EnterpriseWeb®

Enabling Telco Cloud & Edge with CAMARA

Dave Duggal
Founder and CEO

William Malyk
Chief System Architect

Date: Jan 23, 2024
Time: 9AM PT / 11AM ET

intel. network builders partner

EnterpriseWeb®

Enabling Dev-centric Networking with CAMARA APIs

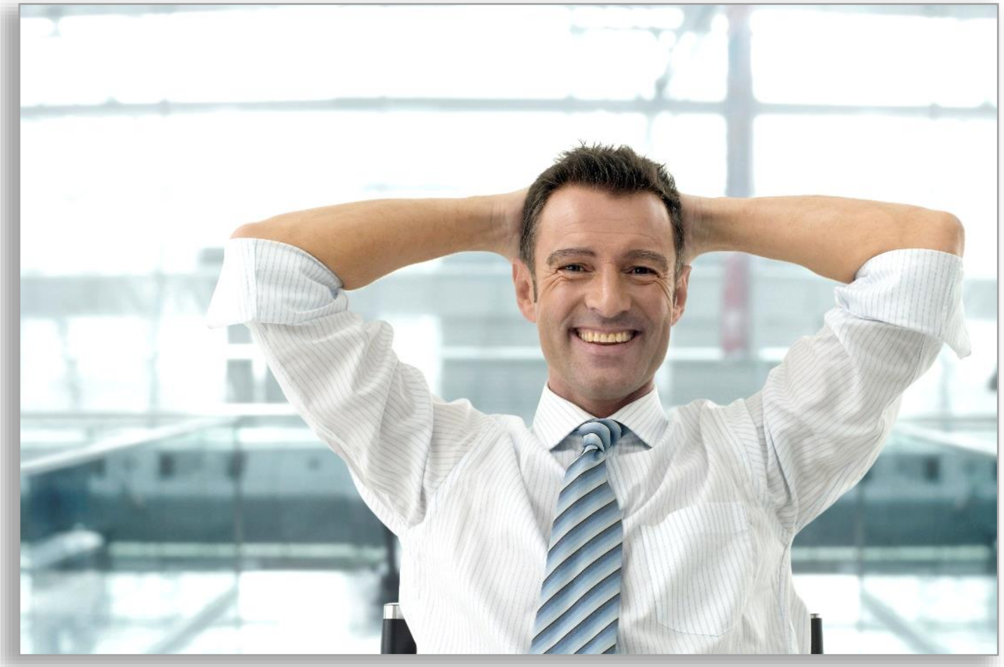
CAMARA APIs expose network data and controls so Developers can build network-aware business apps that dynamically and continuously optimize latency, bandwidth and resources.

The Telecom industry is defining CAMARA APIs for discrete use-cases, but there is no common model or shared library to support their implementations.

EnterpriseWeb platform provides a declarative abstraction across the set of CAMARA APIs along with integration services in order to:

1. Provide a consistent developer experience
2. Simplify and automate developer tasks
3. Centralize management

CAMARA APIs enabled!



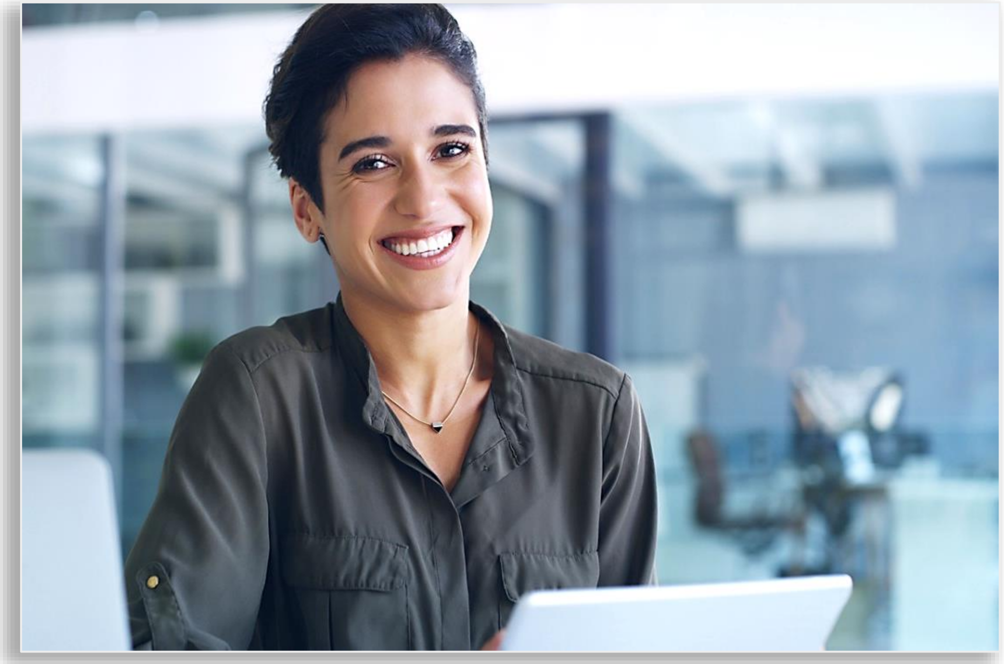
Intel, the Intel logo, and FlexRAN, OpenVINO, and the OpenVINO logo are trademarks of Intel Corporation or its subsidiaries.

EnterpriseWeb®

Securing Dev-centric Networking with CAMARA APIs

Exposing network data and controls to the Developer community opens the network to a new set of exploits.

There is no standard security model for CAMARA APIs that covers the end-to-end scope of the interfaces.



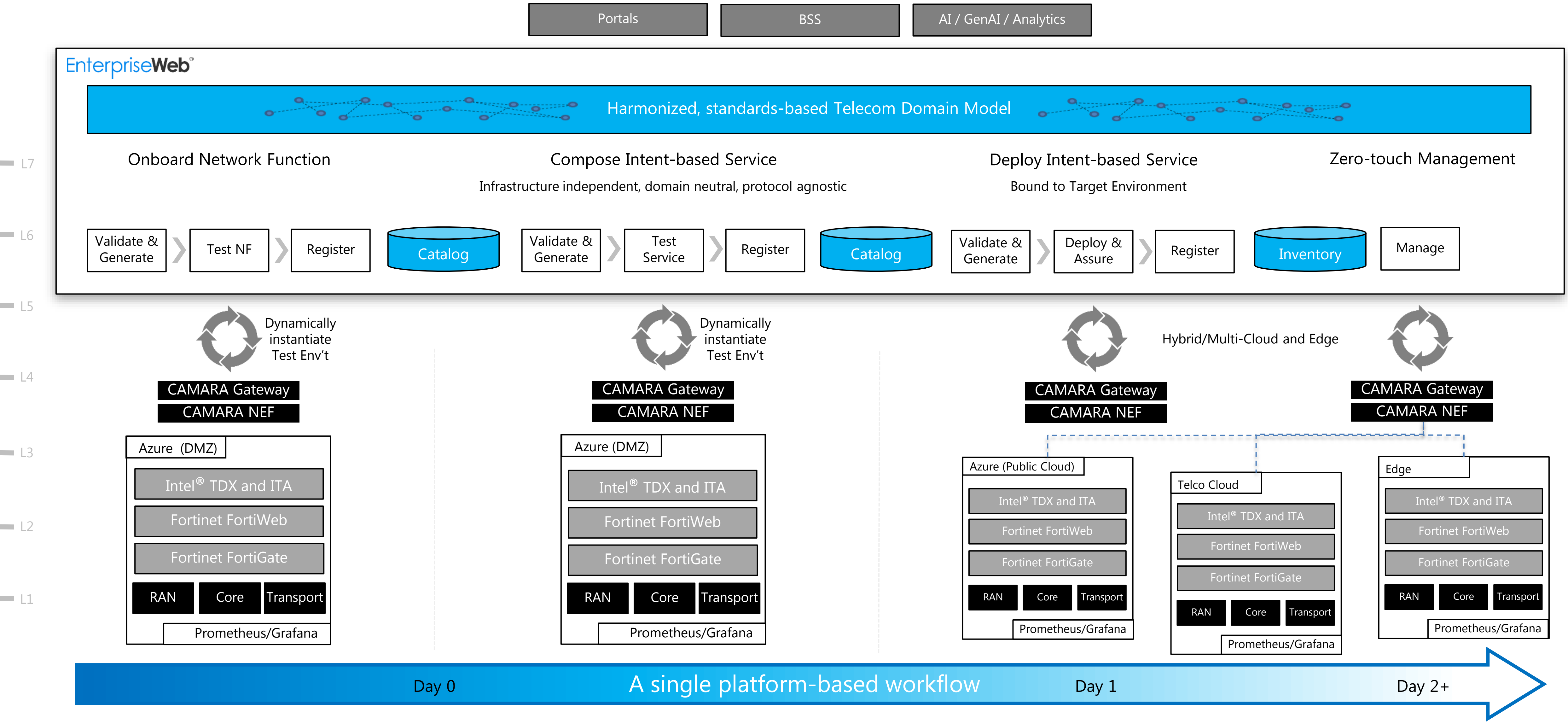
EnterpriseWeb's integrated solution with endpoint to infrastructure security closes the gaps to protect both the business applications and the Telco networks.

1) Intel® Trust Domain Extensions assures security of data in-motion, at-rest and in-memory
2) Fortinet FortiWeb provides application security
3) Fortinet FortiGate provides a Next Generation Firewall

CAMARA APIs secured!

Intel, the Intel logo, and FlexRAN, OpenVINO, and the OpenVINO logo are trademarks of Intel Corporation or its subsidiaries.

Unified Platform for CAMARA APIs



Portals

BSS

AI / GenAI / Analytics

EnterpriseWeb®

Harmonized, standards-based Telecom Domain Model

Onboard Network Function

Compose Intent-based Service

Infrastructure independent, domain neutral, protocol agnostic

Deploy Intent-based Service

Bound to Target Environment

Zero-touch Management

Validate & Generate › Test NF › Register › Catalog

Validate & Generate › Test Service › Register › Catalog

Validate & Generate › Deploy & Assure › Register › Inventory

Manage

Dynamically instantiate Test Env't

CAMARA Gateway

CAMARA NEF

Azure (DMZ)

Intel® TDX and ITA

Fortinet FortiWeb

Fortinet FortiGate

RAN | Core | Transport

Prometheus/Grafana

Dynamically instantiate Test Env't

CAMARA Gateway

CAMARA NEF

Azure (DMZ)

Intel® TDX and ITA

Fortinet FortiWeb

Fortinet FortiGate

RAN | Core | Transport

Prometheus/Grafana

Hybrid/Multi-Cloud and Edge

CAMARA Gateway

CAMARA NEF

Azure (Public Cloud)

Intel® TDX and ITA

Fortinet FortiWeb

Fortinet FortiGate

RAN | Core | Transport

Prometheus/Grafana

Telco Cloud

Intel® TDX and ITA

Fortinet FortiWeb

Fortinet FortiGate

RAN | Core | Transport

Prometheus/Grafana

CAMARA Gateway

CAMARA NEF

Edge

Intel® TDX and ITA

Fortinet FortiWeb

Fortinet FortiGate

RAN | Core | Transport

Prometheus/Grafana

Day 0

A single platform-based workflow

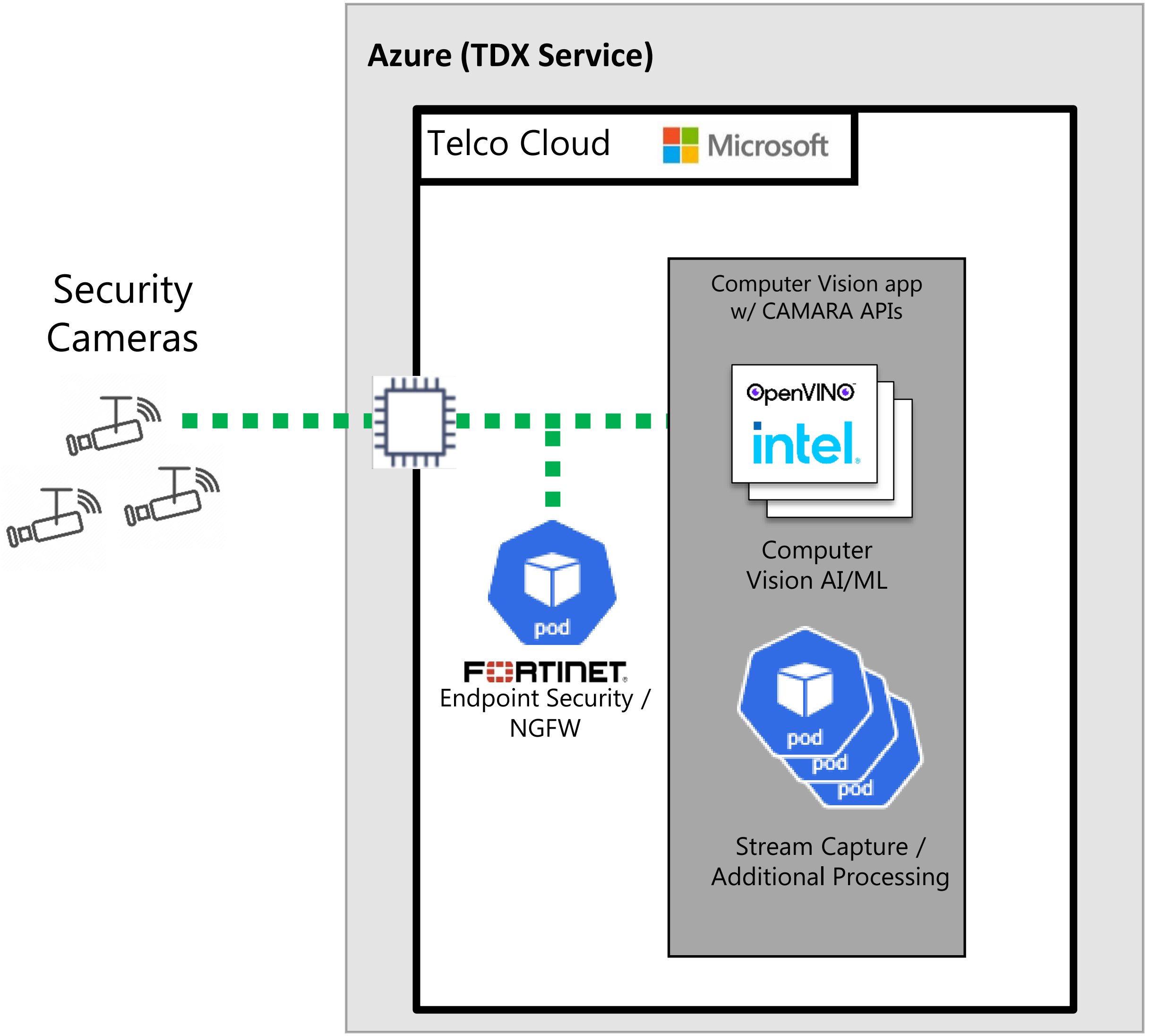
Day 1

Day 2+

EnterpriseWeb®

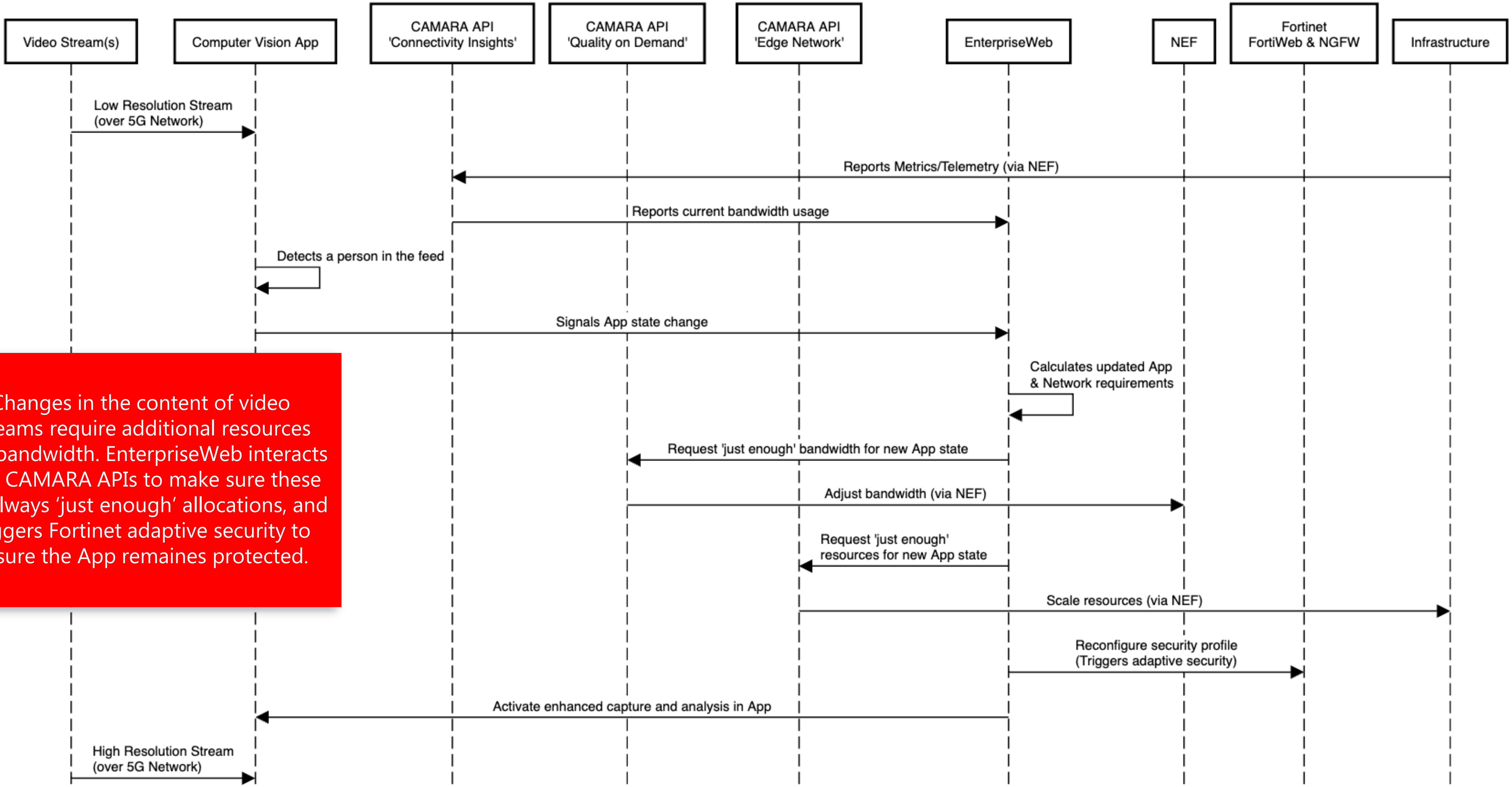
Computer Vision Security over 5G Network Use Case

- Multiple security cameras send low resolution feeds to the monitoring app over a 5G connection
- Using Intel® Distribution of OpenVINO™ Toolkit object detection AI monitors those feeds, when a person (or other object of interest) is detected, it signals the application to:
  - Activate high resolution feeds from the cameras
  - Activate stream capture capabilities within the app
  - Perform additional processing of images
- The new capabilities are intelligently activated / deactivated for each feed in real time, bandwidth and resources are adjusted via CAMARA APIs to ensure optimized (just enough) consumption, and adaptive security is triggered to ensure the app remains protected
- The monitoring app is deployed to an AKS cluster running an Azure's Intel® TDX service, providing confidential computing for the app



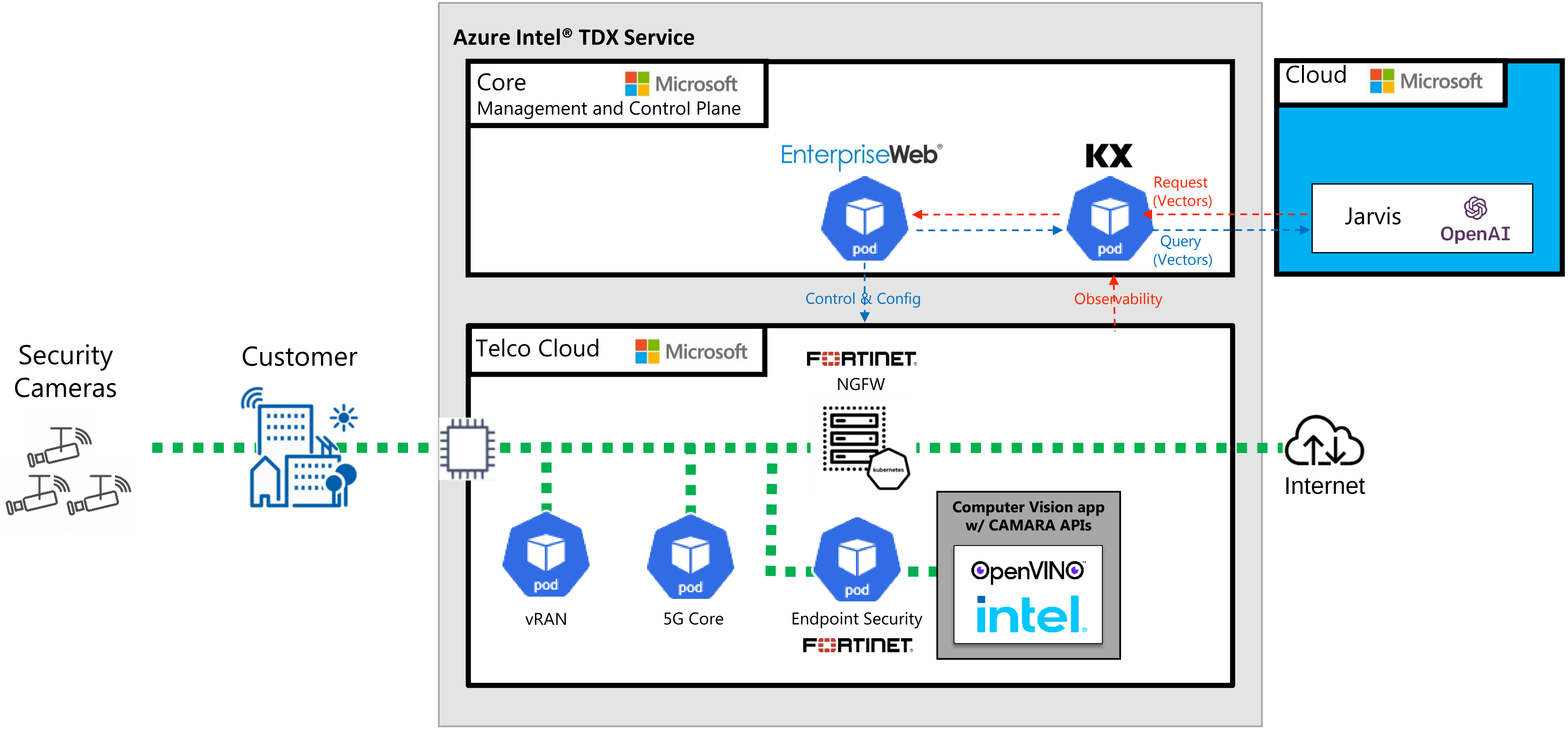
EnterpriseWeb®

Use-case: Sequence Diagram


Video Stream(s)
Computer Vision App
CAMARA API 'Connectivity Insights'
CAMARA API 'Quality on Demand'
CAMARA API 'Edge Network'
EnterpriseWeb
NEF
Fortinet FortiWeb & NGFW
Infrastructure
Low Resolution Stream (over 5G Network)
Reports Metrics/Telemetry (via NEF)
Reports current bandwidth usage
Detects a person in the feed
Signals App state change
Calculates updated App & Network requirements
Request 'just enough' bandwidth for new App state
Adjust bandwidth (via NEF)
Request 'just enough' resources for new App state
Scale resources (via NEF)
Reconfigure security profile (Triggers adaptive security)
Activate enhanced capture and analysis in App
High Resolution Stream (over 5G Network)

Changes in the content of video streams require additional resources and bandwidth. EnterpriseWeb interacts with CAMARA APIs to make sure these are always 'just enough' allocations, and triggers Fortinet adaptive security to ensure the App remaines protected.

Telco-grade Generative AI for Intent-based Automation



Demo Scope

Demo Prep

- An Intel® TDX secured AKS cluster is provisioned, configured and running in Azure to simulate the Telco Edge Cloud
- EnterpriseWeb CAMARA Gateway and EnterpriseWeb NEF deployed to Edge
- EnterpriseWeb End-to-End Orchestrator deployed to Core

Application Onboarding

Developer onboards the Computer Vision App (no-code)

1. Platform maps the app to its Graph, identifying the type of the object, auto-filling properties and generating standards-based interfaces
2. User configures policies for use of CAMARA APIs related to the app
3. Publish service to catalog for use in service composition

Design Environment

Declaratively compose enhanced Computer Vision App with Firewall as intent-based Network Service to be deployed at Telco Edge via CAMARA APIs

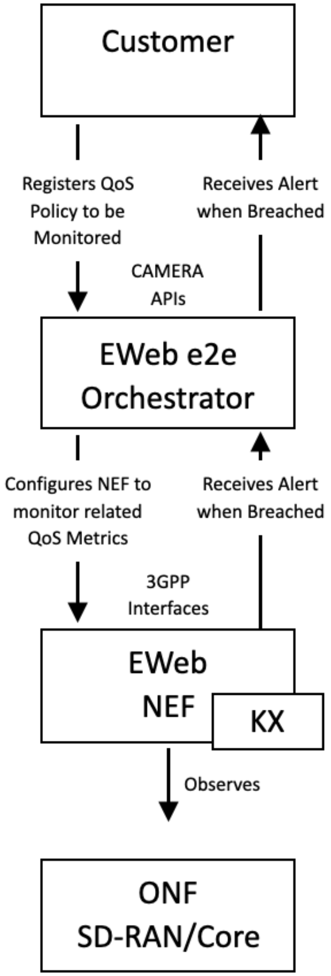
1. Model service graph, service chain, SLA and LCM policies
2. Platform generates deployment workflow along with K8 Operators for each element
3. Publish service to catalog / Expose API for ordering

Execution Environment

1. Day 1: Platform runtime binds to Telco Edge host via CAMARA APIs, executes deployment plan & handles all implementation details
2. Day 2: Platform runtime enforces declared policies, optimizing resource use ("just-enough") by continuously adjusting CAMARA APIs

Optimized "Just-enough" resources using CAMARA APIs

- Once the service is available, a CAMARA "Connectivity Insights" API is exposed northbound by the EnterpriseWeb e2e Orchestrator, allowing consumers to register to receive alerts when QoS policies are breached.
- The EnterpriseWeb e2e Orchestrator translates the intent of the CAMARA registrations into a set of interactions used to configure a NEF to send it alerts when associated QoS metrics pass the related thresholds. (In this case EnterpriseWeb is also supplying the NEF with independent scaling, using KX to aggregate metrics).
- When thresholds are breached, they are detected by the NEF, an alert is sent to the EnterpriseWeb e2e Orchestrator, which it then relays via the CAMARA API back to the consumer, who can then call additional CAMARA APIs (i.e., QoD) to continually adjust their bandwidth usage.



Customer
Registers QoS Policy to be Monitored
Receives Alert when Breached
CAMERA APIs
EWeb e2e Orchestrator
Configures NEF to monitor related QoS Metrics
Receives Alert when Breached
3GPP Interfaces
EWeb NEF
KX
Observes
ONF SD-RAN/Core

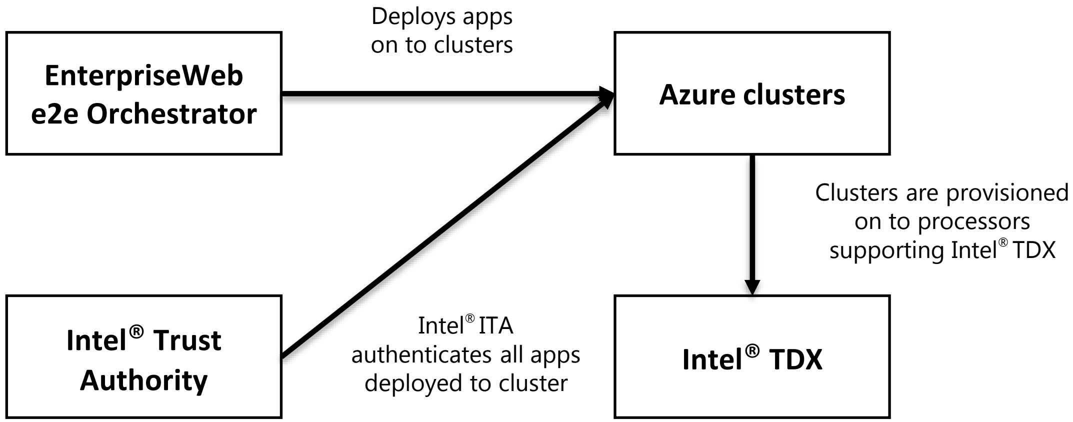
Changes in application state result in changes in network useage, which triggers QoS thresholds to be breached, that is detected by the NEF and alerts are sent via CAMARA APIs to the customer so they can adjust their usage in realtime, consuming “just enough” resources.

Intel TDX on Microsoft Azure

- Intel® Trust Domain Extensions provide isolation, confidentiality and integrity to the underlying compute resources on which the Telco Cloud AKS clusters are provisioned.

- Intel® Trust Authority verifies that all data is encrypted in-motion, at rest, and in-memory for all applications deployed to the Telco Cloud AKS clusters.

- EnterpriseWeb itself, along with all other solution components it provides (CAMARA Gateway, NEF, etc) <u>and</u> all applications / solution elements it deploys, all execute on Intel® Trust Authority verified Telco Cloud AKS clusters with the Intel® TDX service, providing end-to-end confidential computing.



EnterpriseWeb e2e Orchestrator
Deploys apps on to clusters
Azure clusters
Clusters are provisioned on to processors supporting Intel® TDX
Intel® Trust Authority
Intel® ITA authenticates all apps deployed to cluster
Intel® TDX

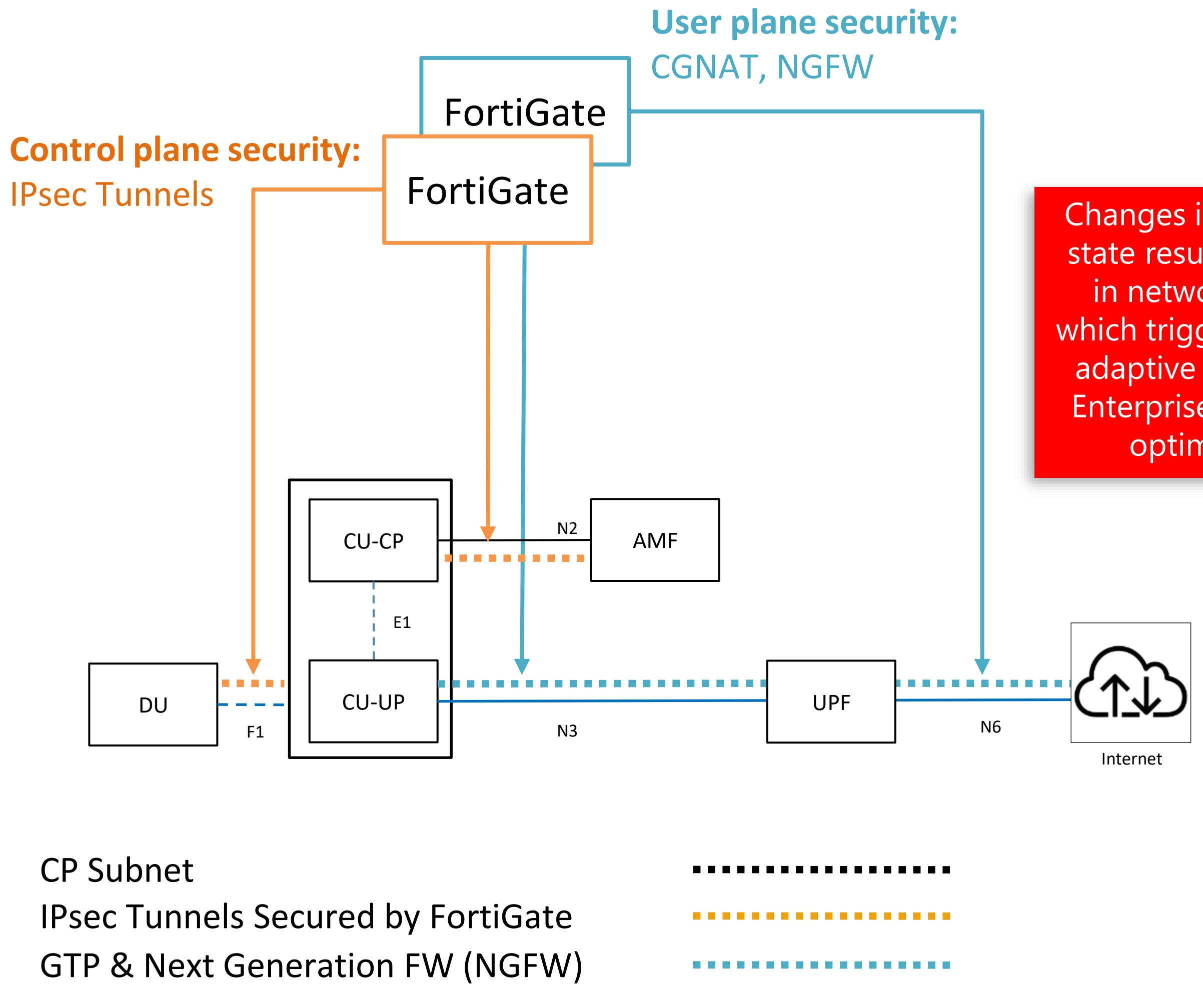
Intel, the Intel logo, and FlexRAN, OpenVINO, and the OpenVINO logo are trademarks of Intel Corporation or its subsidiaries.

EnterpriseWeb®

Adaptive Security for the Control & User Planes

Dynamic Security Configuration

- Identify assigned CP Subnet(s) via CNI Mapping (at time of initial deployment)
- For all Function / Component Pods and Containers identify virtual port assignments / IPs (translated from OpenShift APIs)
- Identify at SDN level IPsec Tunnels (Point-to-Point) between components (from underlying CNI, Service Mesh, ONOS)
- Dynamically configure FortiGate to monitor and secure each / all such tunnels, adding and removing as the service evolves (scales, heals, etc.), ensuring security is always aligned and correctly configured.
- As security demands change, scale FortiGate and/or adjust networking to prioritize traffic to reflect evolving application behavior

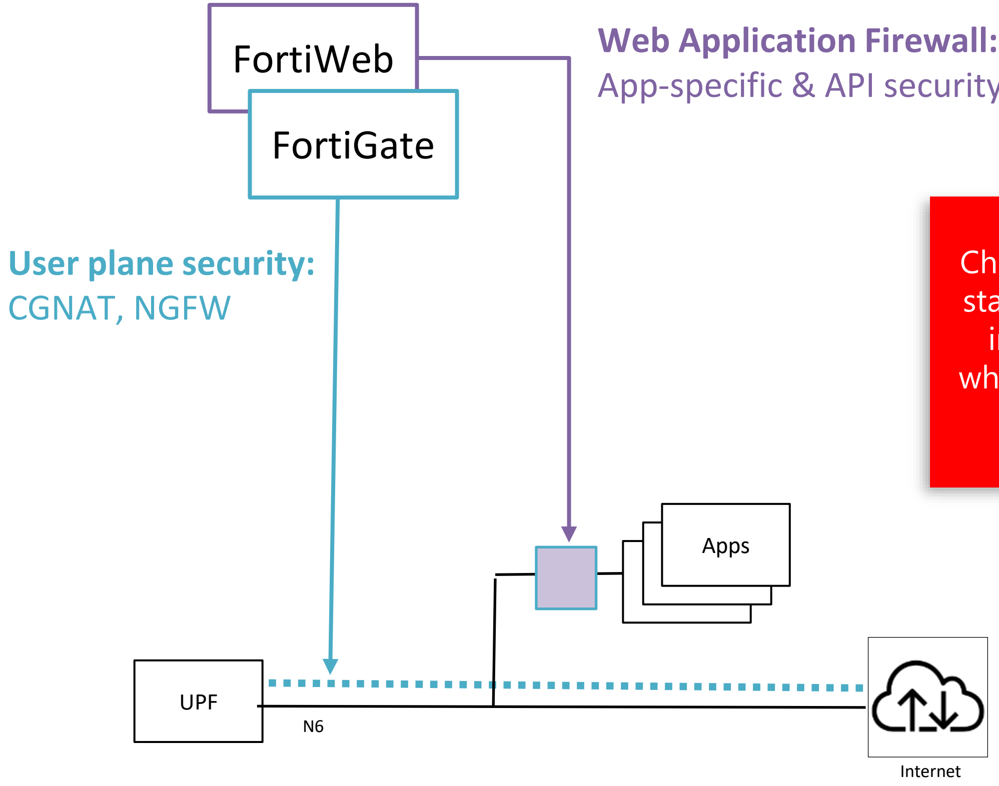


Changes in application state result in changes in network useage, which triggers FortiGate adaptive security and EnterpriseWeb & KX's optimizations

Adaptive Security for Business Apps

Adaptive Application Security

- In addition to traditional negative and positive security models (attack signatures, IP address reputation, protocol validation, etc.), FortiWeb applies a second layer of machine learning-based analytics to detect and block malicious anomalies while minimizing false positives
- FortiGate is dynamically configured to monitor and secure each / all tunnels to Business Apps (CGNAT, NGFW on N6 interfaces), ensuring network security is always aligned and correctly configured.
- FortiWeb is dynamically configured to provide App-specific and/or API security based on App(s) being secured, ensuring application security is always aligned and correctly configured



Web Application Firewall:
App-specific & API security

User plane security:
CGNAT, NGFW

Changes in application state result in changes in network useage, which trigger FortiWeb adaptive security

GTP & Next Generation FW (NGFW) ▪▪▪▪▪▪▪▪▪▪▪▪▪▪▪▪▪

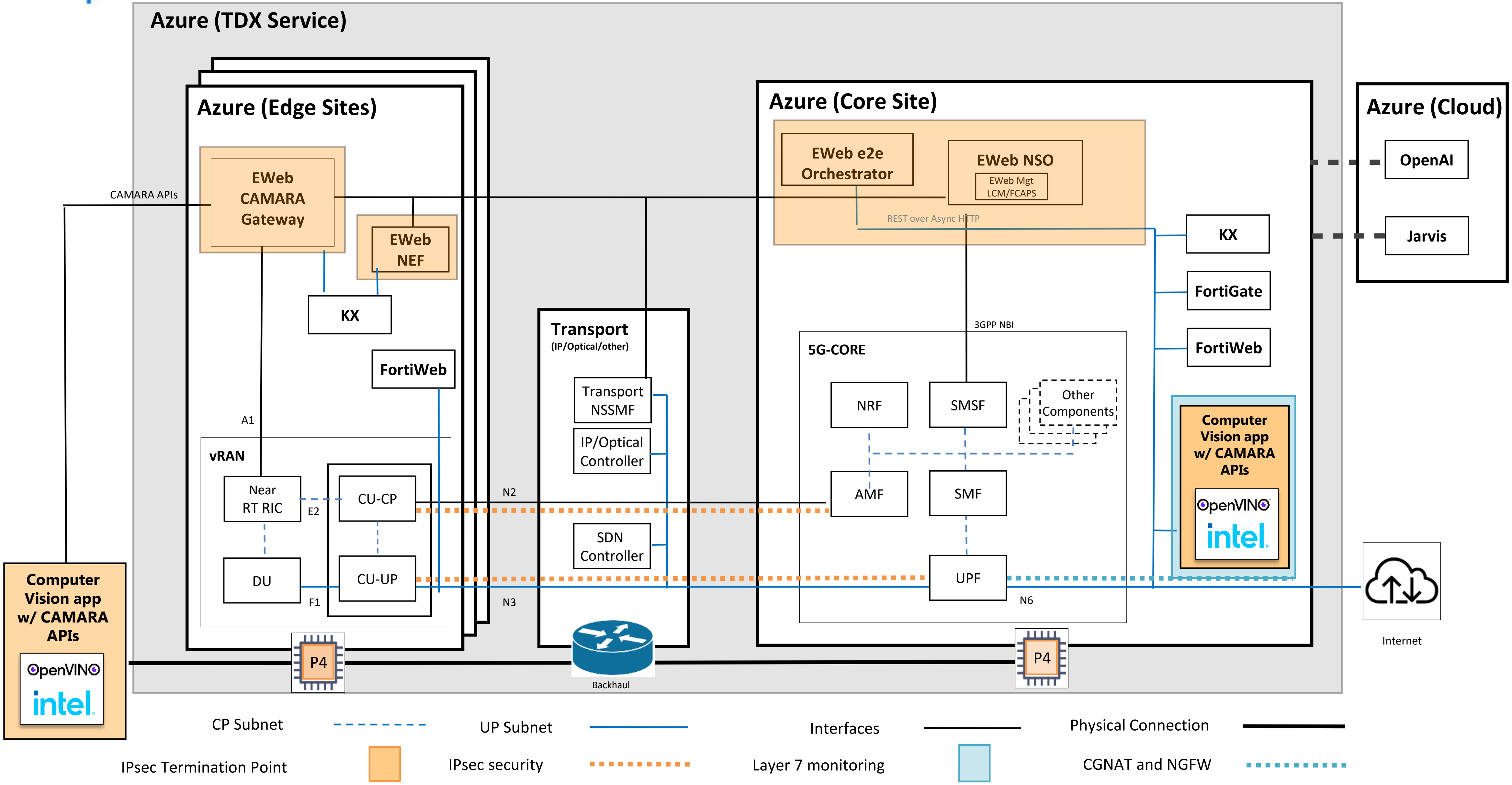
Thanks for your time and interest!

For more information or to schedule a meeting at **MWC**24 please contact dave@enterpriseweb.com

Intel, the Intel logo, and FlexRAN, OpenVINO, and the OpenVINO logo are trademarks of Intel Corporation or its subsidiaries.

EnterpriseWeb®

Solution Architecture



Azure (TDX Service)

Azure (Edge Sites)

EWeb CAMARA Gateway

EWeb NEF

KX

FortiWeb

CAMARA APIs

A1

vRAN

Near RT RIC

E2

CU-CP

DU

F1

CU-UP

N2

N3

Transport (IP/Optical/other)

Transport NSSMF

IP/Optical Controller

SDN Controller

Backhaul

P4

Azure (Core Site)

EWeb e2e Orchestrator

EWeb NSO

EWeb Mgt LCM/FCAPS

REST over Async HTTP

3GPP NBI

5G-CORE

NRF

SMSF

Other Components

AMF

SMF

UPF

N6

KX

FortiGate

FortiWeb

Computer Vision app w/ CAMARA APIs

OpenVINO

intel

Azure (Cloud)

OpenAI

Jarvis

Internet

Computer Vision app w/ CAMARA APIs

OpenVINO

intel

CP Subnet - - - - - -

UP Subnet ———

Interfaces ———

Physical Connection ———

IPsec Termination Point 🟧

IPsec security ▪▪▪▪▪▪▪▪▪▪

Layer 7 monitoring 🟦

CGNAT and NGFW ▪▪▪▪▪▪▪▪▪▪