TrustWrx SuprNets™

06-10-26 11:30

SuprCloak™

Transaction-level non-attribution for the tactical edge and the enterprise

Executive Summary

The breakthrough

For the entire history of IP networking, every packet a node transmits has exposed its IP addresses in the clear – **the two most-harvested, most-weaponized fields on the wire**, and the first input to every reconnaissance sweep and every threat chain. To cloak that exposure, SuprNets conceals the entire packet, both IP addresses and the payload, within two nested layers of AES-256 encryption. It then wraps that encryption with a third encrypted transport layer that must present its IP addresses publicly for routing.

SuprCloak removes the sender's true IP address from the exposed public path – replacing it with a routing-legal decoy address, while the node's real identity travels sealed inside the SuprNet encrypted packet structure. The result is a network that routes normally, performs normally – but bilaterally unbinds the transaction from the identity of any packet source while concealing the payload end-to-end.

What it actually is – and why the framing matters

SuprCloak does not make endpoint addresses invisible. Addresses still exist – sufficiently broad surveillance will know that devices, drones, aircraft, and gateways are present. What SuprCloak denies is the linkage – **which device, among many, is in comms; which gateway, among several, is answering.** The capability is transaction address non-attribution, with payload invisibility, and that is the stronger and more defensible position.

The protection is bilateral. The forward path unbinds **which device is sending,** while the return path unbinds which **gateway is responding**. And it has a property no conventional security control shares – it strengthens incrementally as the operation intensifies. SuprCloak durability scales up with operational tempo. A highly-active net with many emitters and interleaved transactions produces a large anonymity set, all resolving to a single black hole, and an observer's confidence in any binding collapses toward 1/N.

©2026 TrustWrx, Inc.

How the baseline works

The tactical-edge baseline depends only on the one node a device can reliably reach – its local gateway – and on no distant or contested link. Four mechanisms compose:

- **Sender Cloak.** The true source – the outer-layer source sender IP address – is replaced on the wire by a Decoy Anchor – a real IP address the gateway legitimately owns, so nothing is forged and standard anti-spoofing controls (uRPF / BCP 38) pass cleanly. Because all packets share the same sender decoy IP address, all senders look alike, become anonymous and no packet or payload can be traced back to the true sender's or responder's IP address.
- **Gateway anchor.** Every device behind a gateway appears to egress under one shared, gateway-owned address. Because the entire fleet shares it, that address distinguishes nothing about which device sent which packet – and because the gateway is already a visible fixed point on the return path, there is nothing to gain by hiding it and nothing lost by holding it constant. The aggregation point itself is the anonymity – a black hole into which all device transaction identities disappear.
- **Gateway-mix.** The gateway aggregates traffic across devices, normalizes packet sizes, and batches, reorders, and pads egress so input flows do not map one-to-one to output flows – defeating timing-and-volume correlation and normalizing the traffic signature so a single shared anchor reveals nothing about operational tempo. This elevates the gateway from a crypto re-seal point to a true mesh mix node within SuprMesh.
- **Decoy black hole.** The SuprCloak app standing behind the decoy address is a black hole to all inbound traffic – it answers nothing, exposes no service, and silently discards every packet – with one exception. It traps legitimate ICMP path signals, validates them against in-flight state, and forwards only those inward to the sending process. Everything else dies at the decoy address – the only thing that survives is the path feedback the transport genuinely needs.
- **Threat remediation.** Because the app sees only ICMP, it also has a clear vantage to watch overall patterns and detect DDoS and other attacks on the decoy address. On detection, it can simply rotate the decoy address to defeat the attack without impacting live operations – unlike legacy DoS protections, which degrade or interrupt service under load. The decoy address holds constant during normal ops and only moves when there's an attack to shed or a rotation schedule to meet.

Underpinning all four is a handshake-free outer transport keyed by pre-established mesh federations and an in-band encryption key ratchet – which removes the conventional tunnel's return-path dependency entirely – along with identity-based return routing, so a hidden origin stays reachable without ever exposing itself.

Strategic impact

Defense. SuprCloak denies the adversary the first targeting cue – the source field that fixes a sender for follow-on action – and denies the reconnaissance picture that mapping a mission network depends on. Coalition and federated operations interoperate without exposing each other's order of battle. The protection is populated by the operation itself – not by ACLs, iptables, external services or persistent tunnels.

Commercial. You cannot scan, flood, blocklist, geofence, or laterally exploit a sender that is not accessible on the public wire. Reconnaissance loses its anchor, source-targeted DDoS loses its target, metadata harvesting goes dark, and breach playbooks that begin from a known origin stall at step one – for the hospital MRI, the industrial controller, the IoT fleet, and the branch office alike.

Bottom line

Network security has spent decades hardening the addressable node. SuprCloak removes from the contest entirely the binding between the transaction and the source device – on the one link that is always reachable, with cover that grows as the traffic intensifies, and with claims that survive the test bench. We cannot hide that addresses exist. We can ensure no one can tell which one is yours.

TrustWrx, Inc.
George Sidman, CEO
sidman@trustwrx.com
+1.831.601.1777

US Patents:
8,266,421 ▪ 8,819,410 ▪ 12,041,168 ▪ 12,494,911
Patents pending

©2026 TrustWrx, Inc.