Versatility 2025

Transforming Enterprise LAN: The Rise of Next-Gen Zero Trust LAN Solutions

VERSA

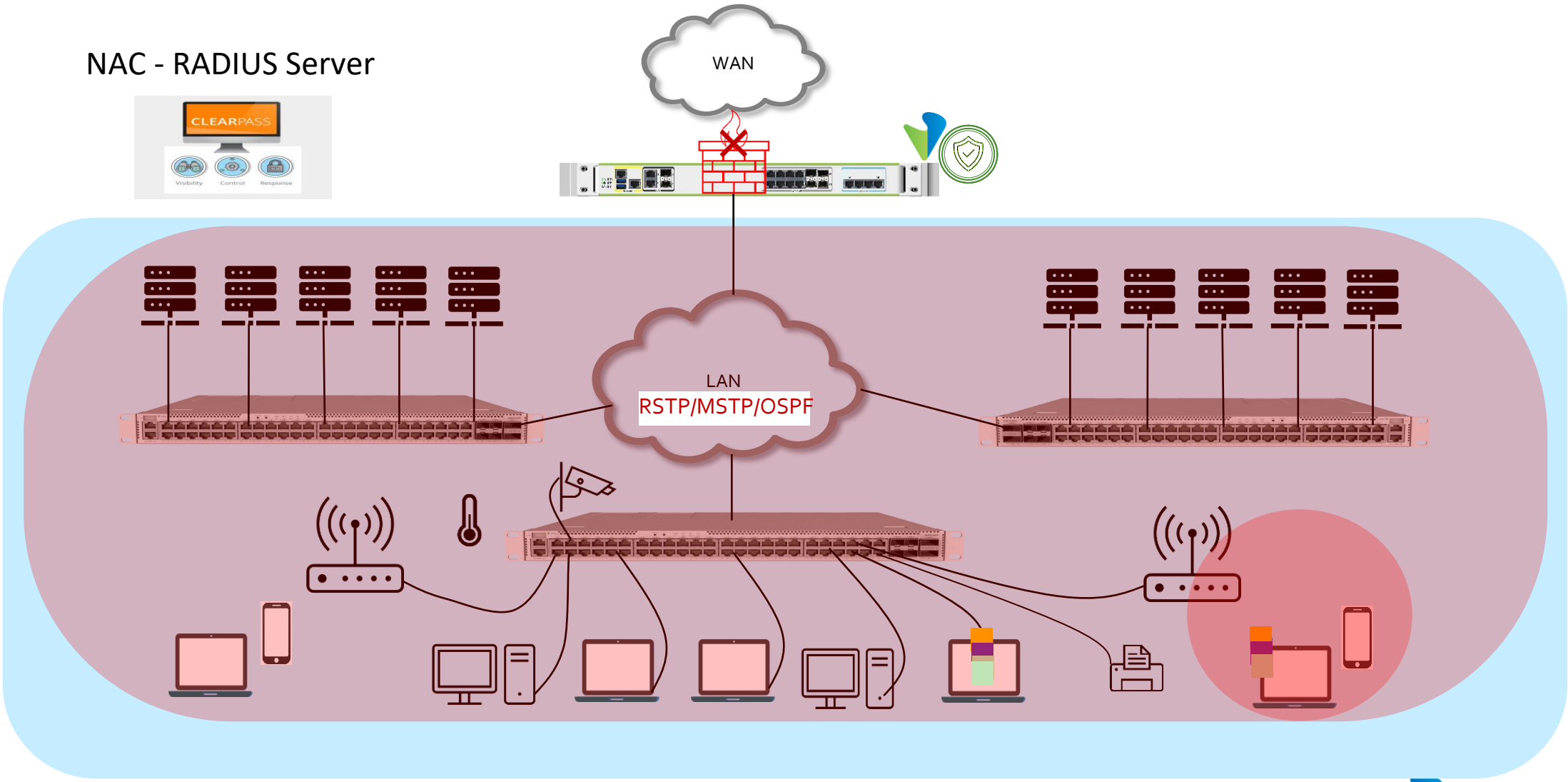

Versatility 2025
VERSA

Legacy Campus Architecture

Versatility 2025

VERSA

Legacy Campus Architecture

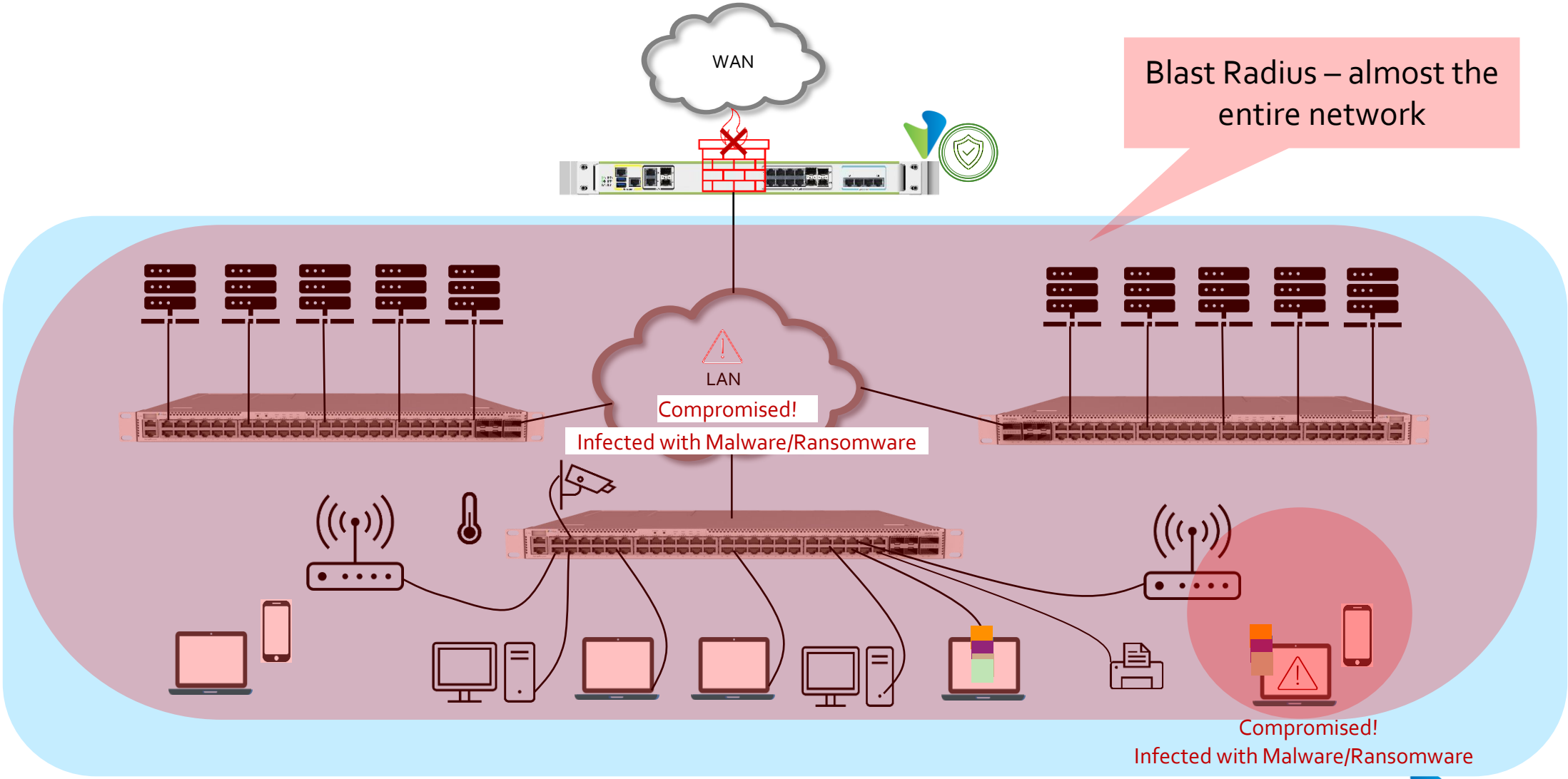


VERSA

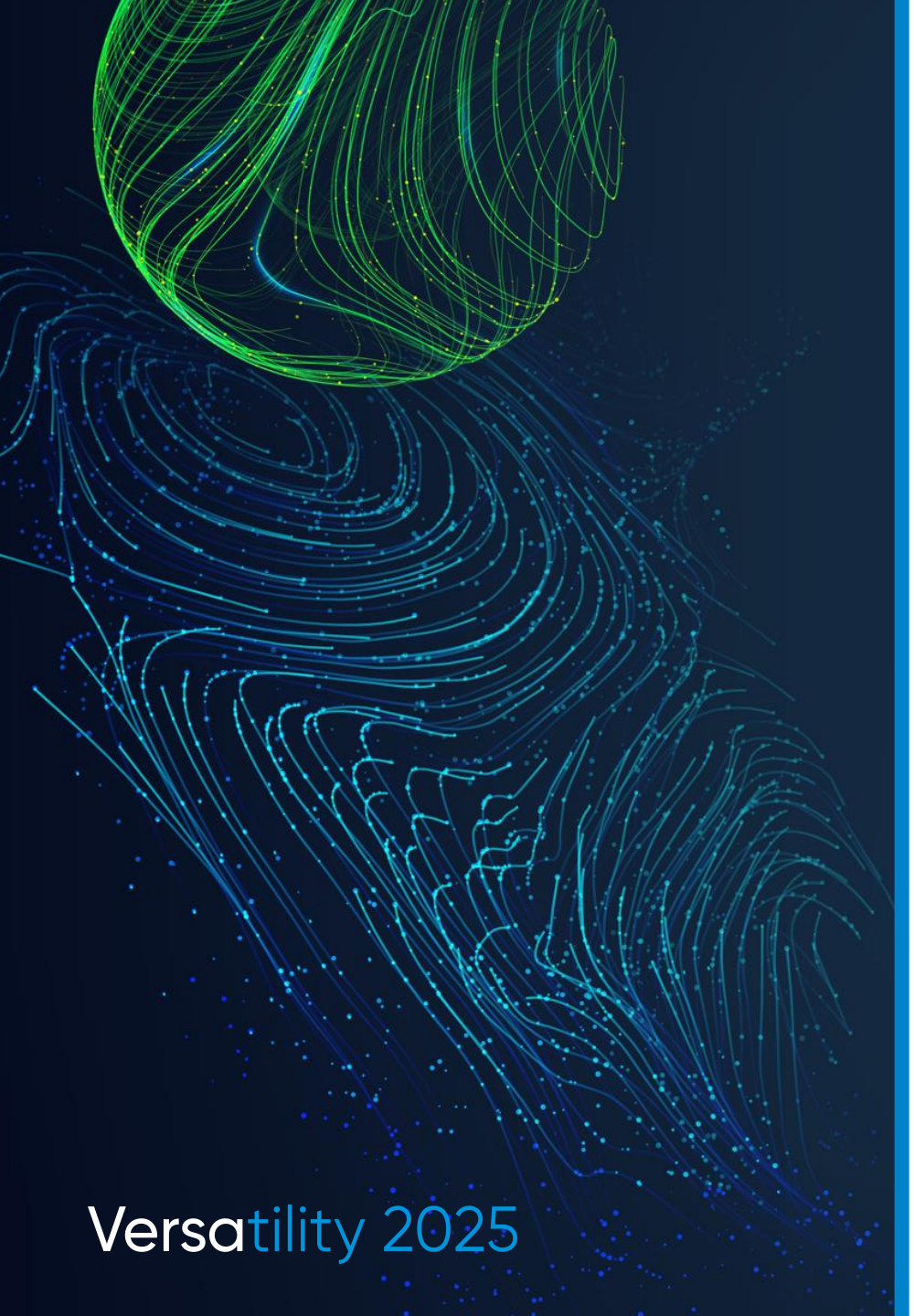
Legacy Campus Architecture

- Built with proprietary Layer2/Layer3 switch appliances and had to be refreshed every few years
- Many complex and failure-prone proprietary technologies like Virtual Chassis, MC-LAG, Fabric path, and ISSU are deployed which creates vendor lock-in and increases the capex and operational expenses significantly
- Various bolt-on approaches for security enforcement - in LAN access, WAN edge, and data center using different vendor solutions.
- 802.1X with external RADIUS servers for admission control and to provide static, unfettered access to any resources on the network.
- Siloed solutions for Switching, WLAN, WAN edge, and Security.
- Legacy networks are not intelligent enough to adapt to the traffic pattern and apply policies, have inconsistency in configuration, and use sub-optimal paths with serious security gaps.
- This results in sub-optimal network design for the new traffic types and traffic patterns with security loopholes, increased customer traffic latency, and higher capex and operational expenses.
- No protection built-in E-W direction: Legacy NAC has significant security shortcomings. An infected device that gets connected to the LAN, can infect the whole network.

Legacy Campus: Infection Blast-Radius is Expansive



VERSA



Versatility 2025

Why NG-LAN?

VERSA

#1: No Security Perimeter on Enterprise LAN

* Enterprise assets are not confined to the HQ and Branches, they're at Clouds, Colos, DCs, Edges, as well as SOHO locations, pretty much everywhere.
* Effective security perimeter is required to protect all.
* Therefore, Castle-and-Moat LAN perimeter strategy for Enterprise security defined by traditional security solutions is now obsolete.

#2: Protection from more readily available Ransomware, Malware

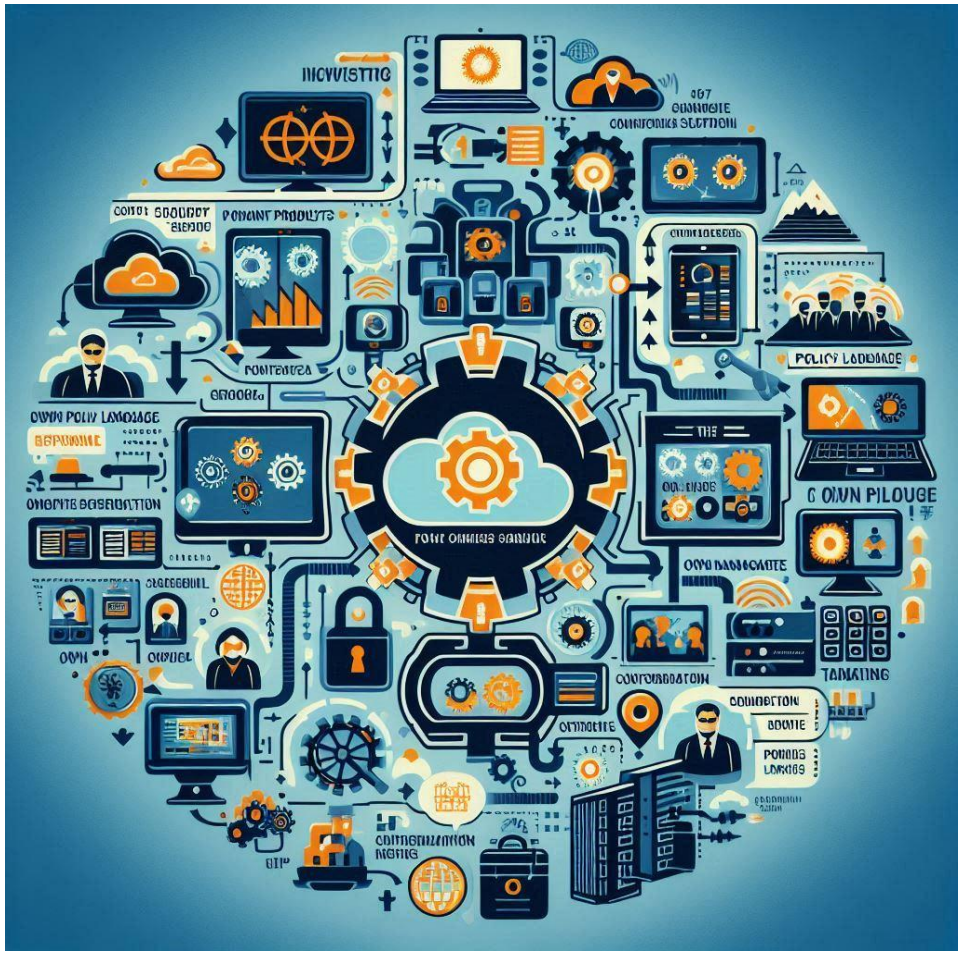
By malwares turning every endpoint into a bot, involvement of powerful actors, and high value market for compromised data & zero-day vulnerabilities, have drastically reduced the costs, increased the appeal, and industrialized Ransomware. Making Ransomware and Malware more readily available to compromise Enterprises.

In many cases Ransomware and Malware make their way in from corporate user's devices. No device can be trusted!

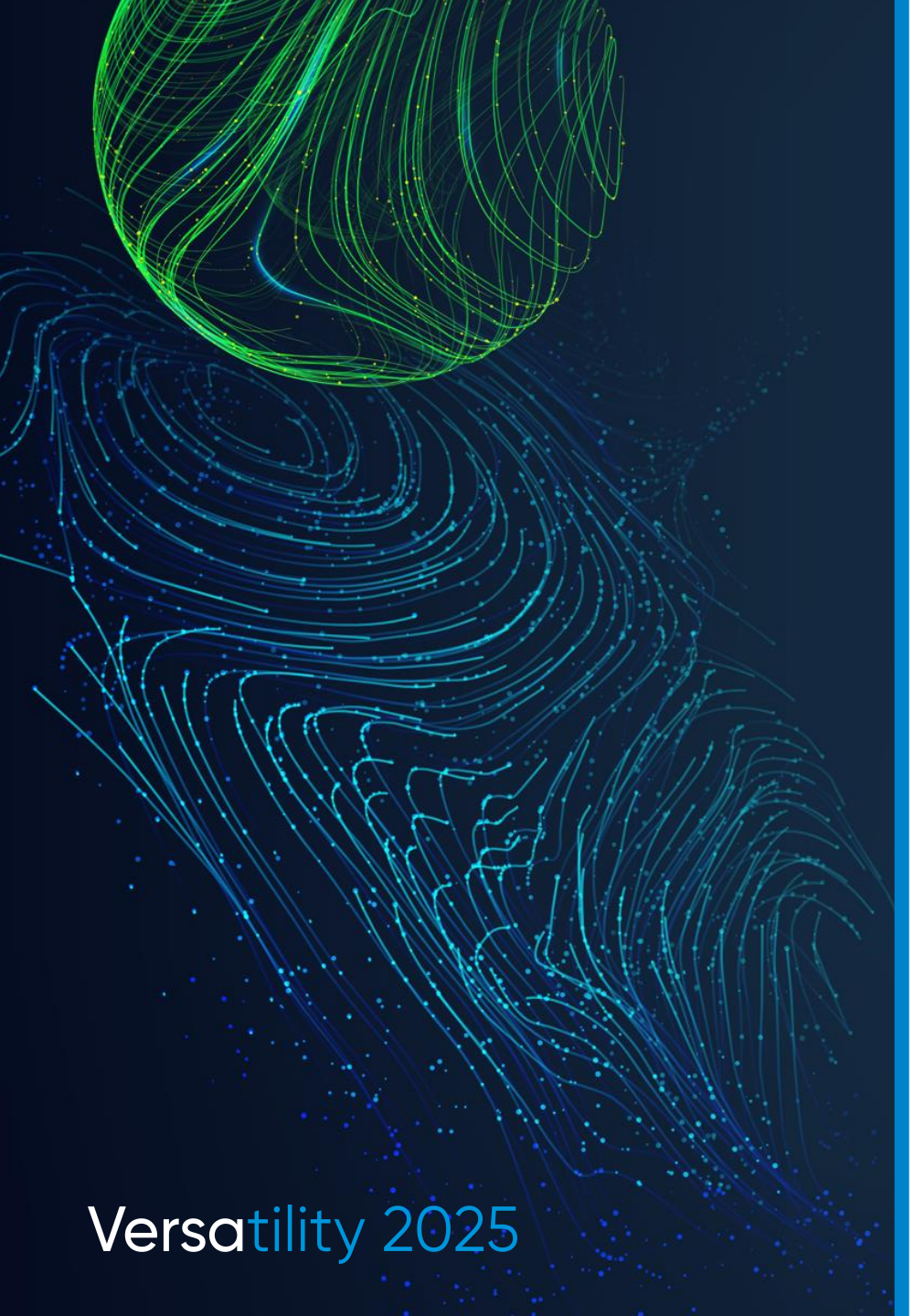
#3: Challenges Brought in by IoT, BYOD Devices

* Weak firmware, lack of built-in security, and distributed supply-chain makes IoT devices an easy and common target for bad actors, they need to be protected.
* Personal devices are used commonly in work environment.
* Hybrid-work culture necessitates that BYOD devices are secured.

#4: Customers Looking for Unified and Software based Solutions



* IT organizations are tired of running point solutions that are locked in by vendor specific hardware, software and architectures
* IT organizations are looking for unified solutions for ease of deployment, manageability and operations.
* IT organizations are looking for standard based products and solutions



Versatility 2025

How are these needs addressed today?

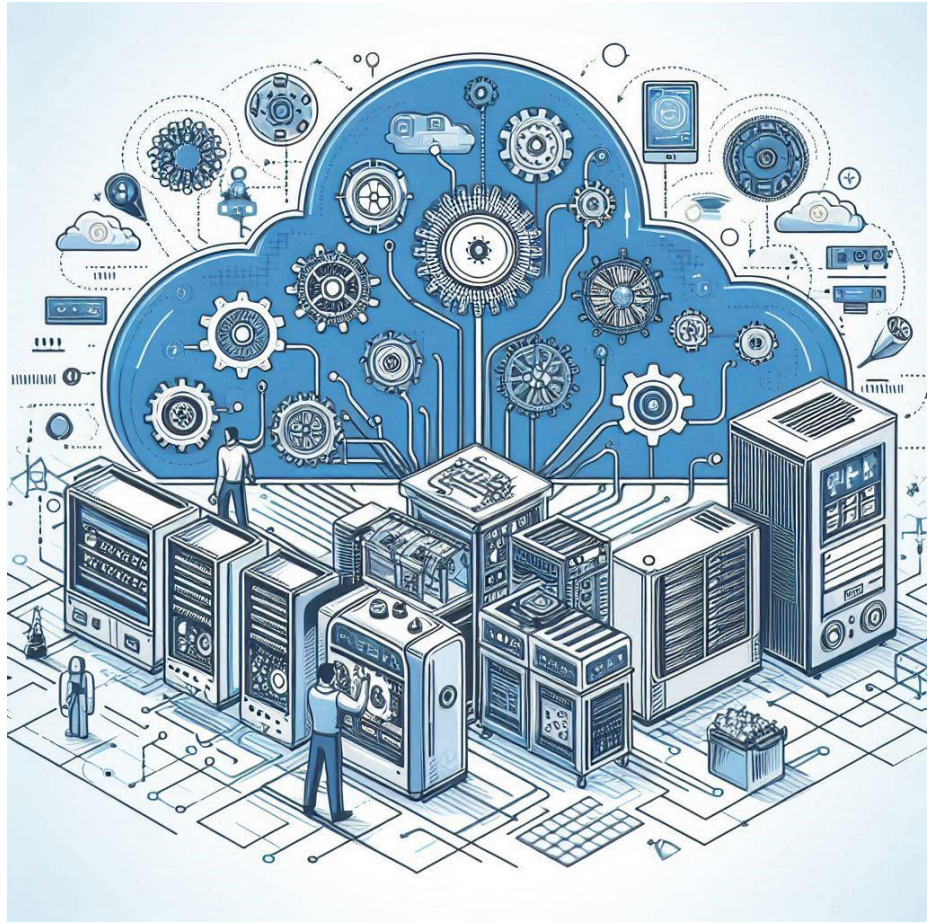
VERSA

#1: Legacy Networking Vendors

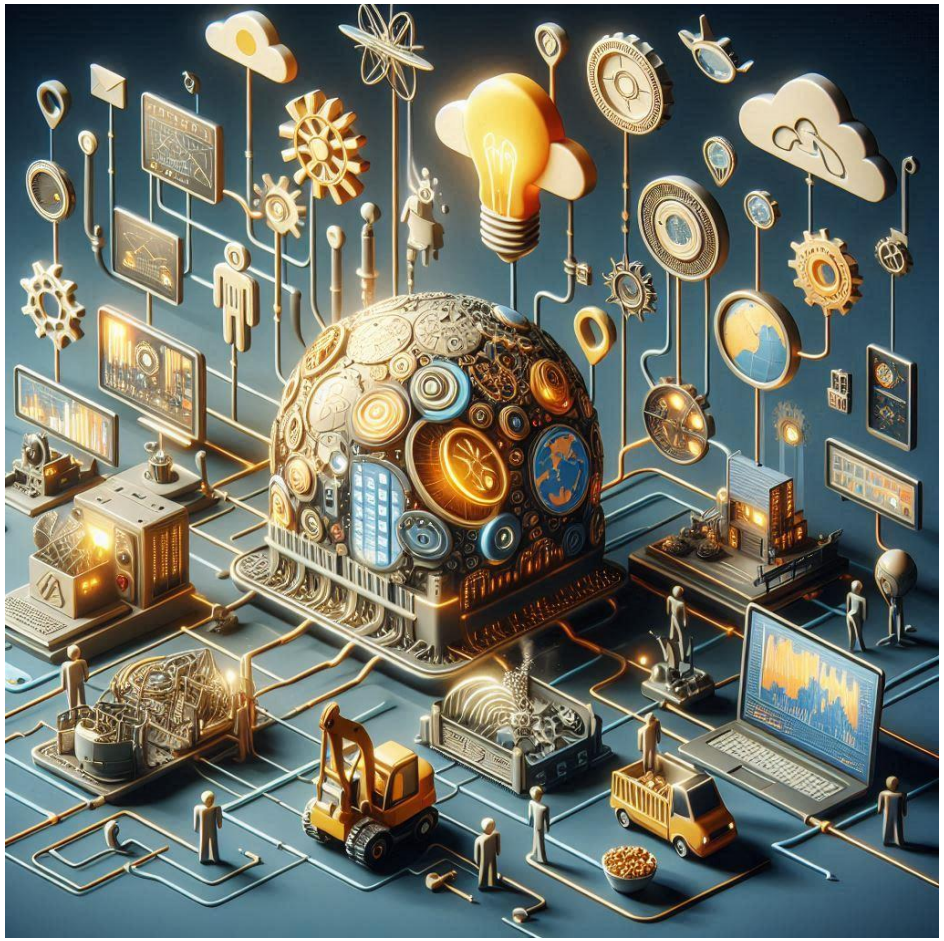
* Complex, fragmented, and buggy integration of aging LAN switches and routers with security solutions that are difficult to setup, operate, and maintain in the face of ever-increasing security threats.
* Point solutions built-in proprietary ways to keep customers locked in. Even business models are built that way.

#2: Legacy Security Vendors

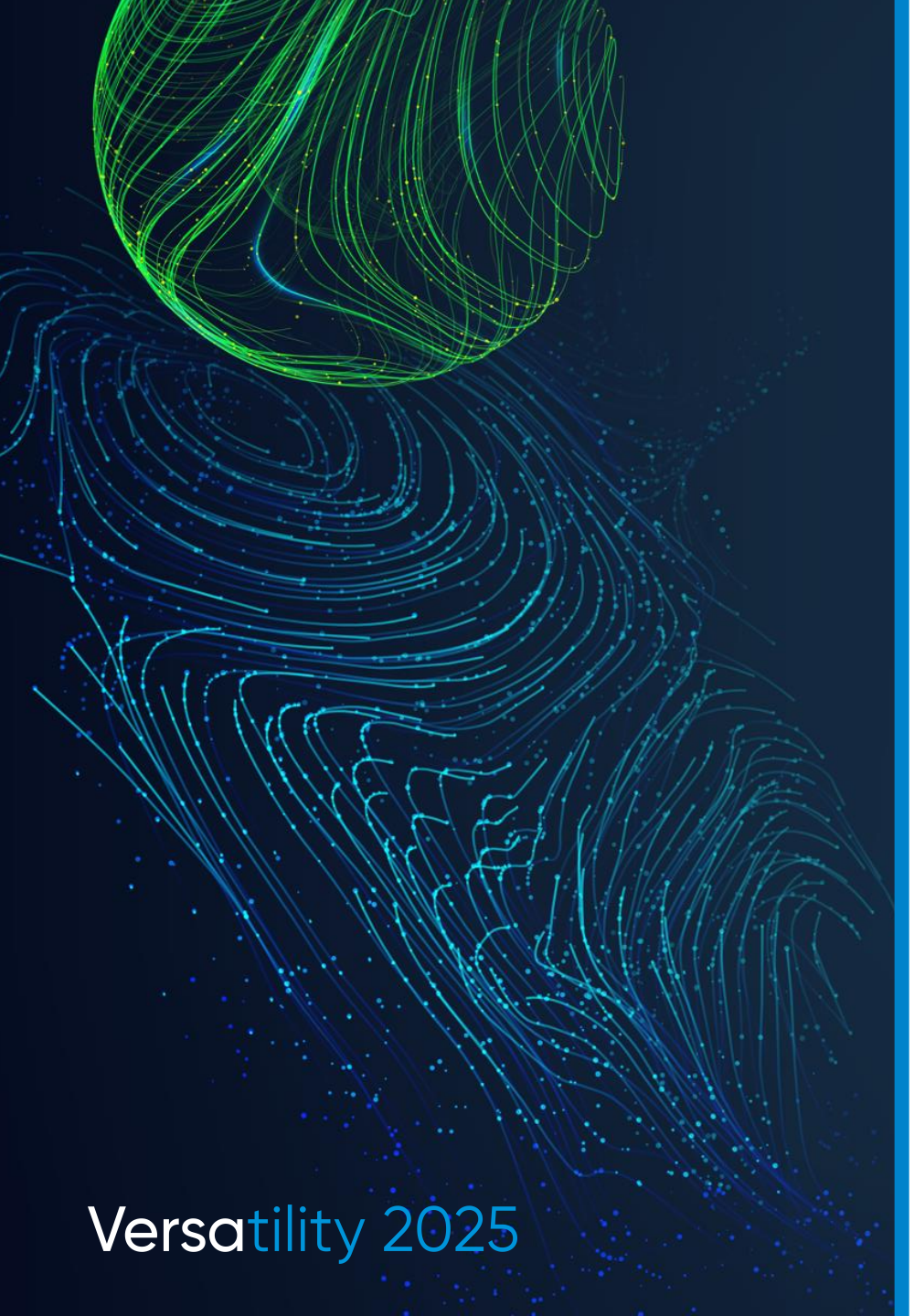
* Non-homogeneous integration of different point security products, each talking different policy languages, and addressing different use-cases into a single solution, makes it very difficult to ensure consistent policy, compliance and threat management.
* Legacy security products are typically located in DMZ or Edge of WAN and offering no protection on Enterprise LAN



Versa Zero-Trust Everywhere



* AI-driven, standards-compliant, and software-defined networking and security converged stack with single pane-of-glass operations, uniform policy language, and entry scans for Enterprise Assets at every *Edge* – LAN, WAN, Cloud, and Compute.
* Other ZTNA solutions are cloud delivered today, useful for employing on-the-go or WFH but offering no use for Enterprise on-premises.

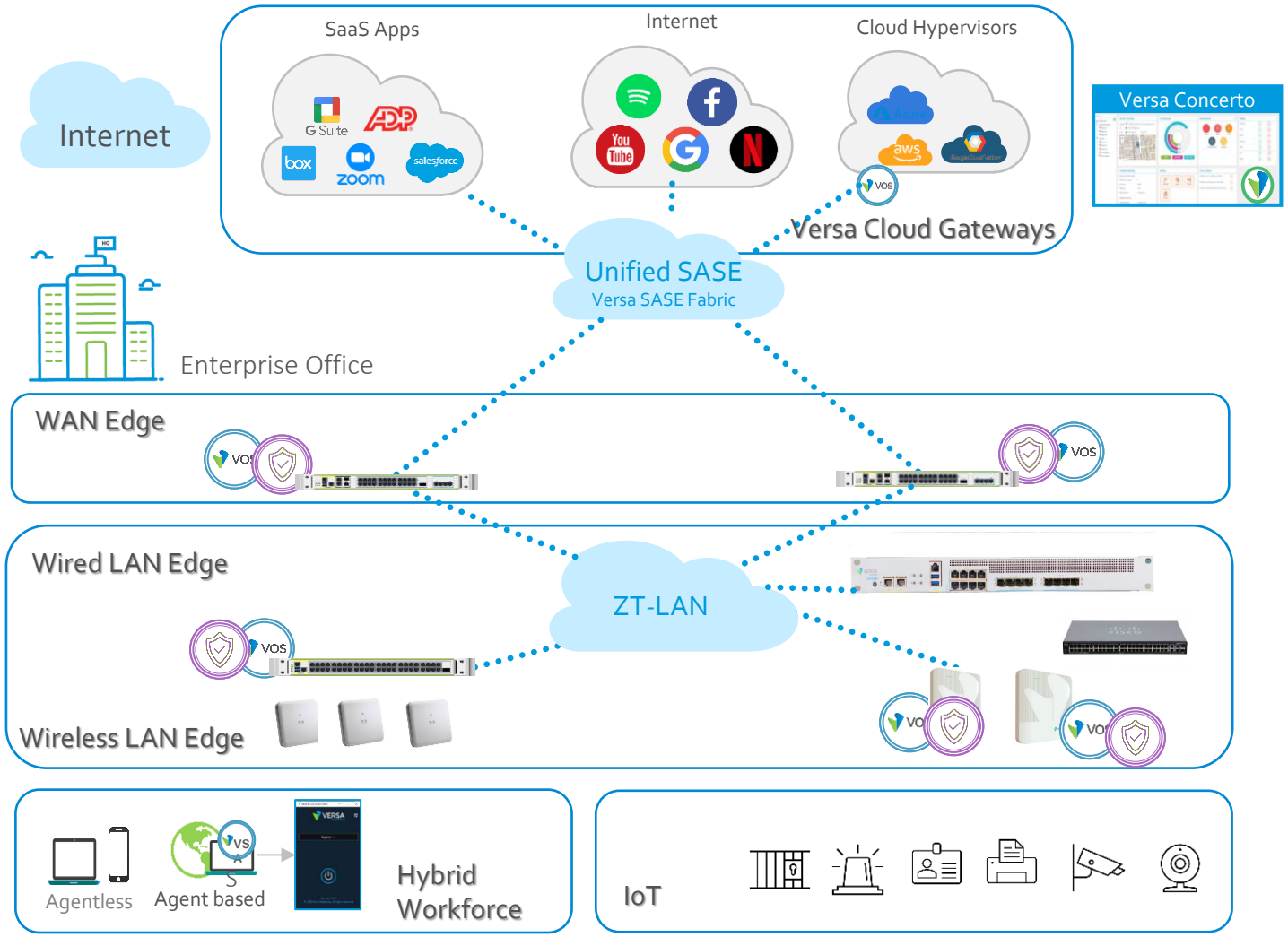


Versa Zero Trust LAN(ZT-LAN)

Versatility 2025

VERSA

Versa Zero-Trust Everywhere for Enterprises

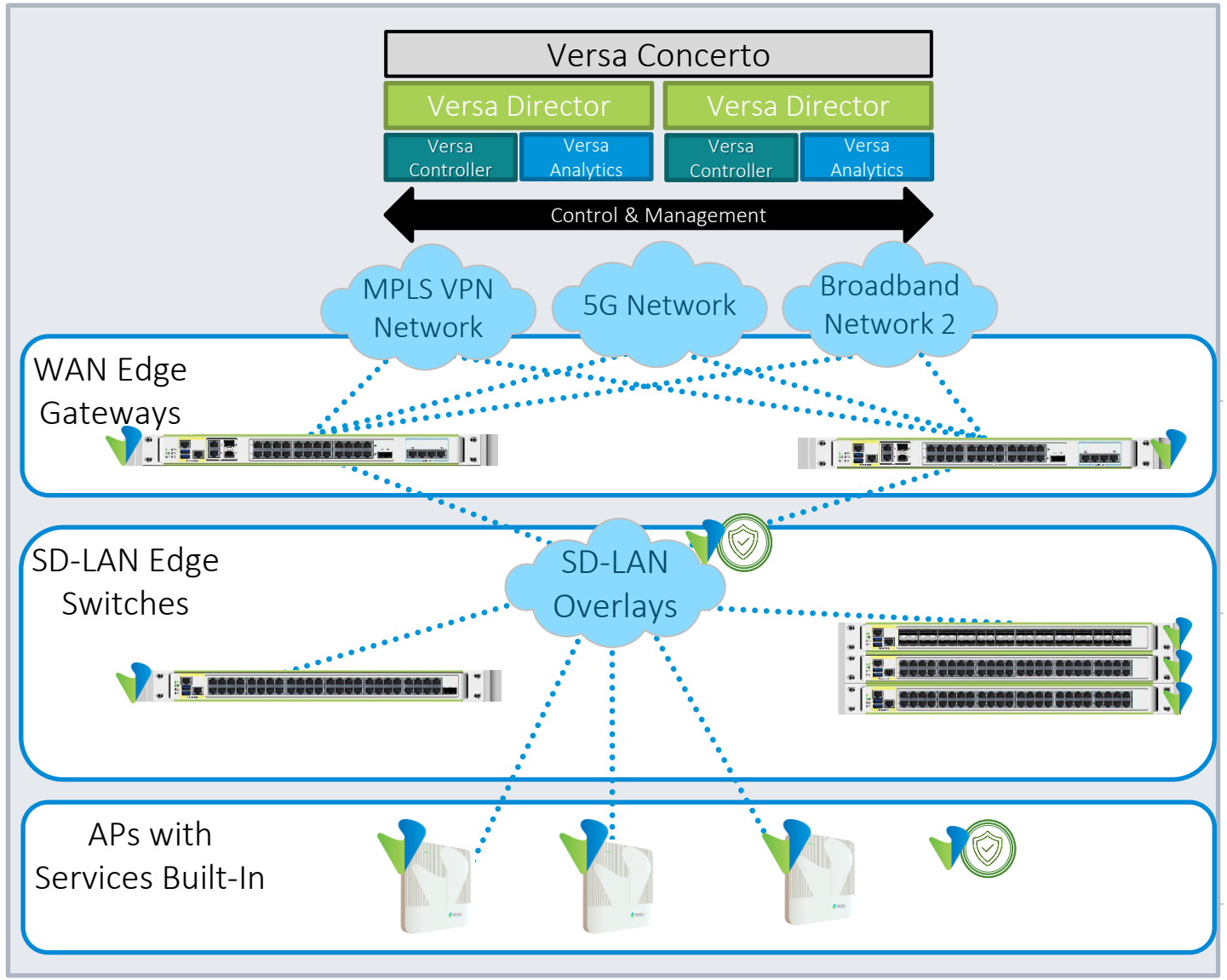


- Software Defined Architecture with intelligent edges
- Standards-based L2/L3 overlays to interconnect smart edges
- Based on single OS, single management plane, single analytics, single policy language
- Built-in, inline security at every edge node
- Built-in inline ZTNA
- Built-in inline device identification, fingerprinting and device management

Versatility 2025

VERSA

A Software-Defined Secure Architecture for Campus and DC



- Versa OS across WAN Edge, LAN Edge and Wireless Edge
- Single Pane of Glass for management, monitoring, and analytics
- Unified L4-7 Policy Control across all layers

WAN Edge w/Services:

- Best in class SD-WAN, ZTNA, NGFW, UTM, Routing, uCPE being expanded with SD-LAN

LAN Edge:

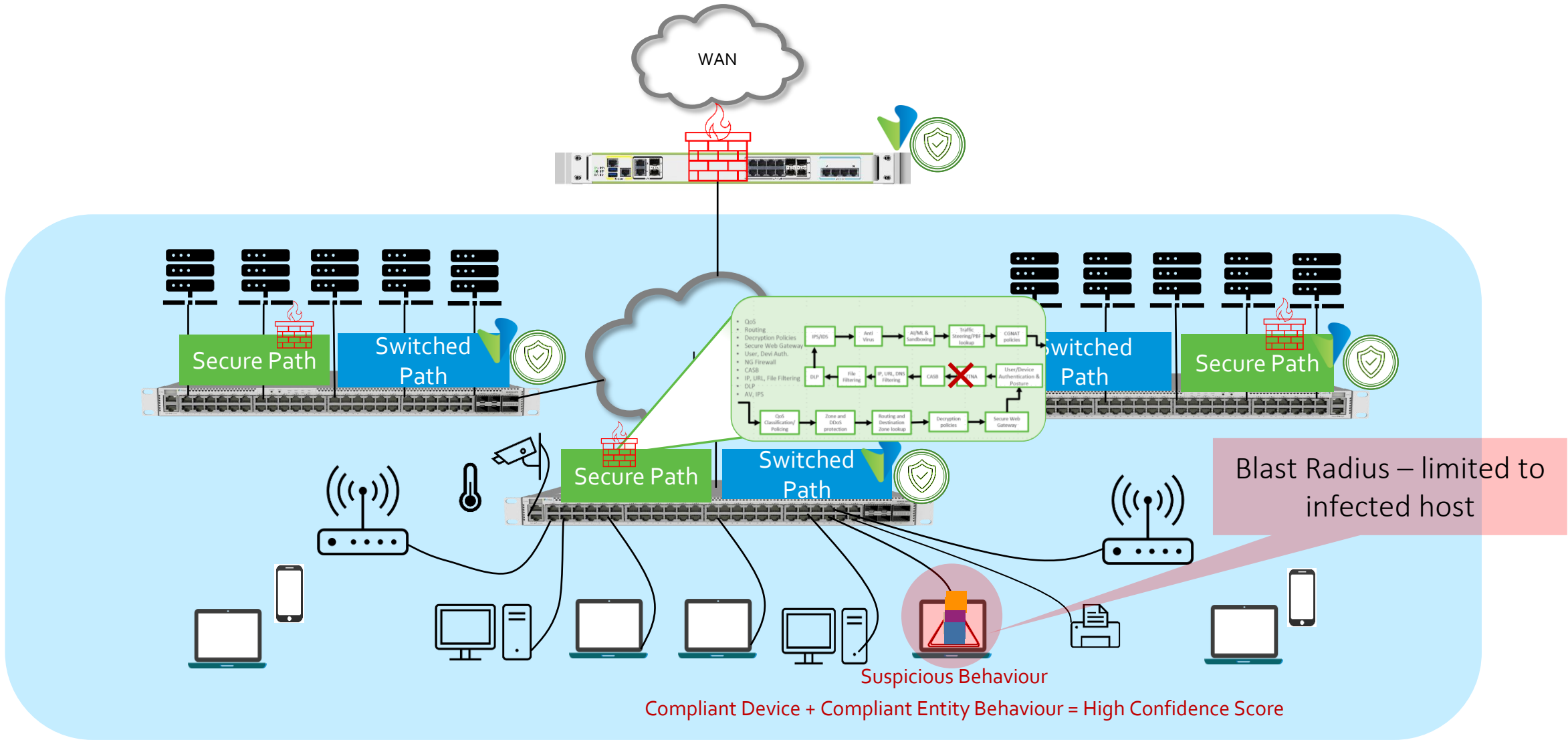
- SD-LAN starting from LAN Edge
- L2/L3, native full NGFW suite, with built-in Access Control, L4-7 Policy Control with line-rate switching
- SD-LAN Overlays for max flexibility and traffic separation in deployment

Wireless LAN Edge:

- L2/L3, native NGFW, Access Control, Policy Control built-in APs integrated with SD-LAN

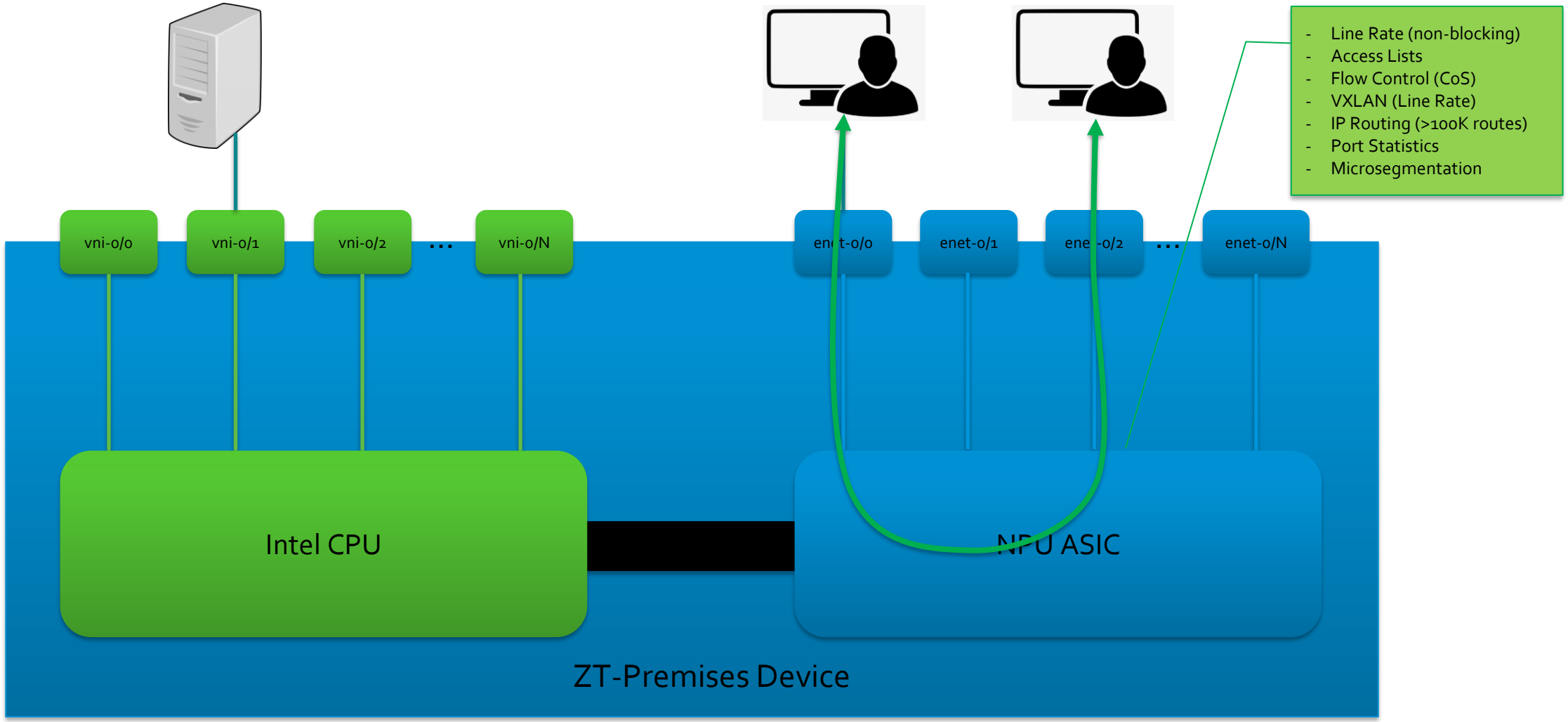
VERSA

Versa ZT-LAN: Blast Radius Confined to the Infected Host



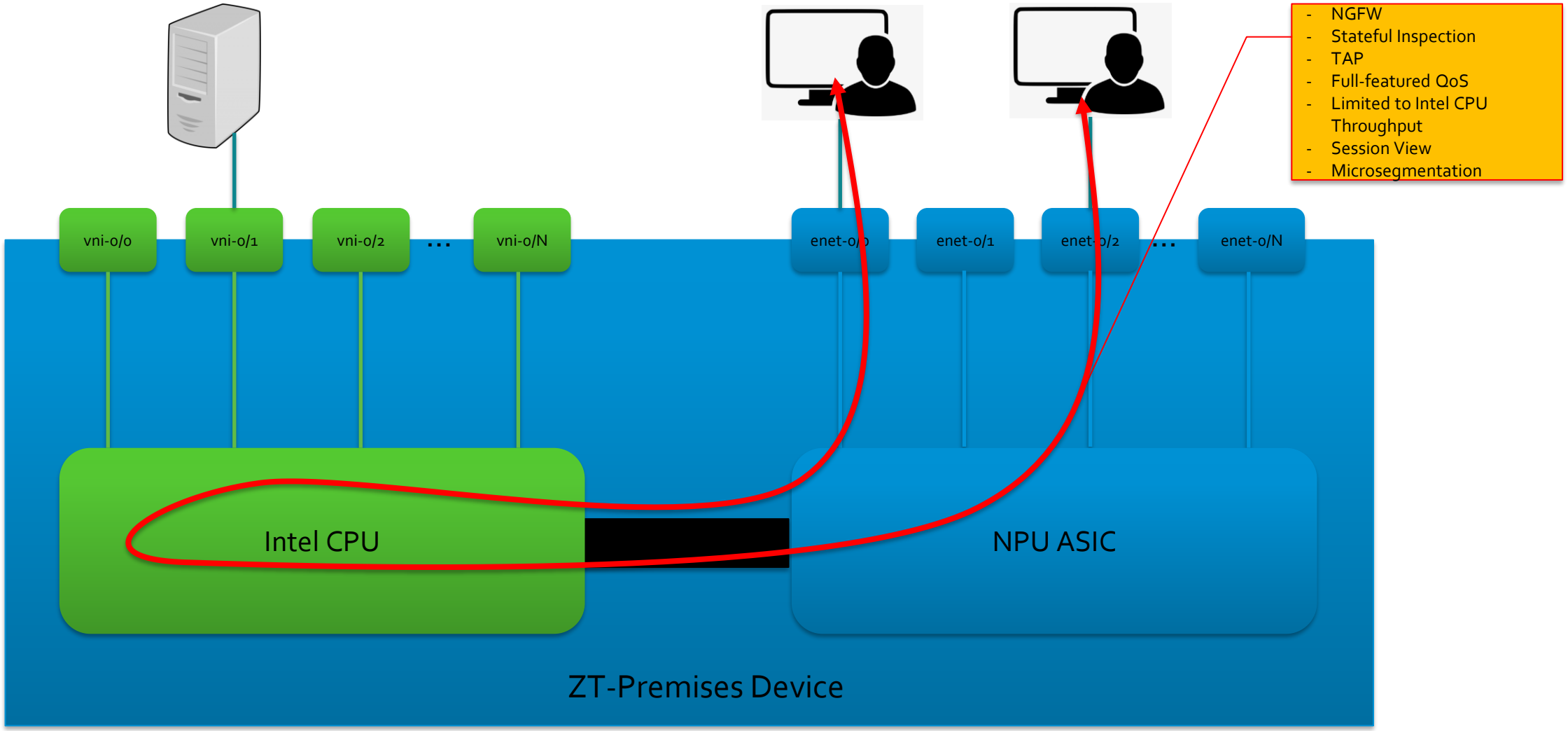
VERSA

Appliance Architecture (Flows and Services)



VERSA

Appliance Architecture (Flows and Services – L4/7)

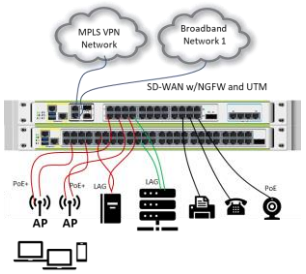


VERSA

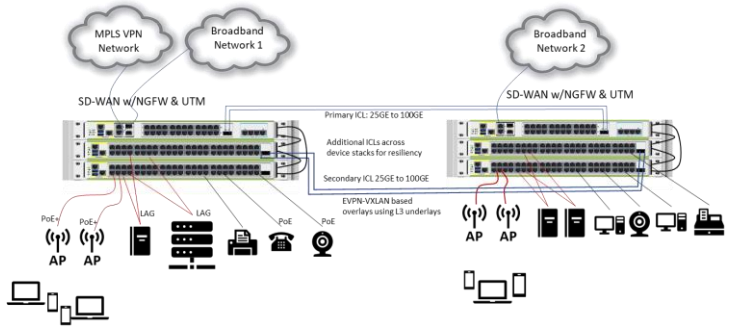
Versatile Topologies – For Greenfield and Brownfield

Branch/Regional Offices

Small Branch

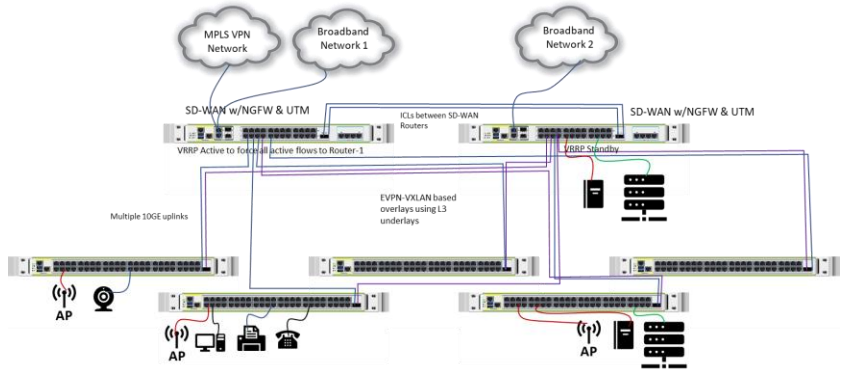


Large Branch/Regional Office



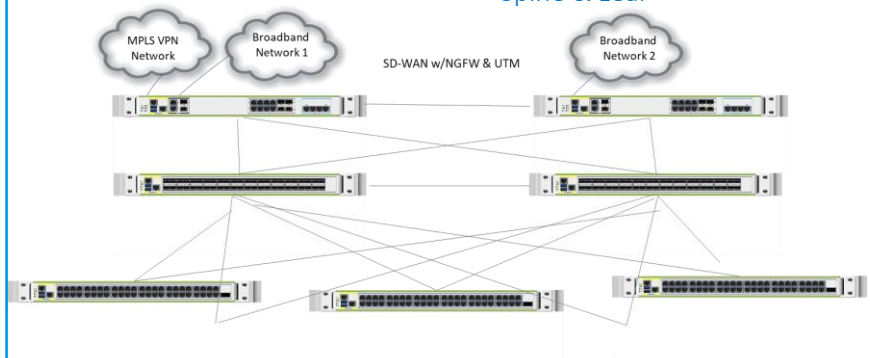
Heavily Distributed Architecture

Example - manufacturing plant

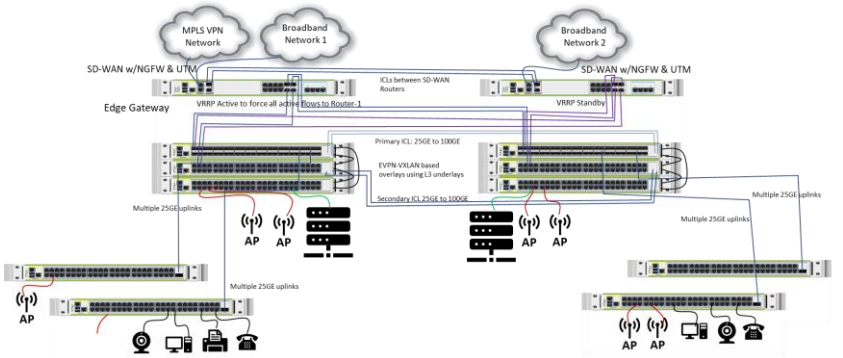


Classic Campus Architecture

Spine & Leaf



Converged – Classic Campus + Distributed

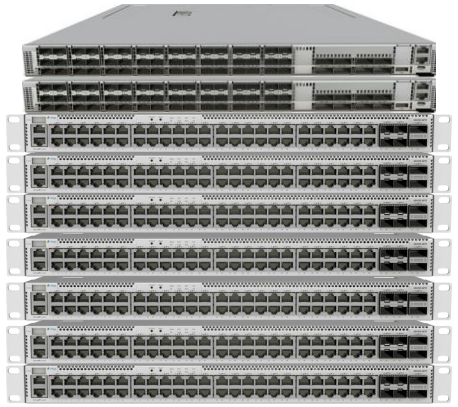


VERSA

Distributed EVPN instead of legacy Virtual Chassis/MC-LAG

Legacy LAN Solution

Versa ZT-LAN

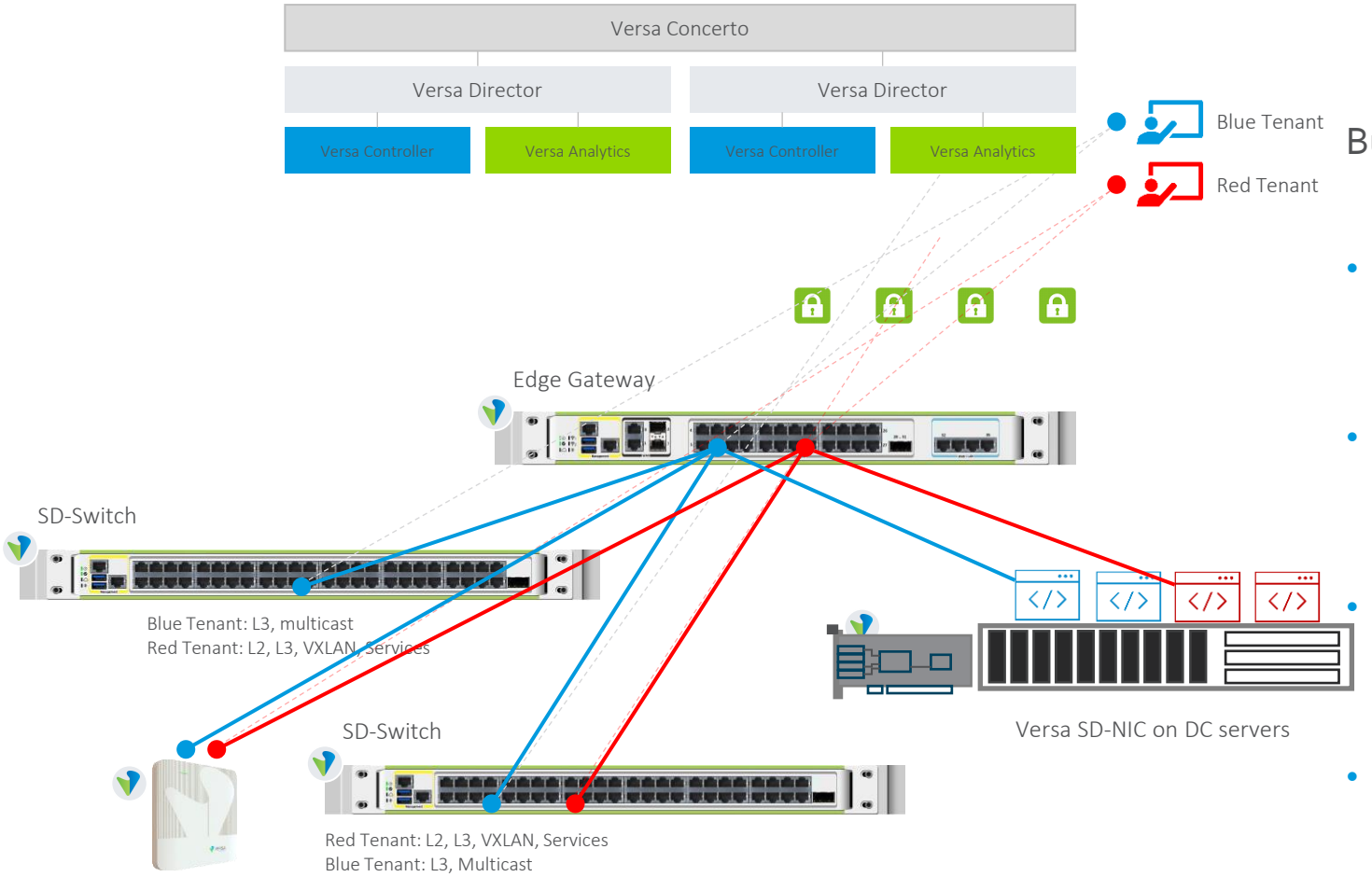


Versa ZT-LAN

- Fungible fabric, easy to increase port density by just adding more switches.
- Highly scalable through VXLAN-EVPN overlay.
- EVPN Active-Active multi-homing is a standards compliant, modern alternative to MC-LAG
- All Versa devices, including switches are managed and controlled by centralized Orchestrator and controllers, without needing to login to individual devices.
- Fully redundant fabric with minimum blast radius.
- Industry standard 1RU form-factor for best space-to-power ratio.
- Future proof: easily upgrade switches independent of each other
- Hardware comes pre-configured with all important functions in an Enterprise deployment like dual PSUs, dual fan FRUs, so on.
- Simplified 3D licensing and fewer SKUs keep costs low.

I am a Service Provider or Multi-tenant Enterprise

Genuine Multi-tenancy: Clean separation of traffic of tenants, users applications, devices by policies



Builds on Versa's proven carrier class multi-tenancy:

- Full Multitenancy across all data and services layers: L2, L3, L4, L7
- Function separation including VRF, VPN, virtual-switch, IRB, and L4-7 services
- Use-case level separation – security, LAN, WAN, WLAN admins, operational roles
- Separate VXLAN overlays between SDN edges to extend multi-tenancy across units

VERSA

Comprehensive Coverage of LAN Capabilities

Comprehensive LAN Functions on ZT-LAN Platforms

Virtual switch	Access, Trunk	xSTP	VXLAN overlays on/off-ramp	EVPN Control Plane	Multi-Active	IRB	ACLs
Bridge domain	VLAN Manipulations	Passive Loop Detection	LLDP	VXLAN overlays on/off-ramp	LAG, Split LAG	L3 protocols	QoS

- Comprehensive stack of L2, L3, ACLs, QoS implemented on LAN platforms
- Standards based, multi-vendor interop tested and verified. Breaking vendor specific lock-ins
- Stateless functions operating at wire-rate on switch and AP platforms
- Stateful functions running on VOS embedded in the platform itself
- Seamless integration between specialized hardware complexes and VOS via SDK
- Leverage of hardware offload engines for wire-rate ZTNA enforcement and micro-segmentation

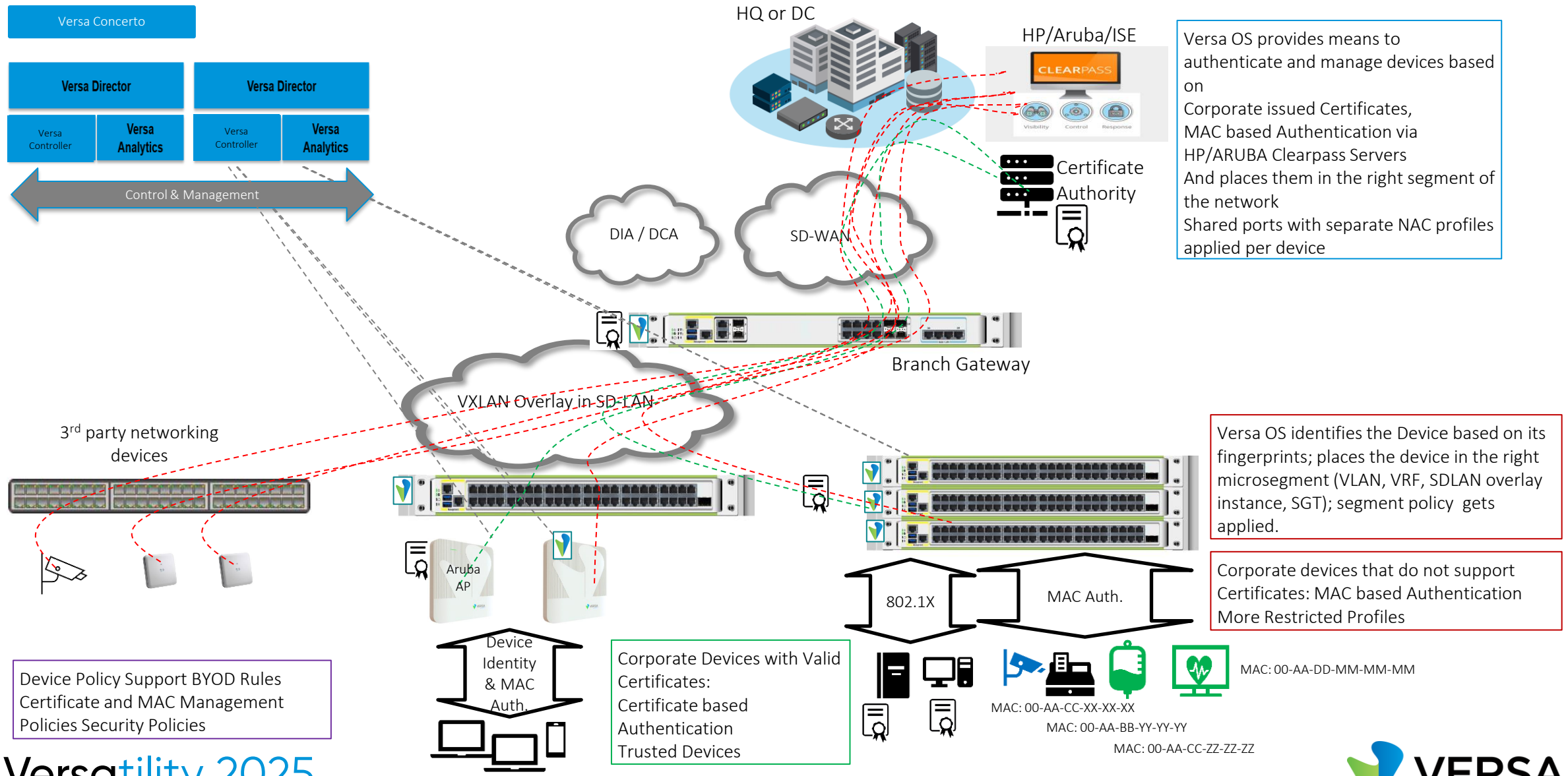
Natively Integrated Comprehensive Security Stack

Comprehensive Security Functions Needed to Fully Secure ZT-LAN Edge

Stateful Firewall	802.1X	URL Feeds and Filtering	NG-Firewall (NGFW)	Secure Proxy, Proxy Chain	Lateral Move. Protection	Security Policies	Malware Protection
DOS Protection	Device ID & Fingerprinting	IP Feeds and Filtering	Security Policies	SSL/TLS Proxy	NG IPS	DNS Security	Predictive Analysis

- Full security stack available in each Secure Ethernet Switch, Secure WLAN AP and ZT-LAN appliance
- Eliminating the need to deploy dedicated firewall appliances
- L4-7 and ZT-Edge functions deployed close to the user
- Inline application of L3-L4-L7 functions within the platform
- L3-L4 Security functions with trust, untrust zones, L7 security functions to manage application, URL traffic
- UTM security functions to scan payload and to secure against malware, vulnerability exploit attacks N-S and E-W directions

Versa ZTLAN fits Into Existing Campus Architecture



Versa OS provides means to authenticate and manage devices based on
Corporate issued Certificates,
MAC based Authentication via HP/ARUBA Clearpass Servers
And places them in the right segment of the network
Shared ports with separate NAC profiles applied per device

Versa OS identifies the Device based on its fingerprints; places the device in the right microsegment (VLAN, VRF, SDLAN overlay instance, SGT); segment policy gets applied.

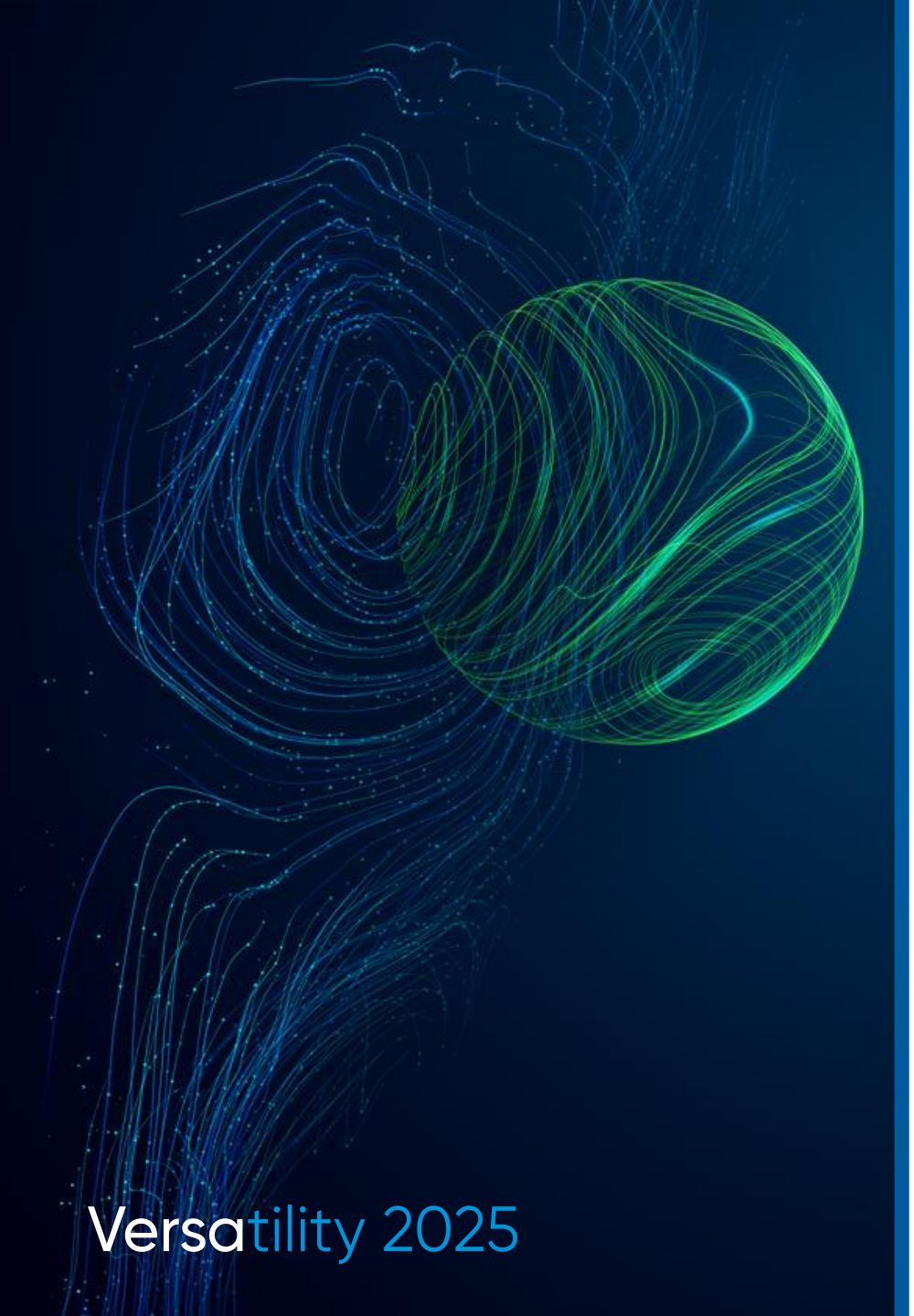
Corporate devices that do not support Certificates: MAC based Authentication
More Restricted Profiles

Device Policy Support BYOD Rules
Certificate and MAC Management
Policies Security Policies

Corporate Devices with Valid Certificates:
Certificate based Authentication
Trusted Devices

Versatility 2025

VERSA



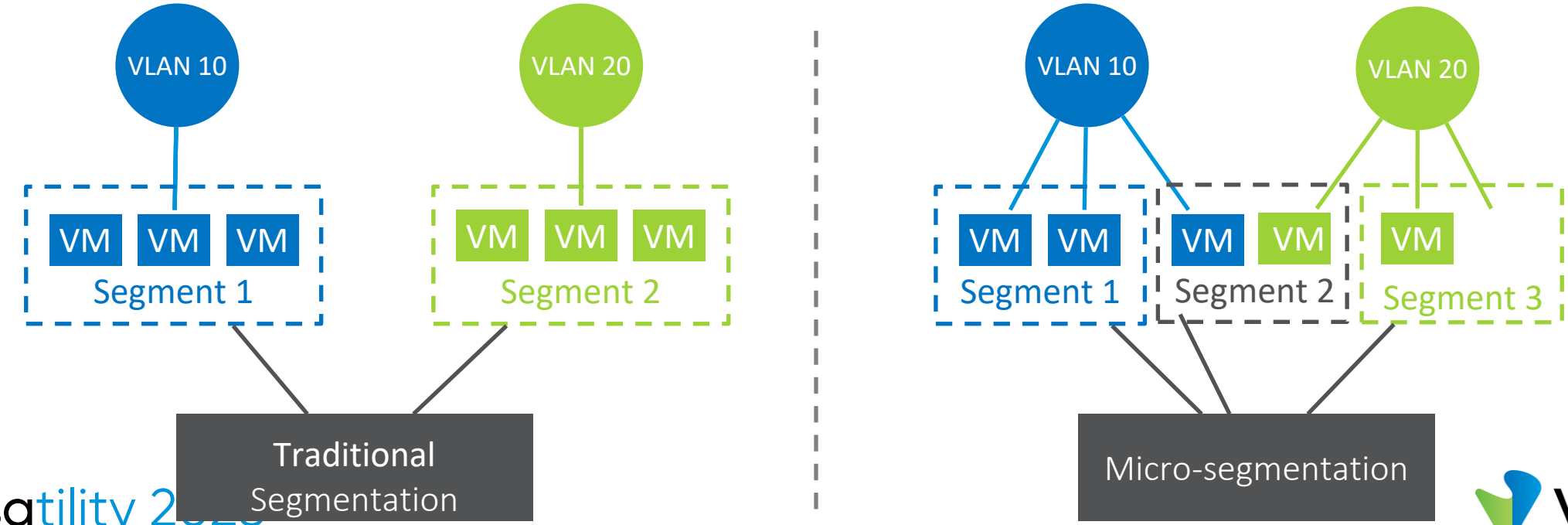
Versatility 2025

Adaptive Microsegmentation

VERSA

What is Micro-Segmentation ?

- Micro segmentation is a security method of managing network access between workloads. With micro segmentation, administrators can manage security policies that limit traffic based on the principle of least privilege and Zero Trust.
- Network segmentation is based on network address/port and geared to north-south data flow -- that is, client-server traffic between data centers.
- But micro-segmentation relies on exhaustive policies and is tailored to east-west data flows, or server-to-server traffic between applications.
- It can be applied to Workloads, VMs, Applications and Intelligent & Headless devices.



VERSA

NAC and ZTNA On-premises

802.1X NAC

- Certificate based client device authentication
- RADIUS backed – rich interop options
- Ability to place clients in respective microsegments
- Single supplicant, multiple supplicant profiles per port

Device Fingerprinting (Dev-ID)

- Inline Analysis of traffic flows for IoT (and Corporate, BYOD/personal) devices
- Device Fingerprint DB – Layer 2 to Layer 7
- Low Latency Rule-based Engine
- Match based on device class for consumption of policies, analytics, and others

User & Group Access Control

- User authentication via common IdP services or via Enterprise's own Active Directory
- Captive Portal or Passive/Inline User Authentication
- User Group policies
- Network access criteria, user policies based on user/group credentials

Adaptive Microsegmentation for Intelligent devices by assessing Device Posture

Facilitating connectivity and End-Device Profile Check

- User and device authentication
- Connects to nearest VOS instances on-prem

End-Point (device) Information Profile (EIP) selection based on

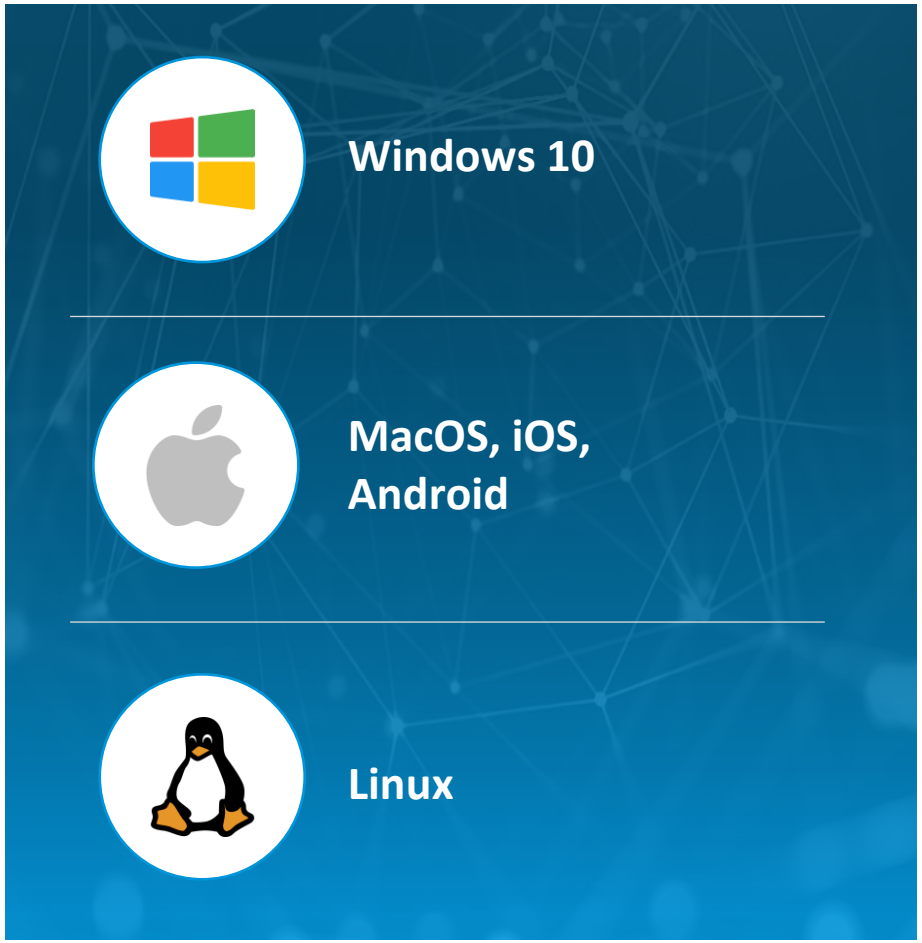
- AV engine version, signature db version running on the End-Point
- OS type & version, Security Patch versions
- Corporate or personal device
- Specific software installed or not
- Disk encryption and other parameters
- Supported with **Versa SASE Client, Palo Alto Global Protect client, and Intune managed devices**.

Policy application starting from client devices

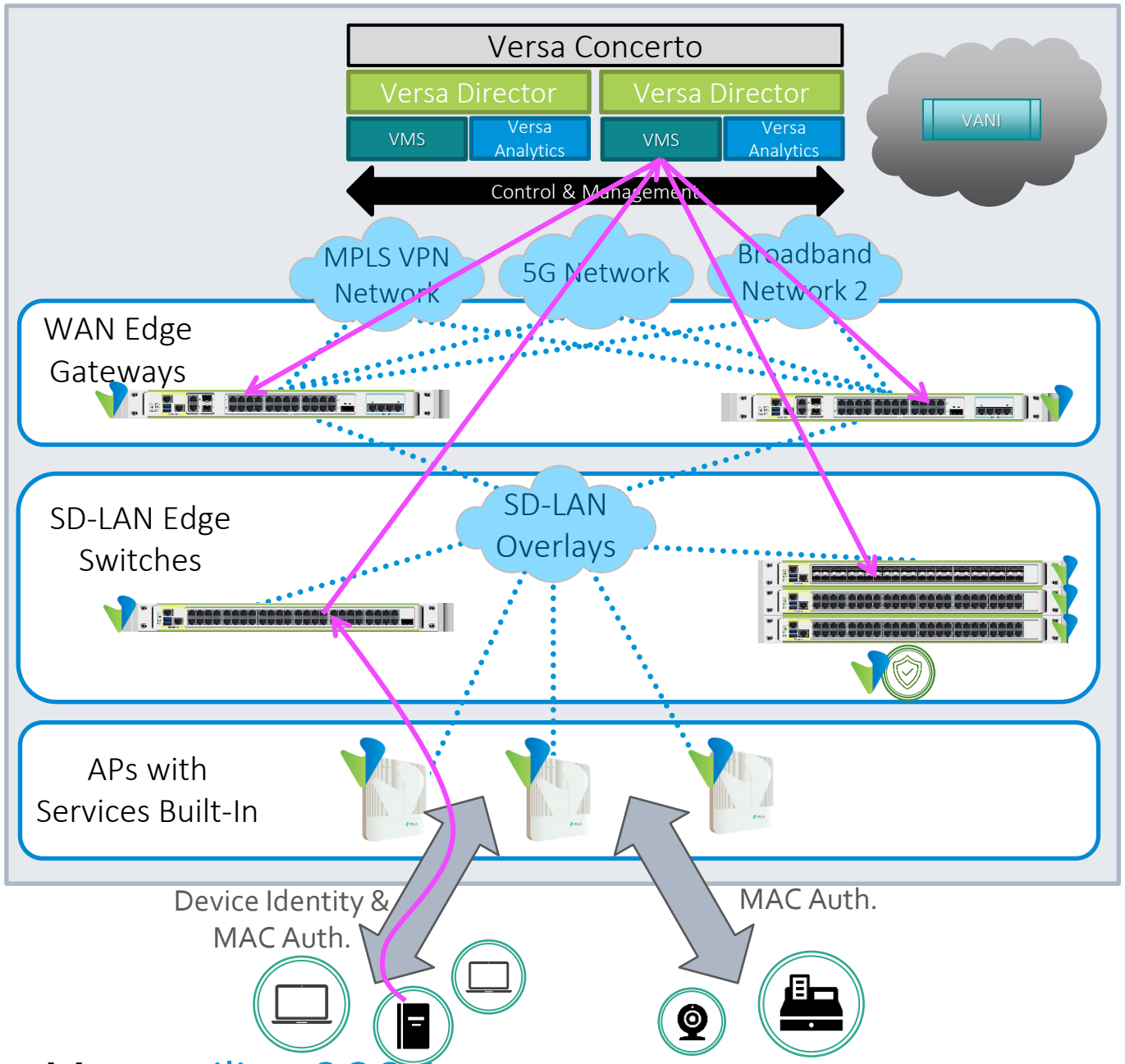
- Compliance check
- Traffic Steering via SASE Client

EIP based Policy Enforcement

- Implemented on the nearest VOS platform
- Inline, high performance traffic processing
- Managed via network and security policies



Zero Trust LAN
Microsegmentation Control Plane



When Versa Client connects to the switch, device posture(EIP) is gathered and distributed to all other VOS devices using VMS

VERSA

Adaptive Microsegmention for IoT/Headless/Agentless devices

- Device is identified and classified based on inline analysis of important fingerprint traffic
- Classification of millions of devices
- Device tag and reputation
- Fine grained device policy configuration
- Dynamic risk based device quarantine
- Integrated device monitoring and analytics

Near Real-Time Remediation of Threats

- Limiting activities that an entity can do
- Constraining or blocking entity
- Flow mirroring

IoT/Headless Devices Fingerprinting

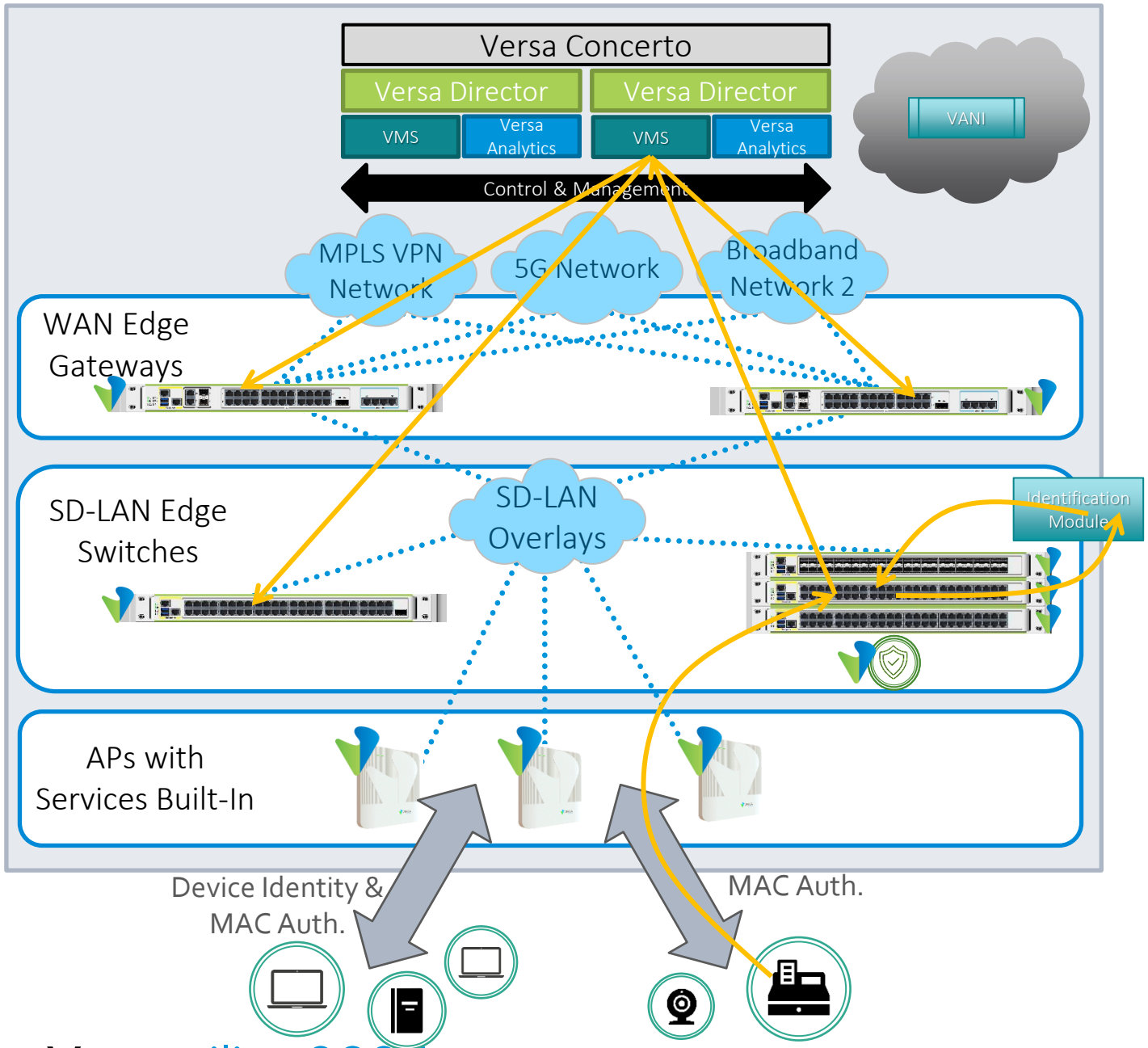
Attributes Considered

- Device MAC Address
- DHCP
- DHCP vendor
- DHCP Hostname
- DNS packets/ Destination Host
- TCP Syn packets
- TCP Syn-Ack packets
- SSL client, server hello packets (JA3 signatures)
- HTTP headers (user-agent)
- MDNS packets
- LLDP fingerprint

Device Information Returned:

- Vendor: Device vendor name - ex : Apple
- Model: Device model - example : iPad
- OS: Device operating system - example : Microsoft Windows Kernel 6.0
- Parent OS: Parent operating system - example : Windows OS
- Family: Device Family - example : Computer
- Subfamily: Device subcategory - example : Desktop
- Prod: Productivity value of the device (low to high) - example: 5 (high productivity device)
- Risk: Risk of the device (low to high) - example: 1 (low risk device)
- Score: Response confidence score - example : 60/100

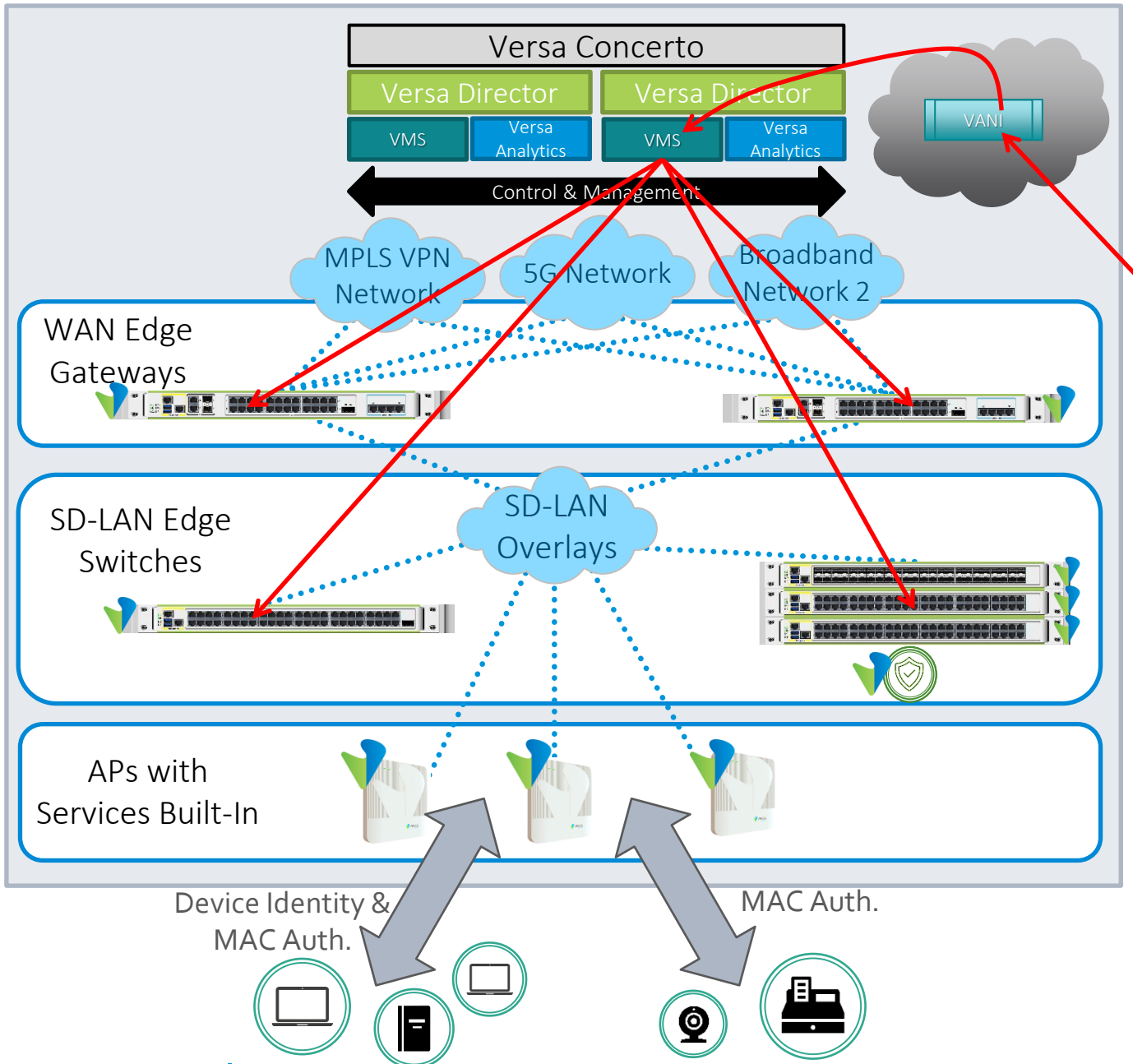
Zero Trust LAN
Microsegmentation Control Plane



When IoT/Headless device sends traffic through the switch, the device is identified and distributed to all other VOS devices using VMS

VERSA

Zero Trust LAN
Microsegmentation Control Plane

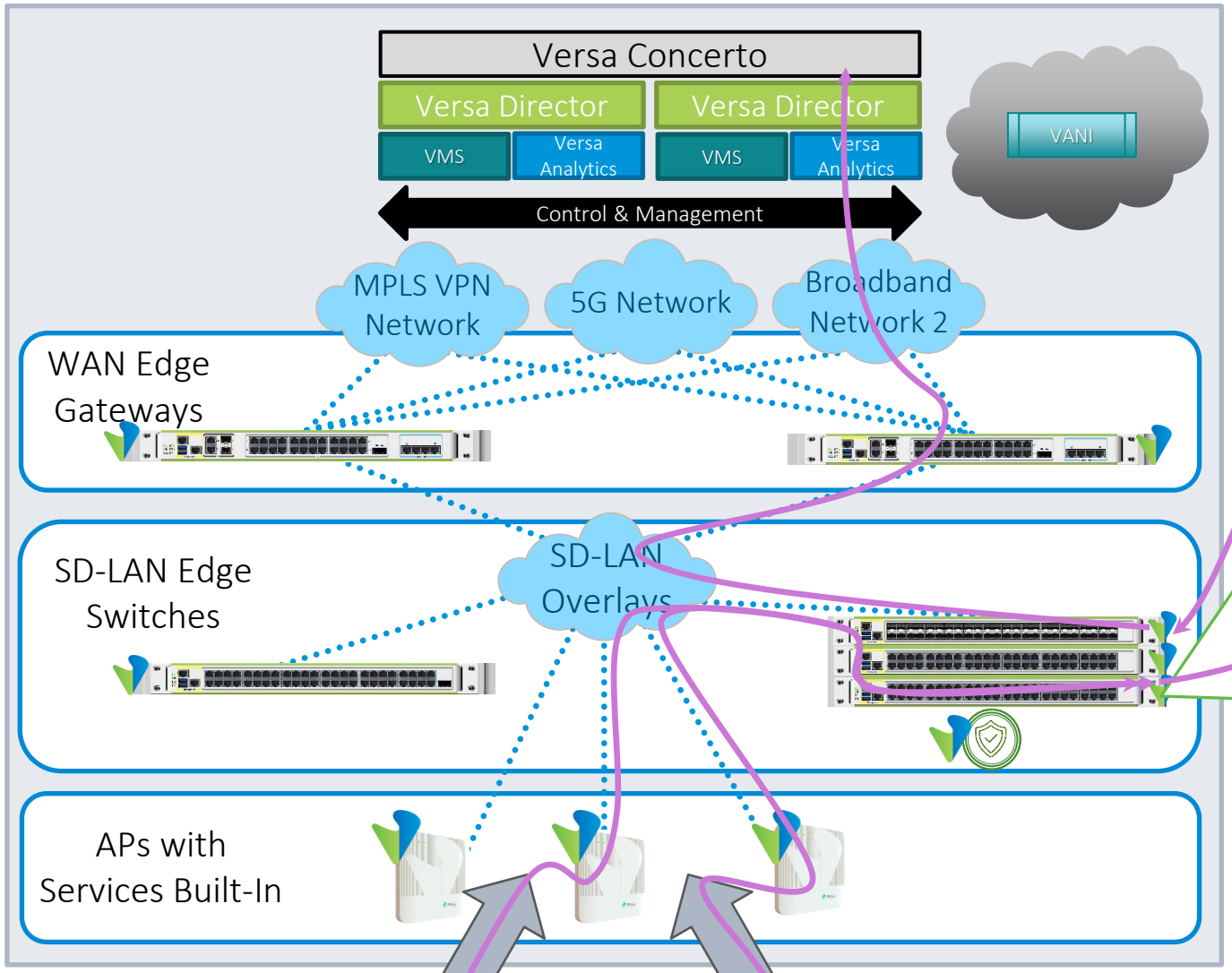


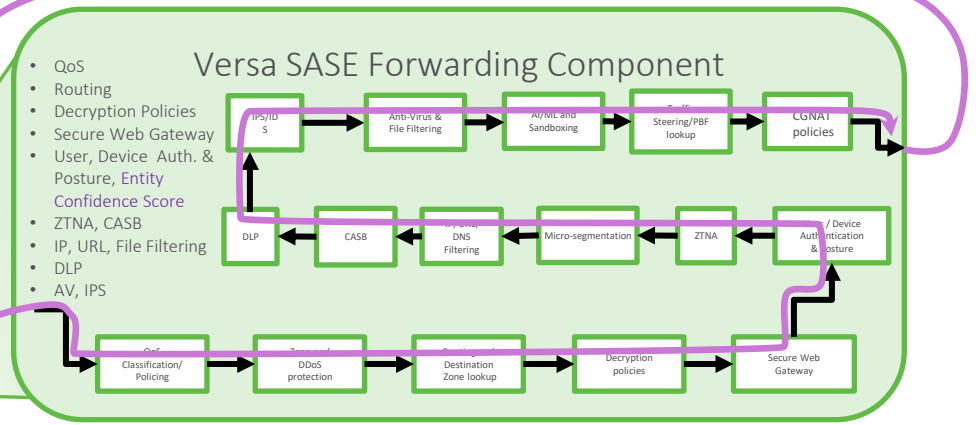
VANI gets feeds from Versa Analytics, Microsoft InTune, PA Global Protect, Crowd Strike and others.

VANI gets signals from various VOS entities and third party security servers, computes the DRS/UCS and distribute it to all VOS devices.

VERSA

Zero Trust LAN Data Plane





Versatility 2025

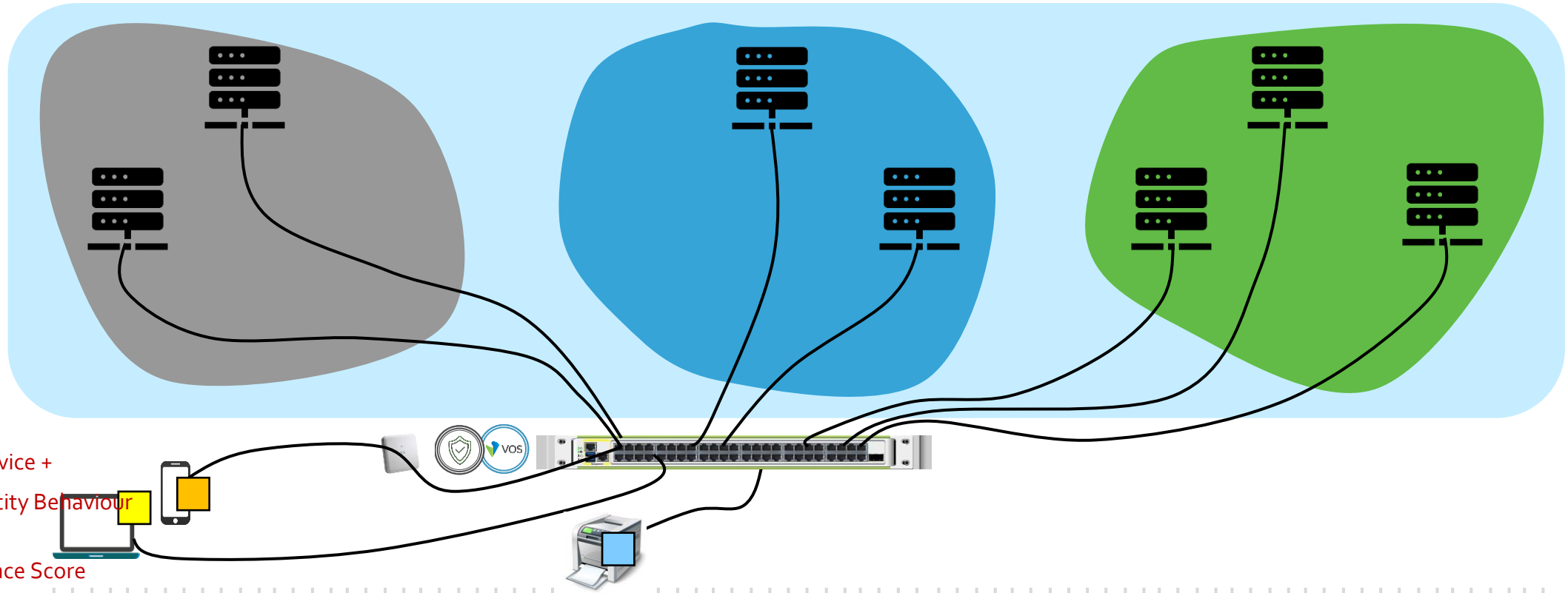
VERSA

Adaptive Micro-segmentation based on RS/Device Posture

Highly Restrictive Policy

Resource Access Policy

Lenient Policy



Compliant Device +

Compliant Entity Behaviour

=

High Confidence Score

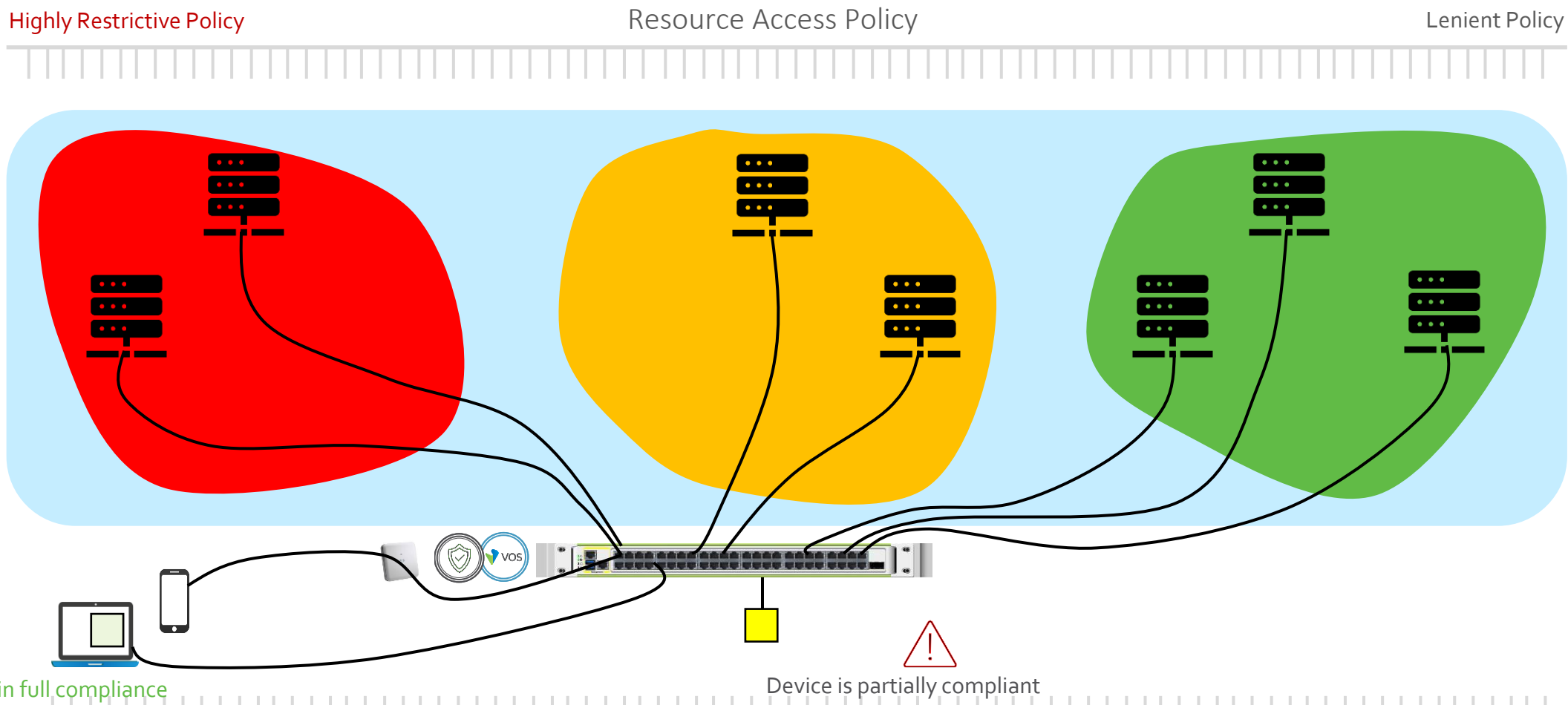
High

Risk Score/Device Posture

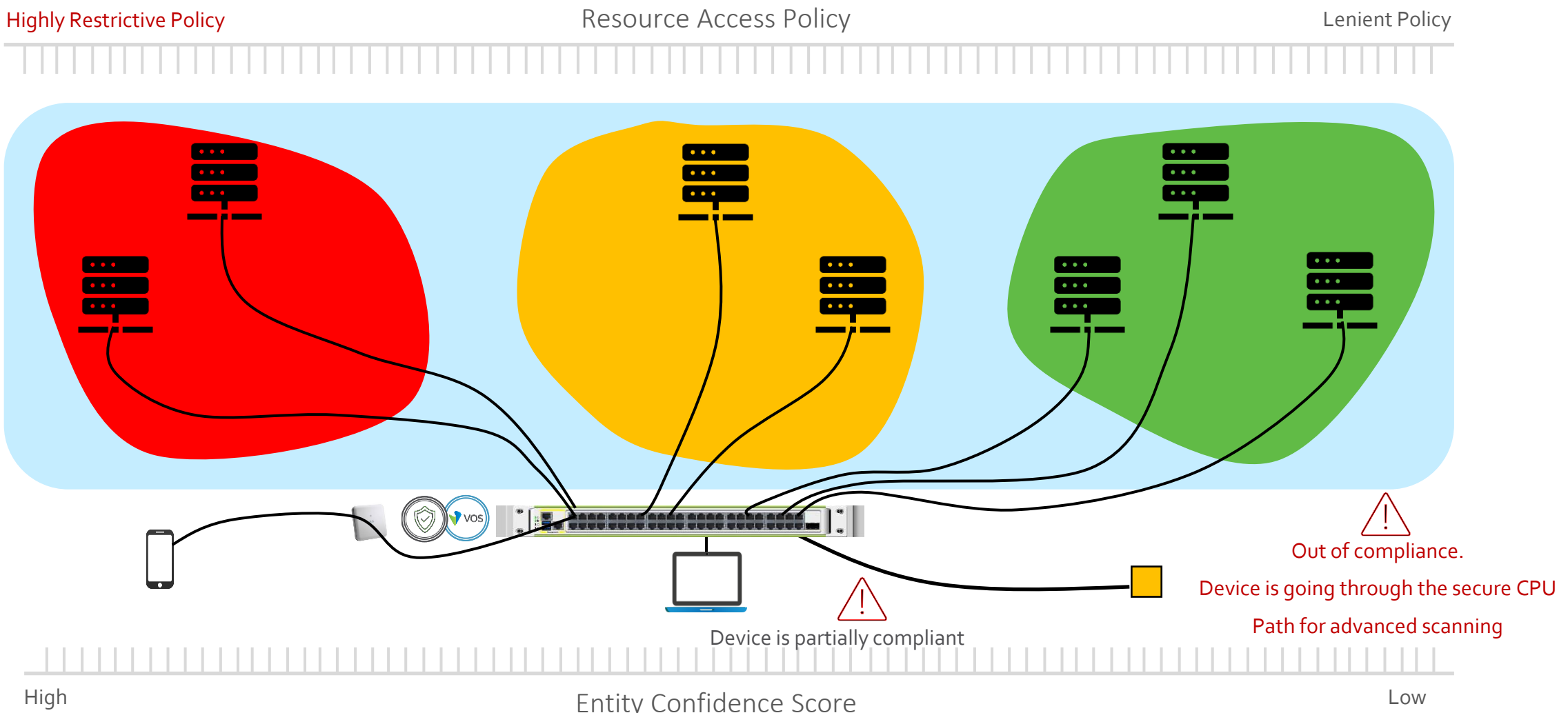
Low

VERSA

Adaptive Micro-segmentation based on RS/Device Posture

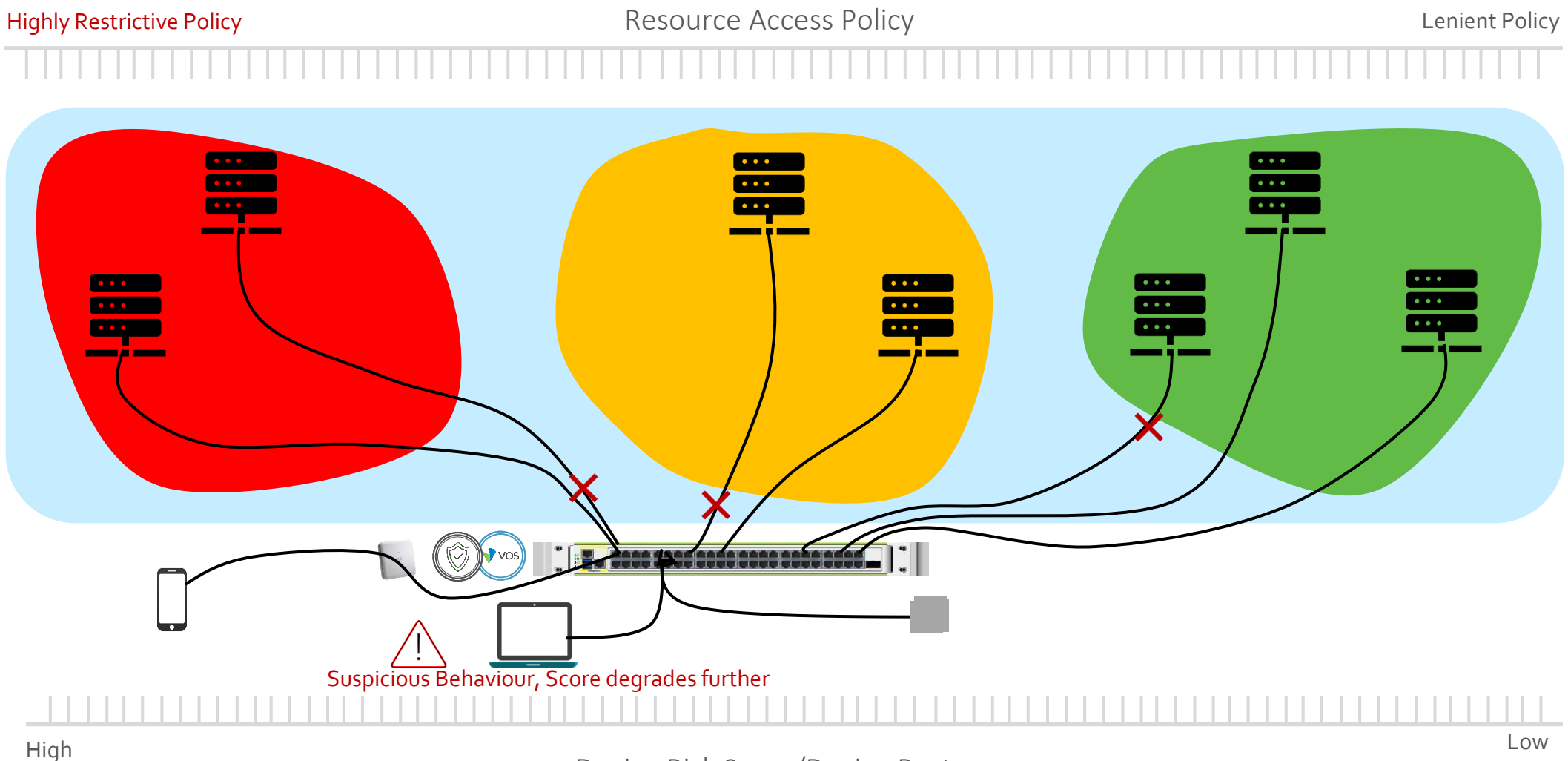


Adaptive Micro-segmentation based on Entity Confidence Score



VERSA

Adaptive Micro-segmentation based on DRS/Device Posture

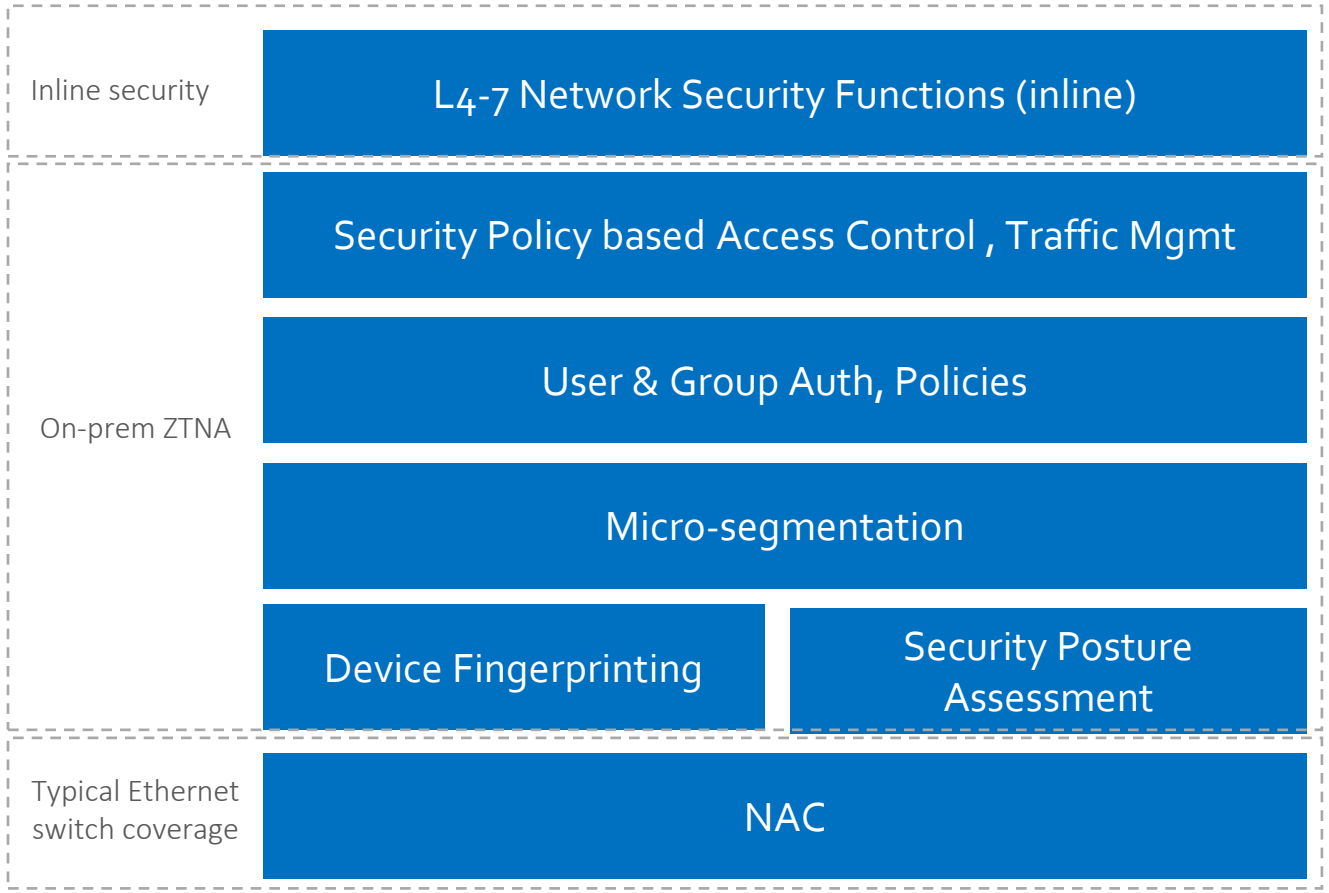


VERSA

Versa's Innovations in Microsegmentation

* Dynamic Adaptive Microsegmentation.
* Inline Secure Path with Microsegmentation.
* IoT/Headless/Intelligent devices support.
* Supports intelligent devices with and without end point agent.
* Standards based SGT ID distribution.
* Multihoming support for Microsegmentation.
* Ingress Kill.
* ML/AI based dynamic end point risk score computation.

Versa's Comprehensive Approach to LAN Security



- Single pane-of-glass Management, Operations
- Single security and networking converged stack of Versa OS (VOS) for contextual decisions.
- Homogenous, well-integrated, and tested code.
- Uniform Policy Language and enforcement.
- On-premises ZTNA with dynamic Security Posture and device fingerprinting.
- Comprehensive Security features.
- Comprehensive LAN L2 to L7 features.
- Simple and transparent pricing and support.

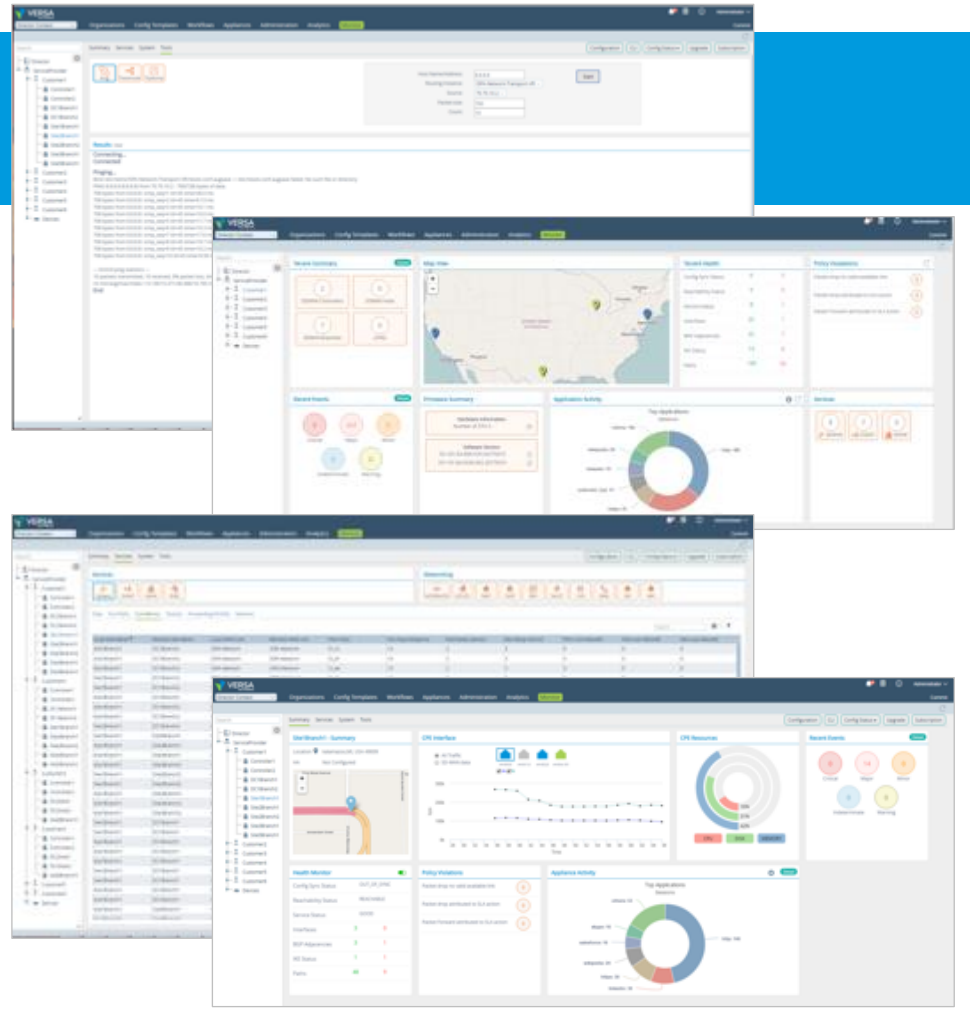
VERSA

Single Pane Of Glass Operations

For WAN, LAN, Campus, and DC

Design, Deploy and Operate

- Centralized Policy Management & Enforcement
- Service Orchestration & Management
  - Versa and validated 3rd Party VNFs
- Cloud Management System Integration
  - Automated AWS and Azure
  - VMware, OpenStack, Docker
- Device, Security and Service Monitoring
- Hierarchical Multi-tenancy with RBAC
- 3rd party API Integration

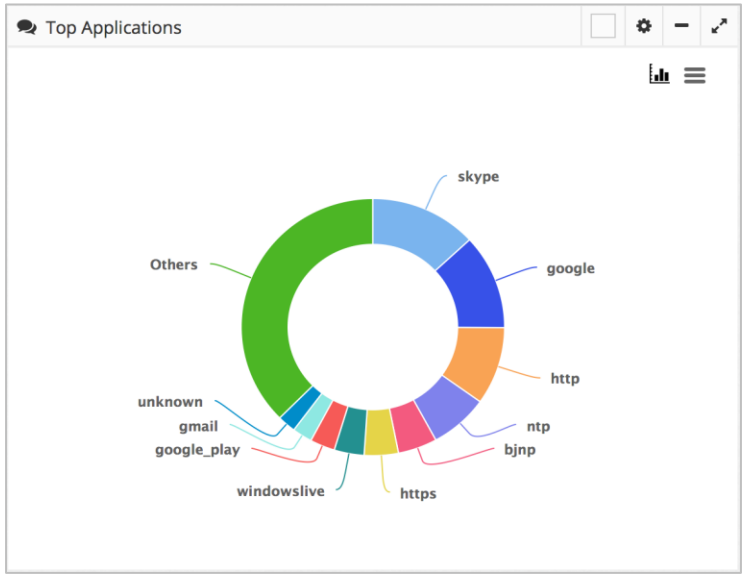


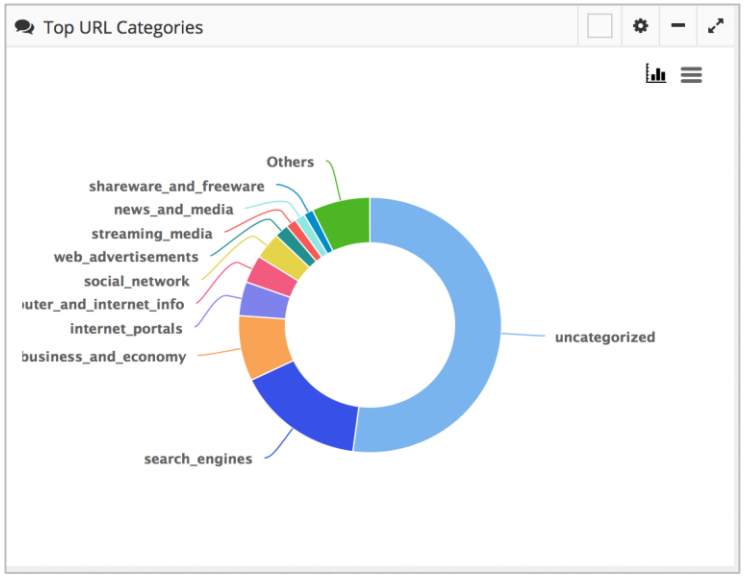
Versatility 2025

VERSA

ML/AI based Insights with Built-in Analytics

Bigdata based visibility and analytics at the switching layer





- Big Data AI/ML Based Analytics
- IPFix and Netflow Based Traffic Flow Reporting
- Reporting of SD-LAN Topology
- Near Real Time Traffic Info
- Application and App Performance Traffic Breakdown
- Per User & Group Traffic Break Down
- Strong Multi-tenancy and RBAC

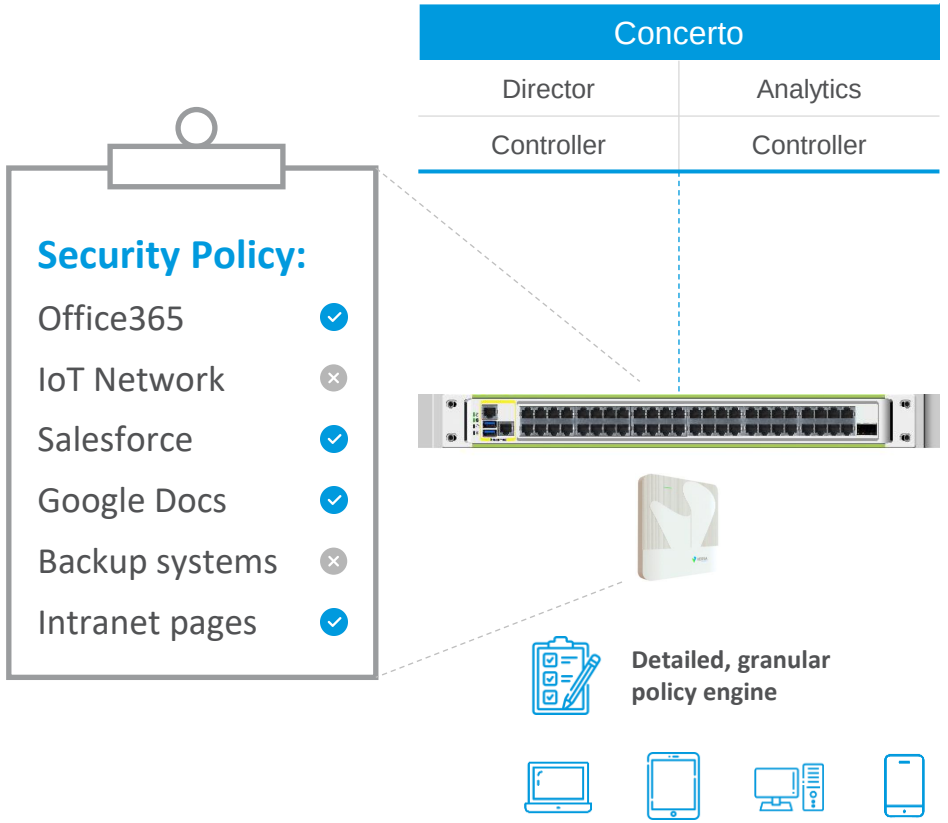
Versatility 2025

VERSA

Uniform, Rich Policy Engine – L2-L7

Flexible policy match triggers	
Applications	ie: Protocols
Applications filters, groups classes of traffic with default actions	ie: Predefined
URL, URL category based	ie: Enterprise App
Events, Context, Logs, etc based on location	ie: Allow, Disallow

- Powerful policy options required
  - Allow, block, rate-Limit, and classify network traffic based on application identification and user defined policies
- Risk-based traffic management
- User policies to control user access to all segments of network



VERSA

Legacy Campus vs Versa ZT-LAN

Legacy Campus	Versa ZT-LAN
Security using NAC (VLAN, ACL, 802.1x, port, IP Source Guard, Private VLANs etc.) results in decreased risk posture	Security using Versa ZT-PREM and Security complex within the switch provides L2 to L7 security.
Multiple Management Consoles, with limited or no management integration between them results in increased Opex.	Single head end for all networking and security layers.
Multiple data planes, multiple places to manage policies, inconsistent policy enforcement and decreased risk posture	Single software defined unified data plane for wired, wireless and IoT. Consistent policy enforcement.
Static segmentation based on VLANs and VRFs leading to increased blast surface and decreased risk posture	Adaptive Micro-segmentation based on continuous assessment of device posture, inline signatures and confidence score(DRS)
No built-in security for E-W direction leading to increased blast surface and decreased risk posture	L2-L7 advanced security enforced both for L2 and L3 traffic right at the source to minimize the blast radius.
Complex failure prone Virtual Chassis and MC-LAG solution	Distributed standards based EVPN-VXLAN fungible fabric
Reactive Secure Networking • Results in increased Opex • Poor user experience	Predictive AI/ML based Secure Campus, Branch, WAN Edge Networking ○ Natural Language Processing (NLP) Engine ○ Anomaly detection engine ○ Prediction engine
Limited or no visibility results in increased opex and poor user experience	Advanced visibility, User Entity Behavior Analytics (UEBA). Every VOS device gets information on every user and endpoints.

CSX Switch Appliances

CSX8500:
32X100G

CSX8300:
48 x 25G + 8 x 100G

CSX 4500:
36x2.5G + 12x10G Multirate PoE + 4x25G + 2x100G Uplinks

CSX4300:
48GE PoE + 4x25G + 2x100G Uplinks

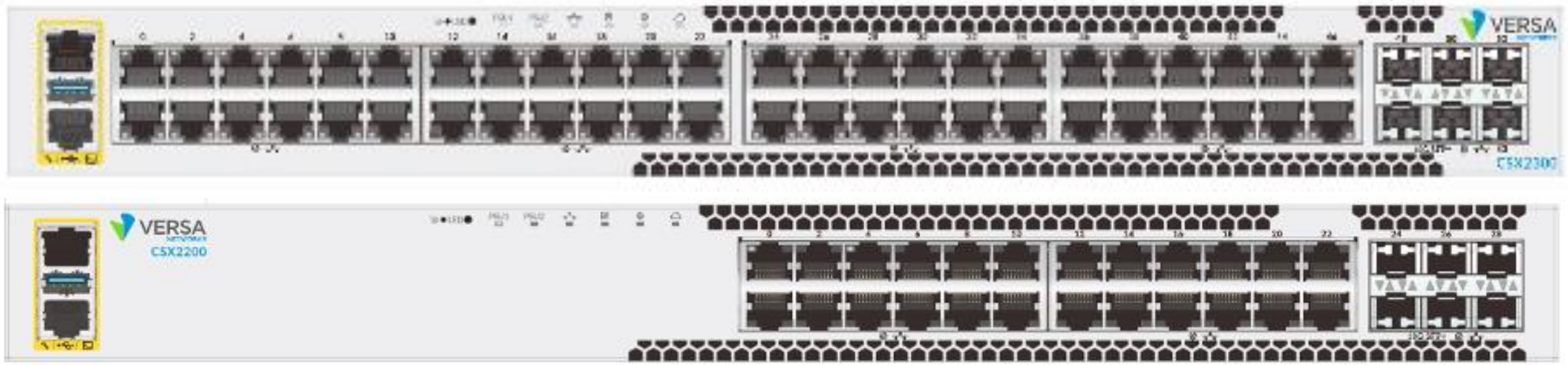
Performance

Access | Access | Aggregation | Core

Versatility 2025

VERSA

CSX New Kid(May 2025 Release) - 2K Series



SKU	Port-I/O
CSX2300	48x1G/100M/10M Copper ports + 6x10G SFP+ Fiber ports
CSX2200	24x1G/100M/10M Copper ports + 6x10G SFP+ Fiber ports

CSG WAN Edge Appliances

CSG3000 > 15 Gbps + 540Gbps switching

CSG5000 > 100 Gbps

CSG2500 > 25 Gbps

CSG1000 > 15 Gbps

CSG700 > 2 Gbps

CSG300 > 800 Mbps

SD-WAN Performance

Small Branch | Medium Branch | Large Branch | Hub Datacenter

Versatility 2025

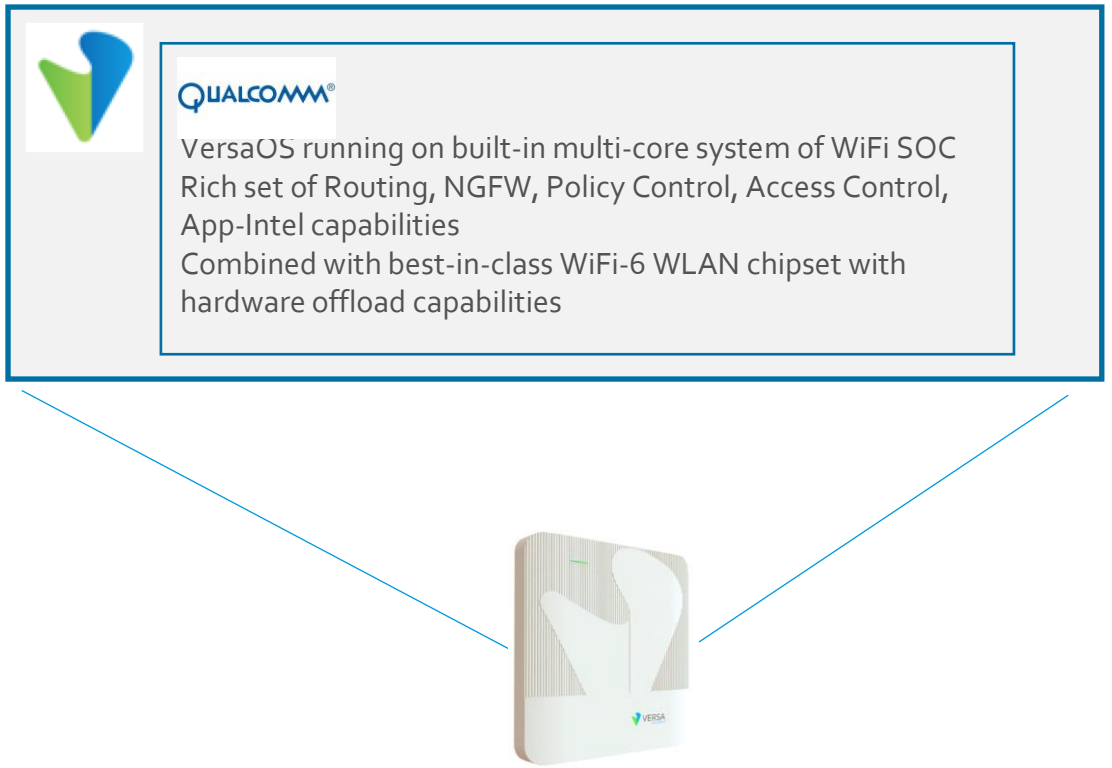
VERSA

Extend the Software Defined LAN to Wireless

* Integrated Versa-OS onto Enterprise Class APs
* Running natively on best-in-class merchant Enterprise AP chipset (Qualcomm Hawkeye-II)
* 802.11AX based product family – H/M/L class APs

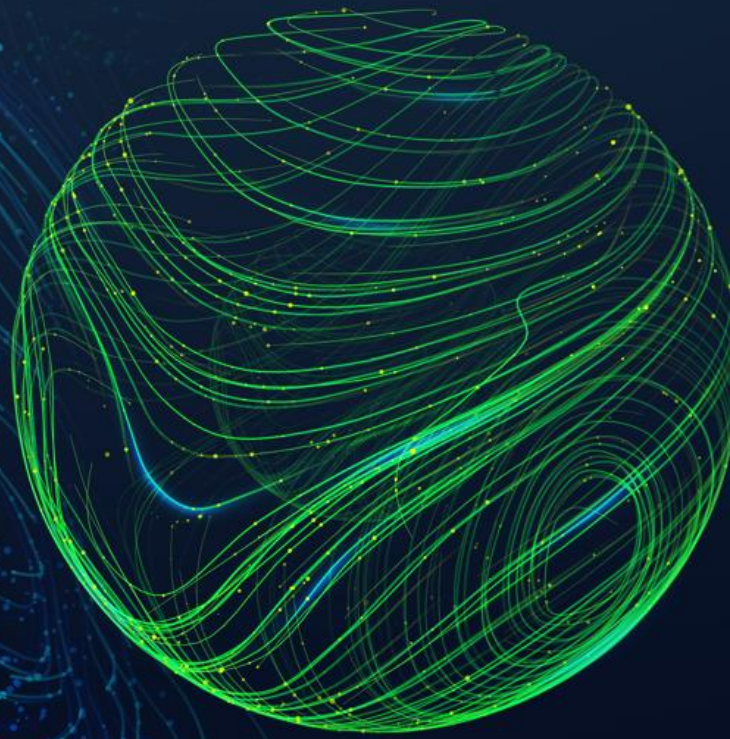
L2, L3, L4-7 functions (NGFW, App Traffic Mgmt, Policy Ctrl, User/Group Access & Auth) natively provided by each AP

* Wired and Wireless Mesh
* Hardware offload for Encryption, QoS and other functions
* Distributed, centralized, hybrid deployment options to provide deployment flexibility
* Full multi-tenancy with RBAC, L2, L3, and across overlays



VERSA

Thank you



Versatility 2025

VERSA