Tempered

What is Airwall?

Securing the world's critical infrastructure with the only identity-based, zero trust segmentation solution.

At the heart of cyberattacks, network insecurity and specifically TCP/IP are central to virtually every cybercrime. Why? The traditional air gap disappears when sensors and devices are connected using TCP/IP on hybrid networks. This is where Tempered comes in. We have a transformative technology that helps protect any type of connected device from cyberattacks.

Airwall protects critical infrastructure with the industry's only identity-based, zero trust platform. Think of Airwall as the virtual air gap protecting the systems in a smart building, the medical devices in a hospital, the machines on a factory floor. These are all use cases Tempered solves today.

Airwall ensures critical assets across the network are impervious to threats, while still allowing secure connectivity from anywhere. It enables reliable cloaking, secure remote access, and secure data transport from critical infrastructure to cloud, and back. Airwall secures every endpoint in your network, with true micro-segmentation.

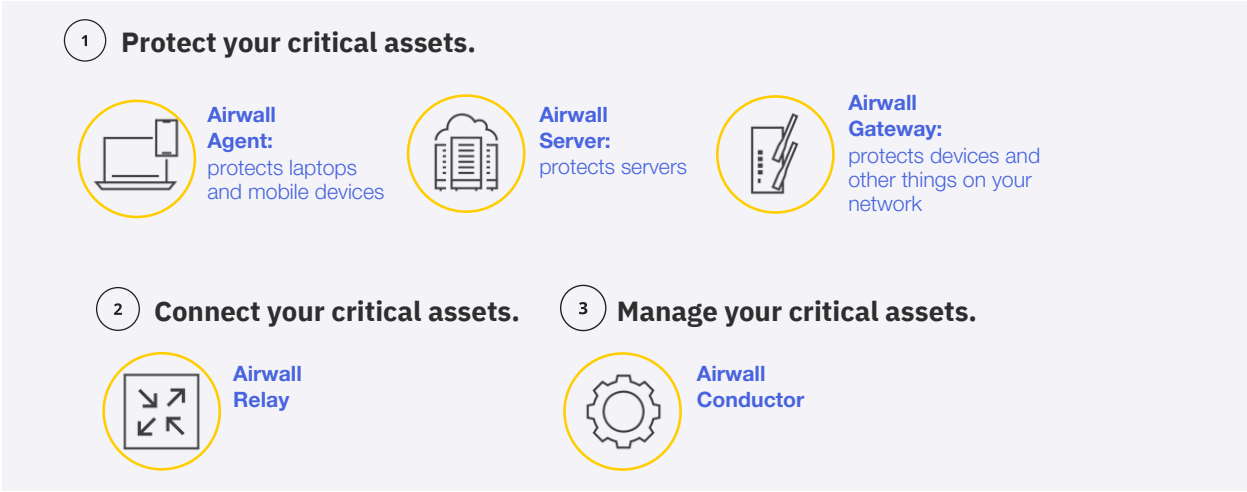
Airwall provides global connectivity and mobility for your entire workforce, wherever they are and for whatever they need to reach, securely.

Airwall delivers defense-in-depth.

1. Zero Trust Network Access (ZTNA)
2. Software-Defined Network (SDN)
3. Software-Defined Perimeter (SDP)
4. Multi-Factor Authentication (MFA)
5. Micro-Segmentation for Every Endpoint
6. Lateral Movement Eliminated

How Airwall Works:

An Airwall secure network uses overlays. These are secure networks that run on top of your existing network (underlay), that set up and manage trust between devices and resources. Airwall Edge Services enforce that zero trust policy and manage communication across the overlay.



Airwall Agent

Protect your critical assets.

Airwall Agents are applications installed on devices (Windows, macOS, iOS, iPadOS, and Android) that enable zero trust network access (ZTNA) from anywhere in the world. By default, all communications are encrypted end-to-end and multi-factor authenticated (MFA), enforcing a software-defined perimeter (SDP) at the distributed edge.

Deployment Options:

Windows	macOS	iOS/iPadOS	Android
7/8/10/11 (32/64-bit)	10.14 & above	12.0 & above	6.0 & Above

Airwall Server

Airwall Servers support Windows Server and Linux, and behave much like Airwall Agents. They effectively make servers invisible and only allow communication with authenticated and authorized endpoints (ZTNA). Air-gap servers prevent unauthorized communication with a software-defined perimeter (SDP).

Deployment Options:

Windows Server	Linux
2012 R2 2016	CentOS 7 and 8 Ubuntu 16.04, 18.04 and 20.04 Fedora 33 Raspbian 10

Airwall Gateway

Airwall Gateways protect critical assets downstream. They are deployed in front of devices, hosts or networks that cannot protect themselves. Examples include legacy systems and machines, or when customers are unable to install Airwall Agent or Airwall Server.

Deployment Options:

Cloud	Virtual	Physical	Connectivity
Amazon Web Services Microsoft Azure Google Cloud	VMware ESXi 6.0 & above, Microsoft HyperV 2012 R2 and 2016	Airwall Edge Airwall Robust Airwall Smart Facilities Airwall Infrastructure	Wired Cellular Wi-Fi

Airwall Relay

Connect your critical assets.

Airwall Relay routes encrypted communications between all your critical devices across all your networks. Reduce network complexity and enable complete connectivity between every endpoint, without modifying the underlying network. Wherever that endpoint is and however that endpoint is online, it can be connected.

Deployment Options:

Cloud	Virtual	Physical
Amazon Web Services Microsoft Azure Google Cloud	VMware ESXi 6.0 & above, Microsoft HyperV 2012 R2 and 2016	Airwall Infrastructure

Airwall Conductor

Manage your critical assets.

Airwall Conductor enforces invisibility and access policy for all your critical assets with point-and-click simplicity. Make your critical assets invisible by creating a software-defined network (SDN) that's micro-segmented, encrypted end-to-end, and multi-factor authenticated (MFA).

Deployment Options:

Cloud	Virtual	Physical
Amazon Web Services Microsoft Azure Google Cloud	VMware ESXi 6.0 & above, Microsoft HyperV 2012 R2 and 2016	Conductor – 1U Platform (software)

Schedule a call with our experts to learn more.

experts@tempered.io | +1 206.452.5500