

Secure, Resilient Networking for Unmanned and Autonomous Platforms

Versa's Approach to Connectivity, Security, and Zero Trust for Autonomous Vehicle Missions

Unmanned aerial vehicles, high-altitude platforms, and unmanned maritime systems operate over intermittent, contested, and constrained links where legacy networking and security architectures fall short. Versa extends its Unified SASE platform, already used in Department of War Zero Trust and tactical networking programs, to these platforms through software-defined networking, built-in security, and Zero Trust policy enforcement running on a single lightweight software stack. Program offices gain consistent policy, security, and visibility across ground, maritime, and airborne nodes without adding separate hardware or management tools.

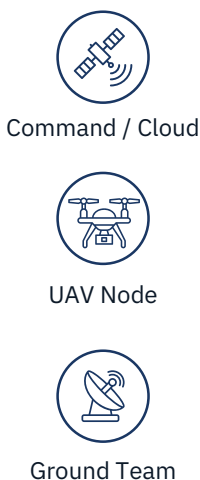
Requirements for Unmanned and Autonomous Platform Networking

Programs deploying unmanned aerial vehicles, high-altitude platforms, and unmanned maritime systems face a common set of networking requirements. Platforms move across radio frequency, cellular, and satellite links that degrade or drop as conditions change, so the network must adapt automatically to keep command and telemetry data moving through denied, degraded, intermittent, and limited (DDIL) conditions. Onboard compute and power are limited, leaving little room for a separate security appliance alongside the mission payload, and the platforms themselves can be targeted by adversaries attempting to jam, disable, or take control of the vehicle through electronic warfare. At the same time, relay and mesh topologies change as nodes join, leave, or move, so routing and security policy has to hold steady through every transition instead of resetting each time the topology shifts.

Versa Approach

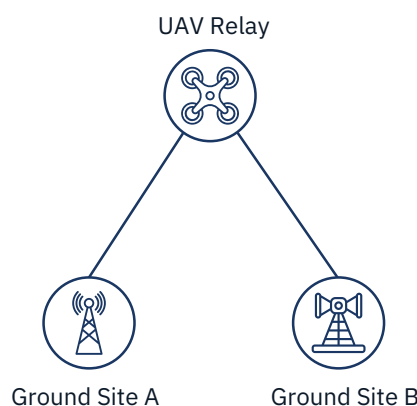
One software platform does all of this, not a stack of point products. Software-defined networking keeps traffic moving as links degrade, native security protects the platform without added hardware, and Zero Trust policy enforcement holds the same access rules as nodes move. No single mission looks the same twice, so the platform has to support multiple types of use cases and architectures, from a single relay to a distributed mesh.

Air to Ground



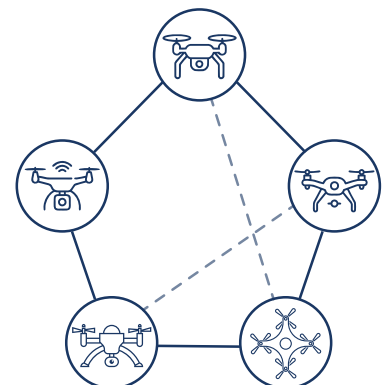
Keeps command and telemetry moving as the link changes

Ground to Ground via Air



Bridges two ground networks through an airborne relay

UAV Mesh / Swarm



Any node can forward traffic as the group moves

Software-Defined Networking

Software-defined networking is the foundation, and it's where Versa has the deepest track record today. It replaces manually configured circuits and static routes with policy that adapts automatically as links appear, degrade, or disappear. The same software handles route selection, traffic prioritization, and link conditioning across every transport a platform carries, from radio frequency to satellite.

- **Dynamic, multi-link path selection** across radio frequency, LTE/5G, and satellite links reroutes traffic automatically as conditions change.
- **SLA-based and link-state routing** steer traffic by application, delay, packet loss, and available bandwidth, keeping command and control traffic ahead of bulk data across DDIL links.
- **Rich routing and switching**, including support for L3VPN and EVPN across full-mesh, hub-and-spoke, and partial-mesh topologies, fits the network to the mission instead of forcing one architecture on every deployment.
- **Hierarchical quality of service**, with ingress policing and both ingress and egress shaping, protects priority traffic as demand shifts.
- **Forward error correction, packet replication, striping, and compression** sustain traffic quality over degraded links, with a tunnel-less option and support for bidirectional and unidirectional traffic, including demanding MTU requirements such as QUIC.
- **Optimizations for low-earth-orbit transports including Starlink** and compatibility with cascaded High Assurance Internet Protocol Encryptor (HAiPE) deployments cover satellite paths as well.
- **Centralized configuration and monitoring** give operators one view across every node.

Security

Security runs as part of the same software, not as a separate appliance bolted onto the platform. This matters most on compute- and power-constrained platforms, where every additional box competes with the mission payload for space, weight, and power. Versa's built-in security stack protects the platform and the data it carries without that added footprint.

- **A built-in security stack**, including intrusion prevention, stateful firewall, and denial-of-service protection, runs natively, not as a separate appliance.
- **The firewall runs inside the same software stack** as the rest of the platform, so no dedicated firewall appliance is required, an important savings on platforms where every unit of compute and every watt of power counts.
- **Encrypted overlays with dynamic tunnels and key rotation** protect data in transit as the network topology shifts.

Zero Trust

Zero Trust applies the same policy model Versa uses in fixed Department of War environments to platforms that move. Rather than trusting a device because it sits on the network, access and segmentation are enforced continuously, node by node, as the topology changes. The same policy runs whether it's a single relay or a multi-node mesh.

- **Zero Trust Everywhere** applies inline policy enforcement to distributed and moving nodes, not just fixed users and sites, so segmentation and least-privilege access hold even as nodes move.
- **Centralized visibility** gives operators a single view of link health, tunnel state, and application performance across ground, air, and maritime nodes.
- **The same Zero Trust Network Access capabilities** Versa provides for DISA's Thunderdome program run on the same underlying software used across autonomous and unmanned platforms.

Key Benefits

- **Lightweight footprint:** runs on x86 systems, ARM-based systems-on-chip, or as a Docker or Kubernetes workload
- **Consolidated function:** removes the need for a separate firewall appliance
- **Resilient by design:** automatic path selection and forward error correction keep priority traffic moving as links degrade
- **Consistent policy:** the same segmentation and Zero Trust policy travels with the platform, from a single relay to a multi-node mesh

Where This Approach Applies Today

Customer Spotlight: DISA Thunderdome

Versa is a core technology provider for DISA's Thunderdome program, delivering software-defined networking and Zero Trust Network Access as part of the Department of War's Zero Trust initiative. Thunderdome achieved all 152 of the Department's Zero Trust target-level goals two years ahead of schedule. The same platform capabilities validated under Thunderdome carry over to autonomous and unmanned platforms.

Commercial Maritime and Icebreaker Deployment

Versa runs on ships, cruise lines, and icebreakers today, demonstrating the platform's ability to operate reliably on moving, remote platforms under intermittent connectivity, the same conditions unmanned aerial and maritime systems face.

Learn more about Versa's approach to autonomous and unmanned platform networking, or [schedule a demo](#).