TEMPERED NETWORKS®

Use Case

Simple M&A Consolidation of Health IT Networks

Secure integration and segmentation of clinical and business systems across separate networks

What Our Healthcare Customers Experience:

50% Lower CapEx and OpEx
through network simplification

97% Faster Integrations
with little to no network changes

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

Challenge Overview – Integrating Separate Health IT Networks

Driven by razor thin margins, health care organizations are increasingly looking at mergers and acquisitions to address the business and financial challenges they face. To be competitive in the market, many hospitals are creating large health systems to achieve economies of scale and boost profitability. However, M&As among hospitals and clinics have created complex network integration issues that lead to downtime, slow service roll-out, and reduced quality of care.

The main challenge our customers encountered when connecting separate health IT networks was the cost and complexity of deploying traditional IT solutions to integrate across enterprise, building, virtual, and cloud infrastructures. The time, expertise, and budget needed to provision and manage firewall rules, NAT, VPNs, routers, switches, ACLs, and VLANs for multiple networks was impractical and left them exposed to hacker reconnaissance and exploits.

Tempered Networks – Rapidly Integrate Health IT Networks

Identity Defined Networking (IDN) for health IT systems creates a highly available and natively secure 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 accelerate integration efforts for separate networks, while delivering superior availability and quality of care.

Network Challenges:

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

Security Challenges:

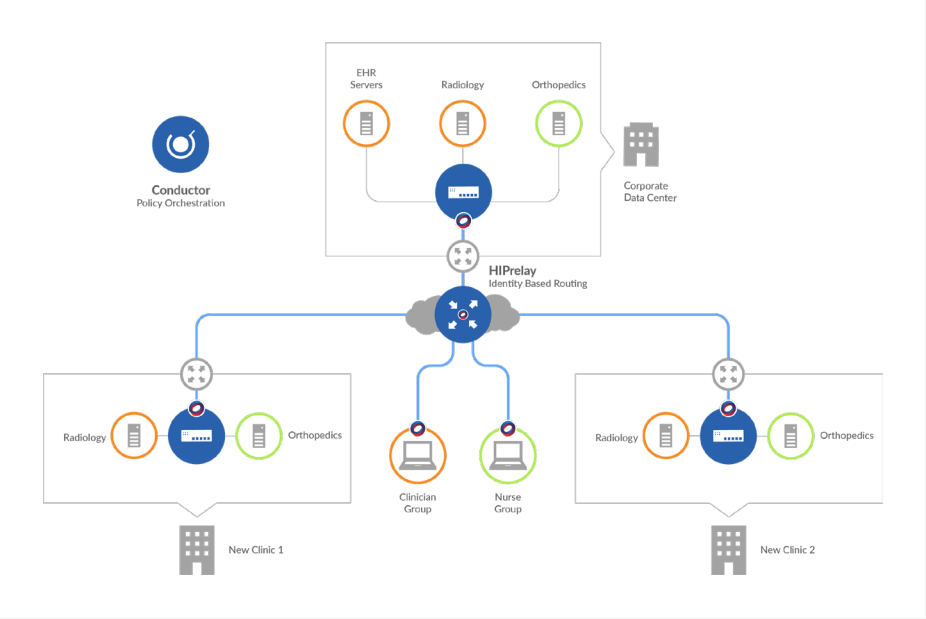
- Network, compute, storage, and application vulnerabilities caused by human error
- Lack of support for latest authentication and encryption methods by aging devices
- SSL VPN access is complex and time-consuming to manually configure

People and Process Challenges:

- Multi-factor auth. is too complex for users

"Tempered Networks' Identity Defined Networking allowed our IT team to securely and quickly integrate business and clinical systems across two smaller clinics we acquired. We had estimated it would take over a year with alternative technologies, but with Tempered it took less than 2 months, was a third of the cost, and is more secure."

Network Administrator
Large Health Care Organization,
Eastern U.S.



Challenges with Traditional IT Solutions

- Inability to quickly connect and segment any health IT systems across any location in the world
- High acquisition and management costs of distributed firewalls, access points, VPNs, routers, and switches
- Inability to quickly provide clinicians and others with micro-segmented access to specific systems
- NAT at scale is significantly complex and time-consuming to deploy and manage
- Costly and complex to validate compliance requirements for appropriate levels of device access

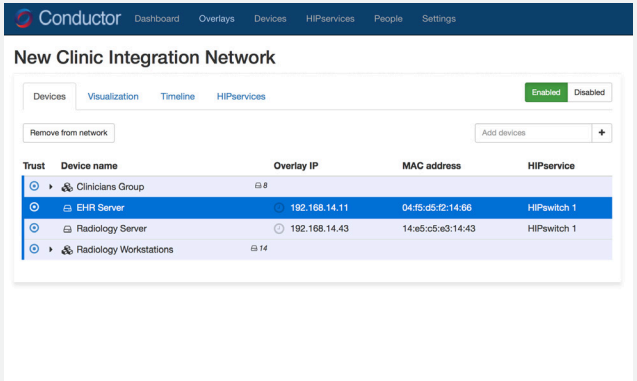
Native Security and Network Simplification with Tempered Networks

- Micro-segmentation and native end-to-end encryption across the LAN, WAN, and cloud
- Rapidly isolate and/or integrate separate networks
- 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 authorized device-level access to specific systems across LAN/WAN
- Simple and cost-efficient compliance reporting of device segmentation

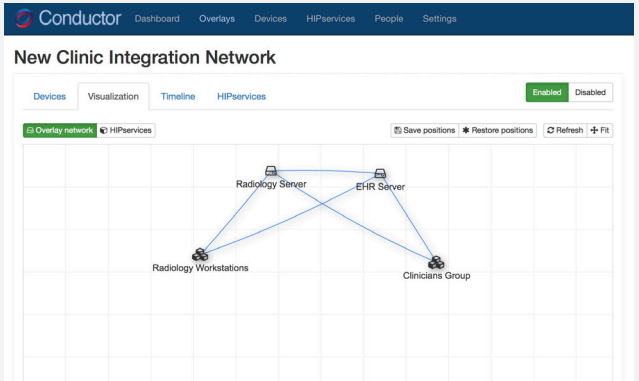
With IDN, hospital IT teams can eliminate network complexity and securely connect any device, over any network, across any location, with little to no changes to the underlying network infrastructure. The process, referred to as instant overlay networking, results in massive simplification of your network, 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 health IT systems 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 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 spoofed.



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 integrating disparate health networks after an acquisition of two smaller clinics. With superior connectivity and segmentation, the hospital was able to deploy instant network overlays to glue together clinical systems across 3 separate networks. And unlike traditional IT solutions, with Tempered Networks all devices and systems are isolated across their own encrypted and micro-segmented overlay network that can't be violated.

IMPACTS	TRADITIONAL IT SOLUTIONS	TEMPERED NETWORKS SOLUTION
EQUIPMENT COST	$250,000+	$75,000
DEPLOYMENT TIME	230 FTE DAYS	10 FTE DAYS
ADDITIONAL HEADCOUNT	~ 1 NEW ADMIN	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/m&a-healthcare to request a demo or call us at 206.452.5500

