BONDED · ENCRYPTED · SELF-HEALING · OPERATOR-TRUTHFUL

FORGE OS
Connectivity that survives the edge.

FORGE OS bonds every uplink a site has — Starlink, LTE/5G, fiber, GEO satellite — into a single encrypted tunnel that survives what the field does to it, then reports the honest state of every link in plain language on one screen. It is delivered as software you run on your own conforming hardware. This datasheet describes how it works, why, and how it scales with the hardware you put it on.

0†	3.5s†	~14s†	78–87%†
dropped packets — WAN cut mid-stream, live traffic	to full fleet redundancy after a hub outage	to detect a silent ISP failure (link light green)	bonded throughput of combined link ceiling

† **Lab-measured** on a faithful WAN-emulation rig under the stated conditions; reproducible on request — see §3. Field results depend on carriers, workload, and hardware.

01 The architecture

A **FORGE HUB** sits at your operations center. **HAMR spokes** deploy at every site, vehicle, vessel, or incident scene. Between them runs a multipath, mutually-authenticated encrypted tunnel that aggregates every WAN the spoke has and drops none of them silently.

- **Multipath bonding (MPTCP)** — all uplinks carry traffic together; any one failing is a non-event.
- **Automatic path intelligence** — continuous per-link scoring promotes and benches links with no operator input, and explains every decision.
- **Dynamic routing** — BGP/OSPF between hub and spokes; networks converge automatically on topology change.
- **Hub failover** — assign a spoke a standby HUB and it reattaches on its own if the home HUB goes away: automatic, no operator input, about thirty seconds. One HUB at a time, never two. Coming home is scheduled by you, not by the box, because it costs a second interruption and you should pick when that lands.
- **Encryption without asterisks** — TLS 1.3, mutual certificate auth, AES-256-GCM running in a FIPS 140-3 validated module (CMVP #5247); spokes ship fail-closed until enrolled.

THE CORE PRINCIPLE — OPERATOR TRUTHFULNESS

Every green light is **earned**. A bonded link counts only if the connection is alive **and** the path answers a live probe this instant. The dashboard is designed so it cannot show a healthy bond over a dead path. When something is wrong, the system says so — in words a non-specialist can act on — rather than showing a comforting green. A dashboard that shows green over a dead link isn't a convenience — it's a liability, and it's your people in the field who find out first.

02 How it works

FORGE OS is built on kernel-native multipath TCP wrapped in modern TLS, with a control plane that continuously measures every path and acts on what it finds — in milliseconds, driven by kernel events rather than polling.

Transport & bonding

Multipath TCP (MPTCP) uses several networks as one connection. Per-path congestion control is tuned for lossy links (BBR), so 2% packet loss degrades throughput gracefully instead of collapsing it. The tunnel is TLS 1.3, mutually authenticated, AES-256-GCM.

Path intelligence

Every uplink is continuously probed and scored on reachability, smoothed latency versus the best path, and loss. Out-of-family paths are benched as warm standby — instant failover without aggregation drag. Recovery is earned: hold-down, a clean window, then a trial under real load.

Fault attribution

The system distinguishes a link's own failure from a shared upstream outage. A hub-side event never penalizes innocent spoke links, so fleet-wide redundancy returns in seconds rather than minutes of unnecessary standby.

Flap governance

A link that drops repeatedly in a short window is automatically benched under escalating probation and reinstated only after it proves itself clean. Unstable links cannot churn the tunnel or the routing table.

Anchor-path recovery

If the tunnel's primary connection is riding a degraded path, FORGE rebuilds that connection onto the best healthy path automatically — a single brief, controlled reconnect instead of an indefinite latency penalty on every packet.

Routing

FRRouting under the hood: BGP or OSPF per spoke, hub-orchestrated. Session state is surfaced in operator language — when routing is down, the screen says *down*, not a protocol state-machine word that merely sounds healthy.

03 Break-tested behavior

Every figure below was produced by deliberately inflicting a failure on a live system, then measuring recovery. All are reproducible on request.

FAILURE INFLICTED	RESULT	WHAT HAPPENS
WAN cut mid-stream	`0 packets lost`	Traffic shifts to surviving paths in-flight; the dashboard shows the honest link count within a second.
Hub uplink killed	`3.5s to 2/2`	Every spoke detects the loss, declares it honestly, and reconnects the instant the path returns.
Silent ISP failure	`~14s detect`	Caught by live path probes even with the link light green and the socket still open. Link lights lie; probes do not.
Flapping link (5×/60s)	`auto-benched`	Parked under escalating probation, reinstated only after a sustained clean window.
Degraded GEO path	`~4s once`	Benched from the bond; if it carries the anchor connection, that connection is rebuilt on the best healthy path — one brief blip, not a permanent tax.
Home HUB lost	`~30s to standby`	A different mechanism from the WAN rows above — this is a change *of* HUB, not a path event inside one. The spoke confirms the outage across every WAN, then moves itself to its assigned standby and reconverges routing. Break-then-make, so traffic is interrupted. No operator input; coming home is scheduled by the NOC, never automatic.
Config change under load	`0 interruption`	Any WAN can be edited live with no tunnel disruption. Tested deliberately and continuously.

MEASURED ON A FAITHFUL WAN-EMULATION RIG · LIVE-RADIO FIELD TRIAL IS THE NEXT MILESTONE.

04 Bonding efficiency

Aggregation efficiency is real throughput delivered as a share of the links' **combined theoretical ceiling**. Two 250 Mbps WANs give a 500 Mbps ceiling; FORGE bonds them to roughly 435 Mbps of usable, encrypted capacity — about 87%. Measured across real link scenarios on a WAN-emulation rig:

GEO SAT ~500 ms+ latency gap → parked as hot standby. The gap is too wide to bond without dragging the aggregate down, so GEO carries no traffic while primary links are healthy, then takes over instantly on failure.

5G + STARLINK RUN CARRIED 0.01% LOSS ON BOTH LINKS AND ~3% JITTER ON THE STARLINK UPLINK — STILL BONDED AT ~84%.

05 Your hardware. Your control.

FORGE OS is delivered as software under a per-HUB subscription license, validated offline. You run it on commodity x86 hardware you own and procure through your existing channels — no proprietary appliance, no vendor-locked box aging in a closet, no RMA between you and a field repair. When a unit fails, the fix is a firmware flash on any conforming hardware.

COMPONENT	REQUIREMENT
CPU	Intel N150 class or better (x86-64)
Memory	8 GB RAM
NICs	Intel network interfaces
Security	TPM 2.0 + Secure Boot recommended enables the shipped encrypted-storage path
Platform	UEFI · x86-64

It scales with what you give it

FORGE is a datapath, and a datapath is bound by the machine under it. The same software spans a fanless mini-PC at a remote site and a rackmount concentrator at the NOC — you size the hardware to the role.

- **CPU** sets encrypted throughput ceiling and how many bonded paths and BGP/OSPF sessions a HUB sustains. AES-256-GCM is the hot path — more cores and AES-NI lift the ceiling directly.
- **NIC quality** governs clean multipath behavior at load; Intel NICs are required for predictable offload and driver behavior.
- **RAM** scales with concurrent spokes, routing table size, and in-flight reassembly buffers on high-latency paths.

TPM 2.0 IS RECOMMENDED, NOT REQUIRED — SEE NOTE BELOW.

ON TPM 2.0 — RECOMMENDED, NOT REQUIRED

Shipped today: with UEFI Secure Boot and TPM 2.0, storage is **LUKS2-encrypted** and auto-unlocks only when the platform's policy state matches — a pulled drive is unreadable anywhere else, and an independent recovery key covers the day the policy can't be satisfied. **Roadmap:** sealing device *identity* keys to the chip — so a physically captured unit is inert hardware, not a stolen identity on your network — and attesting the box booted unmodified firmware. If your gear lives in a locked rack, the shipped protection may be all you need. If it lives in a vehicle, a remote site, or anywhere it can be picked up, you want all of it. You size the protection to where your boxes actually sit.

ROLE	TYPICAL HARDWARE	FITS
HAMR spoke — field	Fanless mini-PC · N150 · 8 GB	Single site, vehicle, or vessel bonding up to four uplinks.
FORGE HUB — NOC	Rackmount x86 · more cores + AES-NI · Intel NICs	Terminates the fleet's tunnels; CPU sets the encrypted ceiling and session count.

06 Security posture

Encryption & identity

TLS 1.3 mutual authentication end to end · ECDSA P-384 device certificates · AES-256-GCM pinned for CNSA 1.0 — data-path cryptography executes in a **FIPS 140-3 validated module (CMVP #5247)** · Ed25519-signed licensing. Product-level certification — roadmap.

Fail-closed by default

A spoke ships in isolation lockdown and forwards nothing until it is enrolled and verified. Lose the tunnel and the site stops forwarding — there is no insecure mode to misconfigure into.

Signed A/B firmware

Ed25519-signed packages, alternating slots, health-checked **automatic rollback**. A monotonic root boundary means even a validly-signed older package cannot restore weaker privileged code.

Recovery escrow

Each field unit's break-glass credential and disk-recovery key escrow — encrypted — to your HUB after first authenticated connection. Field disaster recovery without a bench visit; reveals are Admin-only, step-up-gated, and audited.

Authorization is not authentication

An allowlist gates every transiting packet, independent of tunnel authentication. Certificate revocation is immediate.

Low-touch, NOC-approved enrollment

A spoke powers up, authenticates to the HUB, and waits in the NOC approval queue. Nothing joins the network without a human at the NOC saying yes. Hardening aligned toward DISA STIG baselines; formal mapping — roadmap.

You own the trust path — we're not in it

The certificate authority, the private keys, and both ends of every tunnel run on hardware you own. The chain is two-tier — your root CA signs each HUB's issuing CA, which signs device certificates — and spokes honor an explicit HUB allowlist, so a valid certificate alone doesn't get a box onto your fabric. No HAMR-FORGE cloud, no HAMR-FORGE server, nothing of ours sits between your sites or inside your trust boundary — because there's nothing of ours to compromise. When a vendor brokers your tunnels through their cloud, their breach is your breach, and their key custody is your exposure. Here, no third party — us included — holds any credential that could put a rogue node on your fabric or read a byte of your traffic. There is no vendor backdoor: not for us, not for anyone who breaks into us, not even for recovery. If you hold the keys, your data answers to your policy and no one else's.

No phone home. None.

FORGE OS needs no path to the internet to do its job. Licensing is verified on the box against a signed fingerprint — no activation server to call, no license heartbeat to miss, no update reaching back to us, no telemetry leaving your network. It installs, enrolls, bonds, routes, and runs for as long as you like on a network with no way out. That is not a stripped-down "offline mode" — it is the design center, and it is why FORGE goes where cloud-managed SD-WAN can't: air-gapped and classified-adjacent networks, ships and convoys and forward sites that lose their uplink for days. A product that phones home stops working the moment the network you're trying to survive goes down. This one doesn't.

07 Centralized operations

HUB-PUSHED SERVICES

NTP, DNS, authentication, syslog, and SNMP are pushed from the HUB to every spoke automatically and kept in sync. Operators never hand-configure enterprise services in the field.

NOC VISIBILITY

One HUB gives the NOC a single honest view of every site — live throughput, per-site diagnostics, and an offline geographic Fleet Map served from signed, customer-installed map packs. No external mapping service ever sees your fleet.

INTEGRATION

Syslog over TLS (RFC 5425, TCP 6514) to any standards-compliant SIEM. SNMPv3 to your NMS. Full-fidelity system logs with honest severities.

08 Specifications at a glance

TRANSPORT	
Bonding	MPTCP (kernel-native)
Encryption	TLS 1.3 · AES-256-GCM · FIPS module #5247
Auth	Mutual cert · ECDSA P-384
Congestion	BBR (per-path)
Routing	FRR · BGP / OSPF
Uplinks	Starlink · LTE/5G · fiber · GEO — any routable IP path

PLATFORM & LICENSING	
Delivery	Software · customer hardware
Licensing	Per-HUB subscription · validated offline · failover consumes no seat
Min CPU	Intel N150 class (x86-64)
Min RAM	8 GB
Required	Intel NICs · TPM 2.0 recommended
OEM	Sub-licensing available

SEE IT LOSE A WAN AND NOT CARE

Thirty minutes. Live system. You pick what breaks.

Walk the live console, or send your sites, links, and constraints for a tailored pilot.

inquiries@hamr-forge.com · hamr-forge.com · (706) 910-7952

WAN-emulation validated · Field trial — next · Air-gap capable · zero phone-home · FIPS 140-3 validated crypto module (CMVP #5247) · Product certs / STIG mapping — roadmap · OEM sub-licensing — open