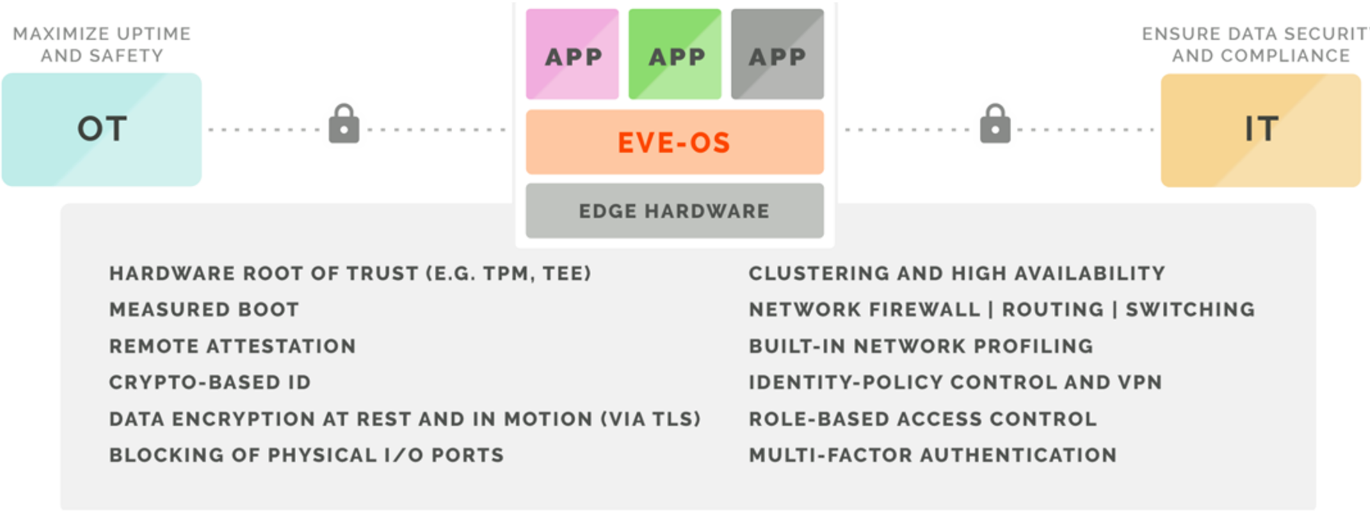
1. **IoT Gateways**
   Data ingestion, normalization and analytics
2. **Security Nodes**
   Root of trust, network segmentation, OT/IT protocol inspection, etc.
3. **Workload Consolidation**
   Single and clustered for SCADA, HMI, Historian, Edge AI, etc.
4. **Cloud Edge Gateways**
   e.g. NFV, Firewall, CPE, Private 5G





Q: Should I secure the data, network or node?

A: All of the above, with defense in depth.



MAXIMIZE UPTIME AND SAFETY

OT

APP

APP

APP

EVE-OS

EDGE HARDWARE

ENSURE DATA SECURITY AND COMPLIANCE

IT

- HARDWARE ROOT OF TRUST (E.G. TPM, TEE)
- MEASURED BOOT
- REMOTE ATTESTATION
- CRYPTO-BASED ID
- DATA ENCRYPTION AT REST AND IN MOTION (VIA TLS)
- BLOCKING OF PHYSICAL I/O PORTS
- CLUSTERING AND HIGH AVAILABILITY
- NETWORK FIREWALL | ROUTING | SWITCHING
- BUILT-IN NETWORK PROFILING
- IDENTITY-POLICY CONTROL AND VPN
- ROLE-BASED ACCESS CONTROL
- MULTI-FACTOR AUTHENTICATION

ZEDEDA

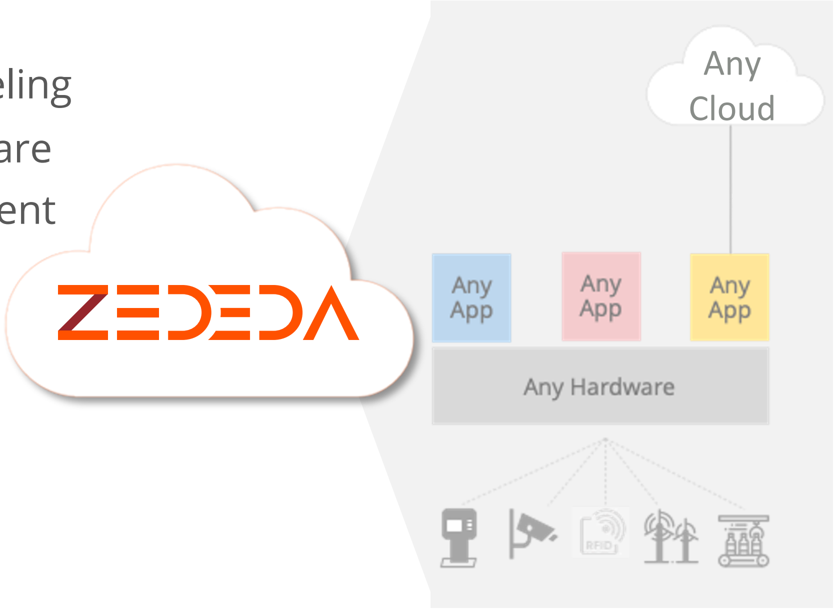
Orchestration for the Distributed Edge

Visibility, Control and Security for the Distributed Edge at Scale

Architected to Address the Unique Needs of the Distributed Edge

ZEDEDA is a cloud-based orchestration service built from the ground up for the Distributed Edge

- Subscription-based SaaS with option for white labeling
- Full remote orchestration of both apps and hardware
- Built on an open edge foundation (EVE-OS) to prevent lock-in



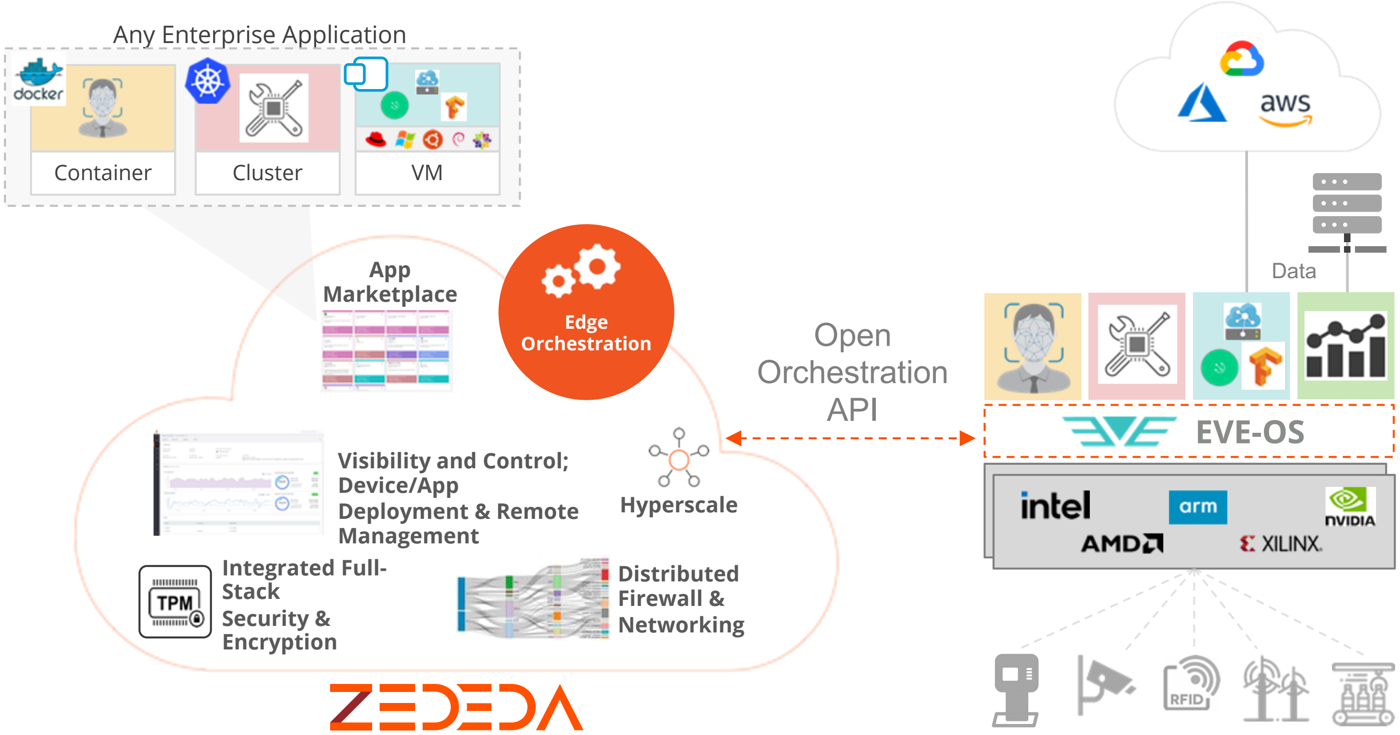
Customers can seamlessly

- Manage any app on any hardware at scale
- Enable a hybrid private/public cloud strategy
- Secure connected operations

The ZEDEDA Solution

ZEDCloud Subscription Service

EVE-OS for Edge Nodes (OSS)



Any Enterprise Application

Container

Cluster

VM

App Marketplace

Edge Orchestration

Visibility and Control; Device/App Deployment & Remote Management

Hyperscale

Integrated Full-Stack Security & Encryption

Distributed Firewall & Networking

Open Orchestration API

Data

EVE-OS

Any Cloud

Any On-Prem System

Any App
(VMs, Containers, Clusters)

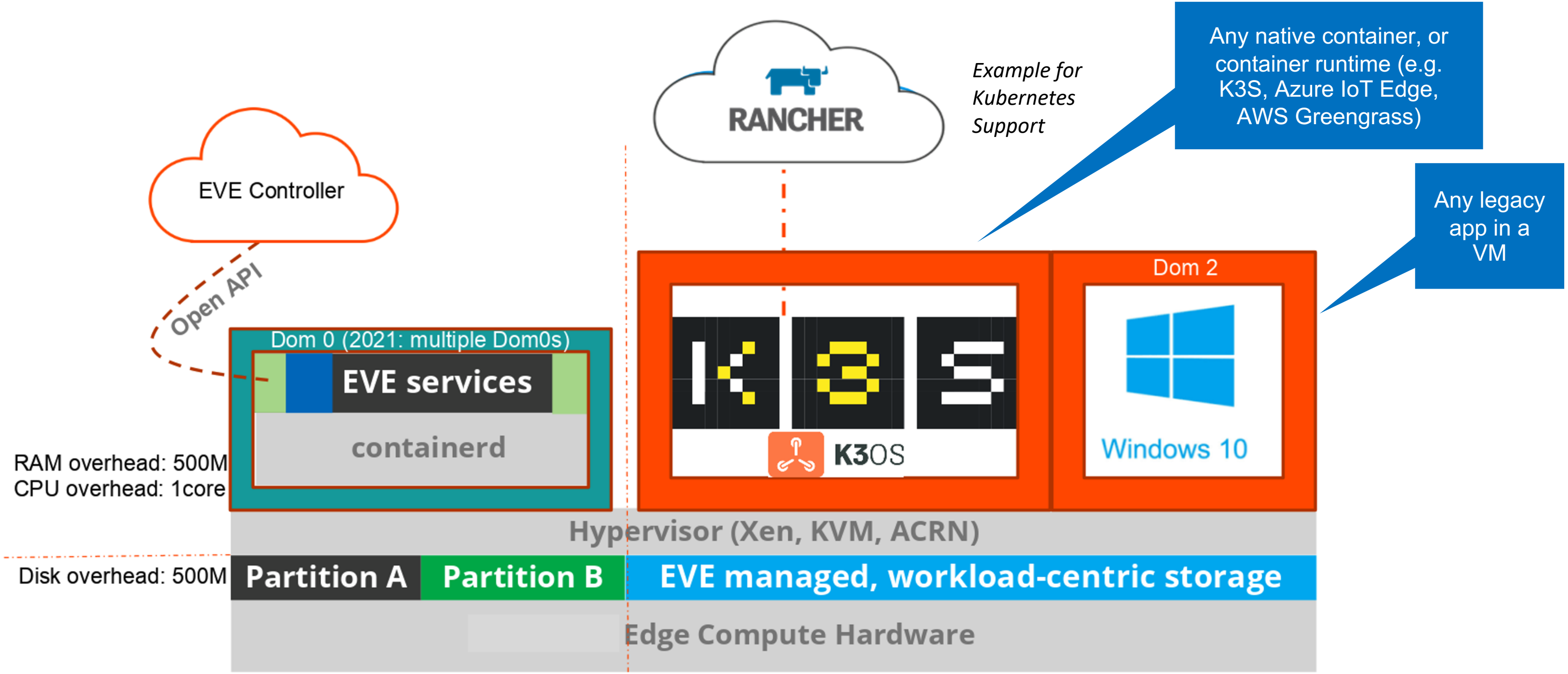
Open Source Foundation
(Part of Linux Foundation)

Any Hardware
(e.g. CPU, GPU, FPGA)

Any Edge
(Deploy Anywhere)

EVE-OS Architecture

Open source, developed within Project EVE in LF EDGE



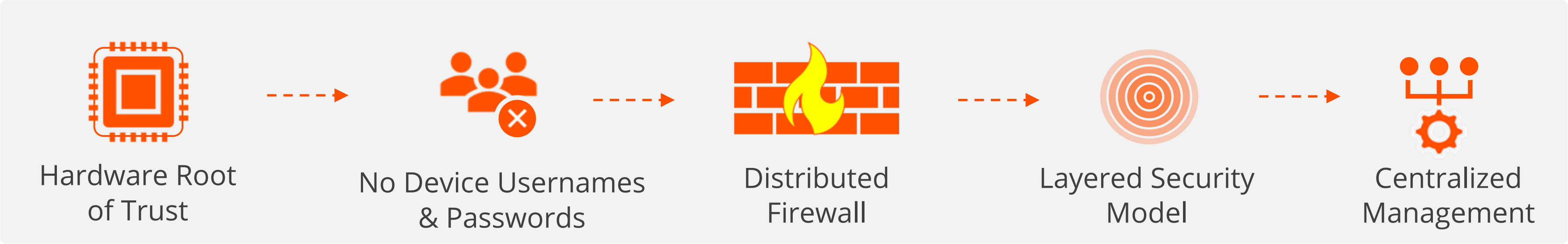
EVE Controller
Open API
RANCHER
Example for Kubernetes Support
Any native container, or container runtime (e.g. K3S, Azure IoT Edge, AWS Greengrass)
Any legacy app in a VM
Dom 0 (2021: multiple Dom0s)
EVE services
containerd
RAM overhead: 500M
CPU overhead: 1core
K3S
K3OS
Dom 2
Windows 10
Hypervisor (Xen, KVM, ACRN)
Disk overhead: 500M
Partition A
Partition B
EVE managed, workload-centric storage
Edge Compute Hardware

Growing Project EVE Community Adoption

- Approaching 60 unique contributors from ZEDEDA, Xilinx, Intel, GE Research, Timesys and more
- >50% not affiliated with ZEDEDA

Zero-trust Security Model

People, Process and Technology



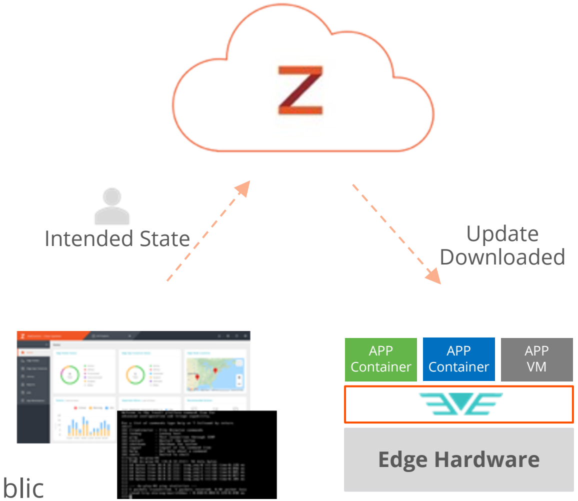
- People
  - Remove need for device usernames/passwords
  - Use cryptographic device identity and APIs for control
  - RBAC and multi-tenancy in cloud controller
- Processes - handle 7+ year lifetime at edge
  - Secure, scalable distribution of updates
  - Anomaly detection across edge fleet in controller

- Technologies for the IoT edge
  - Hardware root of trust (e.g., TPM)
  - Measured boot and remote attestation
  - Crypto-based identification (no device username/password)
  - Data encryption at rest and in-flight (TLS)
  - Distributed firewall for every app/node
  - Physical security—port isolation
  - Role-based access control (RBAC)

Simple Provisioning and Risk-Free Updates

Zero Touch Provisioning (ZTP)

- Connect power and network to both with EVE-OS installed
- EVE-IS creates a crypto-based ID based on root of trust (e.g. TPM)
- Node automatically logs into ZEDCloud where onboarding is completed
- All work can then be done remotely

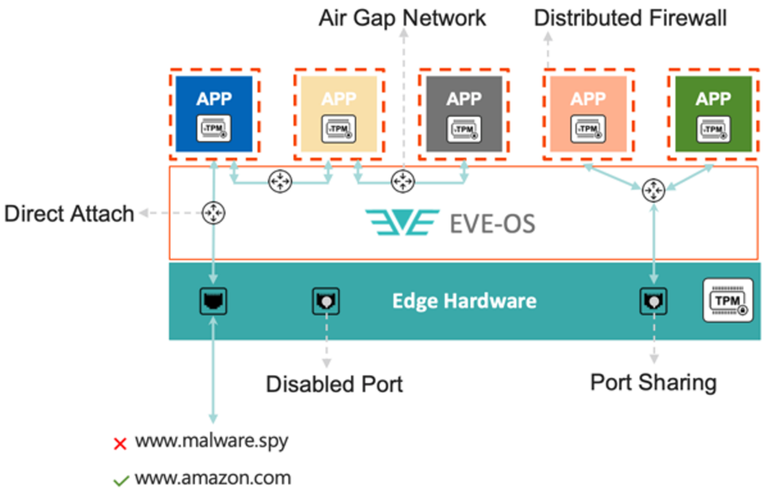


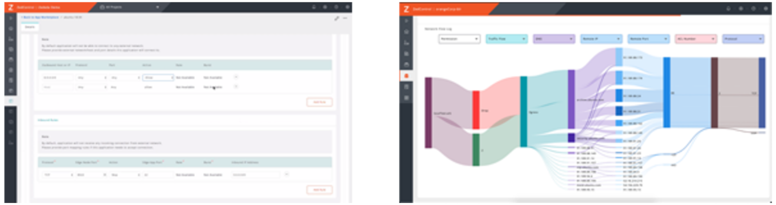
Flexible, Risk-Free Updates

- All components can be managed and updated individually
  - Update EVE-OS
  - Update guest OS
  - Push and update new apps (VMs and/or containers) from ZEDEDA App MArketplace (Public or Private)
- Sandboxing for updates
  - Roll-forward or roll-back images
  - Brick-free and risk-free
  - Group updates (project, location or organization)
- “Eventual consistency” model based on intended state to maximize uptime

Granular Software-defined Controls

- Ability to assign CPU and co-processors (e.g. GPU) to discrete apps
- Distributed Firewall & whitelist connectivity
  - Control east-west & north-south traffic
  - Create air gap & edge mesh networks
- Networking
  - Direct attach (IO Virtualization)
  - Port sharing (Network Virtualization)
  - Disable Ports
- Policy-based WAN control
  - Failover support (e.g. Ethernet, LTE, satellite and Wi-Fi)
  - Load balancing, policy control, policing and shaping
  - Traffic prioritization





Setting Policies and Visualizing Network Flows

Lanner

Intelligent Edge Computing

IoT Solutions

Company Overview

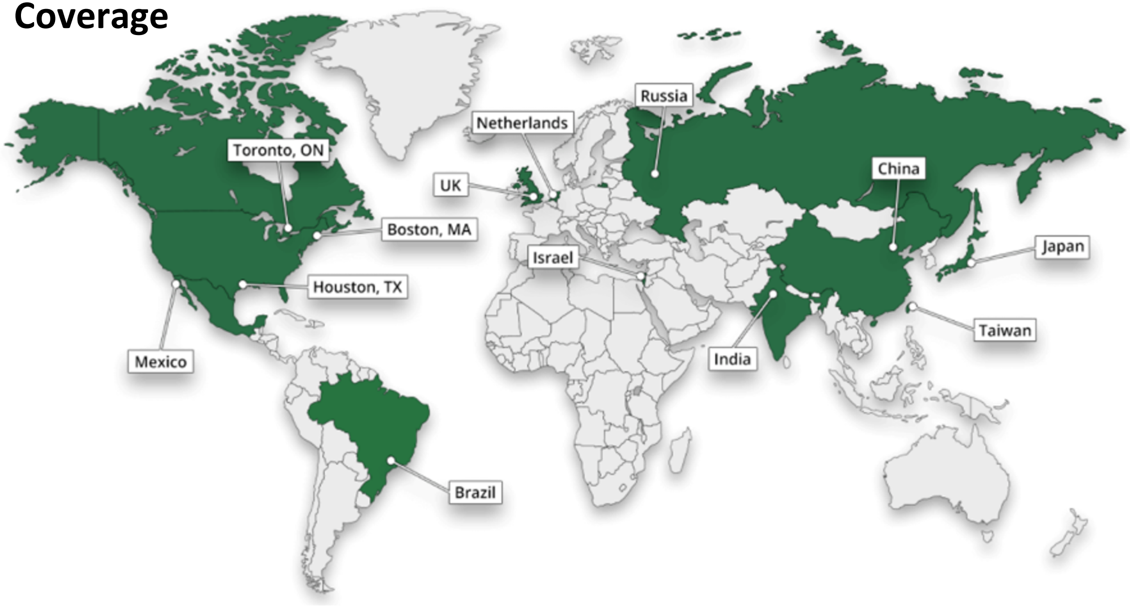
Highlights

- Founded 1986. Corporate office in Taipei, Taiwan
- 35 years experience manufacturing network & computing appliances
- Wide range of highly customizable & scalable HW platforms

Quality

- ISO 9001 (Quality)
- ISO 14001 (Environment)
- OHSAS 18001 (Health and Safety)
- IECQ QC 080000 (RoHS)
- ISO 28000 (Supply Chain Security)
- AEO (Authorized Economic Operators)
- TL9000 (Telecom Quality Management)
- ISO 27001 (Information Security) NEW!

Coverage



Domain Expertise

Telecom/Data Center Platforms

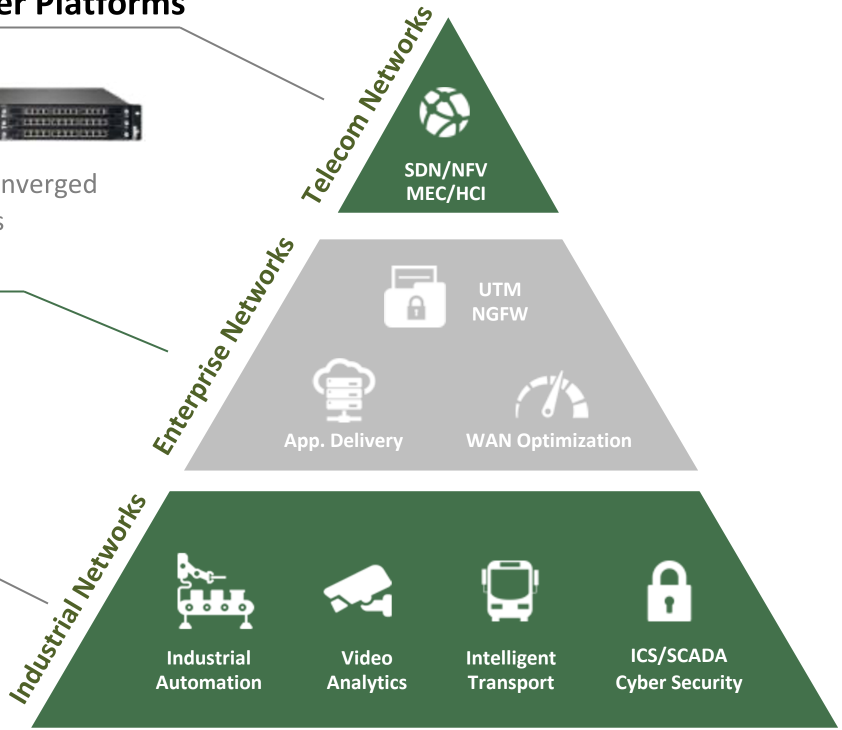
Modular Hyper Converged Appliances

Network Computing Appliances

Desktop, 1U and 2U Network Appliances

Intelligent Edge Computing Solutions

Rugged, Industrial Computing Platform



Telecom Networks

SDN/NFV
MEC/HCI

Enterprise Networks

UTM
NGFW

App. Delivery

WAN Optimization

Industrial Networks

Industrial Automation

Video Analytics

Intelligent Transport

ICS/SCADA Cyber Security

Market-Focused Edge Deployment Solutions

Industries

- Rich in GbE LAN & SFP
- LAN Bypass function
- Wide temperature
- Isolation

Power & Utilities

- IEC-61850-3 & IEEE1613
- Isolation
- Wide temperature
- Flexible I/O selection

Manufacturing

- Fanless IPC
- Small form factor
- Multiple I/Os
- PCIe expansion

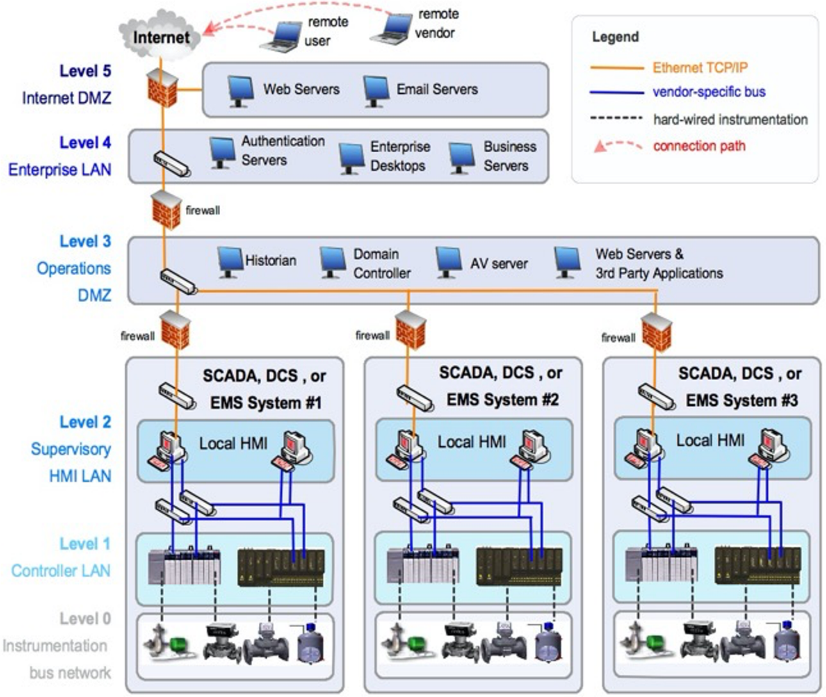
Smart Cities

- Video Platforms
- AI and analytics
- Fanless
- Multiple PoE

Transportation

- EN 50155, EN 45545, SAE & E-Mark certified
- Multiple PoE
- Wide temperature
- Wide voltage input

Industrial Edge Security



IT

OT

Common Best Practices

- **Silicon Root of Trust –** baseline defense
- **Encryption –** resting or traveling
- **Segmentation –** limit data security breaches
- **Access Control –** principle of least privilege
- **Visibility & Monitoring –** IDS & IPS

Security -Driven Industrial-grade Systems

Security Gateway – controllers, PLC, RTU, etc.

Plant Firewall – SCADA, HMI, historian, DCS, etc.

OT Firewall - MES, logistics, supply chain, etc.

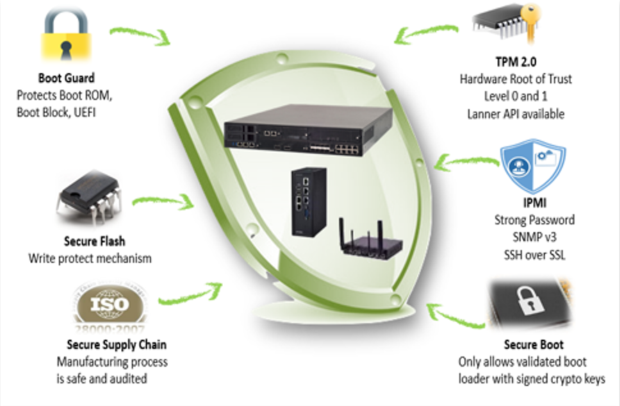
Enterprise Firewall – corporate office, HQ data center, etc.

Secured, Validated Hardware Platforms

Supply Chain Security Management ISO 28000:2007

Information Security Management System ISO 27001 Certified

Enable Faster Time-to-Value!



Boot Guard
Protects Boot ROM, Boot Block, UEFI

Secure Flash
Write protect mechanism

Secure Supply Chain
Manufacturing process is safe and audited

TPM 2.0
Hardware Root of Trust
Level 0 and 1
Lanner API available

IPMI
Strong Password
SNMP v3
SSH over SSL

Secure Boot
Only allows validated boot loader with signed crypto keys

Pre-configured and ready to ship HW models (Fast Availability – no MOQ!)

Security features based on our vast experience servicing global firewall and security leaders

TPM - Hardware Root of Trust

ISO 28000 & 27001 audited & certified manufacturing & delivery processes

Feature rich to meet specific application needs (LTE, Wi-Fi, PoE, accelerator cards, etc.)

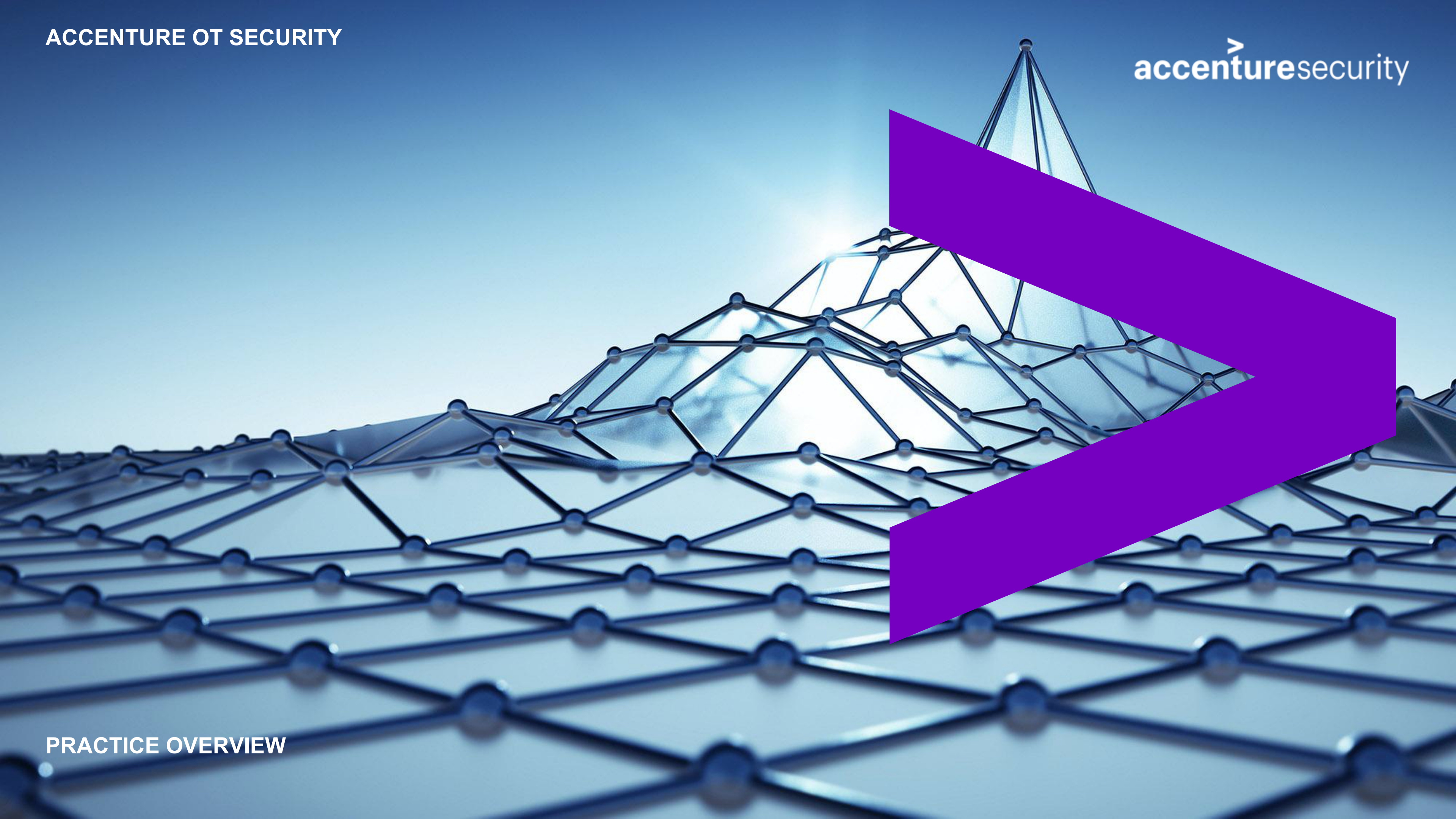
End to end Life Cycle Management (design, manufacturing and end-of-life)

Loaner Program to support pilot projects - demo units available in Lanner online store

Local support network – HUBs, engineering, project management & customer service

ACCENTURE OT SECURITY

accenturesecurity



PRACTICE OVERVIEW

ACCENTURE OT SECURITY

OUR CURRENT OT SECURITY PRACTICE

7500+

SECURITY PROFESSIONALS

1000 +

PLANT OPERATIONS PROFESSIONALS

200+

DEDICATED OT SECURITY PROFESSIONALS

Other Groups with OT Security Capabilities

- Digital
  - Industry X
- Operations
  - MSS Teams
  - Telecom/Network Teams

NETWORK

VENDOR AGNOSTIC, VENDOR KNOWLEDGEABLE

- Honeywell
- ABB
- Yokogawa
- Emerson
- GE
- Rockwell Automation
- Nozomi Networks

- Emerson
- Yokogawa
- Siemens
- OSIsoft
- Schneider
- SEL
- SecurityMatters

OUR VISION

Global OT leader, with deep and unique specialization, end-to-end capabilities and real-time innovation in the field

THINKING DIFFERENTLY ABOUT OT SECURITY

1

2

3

UNIQUE SPECIALIZATION

Unmatched industry and business expertise to create end-to-end, transferable, industry-tailored solutions in changing markets

RESOURCES

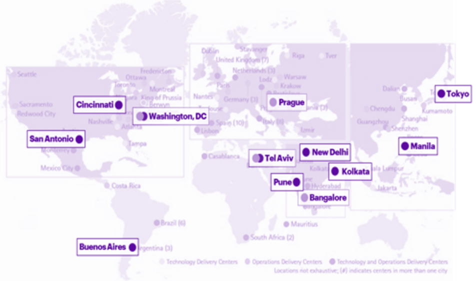
PRODUCTS

HEALTH & PUBLIC SERVICE

COMMUNICATIONS MEDIA & TECH

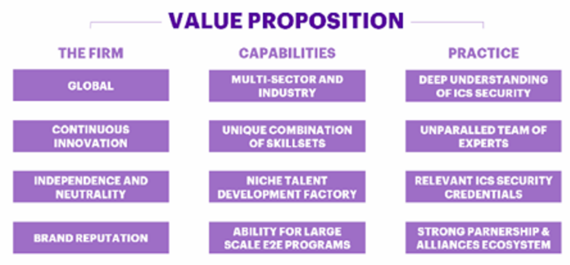
GLOBAL, END-TO-END CAPABILITIES

Delivered seamlessly, on-demand, wherever & whenever our clients need us (i.e. Remote access to our Cyber Fusion Centers & Cyber Ranges)


Cincinnati
Washington, DC
San Antonio
Prague
Tokyo
Manila
New Delhi
Tel Aviv
Kolkata
Pune
Bangalore
Buenos Aires
Technology Delivery Centers
Operations Delivery Centers
Technology and Operations Delivery Centers
Locations not exhaustive; (#) indicates centers in more than one city

CONTINUOUS INNOVATION & DELIVERY

Trusted partner leading the most innovative initiatives in OT Security



VALUE PROPOSITION

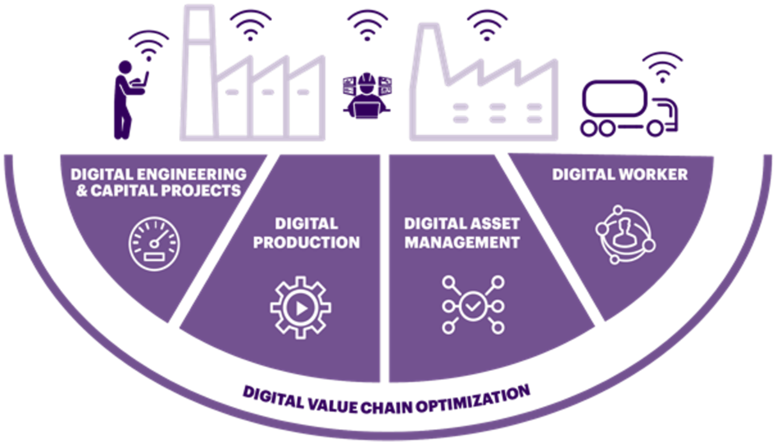
THE FIRM	CAPABILITIES	PRACTICE
GLOBAL	MULTI-SECTOR AND INDUSTRY	DEEP UNDERSTANDING OF ICS SECURITY
CONTINUOUS INNOVATION	UNIQUE COMBINATION OF SKILLSETS	UNPARALLED TEAM OF EXPERTS
INDEPENDENCE AND NEUTRALITY	NICHE TALENT DEVELOPMENT FACTORY	RELEVANT ICS SECURITY CREDENTIALS
BRAND REPUTATION	ABILITY FOR LARGE SCALE E2E PROGRAMS	STRONG PARNERSHIP & ALLIANCES ECOSYSTEM

People

OT SECURITY CLIENT PERSPECTIVES

CHALLENGES

- EVERY CRITICAL INFRASTRUCTURE CLIENT IS INVESTING AT THE SAME TIME
- GLOBAL TALENT SHORTAGE
- COMPLEX ASSET DISCOVERY & VISIBILITY ISSUES
- IOT – GROWING ATTACK SURFACE

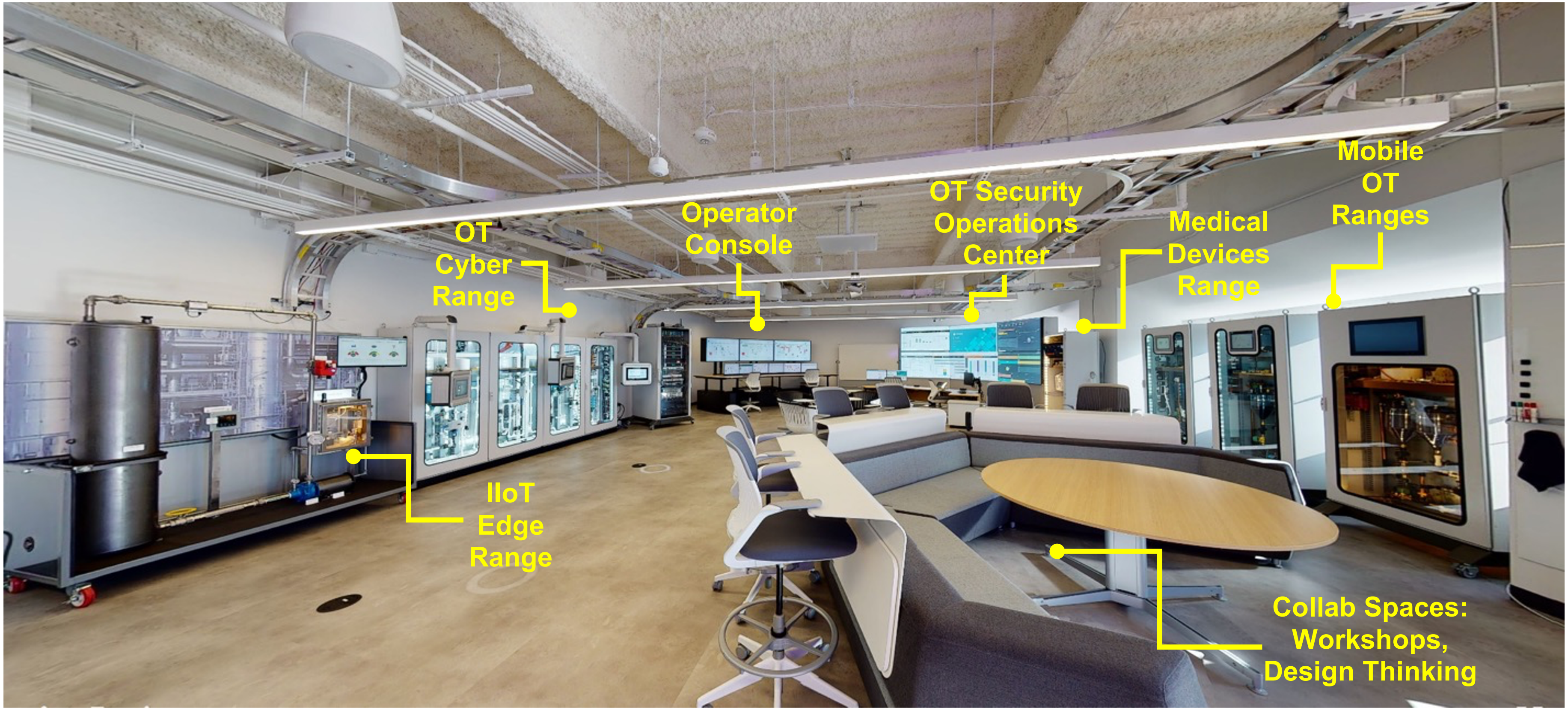

DIGITAL ENGINEERING & CAPITAL PROJECTS
DIGITAL PRODUCTION
DIGITAL ASSET MANAGEMENT
DIGITAL WORKER
DIGITAL VALUE CHAIN OPTIMIZATION

TRENDS

- SECURITY + RELIABILITY = ASSET HEALTH
- SECURITY AS BUSINESS ENABLER
- MANAGED OT SECURITY
- OT IR AND OT THREAT HUNTING

HOUSTON OT CYBER FUSION CENTER

Panoramic photo of the Houston OT CFC Open Lab Layout



OT CYBER FUSION CENTER

Advancing Security for Industrial Control Systems

> a risk-free setting to ***innovate, stage and test*** the ***security solutions*** that protect industrial control systems (ICS) and related assets from cyber attacks

> ***one-stop shop for the creation and testing*** of effective security for people and operations.

> Combines ***advanced OT engineering, vulnerability and malware analysis with threat intelligence*** and security operations

PARTNERS

SIEMENS, ForeScout, Honeywell, NOZOMI NETWORKS, CISCO, paloalto NETWORKS, splunk>, Microsoft, EMERSON

OT Cyber Range
- Test, learn and assess equipment in a safe, realistic, battle-proven setting.

OT Operator Console
- View and control O&G processes from the field.

OT Security Operations Center
- Centrally supervise, detect and mitigate attacks.

ICS / OT Staging Lab
- Ideal for enhancing and testing OT capabilities.

OT Incident Response Equipment
- Specialized tools used by OT experts for response, remediation and recovery.

iDefense OT Threat Intelligence
- Access to actionable OT security intelligence (e.g. Siemens, Rockwell) through the IntelGraph platform.

OT Design-Thinking Lab
- A safe environment to develop OT cybersecurity strategies and plans.

OT IIoT Edge Sensor to Cloud
- AI-Driven Energy and Reliability Optimization of Fixed Speed Motors. Experience Device onboarding, management, integrations, and security.

DEFINE > DEPLOY > SUSTAIN > PROTECT

IIOT EDGE SOLUTION

Sensor to cloud AI-driven optimization and automation for fixed speed motors:

- Advances pump system reliability
- Reduces energy consumption ~50%
- Drives down CO2 emissions

250 MachineEdge units
(50 hp consumed)

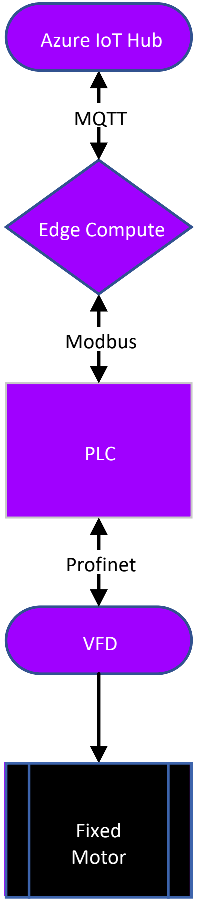
One plant. Every year.

$3,250,000
Energy Cost Savings (USD)

36,000 tons
Reduction in CO2 Emissions

IIoT Edge Experience ~2 hours

- Device onboarding
- Device management
- Azure IoT HUB Integrations
- Zero Trust Security



OT SECURITY CYBER RANGE EVOLUTION

Accenture’s global footprint of centers bring together or **fuses** our **end-to-end security** capabilities spanning our entire business, giving clients direct and **one stop access** to our strategic, transformational and operational security services

ESSEN

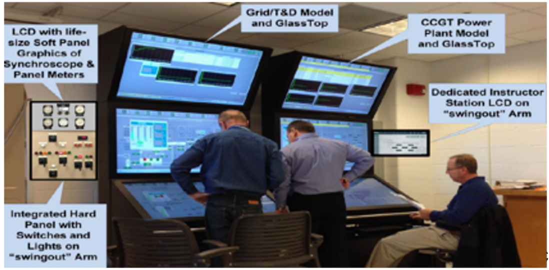
UTILITIES T&D RANGE

HOUSTON

OIL & GAS RANGE
CYBER FUSION CENTER

WASHINGTON D.C.

FLAGSHIP CYBER FUSION CENT
UTILITIES PWR GEN
AND T&D RANGE


LCD with life-size Soft Panel Graphics of Synchroscope & Panel Meters
Grid/T&D Model and GlassTop
CCGT Power Plant Model and GlassTop
Dedicated Instructor Station LCD on "swingout" Arm
Integrated Hard Panel with Switches and Lights on "swingout" Arm

BILBAO

UTILITIES RENEWABLES RANGE

WHAT WE OFFER FOR OT SECURITY

In combining our cybersecurity expertise with OT best practices, we are able to provide the following set of services to protect the availability, integrity and confidentiality of an organization's critical systems

DEFINE

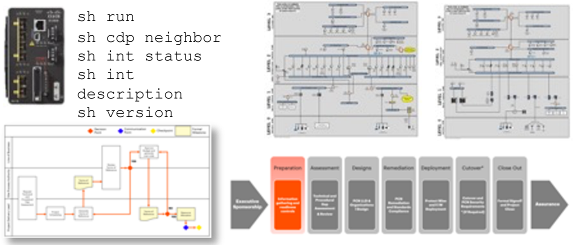
- OT Security Program Development
- OT Security Governance & Strategy
- OT Cyber Security Capability Maturity Diagnostic
- OT Security Technology Evaluation
- OT Security Risk Assessments
- IIoT Edge Architectures and Ecosystems
- CORE & CISO Academy for OT

Proven OT Security Practice

DEPLOY

- OT Security Controls Design & Implementation
- OT Security Anomaly Detection and Asset Management Technology Deployment
- OT Network Security Re-architecture
- Remote Assistant via Augmented Reality (RealWear) for Site Visits
- IIoT Edge Solutions and Security

OT Architecture Design & Deployment Playbooks



```
sh run
sh cdp neighbor
sh int status
sh int
description
sh version
```

SUSTAIN

- OT SOC Transformation & Automation
- OT Managed Security Services
- OT Threat Intelligence & Vulnerability Research
- OT Incident Response
- Secure IOT Cloud Capabilities
- OT IAM Capabilities

OT Cyber Labs for Rapid Security Testing

EDGE/IOT TIER – SECURITY REFERENCE ARCHITECTURE

Physical

🟦 Perimeter Protection	🟦 Device Tracking
🟦 Physical Intrusion Detection	🟦 Tamper Prevention & Detection

Network & Endpoint

🟦 Firewall Protection	🟪 Secure Execution Environment
🟦 Firmware/Memory Attestation	🟪 Host NGFW/HIDS
🟦 Cryptographic Engine	
🟦 Secure Boot	

Application

🟪 Signed App Software	⬛ Secure M2M Service
🟪 Secure FOTA	⬛ Sandboxing
🟪 Secure Development Tools	⬛ API Security
🟪 SDLC Security	

Digital Identity

🟦 Unique Device Identifier	⬛ Edge Identity Management
🟪 Edge Identity Integration	

Data Privacy & Protection

🟪 Secure Storage	🟪 Data In Transit protection
🟪 Data Encryption at Rest	⬛ Certificates and Key Management

Cyber

🟪 Logging	⬛ Security Management
⬛ Security Monitoring	

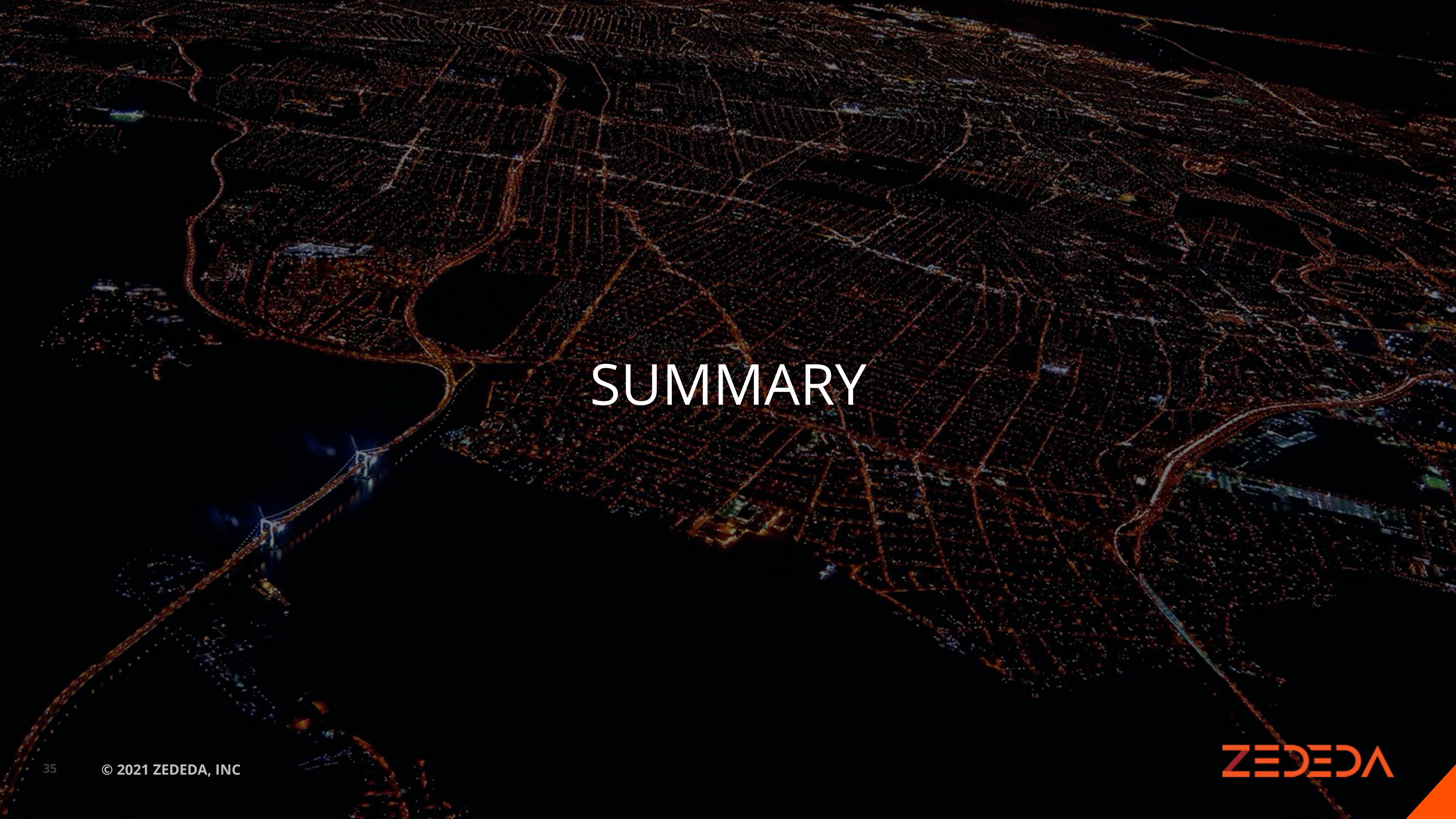
Ultra constrained devices are limited to only supporting basic security capabilities. Ultra constrained devices often rely on high end devices to communicate and enhance security.

Edge constrained devices have more computational power and implicitly optimized security capabilities than ultra constrained ones. This level of embedded security usually implies that manufacturers include dedicated security processor in the architecture of their MCUs/MPUs.

High end devices do not suffer from resources constraints. These type of devices contain advanced security capabilities and/or support to enable add-on security mechanisms via specialized platforms deployed in the Edge Tier. Devices in this category (e.g. IoT gateway) are often times used to enable or enhance security for resource-constrained devices.

Legend

- 🟦 Basic Security Capabilities
- 🟪 Optimized Security Capabilities
- ⬛ Advanced Security Capabilities



SUMMARY

It Takes a Village

Examples of additional ecosystem partnerships to round out our robust security offering

NOZOMI NETWORKS

CYBERX

JUNIPER NETWORKS

OT Network Threat Detection

Virtual Firewall

Summary

- Solutions must balance OT and IT needs, practice defense in depth and prioritize usability
- Together we provide an industry-leading, comprehensive solution for IoT/IIoT/ICS security
- Built on a modular architecture to provide choice in hardware and software
- Open foundation increases transparency and prevents lock-in

Thank You!

Q&A

ZEDEDA accenturesecurity Lanner