VERSATILITY

Versa Zero Trust LAN

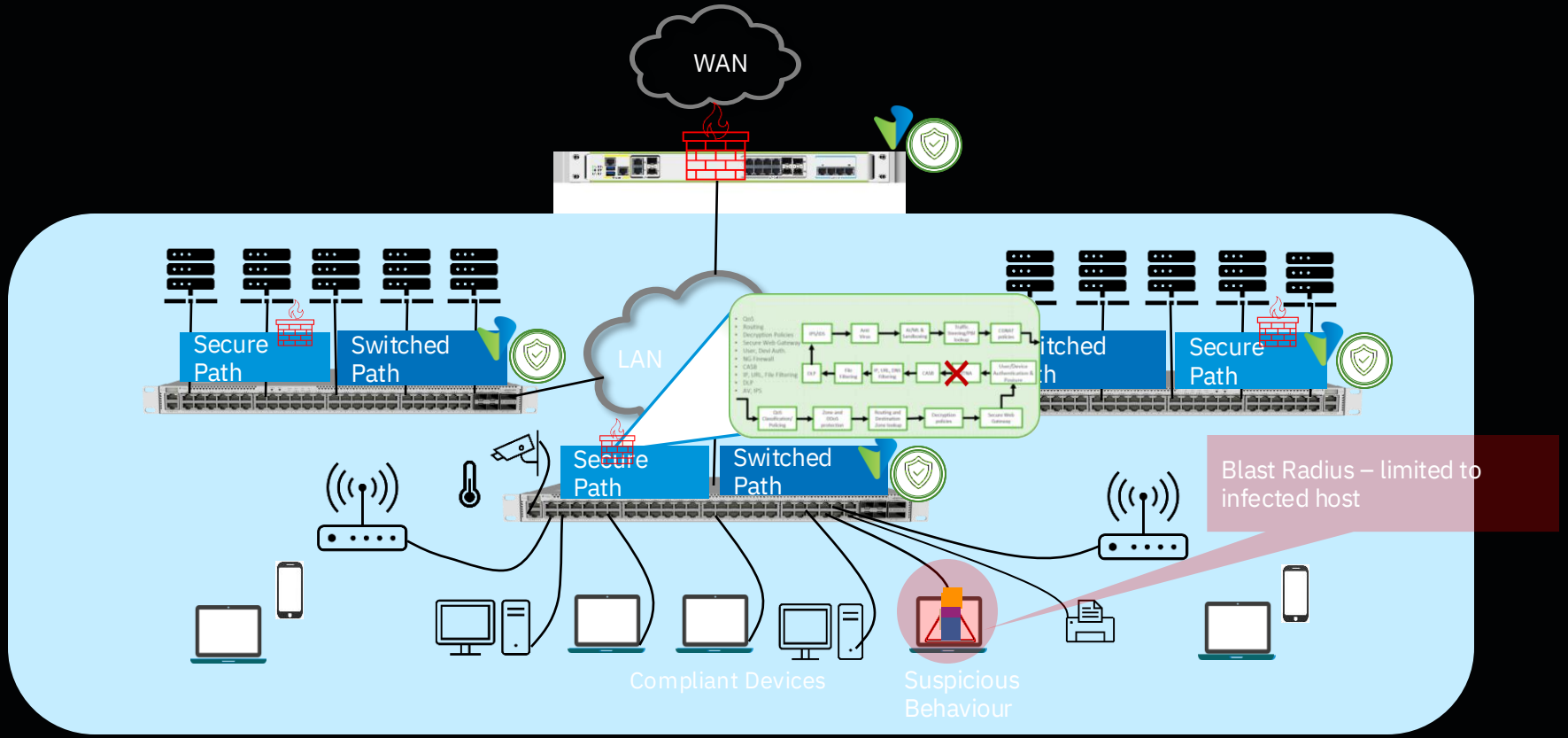
ZT-LAN

Intelligence-Driven Security for Every Edge

Why Zero Trust LAN?

- Historically LAN is a Safe Zone but not anymore.
- **IoT Proliferation:** Devices like smart cameras and printers often lack robust built-in security, making them easy entry points for attackers.
- **Hybrid Work:** Devices move between home and office environments, potentially bringing malware from unsecured home networks into the corporate LAN.
- In a standard "Flat LAN Network", a compromised laptop or a rogue IoT device can often perform "lateral movement." This means the threat can scan the network, find vulnerable servers, and exfiltrate data.

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



VERSATILITY

ZT-LAN: Blast Radius Confined to the Infected Host

Compliant Device + Compliant Entity Behavior = High Confidence Score → Switched Path

Switched Path

Standard switching for verified compliant devices. Full network connectivity with normal routing.

Normal Operation

Suspicious Behaviour

Entity confidence score drops. Dynamic risk assessment triggers enhanced inspection and path isolation.

Enhanced Monitoring

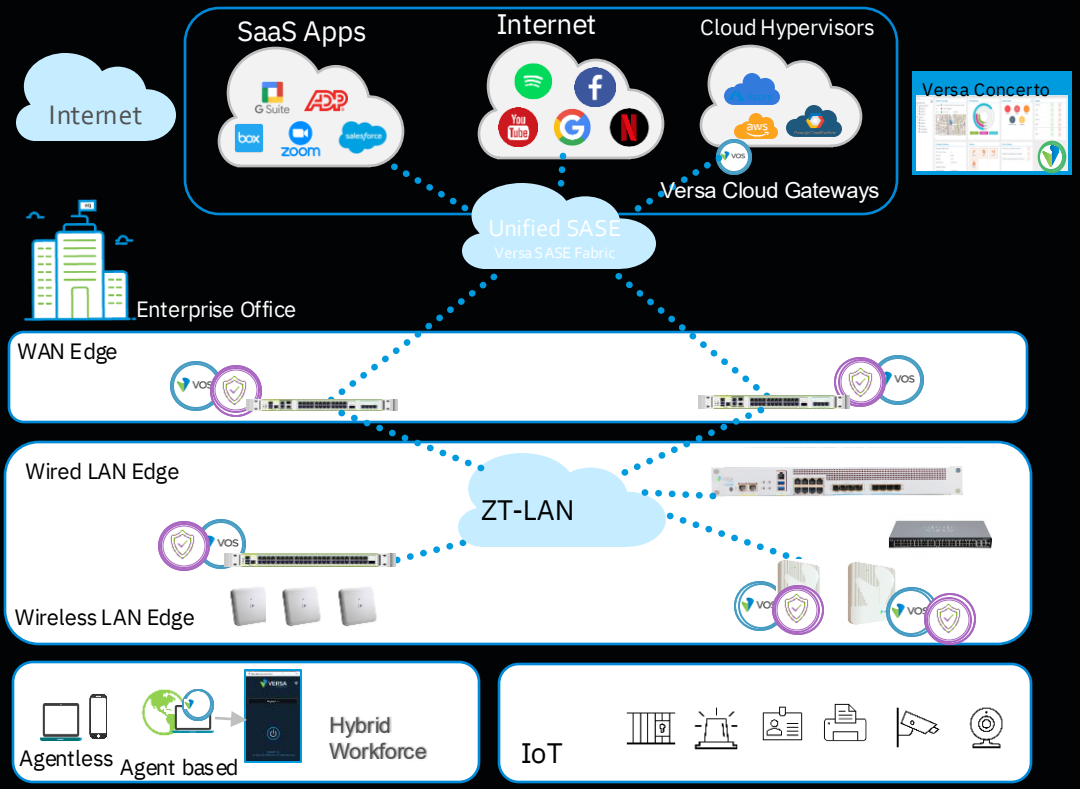
Blast Radius Contained

Compromised host is isolated. Lateral movement is blocked. Threat confined to single endpoint.

Threat Isolated

VERSATILITY

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, and single policy language
- Built-in inline ZTNA in every edge

VERSATILITY

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

VERSATILITY

Adaptive Microsegmentation

802.1X NAC

- Certificate-based client device authentication
- RADIUS-backed with rich interoperability options
- Place clients into respective microsegments automatically
- Single or multiple supplicant profiles per port

User & Group Access Control

- User auth via common IdP or Active Directory
- Captive portal or passive/inline user authentication
- User Group policies with fine-grained access criteria
- Network access criteria based on user/group credentials

Device Fingerprinting (Dev-ID)

- Inline analysis of L2–L7 traffic flows for IoT, BYOD, corporate devices
- Fingerprint DB with millions of device classifications
- Low-latency rule-based engine with device class tagging
- Dynamic risk-based quarantine and integrated analytics

Adaptive Microsegmentation for IoT / Headless / AgentlessDevices

Inline Device Classification

Device identified and classified based on fingerprint traffic analysis across millions of device profiles.

Device Tag & Reputation

Fine-grained device policy configuration with device reputation scoring and tagging.

Dynamic Risk Quarantine

Risk-based device quarantine triggered automatically. Near real-time threat remediation.

Integrated Monitoring

Device monitoring and analytics with deep visibility into device behaviour and anomalies.

Activity Limiting

Constrain or block entity activities. Limit lateral movement and flow mirroring for forensics.

Near Real-Time Remediation

Automated response pipeline from detection to isolation without manual intervention.

Adaptive Microsegmentation – Device Posture for Intelligent Devices

End-Point Information Profile (EIP) Criteria

- AV engine version & signature DB version
- OS type, version & security patch level
- Corporate vs personal device classification
- Specific required software present or absent
- Disk encryption status
- Custom compliance parameters

Supported Endpoint Clients

Versa SASE Client

Windows 10 and 11, macOS, iOS, Android, Linux

Palo Alto Global Protect

Enterprise endpoint agent integration

Intune Managed Devices

Microsoft Intune-enrolled device support

EIP → Policy Enforcement → Nearest VOS Instance → Inline High-Performance Processing

VERSATILITY

Versa’s Innovations in Microsegmentation

01

Dynamic Adaptive Microsegmentation

Continuously adapts based on real-time device posture, confidence score, and inline traffic signals.

02

Inline Secure Path with Microsegmentation

Security enforced directly in the data path — no hair-pinning to dedicated firewall appliances.

03

IoT / Headless / Intelligent Device Support

Full coverage for agentless and agent-based endpoints with unified policy enforcement.

04

Standards-based SGT ID Distribution

Scalable Group Tag distribution without vendor-proprietary protocols or lock-in.

05

Multihoming Support

Microsegmentation enforced across multi-homed EVPN-VXLAN fabric with active-active redundancy.

06

Ingress Kill

Threat eliminated at ingress — lateral movement blocked before it starts.

07

ML/AI Dynamic Risk Scoring

Continuous endpoint risk score computation using behavioral ML models in real-time.

08

Universal ZTNA Fabric

Microsegmentation extends consistently across SD-LAN, SD-WAN, and Cloud SASE environments.

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

VERSATILITY

Recent Innovations in SD-LAN

Simplified SD-LAN Workflow

Campus networks provisioned in hours instead of weeks. AI-guided templates reduce operator error.

AI-Assisted ZTNA in Campus

AI dynamically adjusts ZTNA policies based on user and device behavior signals in campus networks.

AI Network Anomaly Detection

ML models monitor telemetry streams to identify deviations and trigger proactive remediation.

Claude-Based MCP Server

Natural language troubleshooting via Claude MCP server integration for autonomous network ops.

CSX 2200 & 2300 Platforms

New entry-level access switches delivering full ZT-LAN capabilities in a compact 1RU form factor.

Hierarchical Scheduler & Shaper

Enterprise-grade QoS with hierarchical scheduling and shaping for multi-service traffic management.

Roadmap

Q2 2026	• Multicast & IGMP Snooping • Egress ACLs • **CSX 1100 / 1200 / 3200 Platform Launch**
Q3 2026	• Link Level Flow Control • Priority Level Flow Control • Explicit Congestion Notification (ECN) • Inband Flow Analyzer for Path Metrics • MACSec Encryption

Thank You

VERSATILITY