TEMPERED NETWORKS®

Use Case

Simple and Secure Multi-Cloud Peering

Infrastructure as code delivers secure peer-to-peer connectivity and micro-segmentation for on-premises to hybrid cloud peering

What Our Hybrid and Multi-Cloud Customers Experience:

50% Lower CapEx and OpEx
through cloud network abstraction and simplification

97% Faster Connectivity and Access Control
with infrastructure as code

90% Reduced Attack Surface
through cloaking and workload micro-segmentation

Challenge Overview – Workload Peering Limitations

The complexities and limitations of traditional IT solutions for on-premises to hybrid cloud peering has left DevOps teams feeling frustrated by their lack of choice, flexibility, and reliability. The inability to make any combination of VPCs and VNETs look like one broadcast domain not only restricted availability and how their workloads and micro-services could be consumed, but also limited their ability to move between clouds. In addition, having to consistently share and revoke SSH keys among DevOps staff is error prone and opens attack vectors.

The main challenges our customers encountered when peering workloads and containers between on-premises, availability zones, regions and across cloud providers were the limitations of native peering functions. The root cause of this inflexibility is due to each cloud providers unique IP and DNS namespace schemas and how they're used to define and enforce connectivity and access. It shouldn't take 150 manual steps to peer between AWS and Azure, and peering shouldn't be limited by number of connections or VPC locations.

Tempered Networks – Simple and Secure Cloud Peering

Identity Defined Networking (IDN) creates a highly available, radically secure, and programmable overlay network so DevOps can automate workload networking and access control across clouds and on-premises. They can now instantly provision, de-provision, and revoke machine and cloud peering, while exposing nothing to the public Internet. IDN delivers infrastructure as code, so our customers can deploy secure and micro-segmented overlay networks across the LAN/WAN and multi-cloud environments 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.

Network Challenges:

- Complex maintenance of different LAN, WAN, and cloud architectures
- Cloud L2-L4 network dependencies impacting access and mobility
- Inflexible peering across zones, regions, and between cloud providers
- Lack of infrastructure as code prevents network automation at scale

Security Challenges:

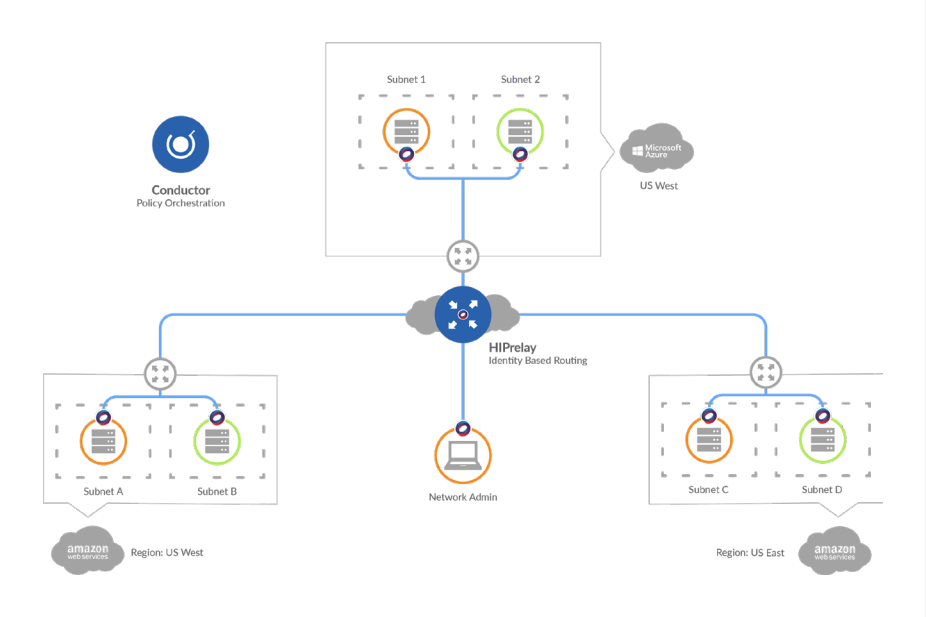
- Public IPs, unprotected ports, and exposed VPNs increase attack surface
- Lack of network AAA exposes workloads to reconnaissance and spoofing

People and Process Challenges:

- Hiring, retaining, and efficiently utilizing DevOps staff
- Lack of network programmability burdens DevOps

"The limitations of cloud workload and container networking to span zones, regions, and between AWS and Azure forced us to consider writing our own network control plane at considerable time and cost. Tempered Networks overcomes those limitations and has significantly improved our release cycles. We're not only faster and release with greater predictability, but our code is secured down to every machine."

Director of Cloud and DevOps
Fortune 1000 Energy SaaS Provider



Challenges with Traditional IT Solutions

- Cross region VPC peering is complex, limited, and slow to implement
- Managing complex network and security rules prevent fast, predictable peer-to-peer connectivity
- Infrastructure dependencies introduce error and machine exposure to public Internet
- Lack of machine-to-machine encryption and verifiable micro-segmentation
- IP addressing and connectivity conflicts caused by separate IP schemas across clouds

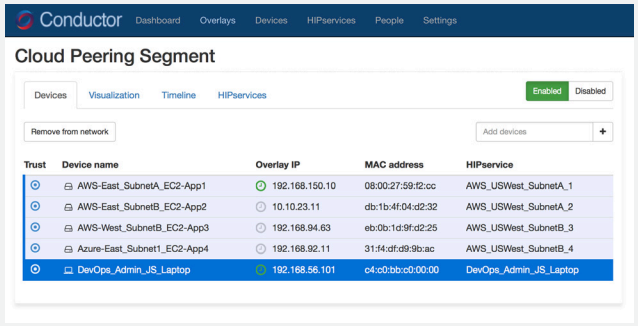
Native Security and Network Simplification with Tempered Networks

- Network and security infrastructure as code delivers fast and simple overlay creation
- Non-disruptive deployment with little to no changes to underlying switching and routing infrastructure
- Private machine-to-machine peering (no public IP exposed) within and across clouds
- Micro-segmentation and native machine-to-machine encryption across LAN, WAN, and clouds
- Ability to instantly connect IoT to cloud over any medium — cell, Ethernet, Wi-Fi, or radio
- Simple network automation to add, disable, move, or revoke machines on demand

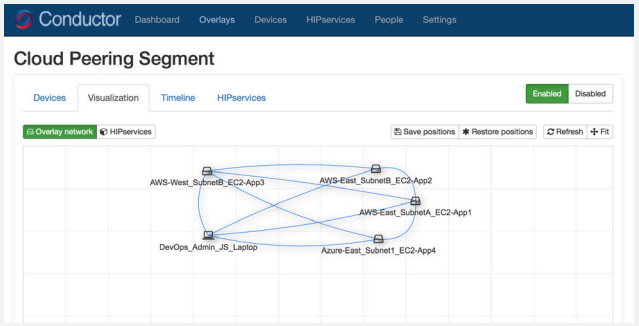
With IDN, DevOps teams eliminate network complexity and gain the freedom of workload mobility, while meeting the goals of agility and reliability through network automation. The process, referred to as instant overlay networking, results in massive simplification of your network, coupled with next-gen security and resiliency that can't be achieved using traditional IT solutions. Teams can now quickly connect, micro-segment, encrypt and manage workload peering and access control based on verifiable machine identity, not ephemeral IP and ports.

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, and is also programmable with a restful API. Unlike the many complex, fragile, and time-consuming steps associated with cloud networking and security, our customers eliminate human error through simple and automated 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. Every cloud workload can now remain private, segmented, and invisible to hackers - eliminating reconnaissance and spoofing attacks.



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 estimates below are based on a customer scenario of isolating and securely peering between the corporate network and 20 regionally distributed AWS VPCs and Azure VNETs. DevOps follow a typical build, test, and release workflow, where all 50 employees require specific remote access from different locations in the world. Benefits do not take into account functions like cloaked micro-segmentation, which would be impossible without developing your own network data and control plane.

IMPACTS	TRADITIONAL IT SOLUTIONS	TEMPERED NETWORKS SOLUTION
ANNUAL SOLUTION COST	$220,000 +	$100,000
NET/SEC PROVISION TIME PER RELEASE	3 FTE DAYS	5 MINUTES
ADDITIONAL HEADCOUNT	6 CCNE LEVEL 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/cloud-peering to request a demo or call us at 206.452.5500

