VersaONE: Delivering Intelligent Edge for the AI-Driven Enterprise

Elastic edge compute. Resilient connectivity. Pervasive security. Autonomous operations.

AI is reshaping how enterprises operate, but most networks were never designed for it. As AI workloads, agents, and inference pipelines spread across branches, campuses, data centers, and cloud environments, the demands on network infrastructure outpace what legacy architectures can deliver. Enterprises need Intelligent Edge, a convergence of networking, security, AI-powered operations, and edge compute based on how modern enterprises actually run. VersaONE delivers the Intelligent Edge today in a single, purpose-built platform optimized for the AI-first enterprise.

Customer challenges: AI demands a new kind of network

Enterprise networks were built for a world where traffic flowed largely in one direction from the data center to the user. AI changes that. Today, inference workloads generate massive data volumes that move east-west between services, south-north from edge devices to the cloud, and back again.

Most architectures are not designed for this. The gaps they leave create performance bottlenecks, security blind spots, and operational complexity that slows enterprise operations and increases risks.

Today's customer challenges

Networks are not built for AI

Topology challenge

AI workloads create east-west, north-south, and south-north traffic flows, but most enterprise networks are only optimized for north-south traffic.

Capacity challenge

AI workloads generate massive data volumes that must be processed and transferred across distributed environments.

Visibility gaps leave organizations exposed

Visibility challenge

Organizations lack full visibility across users, applications, devices, and AI workloads. With these blind spots, security teams can't monitor or enforce policy consistently across the environment.

One-way security falls short in AI-driven environments

Control challenge

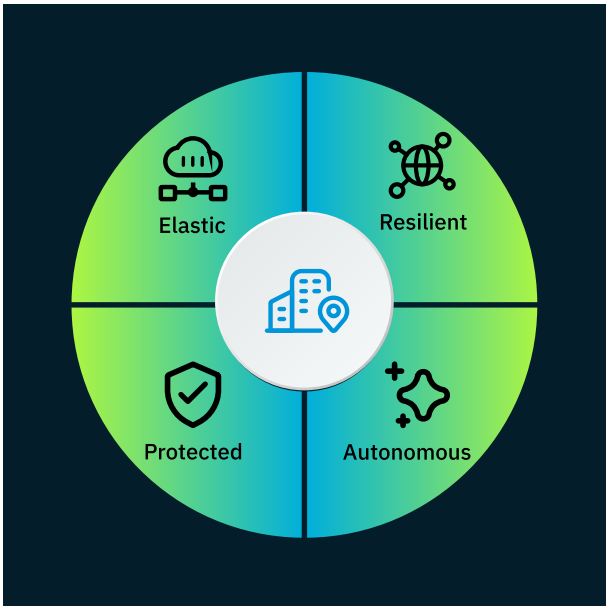
Zero Trust implementations focus on users but typically don't cover devices and AI agents.

Security challenge

Existing security architectures are designed for one-directional traffic. They struggle to enforce policy across distributed trust relationships introduced by AI workloads and agents.

What is Intelligent Edge?

The Intelligent Edge is a new architectural standard where connectivity, security, and compute converge at the edge of the enterprise network. As AI adoption drives distributed intelligence across branches, campuses, data centers, and cloud environments, organizations must replace traditional function-specific appliances with a unified edge architecture built around four core principles.



1 - Elasticity

The edge must do more than connect. It must converge compute, networking, storage, and security.

Required capabilities

- **Hardware convergence:** Intelligently use CPU, GPU, and DPU
- **Workload hosting:** Natively run business apps (e.g. Point of Sales (POS), distributed AI services, mini-LLMs)
- **Operational continuity:** Operate autonomously during connectivity loss
- **Built-in security:** Protect traffic in any direction without point products

2 - Resilience

Enterprise infrastructure must be self-healing and topology-aware for uninterrupted, any-direction connectivity.

Required capabilities

- **Hybrid WAN:** Seamlessly blend 5G, MPLS, satellite, and internet for improved uptime
- **Dynamic topology:** Support full-mesh, partial-mesh, and hub-spoke architectures
- **Traffic intelligence:** Automatically handle AI inference spikes and model synchronization

3 - Protection

Security must become pervasive for humans and machines, moving beyond the gateway for any-direction traffic coverage.

Required capabilities

- **Zero Trust Everywhere:** Inspect traffic in any direction
- **AI-specific defense:** Built-in defense against prompt injection, jailbreaking, and Shadow AI
- **Identity aware:** Zero Trust for humans and non-human AI agents
- **Microsegmentation:** Isolate IT and OT environments

4 - Autonomy

Complexity has outpaced human management. Enterprises must use AIOps to correlate, predict, and resolve autonomously.

Required capabilities

- **Natural language interaction:** Manage infrastructure via AI agents and co-pilots
- **Root cause analysis:** Automatically correlate telemetry to find root causes and suppress noise
- **Complete AI visibility:** Gain visibility into model performance, inference latency, and GPU usage
- **Digital experience management:** Extend user and application experience to AI resources

VersaONE: Powering the Intelligent Edge

VersaONE is a unified platform that integrates networking, security, AI-powered operations, and edge compute, delivering the Intelligent Edge today. It enables organizations to securely connect users, devices, applications, and AI workloads in any direction, with consistent performance, real-time visibility, and Zero Trust protection across the entire edge.

Versa addresses all four Intelligent Edge principles natively:

Versatile, elastic edge compute

VersaONE turns the edge into a full compute platform, converging networking, security, storage, and AI workloads into a single architecture with no dedicated appliances required.

Key Capabilities:

- **Hardware Acceleration:** Can be deployed across physical, virtual, and container form factors with CPU, GPU, and DPU configurations tailored to specific workload demands
- **Native Edge Computing:** Natively hosts diverse services at the edge including AI models, real-time inferencing engines, POS systems, and mission-critical business applications
- **AI-Powered Analytics:** Continuously collects infrastructure performance telemetry, and delivers actionable, predictive analytics powered by AI
- **Autonomous Operation:** Support air-gapped (sovereign) control and management architectures. The platform is capable of extended autonomous operation during connectivity loss
- **Enterprise Multi-Tenancy:** Provides strict tenant isolation across control planes, policy enforcement, and data segregation

Resilient connectivity

AI workloads and traffic are unpredictable. Versa keeps the enterprise connected and self-healing with unified connectivity that adapts automatically to changing conditions. The platform handles LAN, WAN, internet, MPLS, 5G, and satellite connections simultaneously, dynamically routing traffic across full mesh, hub-spoke, and hybrid topologies.

Intelligent traffic optimization ensures AI workloads get priority bandwidth while absorbing the traffic spikes that overwhelm traditional architectures.

Key Capabilities:

- **Unified Connectivity:** Blends WAN, LAN, and wireless with load balancing across MPLS, 5G, broadband, satellite, and internet
- **Granular Policy Control:** Prioritizes traffic by application, user, and device to ensure AI workloads get the bandwidth they need
- **Flexible Topology:** Supports mesh, partial mesh, and hub-spoke architectures to fit any deployment model
- **Dynamic Bandwidth:** Automatically responds to AI inference spikes and unpredictable traffic demands without manual intervention

Pervasive Security

Security must work in every direction across the modern network. Versa enforces Zero Trust across every edge, in every direction: across the cloud edge, data center edge, WAN edge, and LAN edge. Consistent policies are enforced across users, devices, applications, and AI workloads, ensuring no entities operate outside policy. Built-in security capabilities include NGFW, microsegmentation, and protection against malware, phishing, data leakage, and prompt injection.

Key Capabilities:

- **No Security Blind Spots:** Integrated NGFW, IPS, IDS, and microsegmentation protect against lateral movement and secure vulnerable areas including guest Wi-Fi, IoT, and OT devices
- **AI-Powered Threat Defense:** Built-in defenses detect and block modern attack vectors including prompt injection, jailbreaking, and Shadow AI
- **Granular Any-Direction Control:** Comprehensive Zero Trust policies enforce security for traffic flowing in any direction across every edge environment, spanning cloud, datacenter, WAN, and LAN edges

VersaONE Benefits

- **Versatility:** Consolidate point products and eliminate product sprawl. VersaONE combines compute, networking, security, and storage while hosting applications and business services
- **Resiliency:** Improve uptime even with unpredictable traffic spikes. Versa supports WAN, LAN, multiple connectivity types (MPLS, 5G, internet, satellite), and multiple topologies. Traffic is dynamically optimized with application-aware routing and prioritization for AI workloads
- **Pervasive security:** Enforce any-direction security. Versa enforces Zero Trust policies across users, devices, applications, and AI workloads across diverse environments
- **Autonomous networks:** Simplify operations. Versa provides AI-powered analytics, automated correlation of events, and unified observability across networking, applications, and AI workloads

Autonomous operations with AIOps

Manual operations cannot keep pace with AI-driven enterprises. Versa uses AI-powered analytics across its platform to correlate, predict, and resolve issues automatically, reducing the operational burden of managing complex infrastructure.

Key Capabilities:

- **AI-Powered Copilot (Verbo):** Navigate complex infrastructure interactions through natural language with Versa's MCP-based agent, Verbo. Verbo delivers contextual answers, actionable insights, and guided remediation to accelerate decision-making and reduce mean-time-to-resolution (MTTR)
- **Intelligent Root Cause Analysis**: Continuously correlates events across WAN, LAN, cloud, security, and applications. Suppress alert noise and surface root causes to quickly identify and resolve issues impacting the environment

- **Unified AI-Aware Observability:** Get holistic visibility in a single, real-time view with integrated analytics, AI inference activity, model performance metrics, and edge compute resource consumption
- **Extended Digital Experience Monitoring (DEM):** Gain comprehensive visibility into end-user experience, application performance, inference latency, model behavior, and edge compute utilization. Keep AI-powered services running at peak performance with faster issue detection and resolution

Why Versa

VersaONE unifies networking, security, and operations in a single platform, removing the complexity of managing fragmented infrastructure to deliver Intelligent Edge. Where other architectures were built for one-directional traffic, Versa's distributed, dynamic architecture supports multi-directional movement of users, devices, AI workloads, and inference services without constraint. Its multi-path connectivity is designed for the high-volume, bidirectional data flows that AI demands, keeping workloads online and performing under any conditions. Network-level Zero Trust security extends across all clients (users, devices, and AI agents), distributed resources, and AI workloads, ensuring consistent enforcement in every direction. Versa's AIOps correlates and resolves issues autonomously, with identity- and posture-based connectivity covering users, devices, and non-human identities. VersaONE helps teams drive AI and productivity forward rather than managing the infrastructure beneath it.

To see how VersaONE powers the Intelligent Edge, request a demo.

Explore VersaONE.

Versa Networks, Inc
2550 Great America Way, Suite 350
Santa Clara, CA 95054
Tel: +1 408.385.7660
Email: info@versa-networks.com
www.versa-networks.com

About Versa
Versa, a global leader in SASE, enables organizations to create self-protecting networks that radically simplify and automate their network and security infrastructure. Powered by AI, the VersaONE Universal SASE platform delivers converged SSE, SD-WAN, and SD-LAN solutions that protect data and defend against cyberthreats while delivering a superior digital experience. Thousands of customers globally, with hundreds of thousands of sites and millions of users trust Versa with their mission critical networks and security.

Part# SB_INTELLIEDGE-01.0