AIRGAPNET

Physical network isolation, online only when needed.

Product introduction

2026-05

OUR MISSION

Become a leading provider of IT-security solutions through physical airgapping. Not by replacing firewalls, EDR, or segmentation -- by complementing them, so the combination gives organisations a measurably higher security standard.

AirGapNet has been developed since 2020 by a team with more than 20 years of network and security infrastructure experience. The core mechanism was filed for patent in 2023.

THE PROBLEM

Attacks are more complex, and more frequent.

Twenty years ago a firewall and a virus scanner were enough to catch most security problems. Today attackers assume every organisation already has firewalls, antivirus, endpoint security, network segmentation, and operator training in place -- and they breach those organisations anyway.

Most of those breaches start on a service path that the network leaves reachable by default: a vendor VPN, an update channel, a remote-support session, a backup target. The control on that path is software. Software, by definition, is bypassable.

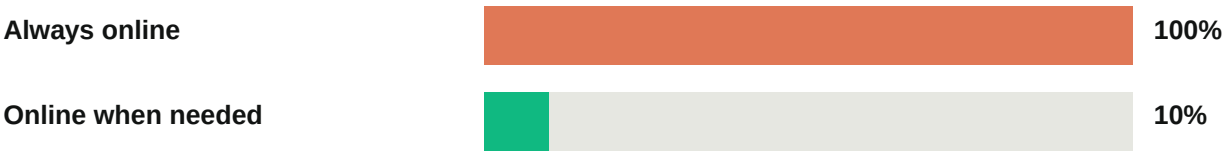
OUR SOLUTION

From always online to online when needed.

AirGapNet does not replace existing network security measures. It adds a layer underneath them: temporary network separation. The shorter the time a system is connected, the smaller the window an attacker has.

Classical airgapping (used in power plants, defence) keeps critical systems with no outside connection at all -- secure, but data has to move through other channels. AirGapNet gives you the upside without the downside: closed by default, opened on intent, closed again the moment the work window ends.

TIME ON THE NETWORK



FIVE CAPABILITIES

Hardware that closes the path at the cable.

AirGapNet devices physically separate network lines through a protected control unit that cannot be modified from the outside. Switching is performed over an independent control channel (e.g. GSM/SMS). The line can be cut manually, on a schedule, or in response to a verified event -- driven from the AirGapNet App or SMS codes.

Higher security

Physical separation removes the attack surface during the closed state. There is nothing to compromise on that path until it is opened.

Flexibility

Open and close the line manually, on a schedule, or on a verified upstream event.

Simple operation

Smartphone control over the closed AirGapNet control network. SMS works as a fallback when the data network is down.

Compatibility

Drops in next to firewalls, EDR, segmentation, and operator training. AirGapNet complements those controls, not replaces them.

Connect and switch

Securely separate, connect, or switch between networks -- by intent, and only for the configured window.

THREE SKUS, ONE DEFAULT STATE

Hardware, rack, and management.

AirGapNet ships two hardware models today and a cloud-based management layer is in development. Every product applies the same idea -- closed at the cable, opened on intent -- at a different scale.

IN STOCK • SHIPS IN 5 DAYS • $1,099

AGN1 -- single-line hardware isolation

Compact device that physically connects, disconnects, or switches one network path. Switched speeds up to 10 GBit. Controlled from a smartphone over the GSM/SMS channel.

- Securely connect, disconnect, and switch a network line
- Smartphone control via SMS codes
- Unplug-resistant power supply
- Patent-pending core mechanism

QUOTE-LED • 4-6 WEEKS

AGN2 -- rack infrastructure isolation

19-inch rack-mount variant of AGN1. Coordinates physical switching across multiple network lines from a single chassis. Built for larger networks, server rooms, and professional environments.

- Server-rack form factor
- Switch multiple lines from one device
- Same independent GSM/SMS control channel
- Unplug-resistant power supply

COMING SOON

AirGapNet Cloud -- central management

Central management for teams running multiple AirGapNet devices. Group switching across the fleet, complex scheduled access windows, audit trail.

- Centralised management of many devices
- Group switching workflows
- Complex scheduled access windows
- Continuously extended functionality

CORE MECHANISM

AGN1.

AGN1 is the entry point to the AirGapNet line -- ideal for commercial and industrial use and equally suited to small environments. It uses the patent-pending AirGapNet principle to securely separate, connect, and switch network lines.

AGN1 -- USB-C powered -- GSM control

CORE FUNCTION

- Securely separate, connect, and switch network lines
- Smartphone control via SMS codes
- Patent-pending technology

PRICE

$1,099

Single unit • ships in 5 days from US warehouse

Technical details

Secure network	GSM
Dimensions (WxHxD)	95 x 156 x 35 mm (3.74 x 6.14 x 1.38 in)
Weight	450 g (15.9 oz)
Power	USB-C 5 V (0.65 W idle)
Switched speeds	Up to 10 GBit
Housing colours	Black or Orange
Warranty	24-month limited warranty

BY INDUSTRY

Six target sectors.

AirGapNet applies wherever a network leaves a service path reachable that does not need to be online between work windows.

1

Industry & manufacturing

Vendor maintenance, PoE devices, controllers.

2

Network administrators

Update windows, segmentation, backup targets.

3

Healthcare

Imaging, EHR vendor access, medical devices.

4

Critical infrastructure

Utilities, transport, plant control networks.

5

Banking & insurance

Core banking, dealing rooms, immutable backups.

6

Government & defence

Classified networks, contractor service paths.

TYPICAL USE CASES

- **Network separation**
- **Server config windows**
- **Backup / immutable**
- **PoE & devices**
- **Maintenance updates**

USER • NETWORK ADMINISTRATORS

Vendor access without the whole network.

Problem

Network-attached devices -- industrial machines, printers, POS systems -- need regular software updates. During those windows the technician usually has access not just to the single device, but to the whole network behind it. Cautious admins try to avoid this by physically supervising the technician. An uncomfortable situation for everyone.

Goal

A way for an external vendor to reach the device that needs maintenance, without exposing the rest of the internal network. The maintenance happens inside a safe, isolated network.

Solution

Step 1. The vendor agrees a maintenance window. AirGapNet switches the device's line over to an alternative network for that window. From this network the vendor can reach the device being maintained -- and nothing else. The production network stays inaccessible.

Step 2. When the window ends, AirGapNet returns the device to the normal network automatically. The switch is performed remotely -- no on-site presence is required to make the physical change.

BUILT-IN PROTECTIONS

Defence in depth on the control channel.

Every state change on an AirGapNet device is signed, timestamped, and exportable. The control channel sits on a network you choose (e.g. GSM), separate from the data network being isolated -- so compromising the LAN does not give an attacker the ability to open the line.

Standard security features

- Control codes are delivered over a separate, independent network (SMS/GSM)
- Phone-number whitelisting -- only specified numbers can issue commands
- Two-factor protection on the control channel
- Sealed control unit -- opening voids warranty
- All state changes audit-logged

Integration

AirGapNet integrates into existing network infrastructure without major rework. In complex scenarios any number of lines can be separated and switched. Self-service for standard deployments; our engineering team is available for special requirements and bespoke architectures.

BUY NOW

Two ways to get started.

AGN1 is available online for self-service purchase. For larger fleets, rack deployments, or special integration scenarios, talk to engineering for a scoped quote.

1 Order online

AGN1 is available for online purchase. Ships in 5 business days from the US warehouse. Black or orange housing, USB-C powered, included regional adapter set.

AIRGAPNET.US/PRODUCTS/AGN1

2 Talk to engineering

For AGN2, fleet deployments, or quote-led configurations, contact the team for a 20-minute scoping call on port count, control channel preferences, and rollout staging.

EMAIL AIRGAPNET@GMAIL.COM

STAY CLOSE

Follow AirGapNet on LinkedIn for new use cases, product updates, and case write-ups. Every new release ships with print-ready PDFs you can drop into procurement and audit packs.

NEXT STEPS

Let's start working together.

We are happy to answer questions, walk through specific use cases, and help you design the most secure network for your environment. Reach out and we will set up a 20-minute call to scope your deployment.

OUR MISSION

Become a leading provider of IT-security solutions through physical airgapping. Not by replacing firewalls or EDR -- by complementing them.

OUR PRODUCTS

AGN1 and AGN2 are IT-security devices using airgapping technology to physically separate network lines. Cloud management is in development for fleet operators.

CONTACT

Web
airgapnet.us

Email
AirGapNet@gmail.com

Phone
+1-305-610-3390

Offices

AirGapNet, Inc. -- 1209 N Orange St, Wilmington, DE 19801

We look forward to helping you run your networks more securely and reliably. Let's get started.