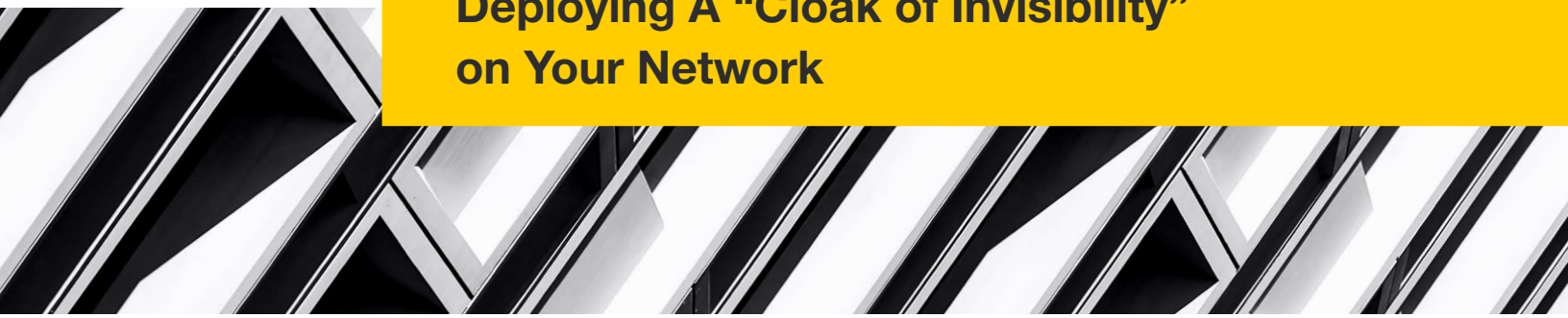
Tempered

Airwall Overview: Zero-Trust Infrastructure for Federal & DOD

Deploying A “Cloak of Invisibility” on Your Network



Airwall enables mission agility, flexibility and resiliency, to adapt to the dynamic demands of the soldier and mission and ensuring continuity of operations and operational security on a global scale.

Abstract

With Federal/DOD agencies increasingly encompassing Cloud, Hybrid, BYOD, IoT/OT systems, the network has become asymmetric. Traditional, network-centric cyber defense approaches (in the time of COVID), allow threat actors to more easily move laterally from system to system. Once they gain network access, they can potentially wreak havoc across the entire organization. Adopting a zero-trust security model that integrates network micro-segmentation and software defined perimeters makes these types of lateral movements much harder for insiders and intruders. Having smaller, segregated networks also significantly reduces the attack surface and constrains potential damage.

IMPRES

Tempered would like to thank and acknowledge the contributions to this White Paper by IMPRES Technologies. IMPRES is a Tempered Federal partner and subject matter expert for Zero-Trust, CyberSpace Operations Infrastructure (CSOI) technologies.

Tempered Airwall delivers a zero-trust security model compatible with the increasingly complex network systems Federal and DOD agencies are supporting. Implementing the Airwall solution cloaks systems from detection, encrypts data as it moves through the network, and assigns hardened identities to any IP-networked device. The Airwall architecture cryptographically defines each endpoint, instead of exposing and tracking it via an insecure, discoverable IP address. Agencies can easily incorporate Airwall into existing networks of connected devices, without disruption and with little to no modification. It enables hyper-secure tunnels between endpoints on existing networks, forming "new" secured and micro-segmented networks. These networks allow information sharing and endpoint isolation across environments of any size, and spread across any geographic location. Airwall's Zero-Trust Architecture (ZTA) further eliminates operational risk and complexity with dynamic provisioning and revocation of trust for endpoints without physical disruption, and secure access for devices, users, and resources wherever they reside.

A zero-trust security model achieves compliance with NIST requirements (NIST SP 800-207, 800-52, 800-171b) and meets the new CMMC requirements for all DIB (Defense Industrial Base) suppliers. By implementing an Airwall Zero-Trust solution across your network, you can simplify the management of network assets, deploy a Software Defined Perimeter to your endpoints and fully cloak the network – make it invisible.

The challenge of secure IP networking

Nearly 100% of all network and security policies use IP addresses as identity — a root cause of complexity in secure networking — and managing a network has never been more challenging. The mass onset of more demanding applications makes traffic prioritization a mandate, not simply a check box for current data and voice in today's architecture. Traffic rerouting, brought on by the massive number of new devices on the network and reaching into the cloud, is only complicated by the increasing need for outside groups to access and share data in real-time. The challenges become even greater when the DOD battlespace includes a multi-domain, coalition environment.

The DOD's Federated Coalition Information Sharing Architecture enables communication and collaboration with Armed Force branches and coalition partners. The demand to allow/deny any branch or coalition partner to access this architecture dynamically (without formal agreement) — while providing full protection and security to the entire information systems quickly and efficiently — has been a challenge to IT staff.

Once you grant access to systems or specific networks, how can you secure a relatively flat network, so that access is granted only to necessary systems and resources, securely and dynamically? In a multi-cloud and heterogenous environment like the Federated Coalition Information Sharing Architecture, how do you offer secure access to any specific part of those resources and securely share information on-demand?

The underlying complexity that comes with these challenges has everything to do with IP networking and IP addresses. Providing secure routing dynamically can confound even the best skilled IT teams.

DOD focus areas from current cyber challenges

Focus Area	Description
Augmented Network Management	**Network Performance Modelling and Simulation:** The DOD must be capable of assessing performance differences between current and planned networks. The DOD seeks the ability to model, simulate, and visually display network changes, including those caused by adversary threats and weather situations. The goal is to analyze and validate expected changes in network performance (that is, connectivity, throughput, propagation/coverage, network health, service health, performance, signal flow, etc.).
	Automated Response: The DOD's Unified Network must be capable of quickly – and without error – managing latency challenges, quality of service concerns, and data throughput issues. Therefore, the DOD seeks to improve tactical network management by incorporating innovative artificial intelligence and machine learning capabilities to notify network administrators when these and other problems arise.
	Risk reduction and counter-response: The DOD must be capable of dynamically and automatically managing and controlling actions on the network. This includes controlling large numbers of network devices, services, topology, traffic paths, quality of service, bandwidth allocation, and speed of service. To do this, the DOD seeks to understand how automated Primary, Alternate, Contingency, and Emergency (PACE) planning and execution capabilities can control network actions and leverage threat-based analytics to mitigate potential risk while conducting network management.

Focus Area	Description
Content Management	In a data-rich battlespace, the DOD must ensure data and information is correctly categorized, prioritized and provided at the required time. It must be provisioned to or from the required entity, then delivered to the appropriate location by appropriate authorities. This will occur during Disconnected, Intermittent, and Limited Bandwidth - Congested, Contested (DIL-CC) network conditions. To address this, the DOD wishes to explore Information Dissemination Management Content Staging (IDMCS) and Content Management (CM) capabilities to improve network operations on the Unified Network.

Based on the above, the requests from U.S. CYBERCOM and SOCOM, and NIST SP 800-207, Airwall's Zero-Trust Architecture (ZTA) satisfies these requirements by treating all users, devices, data, and service requests in the same manner.

What is Airwall?

Zero-Trust Architecture

Airwall's zero-trust infrastructure is the Layer 3 overlay component that provides the foundation to build a robust software-defined perimeter (SDP) solution. It balances accessibility, information security, operational resiliency (mobile, manned, and unmanned systems), and full insider threat protection. Airwall is a strategic resource for those working to build responsive, resilient networks, reducing the network attack surface from insider threats, increasing security protection in coalition environments, and preventing internal/external threats from compromising critical assets. Airwall allows the DOD to rapidly and dynamically adjust unit task organization and network configurations to meet mission requirements, along with the USA's coalition partners to the tactical edge.

Airwall enables mission agility, flexibility and resiliency, to adapt to the dynamic demands of the soldier and mission and ensuring continuity of operations and operational security on a global scale. By providing a comprehensive, centralized approach to secure access control, DOD enterprises can provide more flexibility in how soldiers, contractors, coalition partners, and third-party resources access and interact with the DOD's most critical resources.

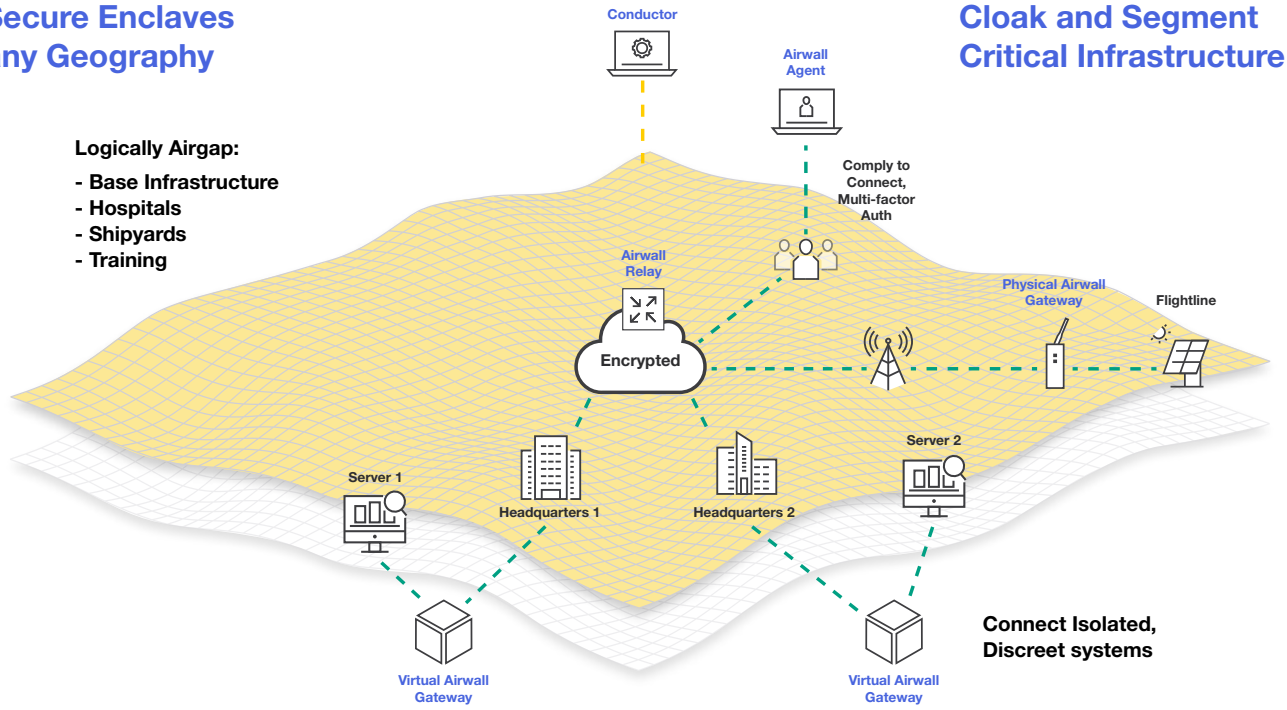
Airwall provides user-centric, real-time network access on a need-to-know basis and enables a unified way to control access while maintaining a high security profile.

Create Secure Enclaves across any Geography

Logically Airgap:

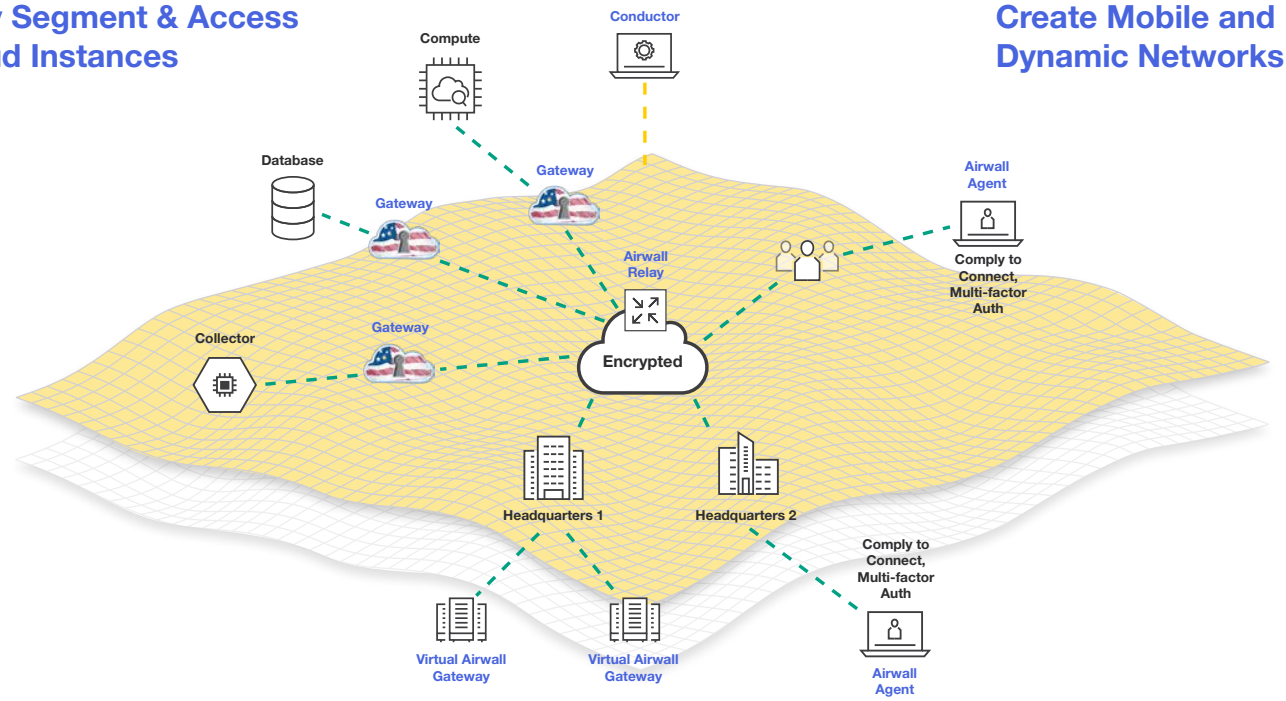
- **Base Infrastructure**
- **Hospitals**
- **Shipyards**
- **Training**

Cloak and Segment Critical Infrastructure



Connect Isolated, Discreet systems

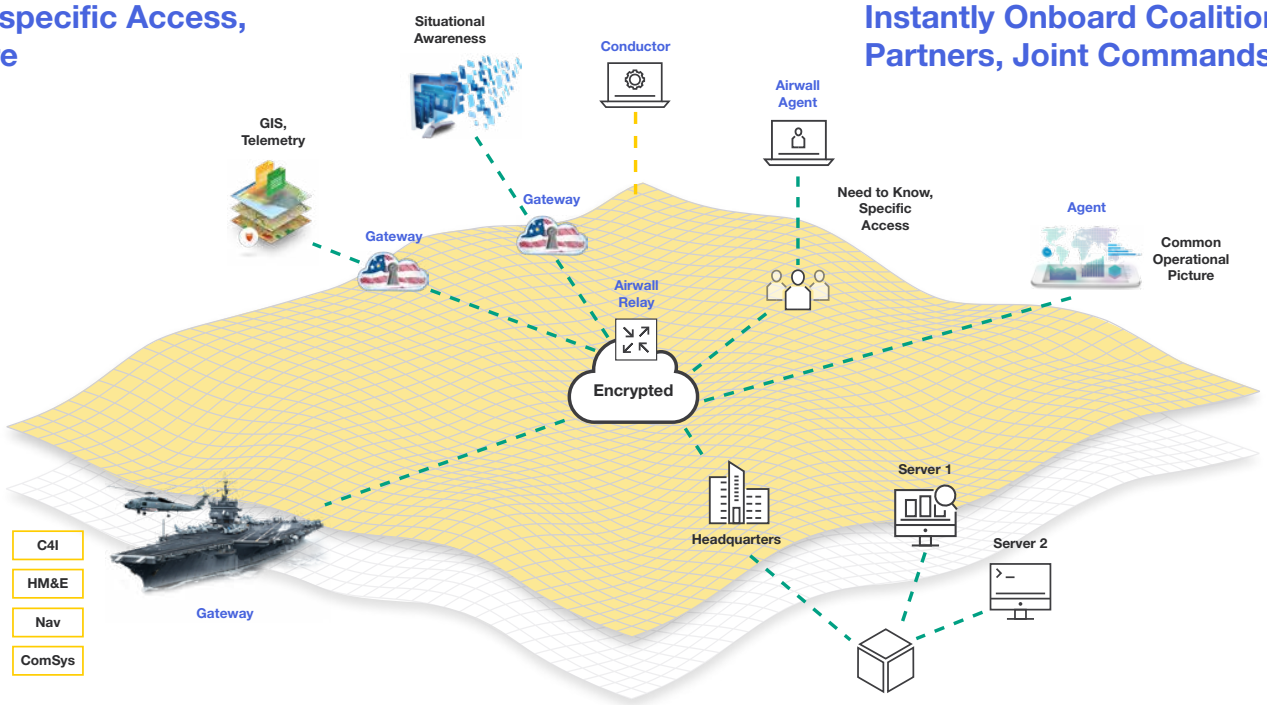
Securely Segment & Access GovCloud Instances



Create Mobile and Dynamic Networks

Mission-specific Access, Anywhere

Instantly Onboard Coalition Partners, Joint Commands



Built on Least Privilege Access

With traditional solutions (NAC, VPN, etc.), unauthorized services are still visible on the network, and at risk for exploitation by a malicious user or cyber-attacks. In a zero-trust world, organizations must assume that users' machines are compromised and that all applications and network services can be exploited. When taken to its logical conclusion, the principle of least privilege implies that organizations must hide all unauthorized resources from users at the network level. It also implies that organizations cannot rely solely on authentication/ authorization to defend against adversaries with malicious intent.

Organizations have worked hard to align user entitlements with what's appropriate to role, function, or mission. However, this is typically controlled at the authentication and authorization level – not at the network level. There is a huge gap between what users are authorized to do, and what they can see. This gap represents a huge and unnecessary attack surface, which we've seen malicious actors exploit time and time again. Airwall simplifies secure access by including pinpoint access control of both users and network resources. It controls individual user access through simple policy-based orchestration, without requiring broad network changes. Airwall combines strong authentication, authorization, encryption, and access control in one system, replacing many point products organizations traditionally use.

Airwall closes the gap of what users can see versus access

Organizations can finally apply the principle of least privilege across networks, ensuring users' access privileges are consistently enforced at the application and network level. Airwall lowers risk and improves security by reducing the attack surface, increases tactical/mission agility, and reduces operational complexity. Airwall delivers fine-grained access control of both users and resources, and makes non-authorized assets invisible and inaccessible. It coexists with the DOD's existing architecture and drastically reduces the operational complexity of the Tactical Internet (TI). Airwall can adapt to mission demands of data dissemination and scaled policy deployment (information-sharing in coalition environments). It encrypts traffic all the way up to application VLANs and unifies internal and external user access in one and the same method.

Deploying Airwall

Abstracts applications and other resources	Unauthorized resources are invisible to users, which is important to C4ISR operations and to insure OPSEC across the DOD Tactical Network and Enterprise.
Session-by-session access control and logging	True 'segment of one' access, and once the user logs out, the secure tunnel disappears.
Reduces complexity	Combines strong authentication, authorization, encryption, and access control in one system, replacing many of the point products traditionally used.
Unified way to control access for all users	Whether resources are on-premises, in the cloud or at the tactical edge, the same access policies apply, which means that deploying in hybrid environments is simple and easy to manage.
Scales across any environment	All resources (whether on-premises, private or public cloud, or coalition environment) remain invisible until authorized. The network turns itself off if data is not being transmitted, and the devices will not respond to ARP, UDP, PING or any such commands at a hardware level, unless there is an authorized token for the device making the request.
Replaces traditional tools	Replaces traditional security and remote access tools — like VPNs, next generation firewalls, and NAC solutions — that provide an all-or-nothing view of access control, carte-blanche access to anyone who is verified, and don't address the potential for insider threats, stolen credentials, and negligence.

Eliminate individual access requests	Eliminate dependence on form-based administrative processes, and significantly reduces system administrators' access-management burden. Users get immediate access to applications and data based on their attributes (e.g., position, training, duty location, and so forth).
Reduces the number of network administrators	Network security operators no longer have to make network appliance configuration changes (e.g., firewalls, proxies, and intrusion detection systems) to "allow only" legitimate traffic and block known, bad traffic.
Single centralized platform	Centralized, dynamic, attribute-based controls determine access across physical, virtual, and cloud infrastructures. Allows system and network administrators to manage all aspects of SDN, legacy networks, and physical and virtual environments, as well as provisioning to and from the cloud, while providing the ability to cloak and respond to attacks (including responding to instances of outsiders probing for network devices).
Reduces insider threat	This new paradigm enables creative approaches to data protection. Vulnerability to an insider threat is reduced since Airwall renders assets invisible to unauthorized access, reducing the attack surface, plus tracks all access to applications, endpoints, and data.

Extend, scale and adapt with Airwall

Leverage a combination of hardware and software that extends, scales, and adapts to the demands of the warfighter, cyber warrior and mission on a global scale.

Vendor objectives made possible include:

Dynamically-secured onboarding of an Ally Partner or Warfighter to a micro-segmented data source.

Secured access to an Isolated VDI Instance (virtual classified network) within a cloud environment.

Secured and isolated overlay across multi-cloud environments (AWS, Google, Azure, on-prem).

Network maneuverability in a degraded environment (DDoS cyberattacks in the battle space, etc.) with one-click ability to cloak the network.

Platform ubiquity

Appliances
Gateway 75, Gateway 110, Gateway 150, Gateway 250, Gateway 500

Agents
iOS, MacOS, Windows, Android, Raspberry Pi OS, OpenWrt

Servers
Ubuntu, Windows Server, CentOS, Red Had Enterprise Linux

Public Clouds
AWS, AWS GovCloud, Google Cloud Platform, Azure

Hypervisors
VMware ESXi, Microsoft Hyper-V Server, Xen, KVM

SDP/SASE Integrations
RuggedCom, AzureEdge

Enable Zero-Trust Architecture for your organization.

Learn how Tempered can help with your Zero-Trust or related compliance efforts. Schedule a meeting with our experts to learn more.

government@tempered.io | +1 206.452.5500