TEMPERED NETWORKS®

Use Case

Simple and Secure Networking for Industrial IT

Peer-to-peer secure connectivity and micro-segmentation for Industrial Internet of Things (IIoT)

What Our IIoT Customers Experience:

50% Lower CapEx and OpEx
through IIoT network simplification

Connect, Segment, and Collect Data 97% Faster
with little to no network changes

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

Challenge Overview – Secure Connectivity for Industrial IoT Systems

The complexity of securely connecting devices such as vending machines, IP cameras, robotics, building sensors, and a whole host of other systems and devices using traditional IT solutions has left teams feeling ill-equipped and exposed. Successful IoT initiatives can transform how organizations do business by improving efficiency and automation, expanding data sources for business intelligence, and offering increased opportunities to deliver new service models for customers. However, this increased connectivity introduces significant risk and exposure.

The main challenge our customers encountered when connecting and integrating IIoT devices was the cost and complexity of deploying and maintaining traditional IT solutions across separate enterprise, remote, and cloud infrastructures. The time, expertise, and budget needed to provision and manage firewalls, VPNs, routers, switches, modems, ACLs, and VLANs for every device was impractical and still left them exposed to hacker reconnaissance and exploits.

Tempered Networks – Simple and Secure Industrial IoT Networks

Identity Defined Networking (IDN) for IIoT systems creates a highly available, natively secure, and simple network so our 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 any device across the LAN and WAN.

Network Challenges:

- Complex L2-L4 network dependencies that impact instant LAN/WAN connectivity
- Different security and networking architectures for IT, industrial IoT, virtual, and cloud environments
- IP addressing issues and conflicts across the network
- Blending legacy and IIoT infrastructure causes frequent maintenance changes and downtime

Security Challenges:

- Flat L2 network creates a large attack surface
- Inability to quickly cloak and segment systems to protect against horizontal network attacks
- 3rd party integrators and contractors have unfettered access to any device on the network

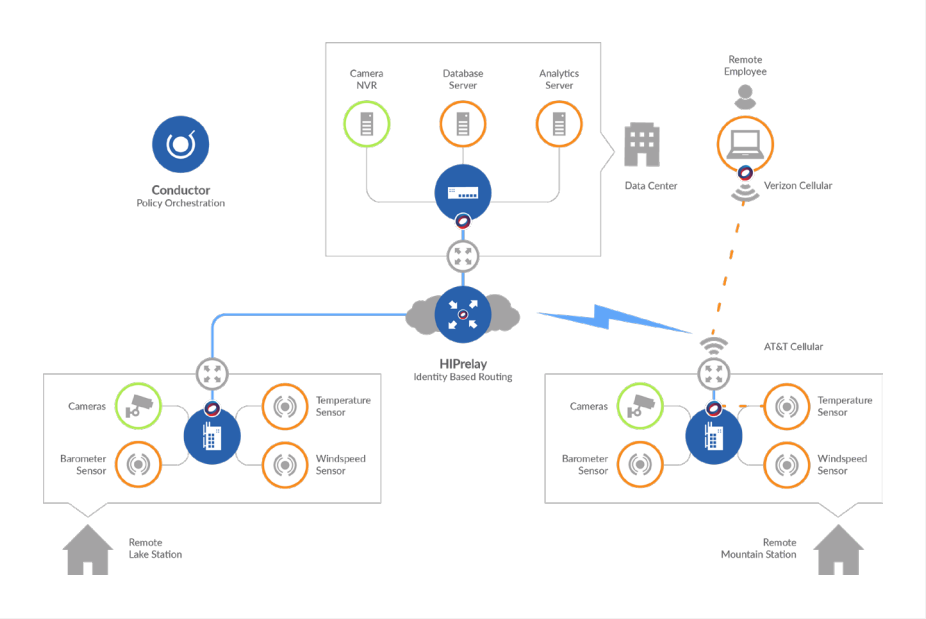
People and Process Challenges:

- Limited staff, security, and network expertise
- Traveling to remote sites is costly and inefficient

"Tempered Networks' Identity Defined Networking gave us a simple way to achieve end-to-end private networks for our Building Automation network that's resilient, scalable, and secure.

In less than 20 minutes, we were able to deploy our first cloaked overlay network without having to modify the underlay or involve IT."

Tom Walker
Facility Automaton Services
Penn State University



Challenges with Traditional IT Solutions

- Inability to quickly connect and collect data from any system, anywhere
- High acquisition and management costs of distributed firewalls, VPNs, routers, cellular modems, and switches
- Complex firewall rules, ACLs, VLANs, certificates, VPN tunnels etc. across distributed systems
- Inability to quickly provide technicians with micro-segmented remote access to specific systems
- Connecting geographically distributed devices often requires costly MPLS lines or private APNs

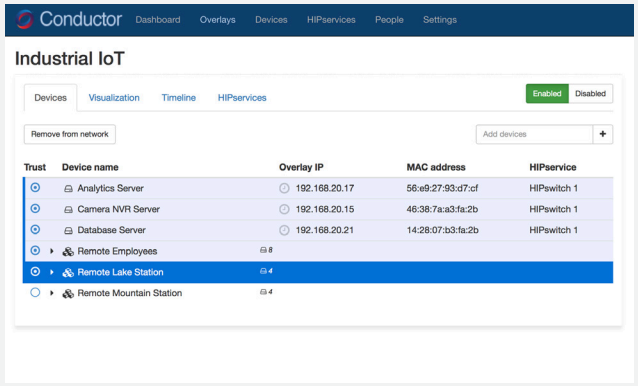
Native Security and Network Simplification with Tempered Networks

- Micro-segmentation and native end-to-end encryption across the LAN, WAN, and cloud
- Instant secure connectivity for layer 2 and layer 3 networks with high availability and resiliency
- Ability to connect remote systems over any medium — cell, Ethernet, Wi-Fi, or radio.
- Eliminate IP addressing issues and conflicts, without having to re-IP devices
- Eliminate costly MPLS lines and private APNs by using standard Internet

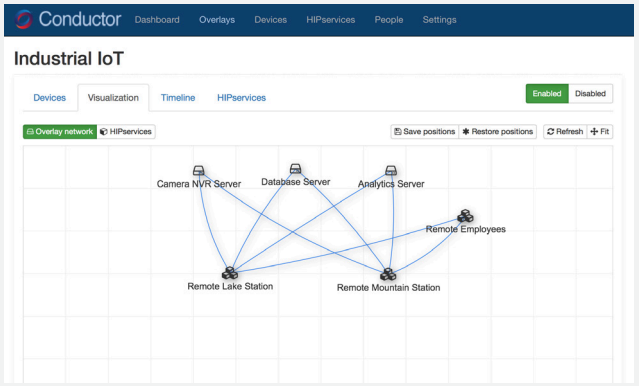
With IDN, IT teams can eliminate network complexity and securely connect any device, over any network, across any location, with little to no changes to the underlying network infrastructure. The process, referred to as instant overlay networking, results in massive simplification of your network, coupled 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 their IIoT deployments based on verifiable machine identity and the simple process of machine whitelisting based on trust.

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. With a single networking architecture spanning IT, industrial, virtual, and cloud environments, you can now enforce consistent security context across all environments.



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 ~100 geographically distributed and remote sites for weather monitoring. Unlike traditional IT solutions, with Tempered Networks every site is isolated across its own encrypted and segmented overlay network that can't be violated.

IMPACTS	TRADITIONAL IT SOLUTIONS	TEMPERED NETWORKS SOLUTION
EQUIPMENT COST	$400,000 +	$100,000
DEPLOYMENT TIME	300 FTE DAYS	20 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/segment-iiot to request a demo or call us at 206.452.5500

