TEMPERED NETWORKS®

Use Case

Simple and Secure Networking for Health Systems

Secure peer-to-peer connectivity and micro-segmentation for medical devices and systems

What Our Healthcare Customers Experience:

50% Lower CapEx and OpEx
through network simplification

Connect and Revoke Devices 97% Faster
with little to no network changes

90% Reduced Attack Surface
through cloaking, micro-segmentation, and encryption

Challenge Overview – Securing Medical Systems

The healthcare industry faces unique challenges when it comes to networking and securing medical devices, where the complexity of traditional IT solutions for Internet of Medical Things (IoMT) deployments has left IT teams feeling ill-equipped and exposed. As the number of connected 'things' such as infusion pumps, PACS systems, mobile x-ray units, EKG monitors, etc., continue to grow exponentially across hospitals, the trend is to converge networks to combine administration and management tasks, enhance patient care, and control costs. However, supporting a variety of medical devices on one common network creates significant operational and patient safety risks.

The main challenge our customers encountered when connecting modern and legacy medical devices was that they were not designed with basic security controls like authentication and encryption that are common in corporate IT networks. As a result, traditional IT solutions were not a good fit for these types of devices. The time, expertise, and budget needed to provision and manage firewalls, VPNs, routers, switches, access points, ACLs, and VLANs for every device was impractical and still left them exposed to hacker reconnaissance and exploits.

Tempered Networks – Simple and Secure IoMT Networks

Identity Defined Networking (IDN) for medical devices creates a highly available, natively secure, and simple network so our healthcare customers have peace of mind when leaving the office. With IDN, our customers deploy secure and micro-segmented overlay networks in minutes, rather than days or weeks compared to traditional IT solutions. And even better, the cost is a fraction of those traditional IT alternatives. Now they can easily connect and integrate modern and legacy medical devices to deliver superior availability and quality of care.

Network Challenges:

- Micro-segmenting wired/wireless medical devices to prevent conflicts and downtime
- Rapidly enabling network access for clinicians and support staff when rolling out new services
- Isolating non-critical care devices (e.g. building controls or PoS systems) on shared network

Security Challenges:

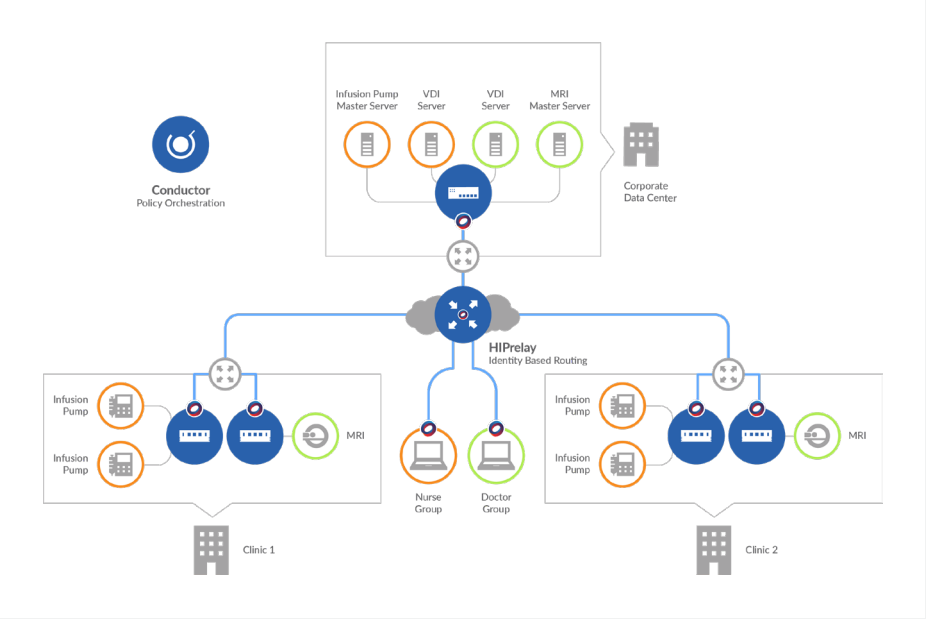
- Network, compute, storage, and application vulnerabilities caused by human error
- Lack of support for latest authentication and encryption methods by aging devices
- Virtual Desk Infrastructure (VDI) gateways exposed to public Internet creating vulnerabilities

People and Process Challenges:

- Multi-factor auth. is too complex for users
- Regulations slow upgrades of hardware and software

"Tempered Networks' Identity Defined Networking allowed our team to securely connect and segment all the infusion pumps on the network across our 10 hospitals. We had estimated it would take a year with alternative technologies, but with Tempered it only took 3 weeks, was a third of the cost, and is more secure."

IT Director
Large Health Care Organization,
Western U.S.



Challenges with Traditional IT Solutions

- Inability to quickly connect and segment any medical device across any location in the world
- High acquisition and management costs of distributed firewalls, access points, VPNs, routers, and switches
- Complex firewall rules, ACLs, VLANs, certificates, and VPN tunnels across legacy and modern IoMT systems
- Inability to quickly provide technicians and others with micro-segmented access to specific systems
- Ongoing IP addressing issues and conflicts for a variety of medical devices
- Costly and complex to validate compliance requirements for appropriate levels of device access

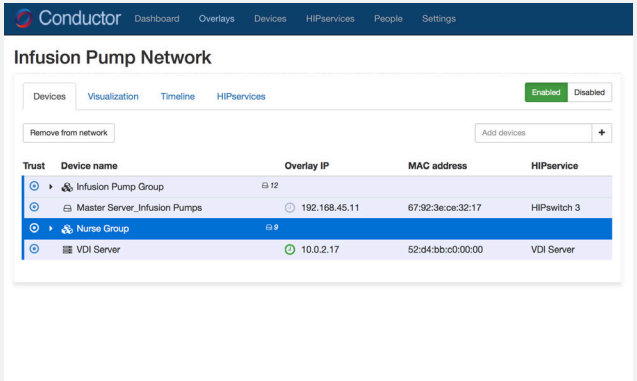
Native Security and Network Simplification with Tempered Networks

- Micro-segmentation and native end-to-end encryption across the LAN, WAN, and cloud
- Automated medical device assignment to isolated overlay segments on the hospital network
- Ability to connect systems over any medium — cell, Ethernet, Wi-Fi, or radio.
- Eliminate IP addressing issues and conflicts, without having to re-IP devices
- Easily give network access to technicians and others that's inherently secure and micro-segmented
- Simple and cost-efficient compliance reporting of device segmentation

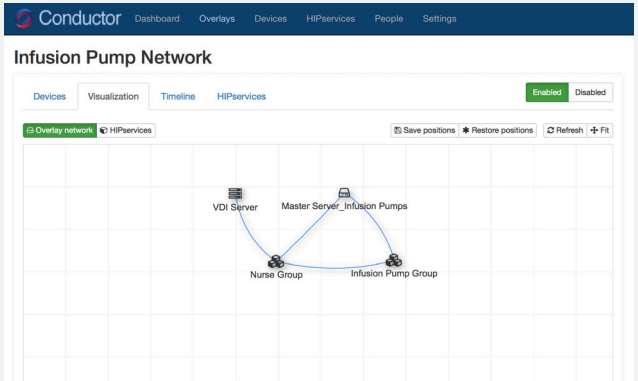
With IDN, hospital IT teams can eliminate network complexity and securely connect any device, over any network, across any location, with little to no changes to the underlying network infrastructure. The process, referred to as instant overlay networking, results in massive simplification of your network, coupled with next-gen security and resiliency that can't be achieved using traditional IT solutions. Teams can now quickly connect, micro-segment, encrypt, and manage a variety of medical devices based on trusted whitelisting of verifiable machine identities.

Trust-Based Connectivity and Micro-Segmentation in Minutes

Tempered Networks' scalable orchestration engine was designed to be extremely easy to use with no advanced technical training. Unlike the many complex, fragile, and time-consuming steps associated with traditional IT solutions, our customers eliminate human error through simple point-and-click policy orchestration. All system-level network connections are automatically authenticated and authorized between every endpoint through trusted and verifiable machine identities that can't be exploited.



Trusted end-to-end connectivity with point-and-click simplicity to add, disable, and revoke machines



The Visual Trust Map verifies connectivity and segmentation, delivering simple compliance reporting

Business Impacts of Traditional IT Solutions vs. Tempered Networks

The benefits below are based on a typical customer scenario securely connecting ~500 infusion pumps, MRI systems, and mobile x-ray units across 4 separate campus buildings. With superior mobility, the hospital was able to bring devices to patients, improving patient care and overall efficiency. And unlike traditional IT solutions, with Tempered Networks all medical devices are isolated across their own encrypted and segmented overlay network that can't be violated.

IMPACTS	TRADITIONAL IT SOLUTIONS	TEMPERED NETWORKS SOLUTION
EQUIPMENT COST	$1 MILLION +	$200,000
DEPLOYMENT TIME	800 FTE DAYS	60 FTE DAYS
ADDITIONAL HEADCOUNT	~ 2 NEW ADMINS	0 NEW ADMINS

*Traditional IT Solutions include: Firewalls, VPNs, Routers, Modems, VLANs, ACLs, NAC, Port Lockdown, etc

Have us prove it to you in less than 30 minutes.

Visit temperednetworks.com/segment-med to request a demo or call us at 206.452.5500

