Tempered

Learn how a national healthcare provider securely connects its multi-state locations, enables remote access, and protects its physicians, caregivers, and high-value assets.

National healthcare provider protects critical systems and simplifies network management

Airwall effectively micro-segments multi-state hospital network, ensuring secure remote access and protecting against network-based attacks.

Challenges

Managing a flat and open business network exposed this healthcare provider to external threats and malware. Ensuring equipment, physicians, caregivers, and third-party contractors were securely connecting and given limited access was problematic. Securing their critical systems and teams would be incredibly complex.

Solution

Airwall was first deployed to protect third-party managed laboratory equipment and staff across all hospitals and clinics. In addition, as critical equipment and systems were upgraded, they were securely connected and easily managed. Airwall was also deployed to remote clinics in rural communities to ensure secure connectivity to the hospital network.

Wins

The hospital network now has effectively segmented access and visibility for users, equipment, server, and cloud. Network attack vectors have been eliminated and there has been significant reduction in CapEx and OpEx. With Airwall being an extensible platform, it was non-disruptive and simple to expand into new clinics and hospitals.

> *“Our journey to protect and segment distributed Healthcare Systems without compromising access, care, and quality, led us to Tempered. Airwall lets us stop networking with yesterday’s tools.”*
>
> **Director of Information Security**

The challenge

A multi-state healthcare provider with 10 hospitals and more than 75 clinics had been hit with ransomware and external attacks. Hospitals and clinics were spread across multiple states with hundreds of regional providers, partners, contractors, and vendors who needed access to the network. With over 3,000 physicians, 16,000 caregivers, and over 3 million patients, the organization knew it had to make changes to secure its critical systems, protect its users, and lower its cyber risk.

There were a variety of challenges associated with ensuring secure connectivity. The entire network was flat and everyone on the network had access. It was highly distributed and mobile, comprised of vendor access needs, thousands of medical devices distributed across three states, server and cloud deployments, and rural clinics with limited connectivity options.

The healthcare provider employed a variety of traditional network security tools including VPNs, IPSec tunnels, certificates, and gateways for access control. But years of layering these tools only further complicated network management. It was a situation that traditional tools could not remedy.

To try and solve these challenges, this healthcare provider looked at adding additional tools like SDN, Firewalls, VPNs, and additional VLANs. They quickly realized these tools would require additional headcount and resources, increase network complexity, and still not be provide true network security. Furthermore, these traditional tools would still move patient data in the clear, unprotected on the LAN.

The solution

The VP of Information Security heard about Tempered and learned how Airwall could help the organization slice up its network into separate networking enclaves. They would be able to create virtual networks where systems, devices, and users would have their required visibility, but everything else would remain invisible and protected. All of this could be done at a fraction of the time and cost, require no additional headcount, and be easily extensible as the network evolved.

The organization began by micro-segmenting the third-party laboratory equipment and vendor access. This ensured that any third-party access to the network was limited to exactly what they needed and nothing more. This helped the Information Security team logically segment critical systems, applications, and users from vendor visibility and access.

The healthcare provider then deployed Airwall to clinics in remote villages with limited internet access. The cost of upgrading MPLS networks for remote clinics was exorbitant. However, with Airwall's global cellular connectivity, enabling remote printing and office phones was now simple. Physicians and caregivers in these remote locations could now securely connect to the systems and applications they needed.

Wireless Bio Med carts were the next place Airwall was deployed. These mobile medical carts are WiFi enabled and used daily by physicians and caregivers. These carts were quickly protected with Airwall Gateways, ensuring secure connectivity to and from these carts, and invisibility from any other device, user, or third-party.

Customer success

This healthcare provider's initial deployments led to further use cases for Airwall expanding into new areas. Airwall made sense as equipment and applications were upgraded or replaced. It also made sense for new clinics and hospitals that were coming online. These greenfield situations provided a perfect opportunity for the information security team.

Airwall was deployed to the hospital network's building control systems. It was now easy to segment access for these building environments. With point-and-click simplicity, secure access could be gratned to employees, contractors, or vendors to specific network segments.

Airwall simplified network management with a clear map of systems, applications, and user visibility and access, while significantly lowering CapEx and OpEx. Airwall has effectively lowered cyber risk and limited network attack vectors.

> *"Airwall has been a game-changer for our organization. It effectively limits our cyber-risk, has been easy to deploy across our hospitals and clinics, and protects our physicians, caregivers, and patients."*
>
> Director of Information Security

Deployed Airwall Solution components

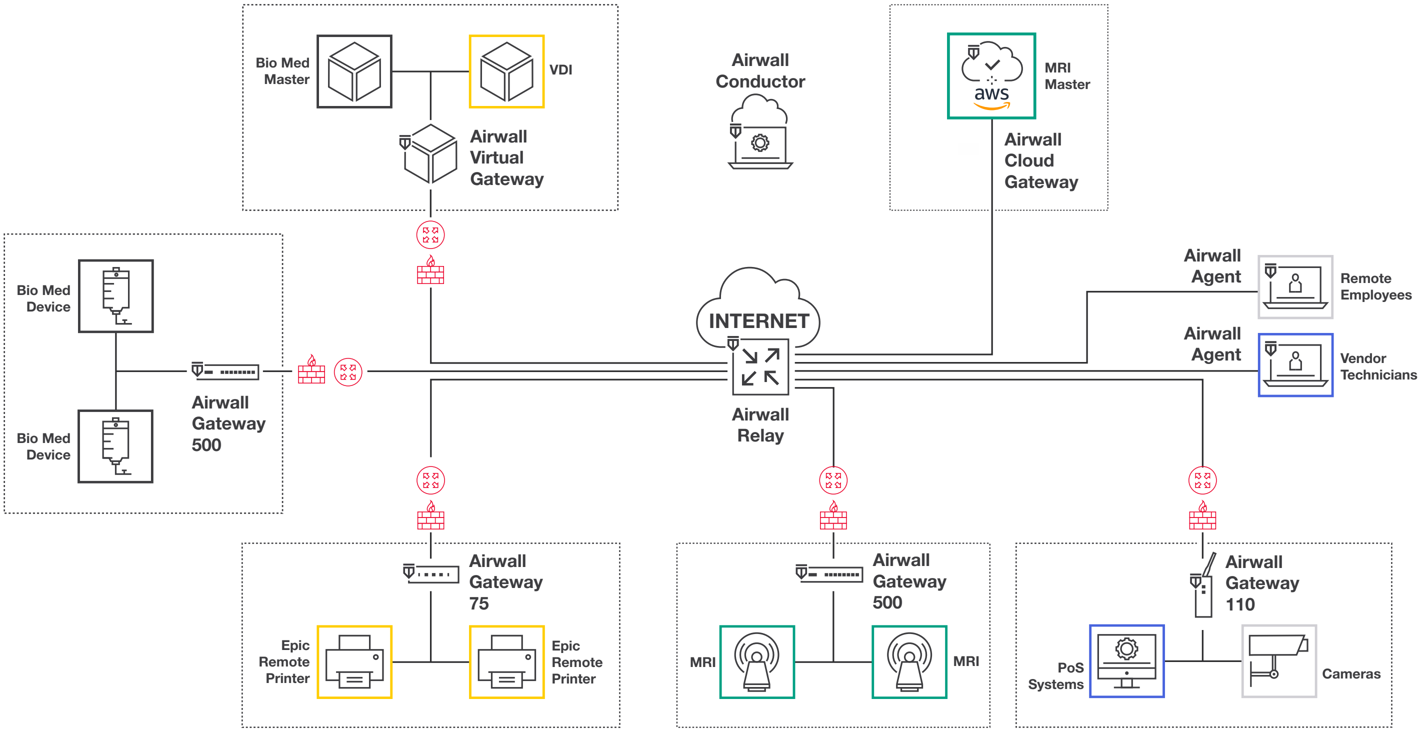
Airwall Conductor: The team deployed the orchestration engine in the cloud, allowing easy provisioning, segmentation, allocation, and revocation across the network. They are now able to quickly provide visibility and access as necessary, while still protecting high-value assets and users on the network.

Airwall Gateways: Physical Airwall Gateways were deployed to protect medical equipment and building automation systems, while cloud Airwall Gateways were deployed to protect servers and applications in the cloud. Now these critical systems stay invisible and protected but are available to whomever or whatever is explicitly given access.

Airwall Relay: The team deployed identity-based routing devices in the cloud to secure traffic across the WAN using encrypted tunnels. This enabled traffic from hospitals and clinics in any location and on any type of network to easily access databases and applications quickly and securely.

Airwall Agents: Secure remote access was enabled for third-party, vendors, and remote healthcare professionals, with Agent software. By assigning a unique cryptographic identity (CID), every user is only able to access the assets they are explicitly given policy to.

Reference architecture



Tempered delivered 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

without expense-in-depth

A fraction of the cost of traditional solutions

Deployed much faster than traditional solutions

Did not require additional network admins

Want to see what Airwall can do for you?
Schedule a meeting with our experts to learn more.

experts@tempered.io | +1 206.452.5500

tempered.io