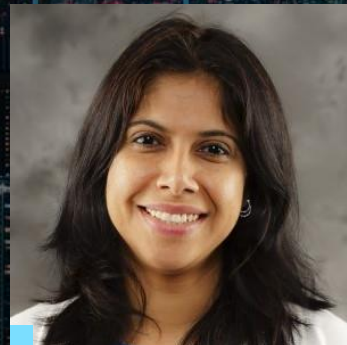Intel® Network Builders webinar
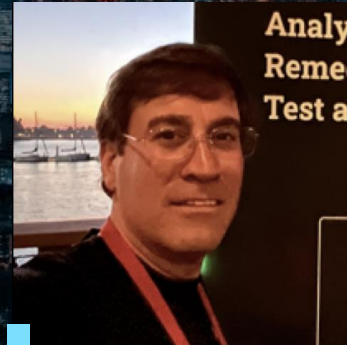
Network Security at the Edge with Intel® NetSec Accelerator Reference Design

October 24, 2023

Jyoti Kolhe
Cloud/Edge Segment Manager – Intel

Ryan B
Technical Director of Strategic Alliances – Noname Security

Adam Bennett
CEO – Red Piranha

Dogu Narin
VP of Product Management – Versa Networks
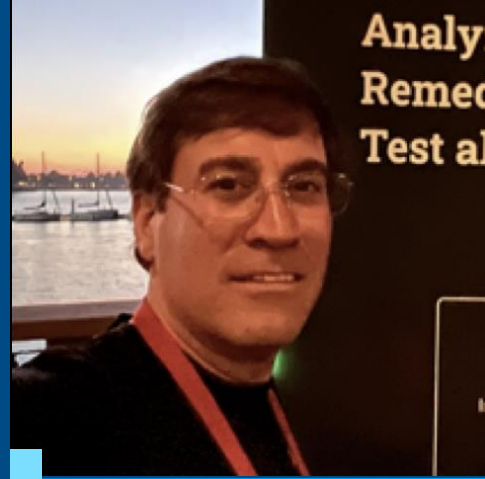
intel®

Today's Host and Presenters

Jyoti Kolhe
Cloud/Edge Segment
Manager – Intel

Ryan B
Technical Director of Strategic
Alliances – Noname Security
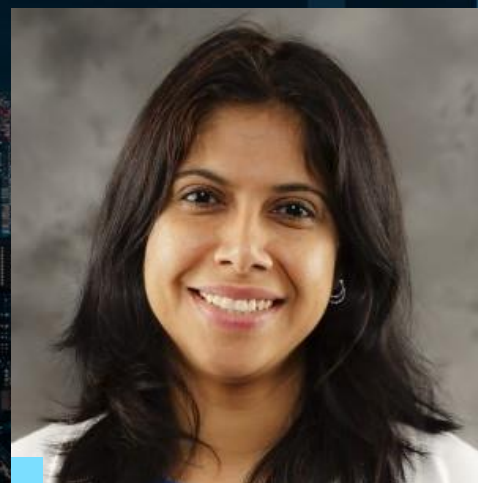
Adam Bennett
CEO – Red Piranha

Dogu Narin
VP of Product Management –
Versa Networks

Transformation of the Network Edge

Enterprise workloads are driving need for scalable infrastructure at the edge to support latency, local data processing and security

- Enable workloads to be deployed where they are needed
- Shift towards micro-segmentation and distributed architectures - > edge cluster nodes
- Anchored on 5G and SDN with SASE/SSE becoming the security fabric

Application Processing

Firewall, IPS/IDS, AppID (Layer 7), Classification, NAT

Control Plane Processing

SD-WAN Routing - BGP, OSPF, SRv6 etc.

Packet Processing

IPSec/SSL, Traffic Management, QoS, DPDK, VPP, WiFi 6E, LTE, 5G

Industri Transport Healthcare Retail

AI Inferencing, IOT

UTM, Object Detection, Threat Detection, Media Transcoding

Latency Reduction   Data Reduction   Scalability

~ 1 – 30 ms   ~ 100 – 200 ms   Server   Large Bandwidth   Edge Cluster   Server   Anchor   Server   Edge Host   Server
Edge Host   Server

intel.

Intel® NetSec Accelerator Reference Design
....an autonomous server on a PCIe add-in card

- Server on a card: orchestration and mgmt. independent of the host

- Intel® Ethernet Network Adapter E810 + Intel SOC
  - Flexible compute augmentation for Host Platform
  - Workload migration from host to free up Cores

- Intel scalable Architecture for common Network Functions

- Maintain Architectural Consistency with Intel Architecture

- Low software lift (if any) to on-board
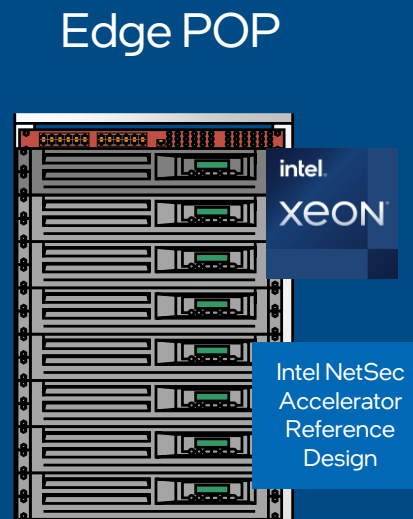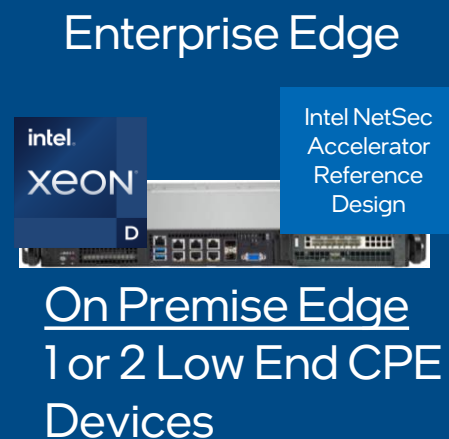

Intel Atom: 8C, 16C
Production: NOW

Intel Xeon-D: 4C, 8C, 10C
Coming Soon

Deployment Models	Use Cases and Workloads
Network Accelerator Aka Partial Application Offload	Network and Security Appliances Ipsec, SSL, IDS/IPS, NGFW
Full Application Offload Aka Distributed Appliance	SASE and Network Edge Connectivity SD-WAN, Head End and Far Edge

intel.

Intel® NetSec Accelerator Reference Design
Product Positioning

- Acceleration of Networking and security workloads

- Customers looking for Intel coherency
  - Same NIC/SOC as used on appliances
  - Ease of consumption; low software effort, if any

- Anchors on driving scale and TCO
  - Workload accel. - > platform scaling
  - Deployment of fully packaged apps/appliances in 3rd party hosts
    - ❑ Edge: enable scalable cluster nodes
    - ❑ 'Appliance on a card' that works autonomously in a host

Edge POP

Enterprise Edge

intel XEON D

Intel NetSec Accelerator Reference Design

intel XEON

Intel NetSec Accelerator Reference Design
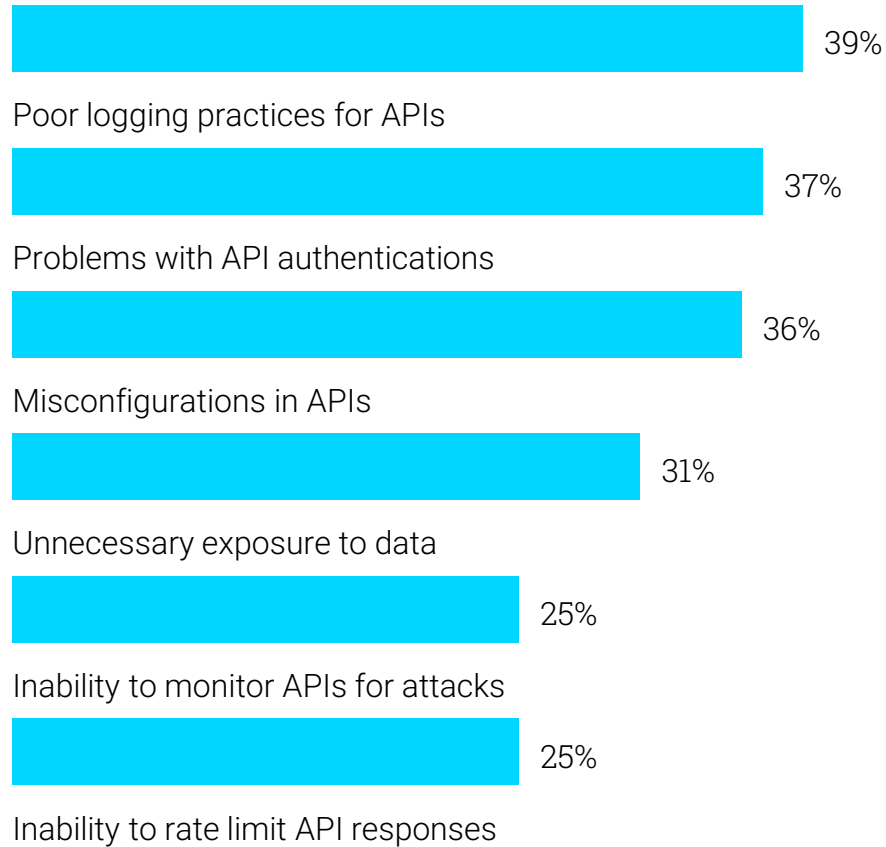
On Premise Edge
1 or 2 Low End CPE Devices

Polling Question

How much of your organization's resources - applications and data - run at the edge?
  A. More than 70%
  B. 40-70%
  C. Les than 40%
  D. None

intel.

API Security requires Machine Learning, because it is a superhuman problem to solve

39%

Poor logging practices for APIs

37%

Problems with API authentications

36%

Misconfigurations in APIs

31%

Unnecessary exposure to data

25%

Inability to monitor APIs for attacks

25%

Inability to rate limit API responses

15,564
Average number of Production Enterprise APIs

76%
of organizations experienced a security breach in the past year

37 days
27 days for discovery

10 days for remediation

per incident

Whitepaper

The 2022 API Security Trends Report

[Learn more](#) →
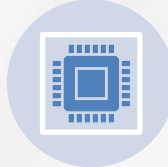
Security First SASE, for Partners

Dedicated Hardware Control plane, eliminates virtualisation based attack risk

High Assurance , with 11 times increased visibility across cloud, network and end point

Implement a Declarative Authorisation Service - DAS

Best of class TDIR to meet the challenge of the ever-evolving threat landscape

Implement CTEM through Vulnerability Management all the way down to the SBOM

Up to 2.4 Gbps Security Scanning Throughput*

Compact hardware footprint, 5 times Energy Saving, Improved data center profit

CRYSTAL EYE SECURE EDGE

Mobile Devices

On-Premise Devices
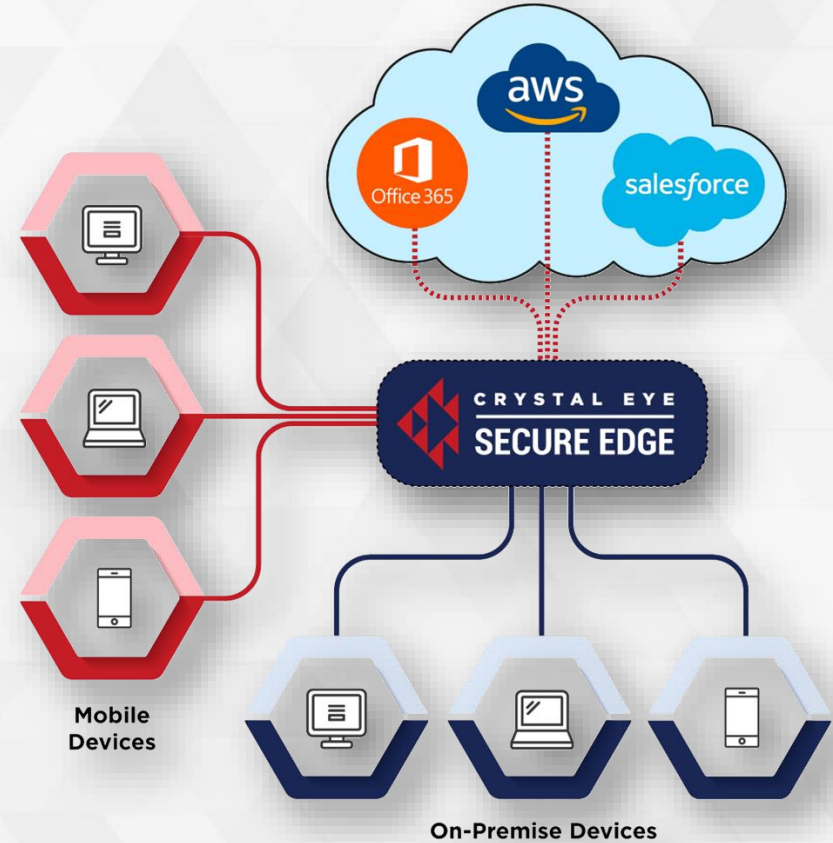
Crystal Eye Cloud Access Security Broker

Red Piranha
unified threat management

redpiranha.net

Australia

AUSTRALIAN MADE

CREST

OISF

CYBER THREAT ALLIANCE

JAS-ANZ
GICG
ISO 27001:2013 Certified Cert.No.: 781489

JAS-ANZ
GICG
ISO 9001:2015 Certified Cert. No.: 703236

Securing Data Center Infra and Tenants

ZTNA and Full Stack Security Inline within Data Center Servers

The Need

- Multi-tenant or compliance certified deployments need policy controlled, secured access for tenants and workloads
- Seamless inline security stack does not exist today

The Solution

- VOS running on Smart-NIC – with full functionality
- Extending ZTNA, Micro-segmentation, Secure SD-LAN into Data Center servers
- Security, policy-based traffic control and traffic management natively provided inline
- Seamless insertion – fully transparent to workloads and OS

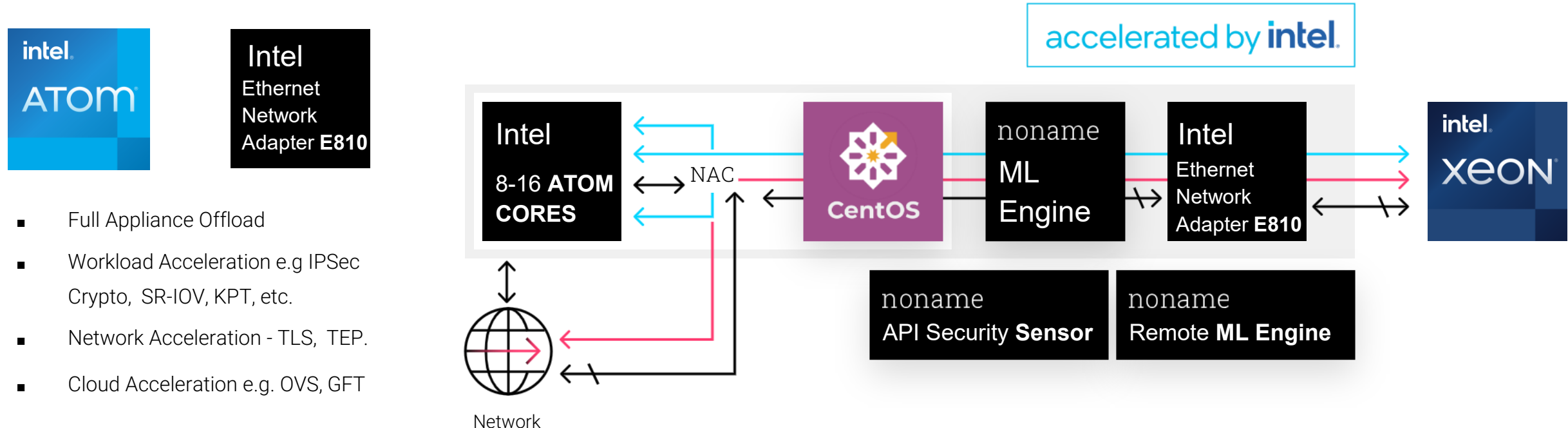Virtualized or bare-metal data-center servers
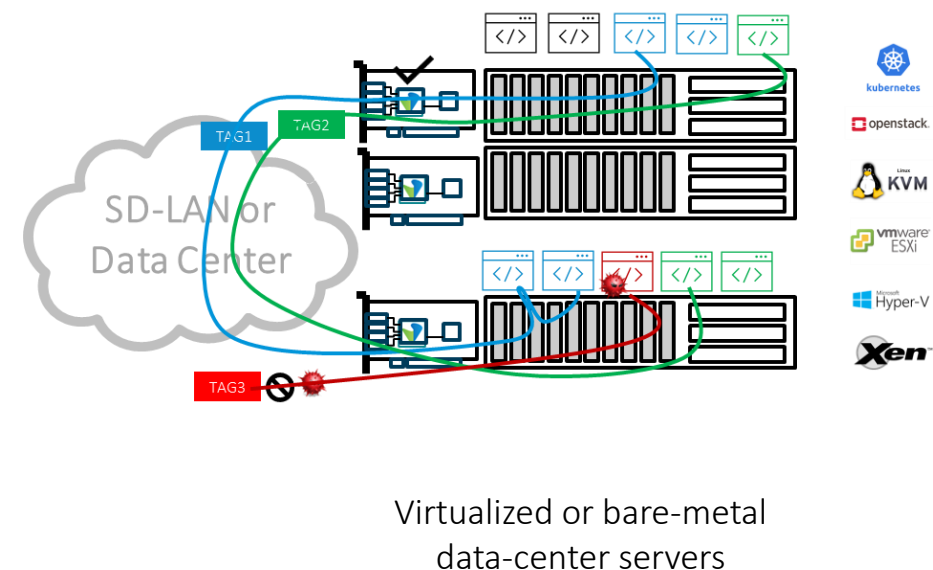
Intel® NetSec Accelerator Reference Design

with 100GbE Intel® Ethernet Network Adapter E810 Edge Telco Grade network interface & low latency API Security powered by Noname Security Machine Learning

Family of Intel SoC-based Reference designs intended to accelerate networking and security workload
Use cases: IPSec/SSL/Http offload, SASE, FW | **AI Machine Learning integration with:**

intel® **ATOM**

Intel Ethernet Network Adapter **E810**

accelerated by intel.

- Full Appliance Offload

- Workload Acceleration e.g IPSec Crypto, SR-IOV, KPT, etc.

- Network Acceleration - TLS, TEP.

- Cloud Acceleration e.g. OVS, GFT

Intel 8-16 **ATOM CORES**

NAC

CentOS

noname **ML Engine**

Intel Ethernet Network Adapter **E810**

intel. **XEON**

noname API Security **Sensor**

noname Remote **ML Engine**

Network

A complete autonomous server with full Orchestration and Management on a PCIe add-in card

Security without Compromise, for Integrators

Ready to scale, module design, build and deploy past 100GB, for large scale traffic monitoring

Customizable adapter and node controllers, manage traffic across node or port-to-port

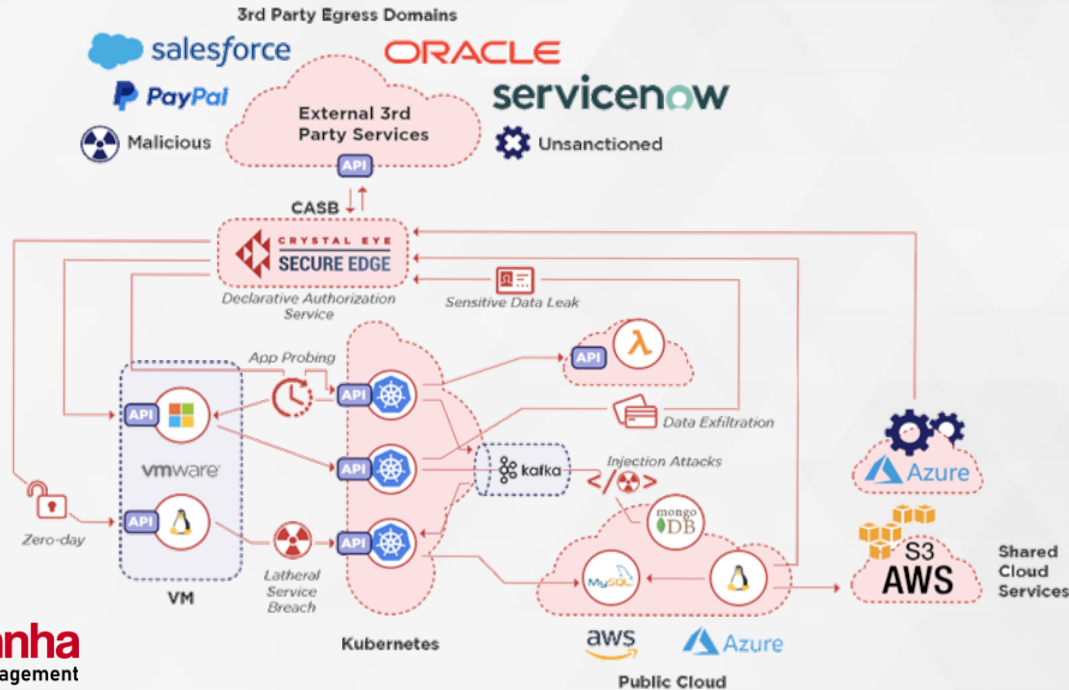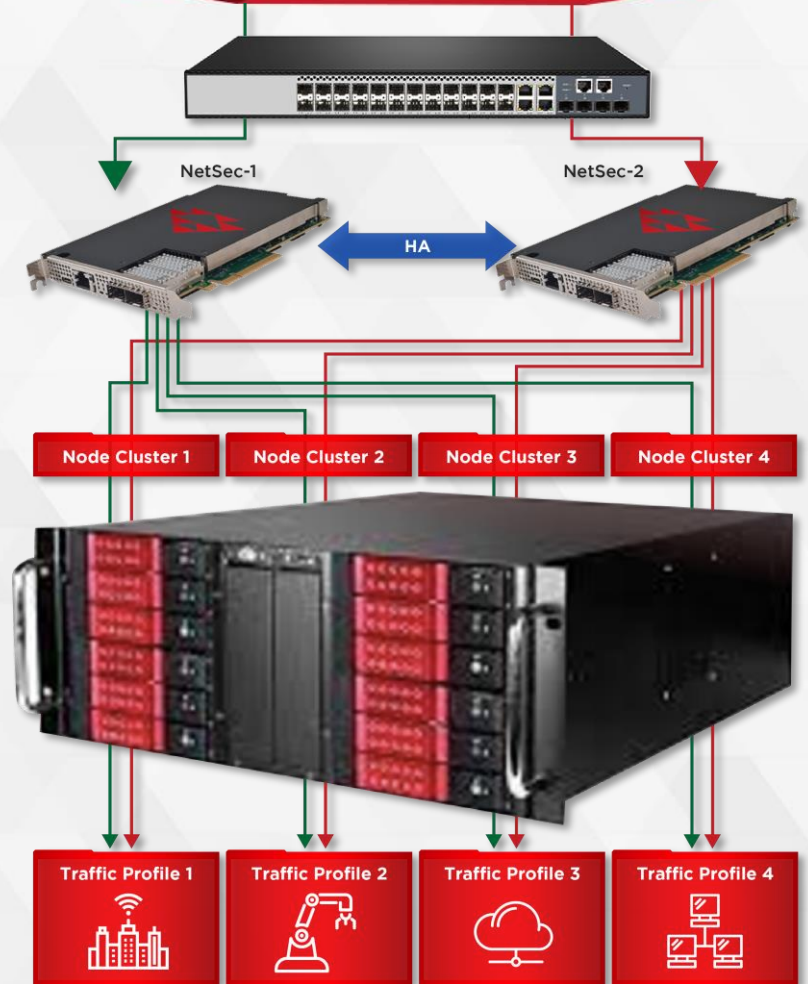Configurable for DOS protection profiling

Custom proxy profiles for increased TLS interception and inspection capabilities

Redundant cluster node failover

Instant SOC capability across custom traffic types

NetSec-1

NetSec-2

HA

Node Cluster 1 | Node Cluster 2 | Node Cluster 3 | Node Cluster 4

Traffic Profile 1 | Traffic Profile 2 | Traffic Profile 3 | Traffic Profile 4

3rd Party Egress Domains

salesforce
ORACLE
PayPal
servicenow
Malicious

External 3rd Party Services

API

Unsanctioned

CASB ↓↑

CRYSTAL EYE
SECURE EDGE

Declarative Authorization Service

Sensitive Data Leak

App Probing

API

API

API

vmware

API

Zero-day

VM

Kubernetes

kafka

Injection Attacks

Data Exfiltration

mongoDB

MySQL

Lateral Service Breach

aws

Azure

Public Cloud

Azure

S3 AWS

Shared Cloud Services

Red Piranha
unified threat management

AUSTRALIAN MADE

CREST

OISF

CYBER THREAT ALLIANCE

GICG JAS-ANZ
GICG JAS-ANZ

ISO 27001:2013 Certified Cert.No.: 781489   ISO 9001:2015 Certified Cert. No.: 703236

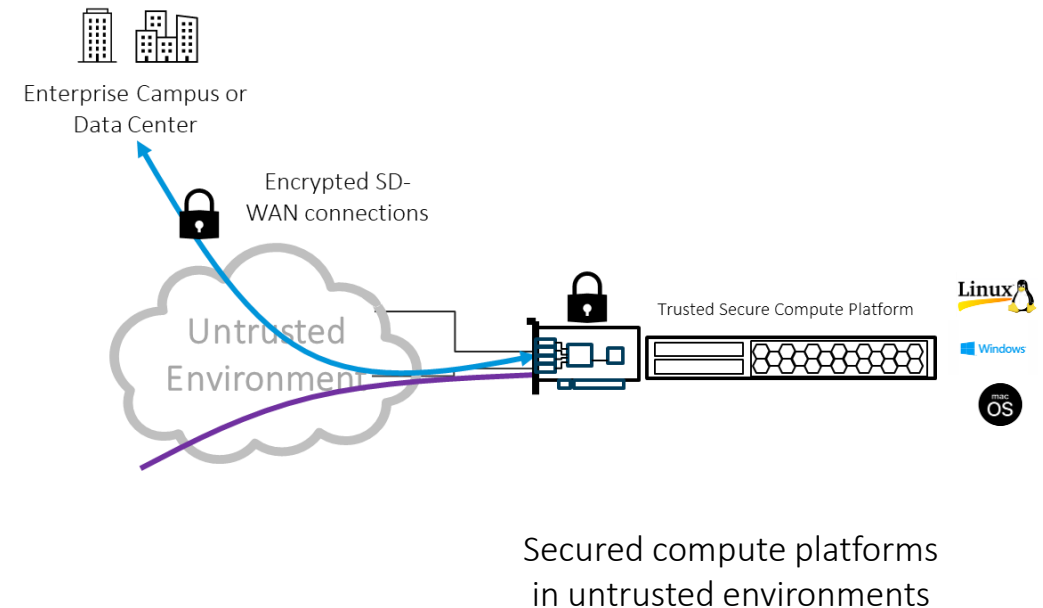# Securing Compute Platforms in Remote Deployments

SD-WAN style Encrypted Connections with full WAN Edge Security for Compute Platforms

The Need

- Enterprises may need to deploy compute solutions in untrusted or 3rd party environments
- Enterprises need to seal the compute and have a trusted and encrypted way of connecting to it
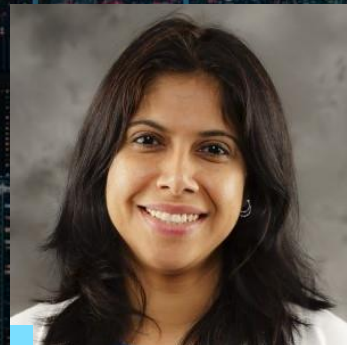
The Solution

- VOS running on Smart-NIC – with full functionality
- Extending SD-WAN, NGFW and UTM based edge security to compute platforms deployed in untrusted environments
- Security, encryption, policy-based traffic control and traffic management natively provided inline
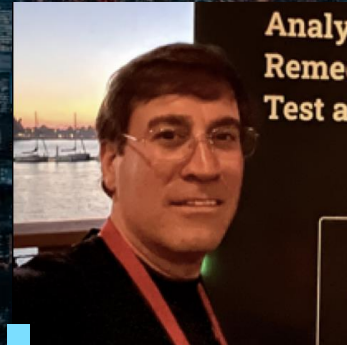- Eliminating need for external appliances

Enterprise Campus or Data Center

Encrypted SD-WAN connections

Untrusted Environment

Trusted Secure Compute Platform

Linux
Windows
mac OS

Secured compute platforms in untrusted environments

VERSA
NETWORKS