white paper

Tempered

Airwall

A Revolution in Secure Networking

Airwall™ makes your connected ‘things’ invisible. It eliminates network-based attacks, secures remote access at scale, and extends the life of existing infrastructure investments. It effectively reduces cyber risk and makes securing a corporate network less complex.

Securing a company’s distributed network is incredibly expensive and difficult to scale with growth. Attacks or breaches present massive risks to your company’s reputation. Managing your company’s IoT deployments and network access demands is only getting more complex as time goes by.

Today’s solutions tell you: (1) visibility is security, (2) attacks are when, not if, and (3) connect first and secure later. They say you need more firewalls, VPNs, VLANs, ACLs, SSH keys, etc., but that you’re never really secure.

There’s a steaming heap of the world’s economy and welfare literally hanging in the balance.[1] Stop believing the lies.

We've found an infinitely better way to keep it all safe.
Airwall enables secure access and total invisibility at any scale, across any network.

Airwall secures every endpoint in your network, with true micro-segmentation and secure remote access. You can secure your local datacenter and your global infrastructure.

Airwall works with your existing network investments, so no need for rip-and-replace or forklift upgrades. Network-based attacks are a thing of the past and managing your network is no longer complex or costly.

After Airwall	Before Airwall
Your network and every endpoint become invisible at scale	Vulnerable network infrastructure
Identity-defined perimeter at the device level	Complex and hard-to-manage security policies
Zero-trust network access (ZTNA) for endpoints across any network	Lack of secure access and mobility for endpoints across networks
Augments existing infrastructure, no rip-and-replace or forklift upgrades	Not able to extend life of existing network investments
End of lateral movement of threats	Risk of lateral movement of threats
Eliminates network-based attacks	Attacks are when, not if

Airwall Conductor
set secure access policy

Airwall Relay
encrypt routing across any network

Airwall Gateway
protect everything downstream

Airwall Agent
protect devices anywhere

Airwall Server
protect server workloads

What is Airwall?

Airwall is a virtual airgap solution that ensures your devices are completely invisible and eliminates lateral movement from bad actors across your network. Airwall uses Host Identity Protocol (HIP)[2] to secure network communication between devices, enabling micro-segmentation and remote access at scale on any network.

Airwall is a combination of software or hardware that extends to physical, virtual, and cloud environments, at scale. Deploy on any workload or endpoint, and secure access across any network.

Your Network with Airwall

Airwall enables your organization to create a secure, private, easy-to-manage, mobile Internet. You can define one or more overlays, with each overlay made up of virtual trust segments, and each Airwall Edge Service possessing its own unique 2048-bit Cryptographic ID (CID) following the HIP RFCs. The result is a solution with military-grade encryption that can span nearly any device, network, or environment.

Airwall is set up using an intuitive, visual, and point-and-click management and orchestration engine. Unlike traditional IP networking and SDN approaches, Airwall requires little to no modification of the underlying network or security infrastructure. It provides a simple, policy-based configuration of devices or groups of devices that are explicitly trusted based on whitelisting. This trust, based on unique CIDs,[3] determines what systems or machines can initiate and establish communication before any data is exchanged.

Secure Networking Across OSI Stack

OSI Model	Airwall Gateway	Airwall Agents / Servers
Physical – Layer 1	√	√
Data Link – Layer 2	√	√
Network – Layer 3	√	√
Transport – Layer 4	√	√
Application – Layer 7	√	√

An Airwall Solution can span multiple existing VLANs, subnets, and cross networking boundaries – across data centers, public clouds, campus networks, remote locations, and even unmanaged networks. You can connect or disconnect in seconds without disturbing the existing networking and security infrastructure.

Airwall enables a unified secure networking architecture that reduces complexity and creates consistent application of policy across all connected systems and devices. This trust-based enforcement model is easily verified for compliance purposes.

By creating operational efficiencies, Airwall significantly reduces configuration errors and the resulting lateral attack vectors. Network and resource provisioning are simplified and can now be done in minutes.[4]

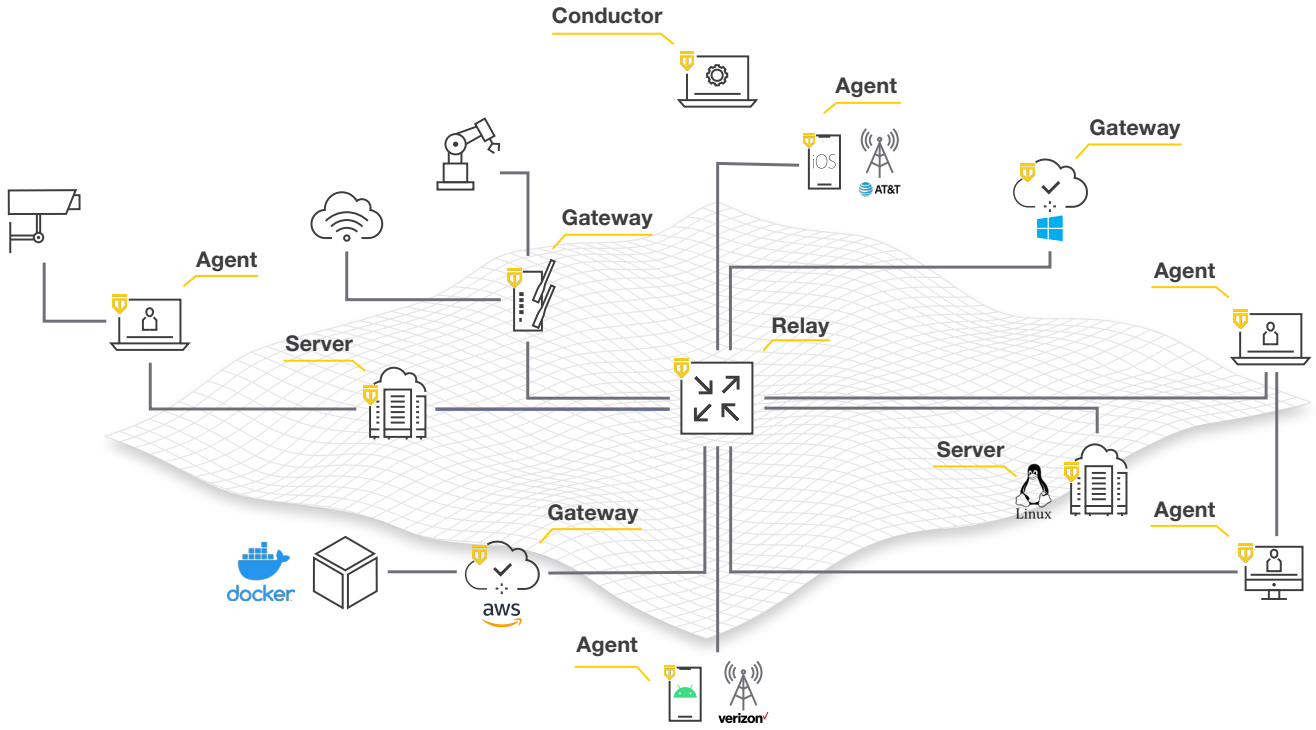
+ Devices are natively invisible to hacker reconnaissance, and protected against DDOS, MiTM attacks, IP spoofing, and other types of network and transport layer attacks.
+ Set policies across hundreds or even thousands of devices with a few clicks – reduce complexity and overhead as you manage your network.
+ Secure connection with devices in remote field locations with limited connectivity, to factories, offices, datacenters, and mobile devices.
+ Deploy with any major cloud service and across any mainstream server, desktop, or mobile operating system; as well as in front of any networked device.
+ No need to replace existing infrastructure or add more staff; far less expensive to manage and maintain than either firewalls or VPNs.

Airwall Solution Components

Building an Airwall Overlay requires that you deploy two or more Airwall Edge Services in a hub-and-spoke topology, mesh, or both. Every endpoint in an Airwall Overlay knows the IP-layer state of its peers, and every peer maintains identity-based routing tables. Airwall's policy-based approach[5] helps any edge service establish the most direct route to a resource within an overlay.

Airwall Edge Services (Gateways, Agents, and Servers) provide invisibility, secure connectivity, identity-based routing, and IP mobility.[6] They enforce Airwall Conductor's provisioning, de-provisioning, and revocation of trust for any managed IP resource. Using the cryptographic identity, Airwall Edge Services enable the mobility and migration of an IP resource anywhere within the Airwall Overlay without requiring changes to the existing networking or security infrastructure. This decoupling overcomes many of the addressing, routing, mobility, and failover challenges associated with traditional IP networking and SDN technologies.[7]

Our approach makes it easy to deploy and extend a unified, trust-based, and encrypted network. This ease of deployment enables micro, macro, and cross-region segmentation, as well as global IP mobility. Deploying and maintaining intra-cloud (region to region), cloud-to-cloud, and cloud-to-data center cryptographic trust-based communications becomes simple, verifiable, and secure.



Set Secure Access Policy
Airwall Conductor

Deployment Options

Cloud: Amazon Web Services, Microsoft Azure, Google Cloud

Virtual: VMware ESXi 6.0 and above, Microsoft Hyper-V Server 2012 R2 and above

Physical: Conductor - 1U Platform

Airwall Conductor manages policy for all distributed Airwall Edge Services, delivering effortless control of the network. Using Conductor, you define the overlay network segments and systems that protected machines are allowed to access, as well as how they connect on the LAN, WAN, and public Internet. Policy creation and management is simple and requires no advanced training.

Available in cloud, virtual, and hardware form factors, Conductor enables fast network provisioning, micro-segmentation, and secure connectivity. All of this is based on unchanging cryptographic machine identities, not network addresses that change and can be spoofed.

Intuitive network orchestration eliminates the complex, disruptive, and time-consuming provisioning steps associated with traditional IT solutions like firewalls and VPNs. Our customers deploy and revoke secure overlay network access in seconds, with little to no change to their existing network infrastructure.

Encrypt Routing Across Any Network
Airwall Relay

Deployment Options

Cloud: Amazon Web Services, Microsoft Azure, Google Cloud

Virtual: VMware ESXi 6.0 and above, Microsoft Hyper-V Server 2012 R2 and above

Physical: 500 - 1U Platform, 250 Series

Airwall Relay routes encrypted Airwall Edge Service connections across all networks and transport options, without modifying the underlying network. Secure end-to-end connectivity is now simple whether you have a Layer 2, Layer 3, or bridged L2/L3 network using Ethernet, Wi-Fi, Cellular, MPLS, or Radio.

Available in cloud, virtual, or hardware form factors, Airwall Relay allows the WAN and Internet to behave like one local broadcast domain, making WAN micro-segmentation a reality. It provides a private identity namespace that eliminates the need for expensive public IP addresses and inbound firewall rules to connect devices.

Airwall Relay is the only routing technology that doesn't rely on Layer 3 rules, network addresses, or traditional routing protocols to securely connect and route privately-addressed systems across networks. Airwall Relay relies on verifiable cryptographic identities to determine if a WAN connection is allowed and forwards only authenticated and encrypted traffic to authorized endpoints. It reduces network complexity by eliminating connection barriers like NAT, different addressing realms, IP conflicts, and complex firewall rules.

Protect Everything Downstream Airwall Gateway

Deployment Options

Cloud: Amazon Web Services, Microsoft Azure, Google Cloud

Virtual: VMware ESXi 6.0 and above, Microsoft Hyper-V Server 2012 R2 and above

Physical: 75 Series, 150 Series, 250 Series, 500 Series

Connectivity: Wired, Cellular, Wi-Fi

Airwall Gateway is typically deployed in front of devices or hosts that cannot protect themselves. Examples include legacy systems and machines, or when customers are unable to install software-based edge services. You can deploy Gateways physically, virtually, or via the cloud.

Physical Airwall Gateways have built-in Ethernet, Wi-Fi, Cellular (2G, 3G, 4G LTE modems), as well as Serial-over IP for the most flexible link connectivity options found in the industry. The physical devices can fail-to-wire, Wi-Fi, and/or cellular. You can configure phsyical devices for high availability depending on customer need. Gateways often replace existing cellular modems, access points, VPNs, and internal firewalls for significant CapEx or OpEx savings.

Virtual and cloud Airwall Gateways function in the same manner as the physical Gateways. For the first time, an organization can instantly connect, protect, segment, move, failover, and disconnect any private or public cloud-based workloads anywhere in the world. Unlike SDN or traditional networking and security technologies, organizations no longer need to deploy and maintain separate networking and security policies for their on-premises and cloud-based resources.

Protect Devices Anywhere Airwall Agent

Deployment Options

Windows:
7/8/10 (32/64-bit)

MacOS:
10.14 and above

iOS/iPadOS:
12.0 and above

Android:
6.0 and above

Airwall Agent is a software application installed on Windows, macOS, iOS, iPadOS, and Android devices that enable customers to give managed devices a trusted and verifiable identity. This ability opens up a broad array of end-user secure access, networking, mobility, and segmentation use cases. Trust-based client segmentation, granular access control, encryption everywhere, and auditing is now possible in both static and dynamic IP environments.

For the first time, you can easily integrate user authentication with device-based authentication, overcoming much of the complexity associated with extending directory services to include device-based trust. Unlike traditional VPN technologies, Airwall Agents allow an organization to explicitly allow or deny any device to not only securely connect to a network, but easily segment access by explicitly defining resources that a device or group of devices can and cannot access. Airwall Agents also overcome the typical session constraints of legacy VPNs and are not restricted by the number of concurrent client-to-resource encrypted sessions.

With Airwall Agents, an Airwall Overlay becomes the first place to enable and revoke user access, even before performing revocation in a directory service. Once device-based trust and authentication have been revoked, even active user credentials no longer work, because users cannot access any resource from an untrusted device. Revocation of trust is a one-click operation. Because of Conductor's ability to immediately orchestrate and update distributed policies to all edge services, the rest of the Airwall Overlay knows the device and its CID have been revoked. No edge service will respond to any request, anywhere, even if the revoked user knows hostnames, IP addresses, and user credentials to those resources.

Protect Server Workloads Airwall Server

Deployment Options

Linux: CentOS 6.9 and 7, Ubutu 16.04, Fedora 25 (REHL compatible)

Windows: 2008 R2, 2012 R2, 2016

Airwall Server support Windows Server and Linux and behave much like Airwall Agents. They give organizations the option to completely cloak the server itself, so only authenticated and authorized endpoints can discover and communicate with it. Cloaking, software-defined segmentation, and encryption are driven down to the server level, effectively enforcing a perimeter of one. Simplified and consistent global IP mobility and migration becomes a reality for applications and servers running Airwall Server.

Airwall Use Cases

Airwall can be deployed in a wide variety of use cases. Here are a handful of ways customers leverage our solution:

+ **Critical infrastructure protection, rapid provisioning, and cost-effective remote support** – Automatically network, cloak, secure, and manage critical infrastructure such as oil and gas pipelines, electrical substations, smart meter systems, and healthcare devices from anywhere in the world. Implement this solution without the cost and complexity of attempting to deploy and maintain separate routers, firewalls, and VPNs. Because access is based on cryptographically-signed, authenticated, and authorized devices, the risk resulting from the common practice of using shared administrator credentials is eliminated. Organizations can significantly reduce their cyber-risk and the productivity loss of having to send field technicians to remote locations for maintenance.

+ **Instantly provision or revoke vendor, third party, or supply chain access** – Some of the most common attack vectors today are third-party systems that are either permanently or temporarily connected to a corporate network. HVAC systems, building automation, web services, vendor technicians, PoS systems, and even guest Wi-Fi all increase an organization's attack surface. Pinholes are opened in firewalls and then frequently forgotten. Configuring temporary VPN access is laborious, slow, and cannot be easily segmented down to a specific resource. Permanent connections for things

like building automation are difficult to maintain over time. Using VLANs or ACLs cannot prevent lateral movement by a bad actor. With Airwall, you can provision temporary or permanent access instantly that cannot be traversed, is immediately verifiable, and can be instantly revoked regardless of user credentials.

+ **On-demand secure network provisioning and PCI compliance** – Provision Point of Sale (PoS) systems, kiosks, or pop-up stores in seconds, then cloak, segment, and move out of scope for PCI compliance over any network. Shared and unmanaged networks become a non-issue because Airwall prevents hackers from using temporarily or permanently-connected systems on a corporate network as an attack vector. All communication is automatically AES 256 encrypted.

+ **MPLS replacement, remote office security, and instant failover** – Replace costly MPLS networks with Airwall and commercial broadband for distributed remote sites. This approach provides better security, faster provisioning and much simpler management. At each site, you can deploy an inexpensive Airwall Gateway, creating a cloaked, secure, and private corporate WAN. Adding a new link to an Airwall Overlay requires just a few clicks in Conductor. Remote office exposure to Man in the Middle (MiTM) attacks is prevented because hackers are unable to find and fingerprint devices in order to execute attacks. And if a link fails, the Airwall Gateway immediately fails over between links, ensuring high availability.

+ **Secure and segmented user, vendor, and application access control** – Unlike traditional VPN technologies, an Agent or Server can now have many concurrent encrypted virtual trust segments (VTS) or tunnels to specific applications and services without requiring an appliance. Building automation vendors can deploy OT systems at customer locations and provide encrypted and verifiably-segmented access to those systems for faster and less expensive maintenance without their customers fearing those systems as a potential attack vector. Vendor systems can be verifiably segmented and cannot communicate with any other system on the corporate network. You can cloak all other systems on the corporate network so they will not respond to any communication with those systems unless it is explicitly allowed. Secure internal and remote access for employees anywhere in the world becomes far more practical and cost-effective than traditional VPN and firewall technologies by eliminating failover, key management, and networking problems associated with client appliance access and mobility. Agents and Servers can now connect directly or through Gateways without opaque and complex legacy network constraints.

+ **Secure and segmented machine-to-machine communication** - Servers running Airwall Server can bind a unique ID that is only known and available to other Airwall Edge Services. This unique ID frees the application server from the constraints of the hosted network, allowing it to freely move from network segment to network segment and even to a public cloud within an Airwall Overlay without losing its IP address. Only whitelisted devices can locate the Airwall Server's enabled service by its CID and its unique IP address.

Airwall Delivers

- Device invisibility and automatic AES-256 encryption tunnels between Airwall Edge Services.
- A default zero-trust model with one-click trust establishment based on unique device CIDs.
- Secured VLAN isolation and micro, macro, and cross-boundary segmentation.
- Transparent mobility of secured devices and services within an Airwall Solution.
- Connectivity for secure Layer 2 or Layer 3 networks across any link medium.
- Network transparency, resiliency, and instant failover.
- Rapid provisioning, revocation, and instantly-verifiable quarantine.
- Visual Trust Map to assist with proving PCI and other compliance requirements.
- Flexible deployments supporting physical, virtual, and cloud appliances.
- Extensibility down to clients, servers, applications, and embedded hardware.

Is your enterprise network secure at scale?

Schedule a meeting with out experts to learn more
call **(206) 452-5500** / email **info@tempered.io**

Appendix

Endnotes

1. **Billions of devices without built-in cybersecurity are connecting to IT networks and are creating a massive and rapidly-growing attack surface.** Enabling the remote control of critical and physical infrastructure has created attack vectors that didn't exist when today's security solutions were being designed. The result is rapidly rising cost and complexity, with a measurable decline in protection. The original inventors of the networking technologies that became the Internet never imagined the billions of devices we use today. They introduced something that turned out to be a huge, critical assumption. The fatal flaw is that your IP address is used as both your location and identity. Every device gets an IP address. That address is used as its identity. And that address can be found. If it can be found, it can be hacked. Moreover, every device hacked can be used to hack other devices.

2. **Host Identity Protocol (HIP) was conceived as a solution to overcome the fatal flaw in TCP/IP networking, which has made networking security the complex Rubik's Cube it is today.** The Host Identity Protocol standard (HIP RFC's 5401, 7401, 7402 and VPLS 4665) were first proposed by Robert Moskovitz in 1999, as an individual IETF submission. It has been used in production since 2006 for everything from secure field communications by the military to accelerating manufacturing operations at Boeing by securing and enabling network mobility of their tooling infrastructure. The cornerstone of HIP "is the idea of separating a host's identity from its present topological location in the internet" for the sole purpose of "enabling a secure and mobile internet." One of the most important principles is that HIP is backward and forward compatible with any IP-based network, application or resource. HIP is an open standard, but to realize the vision of "a secure and mobile internet," a new management paradigm was needed. It required scale, policy-based orchestration, and the compatibility of HIP-based services across any operating system, hypervisor, container, or hardware platform.

3. **Using unique CIDs makes Airwall extremely resilient.** Decoupling the identifier and locator functions of an IP address restores its original purpose as a resource locator. Unlike other technologies, networking and security policy orchestration is so simple that authorized business teams could easily make their own policy changes without involving other teams or risk exposing corporate networks and other connected resources.

4. **Network and resource provisioning are much simpler with Airwall.** Failover is faster, predictable, and easily verifiable. Dependencies on complex firewall rules, VPN policies and key management overhead, ACLs and VLAN configuration is greatly reduced. Managing a simple IP address change, migration, addition of a new network, office or kiosk, or providing temporary/controlled third-party access no longer requires significant time and expertise.

5. **Airwall uses a policy-based approach, enforced at the device level.** This approach enables all endpoints to know and maintain knowledge of where resources within and across networks are located, and what Airwall Edge Service is in front of a single resource or many resources. Every edge service has the equivalent of a policy-based table that is instantly updated via the Conductor any time an administrator or a secure API call makes a change. The policies maintain state across edge services via Conductor, but do not require persistence, ensuring only authorized resources are in fact communicating only with others that have been explicitly allowed.

6. **Airwall Edge Services follow the Host Identity Protocol standard.** This standard initiates trust before transport communication is established and before any data is exchanged between authorized edge services. Conductor orchestrates policies across edge services that are distributed throughout an Airwall overlay, where the Conductor maintains state but does not require persistence for edge services to function.

7. **Airwall Edge Services adapt to your network deployment.** They effectively function as a switch, eliminating or reducing the need to maintain VPNs, complex firewall rule sets, VLAN segmentation, routing convergence and DNS for failover, and ACLs in an attempt to accomplish secure connectivity, access, availability, and segmentation. This functionality allows for a flexible deployment model that can span nearly any type of resource, location, or environment. This capability of easily extending a secure networking overlay as broadly or deeply as an organization chooses across any environment cannot be matched by any other SDN, SD-WAN, traditional networking, or security vendor.

Additional Resources

- tools.ietf.org/html/rfc7401
- tools.ietf.org/html/rfc7402
- www.cs.helsinki.fi/u/gurtov/papers/hip_survey.pdf
- www.nist.gov/system/files/documents/cyberframework/cybersecurity_framework_bsi_2015-04-08.pdf