VERSA

WHITE PAPER

# The Intelligent Edge: The Future of Branch & Campus in the AI Era

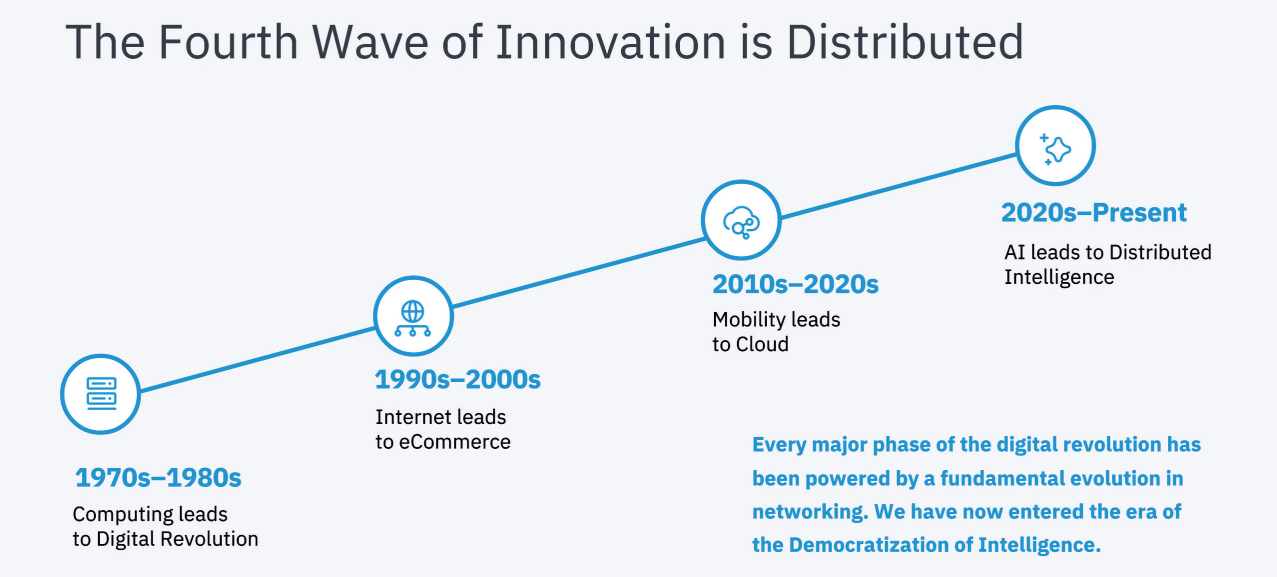
## Contents

# The Evolution of the Network for AI

Artificial Intelligence is driving a fundamental shift in enterprise architecture. Traditional networks designed for predictable, north-south traffic patterns are no longer sufficient to support distributed AI workloads, agents, and data flows.

Every major wave of innovation has been enabled by advances in networking. From computing to the internet, to mobility and cloud, the network has evolved to support new application demands. Today, AI represents the next wave that requires distributed intelligence across edge, cloud, and data centers.

Unlike previous shifts, AI is not centralized. It requires inference, data processing, and decision-making closer to users and devices. This drives a need for distributed infrastructure capable of supporting real-time interactions, massive data movement, and secure connectivity across all environments.



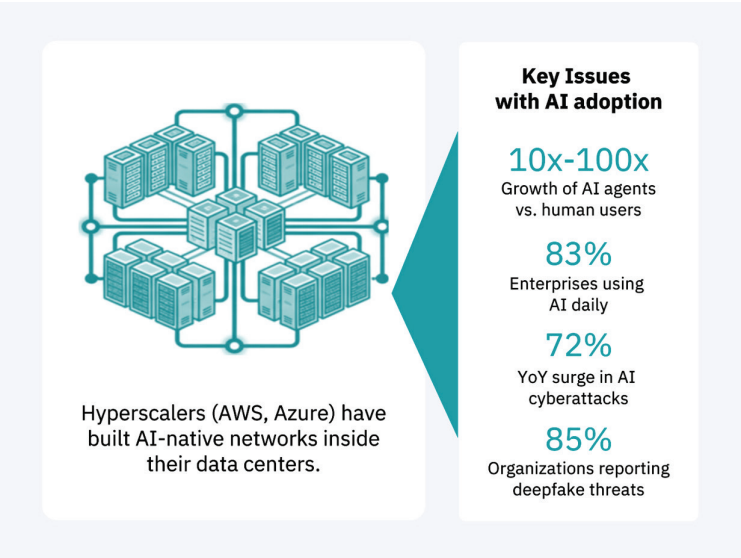

# AI is Forcing an Architectural Inflection Point

AI adoption is accelerating across enterprises. With the rapid growth of AI agents and increasing reliance on AI-driven applications, traffic patterns, security requirements, and operational complexity are changing dramatically.

Enterprises face:

1. Explosive growth in AI agents compared to human users
2. Increased cyber threats including AI-driven attacks
3. Lack of governance and readiness for AI adoption

Hyperscalers have addressed this by building AI-native data centers. Unfortunately, they were not designed for the explosive growth in AI agents, threats and general AI usage. Enterprises must now extend these capabilities to the edge, where real-world interactions occur.




Rapid innovation across silicon, systems, and AI models is significantly lowering the cost and complexity of deploying AI. This shift is enabling enterprises to move beyond centralized AI architectures and adopt distributed models where applications, inference, and data processing occur closer to users, devices, and operational environments.

As organizations accelerate AI adoption, they are actively redesigning their infrastructure to support these new requirements. Many are leveraging hyperscalers, neo-cloud providers, and OEM platforms to access AI inference capabilities and foundational building blocks, which are then integrated into their enterprise environments.

# Enterprise Challenges in the AI Era

AI exposes structural limitations in current enterprise architectures. In the past, enterprises have been able to navigate the evolving requirements, but with AI, it's not as simple. Why? In addition to any technical or architectural debt that exists, new requirements are emerging:

- **Topology of traffic:** Distribution of AI workloads will create an any-directional flow including east-west, south-north and north-south flow of traffic, but current networks are designed primarily for north-south flows
- **Capacity or Volume of data:** With AI workloads become the endpoint, creating need for vast volumes of data in the reverse direction of what most networks are designed for today's server-to-client
- **Visibility to who, what, where and when:** This access information will be essential to ensure policy controls, but enterprises still lack visibility to users & applications
- **Control of users, devices, applications, Agents and more:** while many have begun the transition to zero trust, it is only for users (not devices or non-human identities) and current islands of policy create inconsistency and increase risk
- **Security:** Today's architecture of uni-directional cloud security (client to app) will need to shift to any-directional security for combination of clients (users/devices), AI workloads and Agents being distributed across the enterprise.

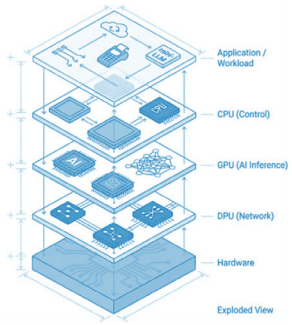
| Topology | Capacity | Visibility | Control | Security |
|---|---|---|---|---|
| Designed for north-south (client-to-server), but AI demands any-to-any (east-west, north-south, south-north) traffic. | AI creates massive reverse-flow data overwhelming download-centric pipes. | Leads to blind spots for non-human identities, AI agents, and lateral movement of devices and users. | Fragmented Zero Trust frameworks fail to cover device, application and agents | One-way trust models (Client-to-App) fail against bidirectional AI risks (App-to-Client). |

# Introducing the Intelligent Edge

The Intelligent Edge is a new architectural paradigm where compute, connectivity, and security converge. It enables enterprises to support AI workloads, ensure performance, and maintain security across distributed environments. It is defined by four core pillars:

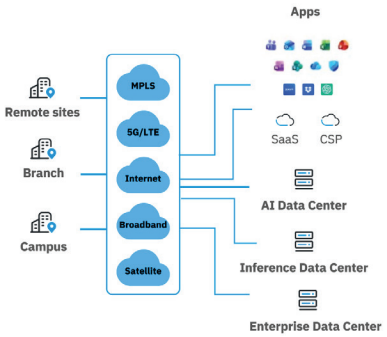
## Elastic: Converged Compute at the Edge

The days of function-specific appliances are far gone. The Intelligent Edge combines compute, network, security, and storage in a single platform. It supports the right mix of CPU, GPU, and DPU. CPU handles control functions. GPU powers AI models and real-time inference. DPU accelerates network performance. The Intelligent Edge runs applications and services natively. These include Point-of-Sale systems, incident management platforms like ServiceNow, and distributed AI services such as small models, mini-LLMs, inference pipelines, and AI agents. It collects and stores analytics data and uses local AI inference to improve performance and reduce latency. It operates autonomously during connectivity loss. While continuing to enforce security, manage inference, maintain routing, and preserve visibility. Most importantly, it supports multiple use cases with separate data, control, and management planes.




## Resilient: Any-Directional Connectivity

This edge intelligently leverages all available networks, including wireless and wired LAN, internet, MPLS, 5G, and satellite connections, to ensure uninterrupted connectivity and consistent user experience. It supports full-mesh, partial-mesh, hub-and-spoke, and other topologies to enable dynamic, any-directional connectivity. It prioritizes and accelerates applications and workloads, including SaaS, cloud, and AI applications. It also handles unpredictable traffic spikes from AI inference, telemetry, data transfers, and model synchronization without requiring manual bandwidth provisioning across networks.




## Protected: Pervasive Security

AI-generated content may be incorrect.The Intelligent Edge provides granular, zero trust controls in any direction across cloud, data center, WAN, and LAN. It is identity-aware for both human and non-human entities and includes built-in security with threat detection and remediation to defend against malware, phishing, data leakage, shadow IT, and AI-driven threats. It ensures every user, device, and application is authenticated, authorized, and continuously validated, including against risks such as prompt injection and agentic AI misbehavior. It supports both IT and OT environments and uses micro-segmentation to reduce the risk of lateral movement. It defends against AI-driven threats such as prompt injection, jailbreaking, and shadow IT, and shares detected threats with other edges in near real time to stop known attacks. Because the edge can be deployed anywhere, it does not rely on south-north inspection alone and instead enforces security policies for traffic in all directions.


## Autonomous: AI-Driven Operations

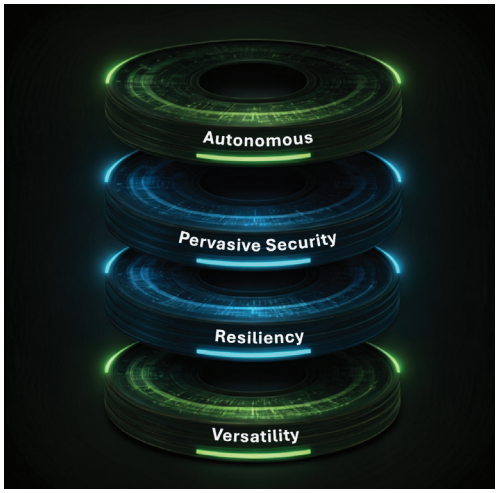
The right solution is centrally managed and controlled in a software-defined manner. It is manageable through natural language for administrators and through AI agents that use modal context protocol (MCP). The edge streams all telemetry and logs for processing, correlation, and prediction. Observability includes real-time visibility into AI traffic flows, inference request rates, model response latency, and GPU resource consumption. It also extends digital experience monitoring beyond users and applications to include AI resources.

## Versa Intelligent Edge: Delivering Today

Versa delivers the Intelligent Edge through its unified platform powered by Versa Operating System (VOS). The platform integrates networking, security, and AI-driven operations into a single architecture.

Key capabilities include:

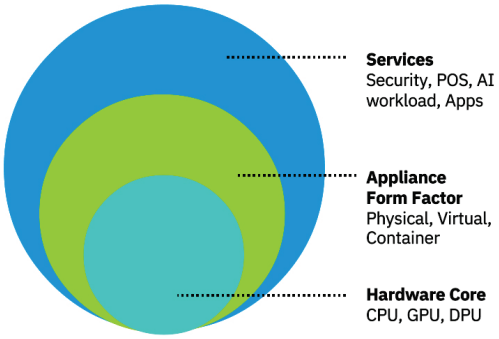
- Multi-form factor deployment (physical, virtual, containerized)
- Integrated compute with CPU, GPU, and DPU
- Native support for AI workloads and applications
- Multi-tenancy with strict isolation
- Unified policy and orchestration



## Versatility

Versa supports diverse deployment models and workloads, enabling AI inference and applications at the edge.

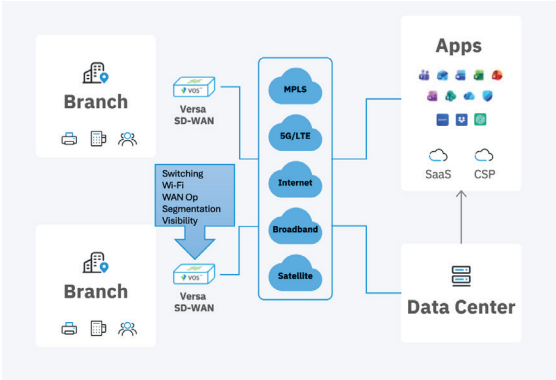
- **Hardware Acceleration:** Versa Intelligent Edge is offered in multiple form factors with CPU, GPU, and DPU configurations tailored to specific workload demands.
- **Native Edge Computing:** The platform natively hosts diverse services including AI models, real-time inferencing engines, Point-of-Sale systems, and mission-critical business applications.
- **AI-Powered Analytics:** Versa Intelligent Edge continuously collects infrastructure performance telemetry and delivers actionable, predictive analytics powered by AI.
- **Autonomous Operation:** VOS-based edge deployments support airgapped (sovereign) control and management architectures and extended autonomous operation during controller connectivity loss.
- **Enterprise Multi-Tenancy:** Versa Networks delivers comprehensive multi-tenancy with strict tenant isolation across control planes, policy enforcement, and data segregation.




## Resiliency

Unified connectivity across WAN, LAN, and wireless ensures consistent performance and reliability.

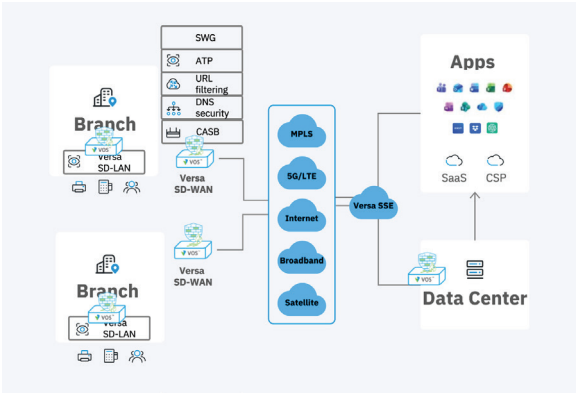
- **Unified Connectivity:** Supports WAN, LAN, and wireless networks in a single integrated architecture with built-in load balancing and failover. This ensures continuous connectivity and optimal path selection across multiple links, improving availability and user experience.
- **Granular Policy Control:** Enables fine-grained prioritization based on application, user, and device context. This allows enterprises to enforce consistent policies, optimize performance for critical workloads, and maintain control across diverse environments.
- **Flexible Topology:** Supports multiple deployment models including full mesh, partial mesh, and hub-and-spoke architectures. This flexibility allows organizations to design network topologies that align with their performance, scalability, and operational requirements.
- **Dynamic Bandwidth:** Automatically adjusts bandwidth allocation in response to traffic spikes. This ensures that AI workloads, applications, and data transfers receive the required resources without manual intervention, maintaining consistent performance.




## Pervasive Security

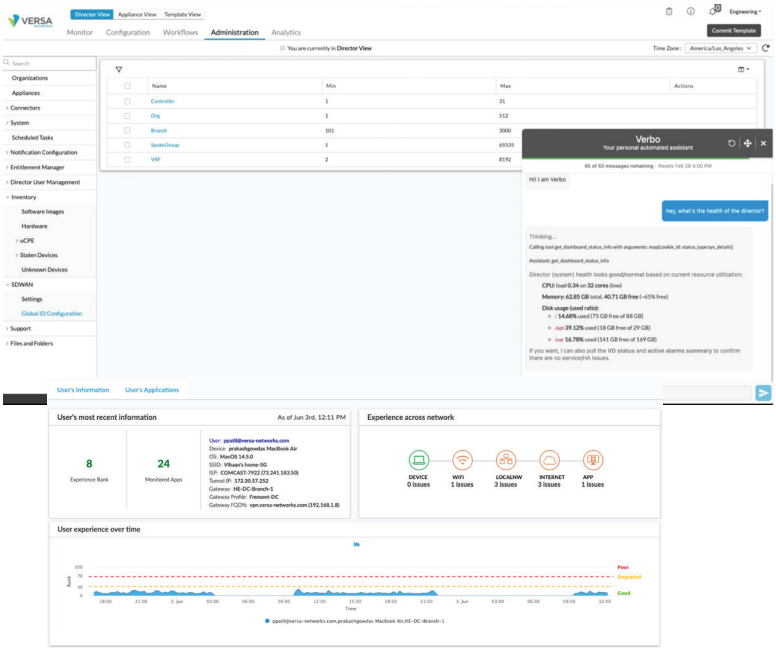
Integrated security capabilities provide Zero Trust enforcement and protection against AI-driven threats.

- **Eliminate Security Blind Spots:** Integrated NGFW, IPS, IDS, and micro-segmentation capabilities help protect against lateral movement and secure vulnerable areas such as guest Wi-Fi, IoT, and OT environments. This ensures consistent visibility and enforcement across all segments of the network.
- **AI-Powered Threat Defense:** Built-in AI-driven security capabilities detect and defend against modern threats such as prompt injection, jailbreaking attempts, and shadow IT. This enables proactive identification and mitigation of evolving attack vectors.
- **Granular Any-Direction Control:** Enforces Zero Trust policies for traffic flowing in any direction across cloud, data center, WAN, and LAN edges. This ensures consistent security posture regardless of where users, devices, or workloads are located.



## Autonomous Networks with AIOps

AI-powered analytics and automation reduce operational complexity and improve outcomes.




- **AI-Powered Copilot with Verbo:** Transforms infrastructure interaction through natural language. Verbo, an MCP-based agent, converts conversational inputs into contextual insights, precise answers, and guided actions to accelerate decision-making and reduce mean time to resolution.
- **Intelligent Root Cause Analysis:** Continuously analyzes data across WAN, LAN, cloud, security systems, and applications. It correlates events, suppresses noise, and identifies true root causes instead of isolated symptoms, improving operational efficiency and accuracy.
- **Unified AI-Aware Observability:** Provides comprehensive visibility by correlating network telemetry, AI inference activity, model performance metrics, and edge compute resource consumption in real time to ensure optimal AI application delivery and performance.
- **Extended Digital Experience Monitoring:** Expands beyond traditional user and application monitoring to include inference latency, model behavior, and edge compute utilization, enabling faster issue detection and improved overall experience.

## Business Outcomes

The Intelligent Edge enables:

- Secure and dynamic connectivity for distributed AI workloads
- Reliable performance across all environments
- Comprehensive visibility and control
- Automated operations and reduced complexity


# Conclusion

AI is redefining enterprise infrastructure. The Intelligent Edge provides the foundation for this transformation, enabling organizations to adopt AI securely and efficiently.

Versa's unified platform delivers this architecture today, helping enterprises transition from connectivity-focused networks to intelligence-driven infrastructure.

VERSA

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# WP_INTELEEDGE-01.0