



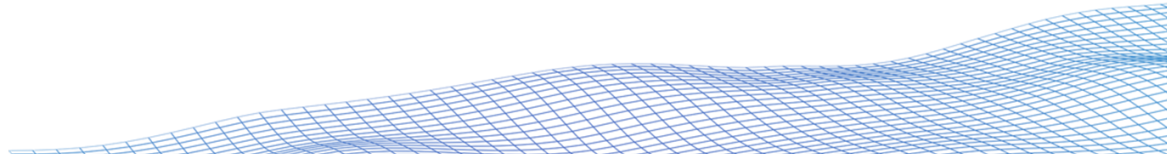
Tempered Networks' New Identity Networking Paradigm

The Cure for IT Risk, Cost, and Complexity –
unified secure networking made simple

Jeff Hussey
CEO

AGENDA

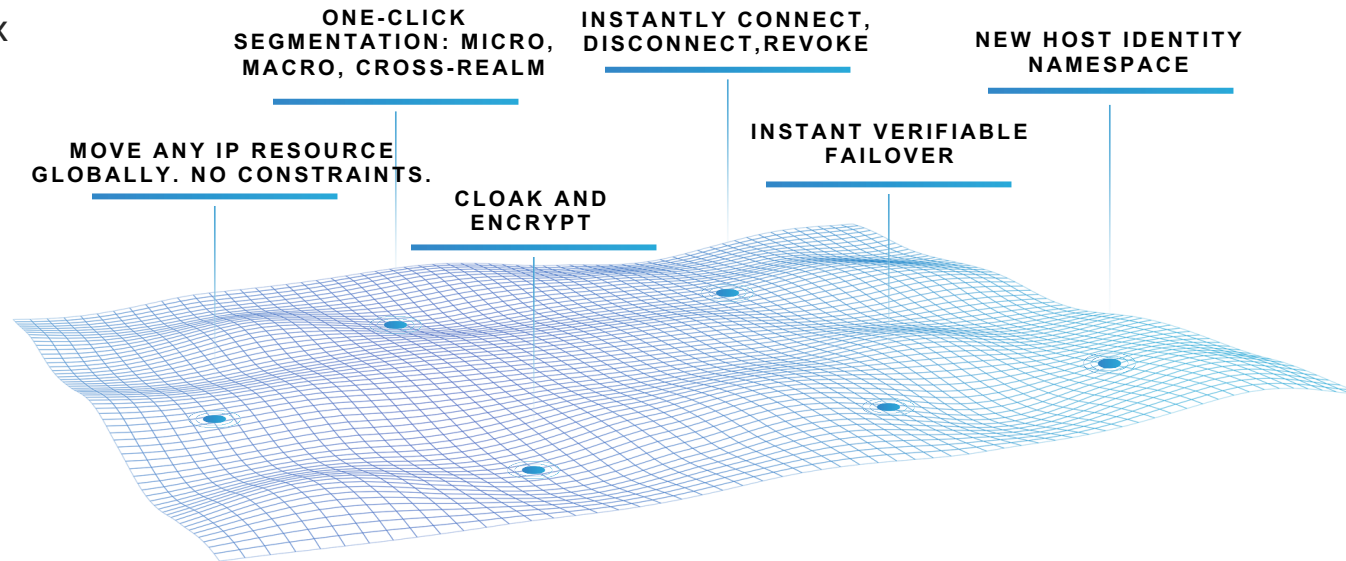
- A New Identity Networking Paradigm
 - Freeing IP from a role that was never meant - the cause of complexity, insecurity, cost, and inflexibility
- Tempered Network's Approach
 - An identity-first architecture with simple and instant policy orchestration
- The Outcomes:
 - Accelerate provisioning by 97%. Reduce the attack surface by 90%. Reduce complexity and cost more than 25%
- Getting Started:
 - Simple and fast options to show Proof of Value (PoV)



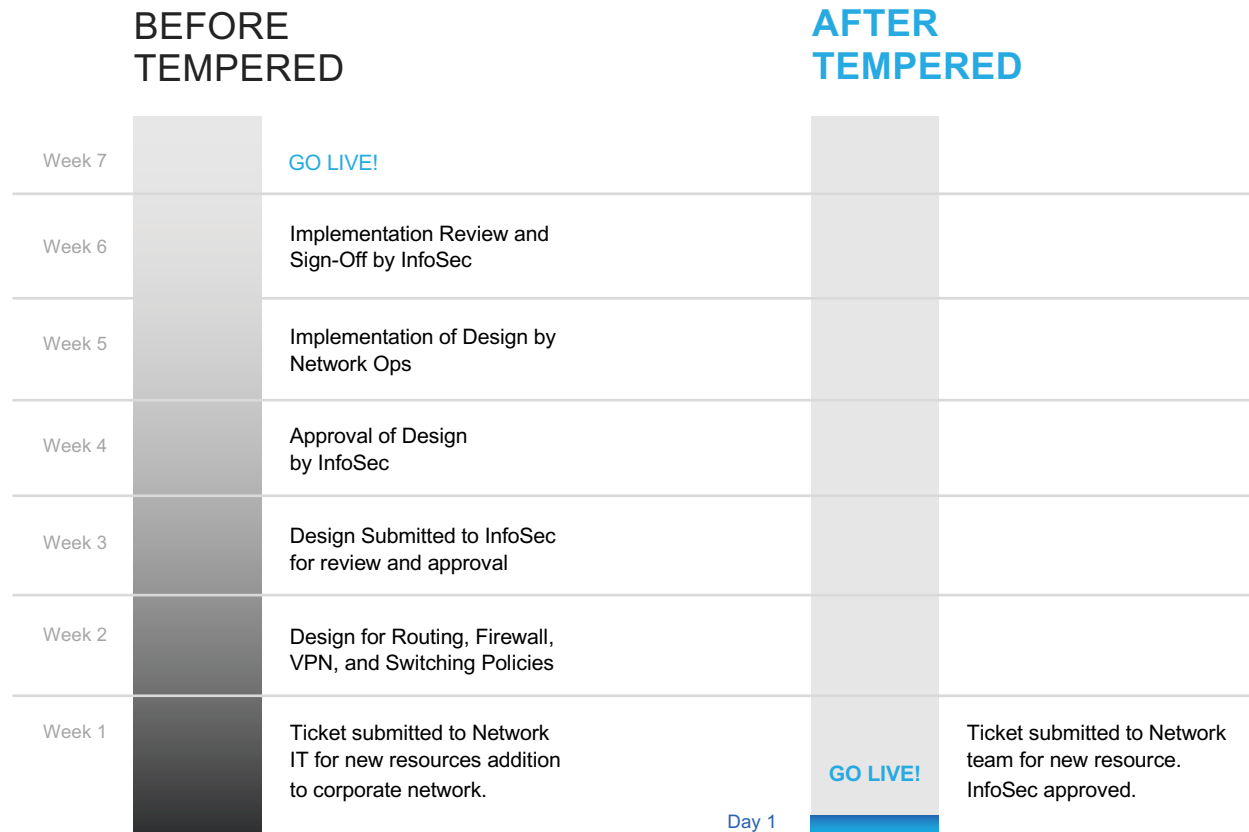
Tempered Networks' Identity-Defined Network (IDN)

It's never been possible, until now

- Significant reduction in capex & opex
- Dramatically reduces business risk
- Simple and instant orchestration for any connected “thing,” anywhere, anytime
- Unifies networking and security



Reduce time to provision

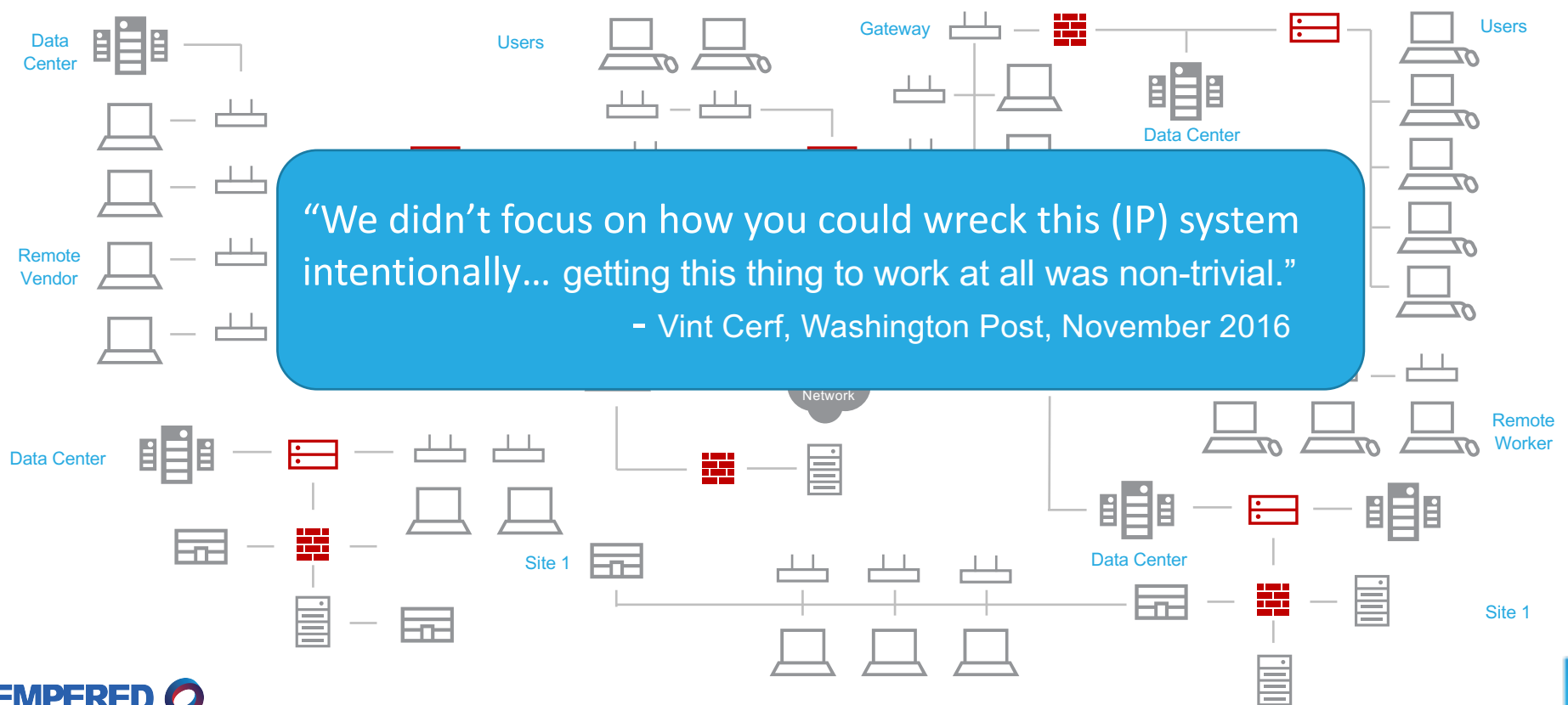


Secure networking time reduced by

97%

Resource added with explicit trust segmentation, cloaked and encrypted communication. Deployed by NetOps and easily verified by InfoSec.

Traditional Networking is **Complex, Costly** and **Fragile**

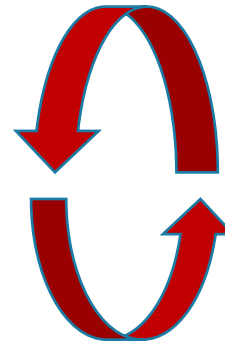


Flawed identity, only complexity. Unsustainable.

Network and Security Policies
USE IP ADDRESSES as IDENTITY

100%

Use IP addresses as identity for policy—
This is the root cause of **complexity**,
network **security vulnerabilities**, **poor segmentation**,
and **lack of mobility**



DNS and routing
updates for failover



Routing policies,
VLANs and
ACLS overhead



Complex firewall and
networking rule sets



VPN access
controls for each
network

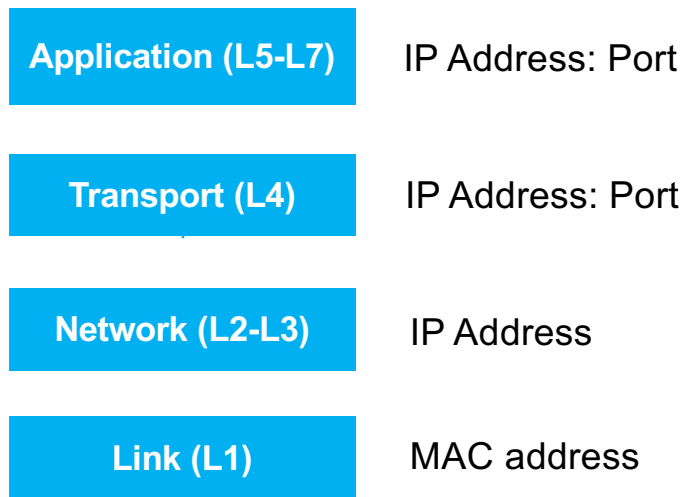
... per networked “thing”

$$(c^n \times r^n) \times p^i = y^*$$

$$(\text{clients} \times \text{resources}) \times (\text{net \& sec policy}) \times \text{updates} = \text{complexity}$$

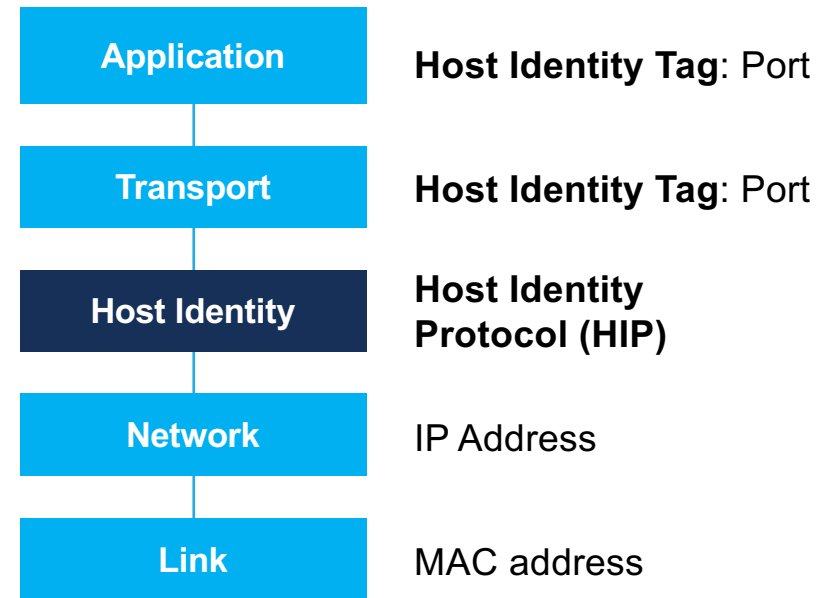
A new Identity Networking **paradigm** is required

Internet 2.0 – “Network everything”



To a secure,
mobile and
private Internet

Internet 3.0 – “Network ONLY CRYPTO-IDENTIFIED things”

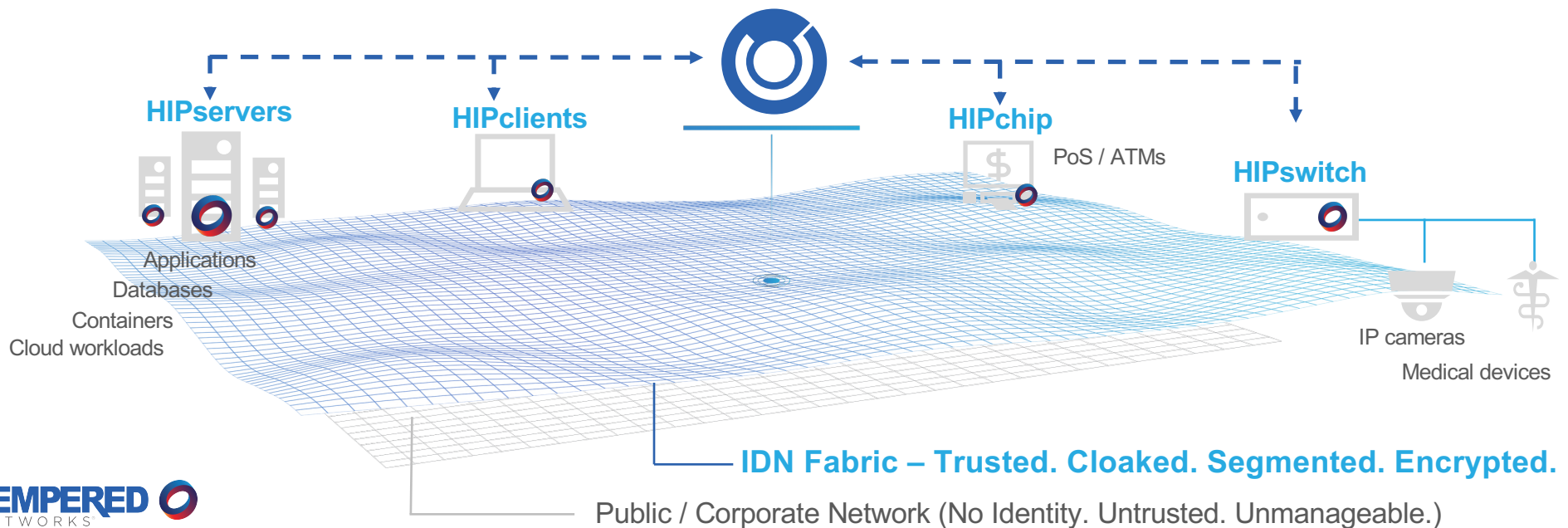


Identity-Defined Networking (IDN) – the way forward

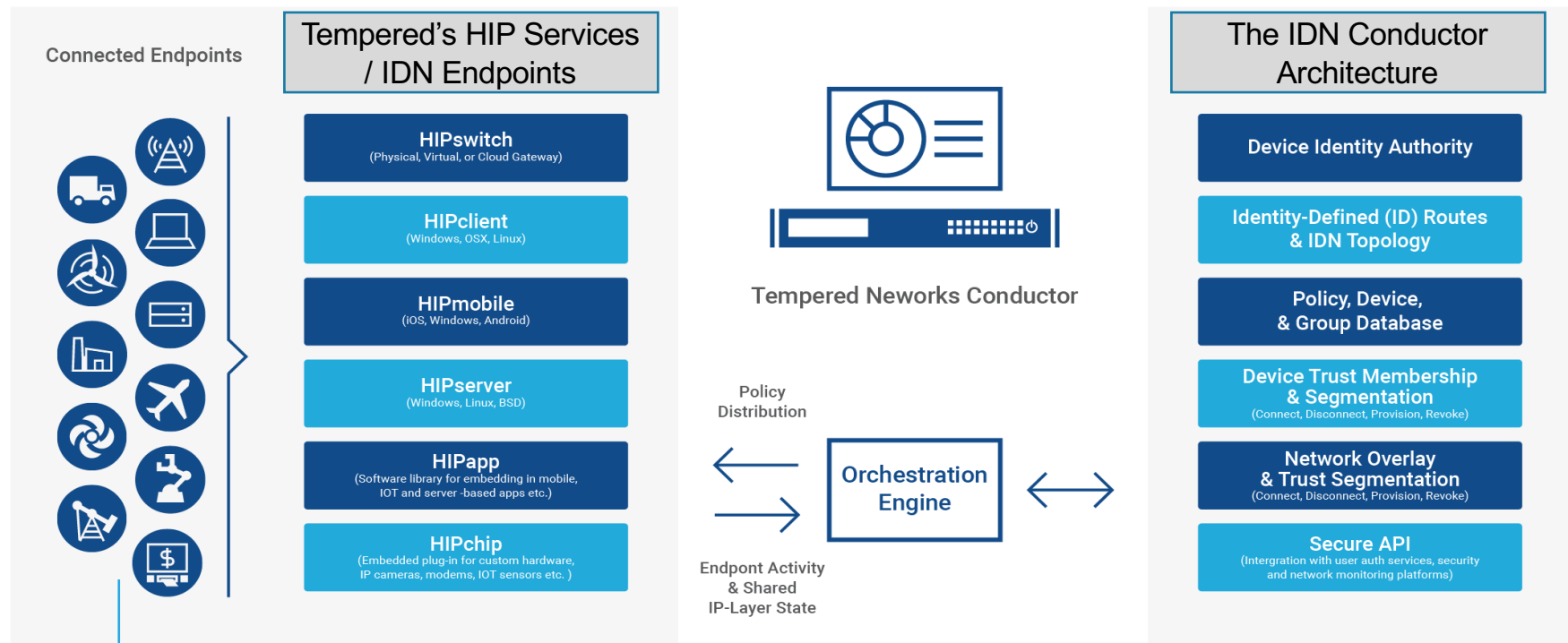
Securely network and orchestrate any thing, anywhere, anytime - instantly.

Tempered Networks' IDN Conductor

Control based on unique crypto-identity for every networked thing. Seamless deployment, simple policy orchestration and enforcement based on identity. Securely connect, cloak, segment, revoke, move, failover and revoke instantly within the IDN's encrypted fabric.



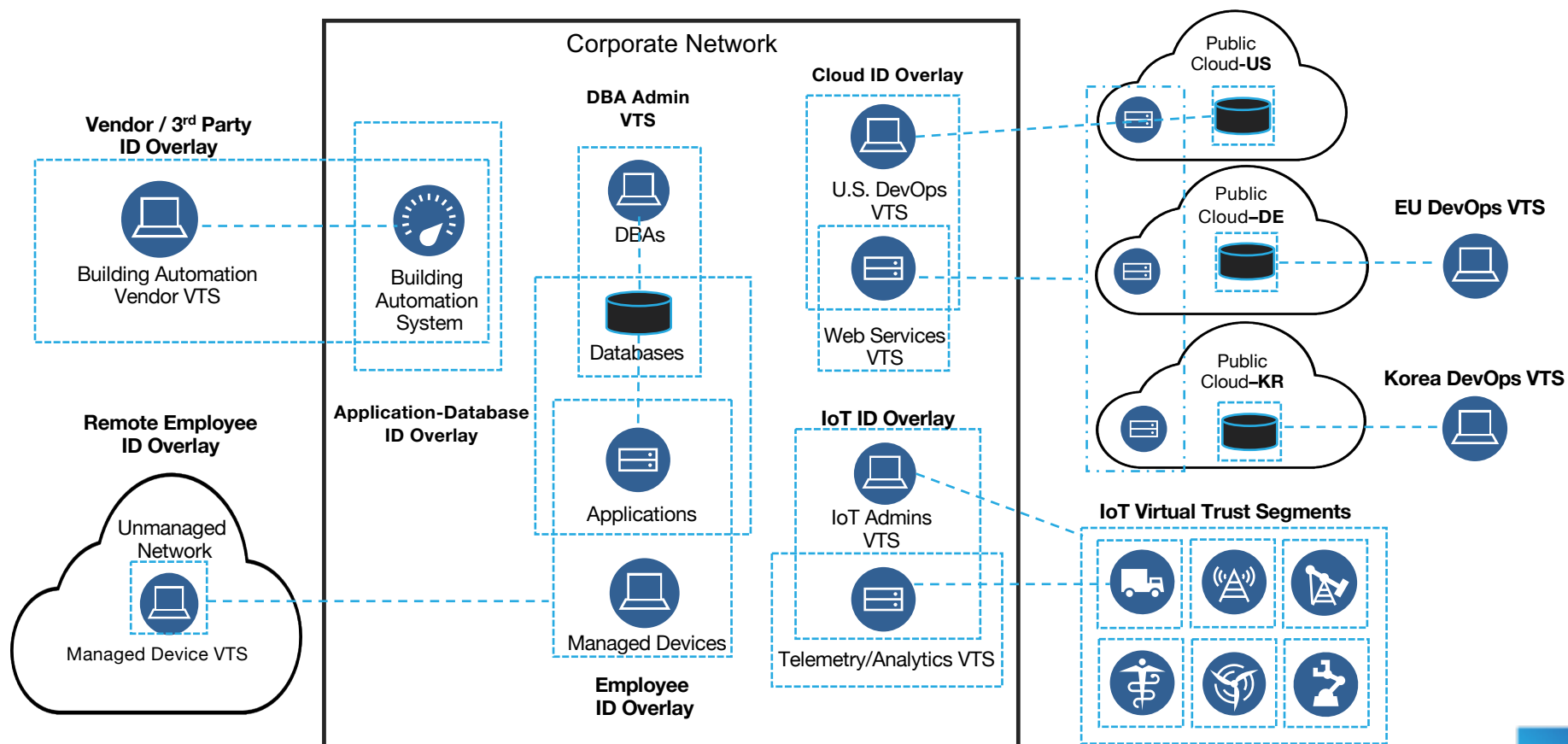
Flexible and Pervasive: Identity-Defined Networking Solution



Any networked thing can be joined to the IDN's secure and mobile fabric creating a unified and common architecture spanning nearly all environments.

Unique Identity-Defined Overlays (IDO) and Virtual Trust Segments (VTS):

Macro and micro-segmentation is based on unique host identity and every IDO is cloaked and hardened.
Allowed VTS connectivity and communication is explicit, non-traversal, encrypted and verifiable



The New Identity Networking Paradigm

Driven by Outcomes

Reduce networking
and resource
provisioning time
up to:

97%

Increase in network
and security team
productivity

25%

Decrease IT
CapEx and OpEx
costs up to:

25%

Make 100% of your
connected IP
resources invisible

100%

Reduce attack
surface up to:

90%

Improve time to
mitigation, revocation,
and quarantine up to:

50%

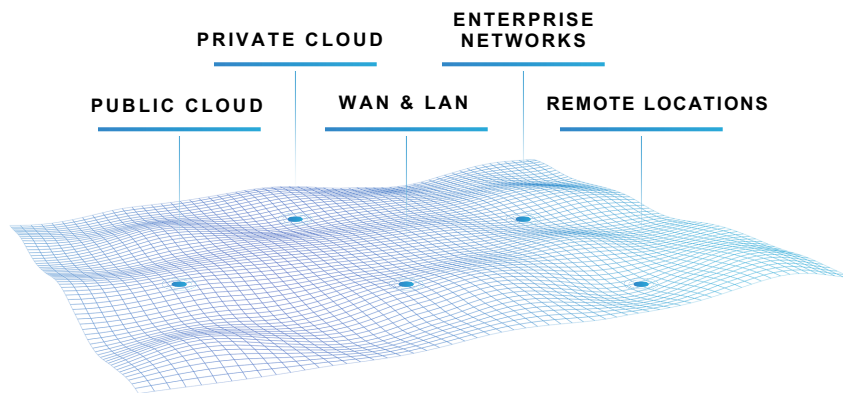
Decrease failover
and disaster recovery
times to as little as:

1 Second

Deploy anywhere – Create a Unified Fabric

Connect, protect, and disconnect any resource anywhere, anytime – instantly.

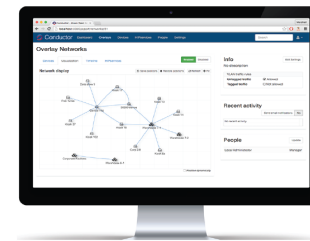
Any Environment



Any Connectivity Medium

Ethernet | Cellular | Wireless | Radio | Serial over IP

Available in Cloud or Physical



CONDUCTOR
CENTRALIZED
ORCHESTRATION

Any Form Factor



IDENTITY-ENABLED HARDWARE



**IDENTITY-ENABLED CLOUD
& HYPERVISOR PLATFORMS**

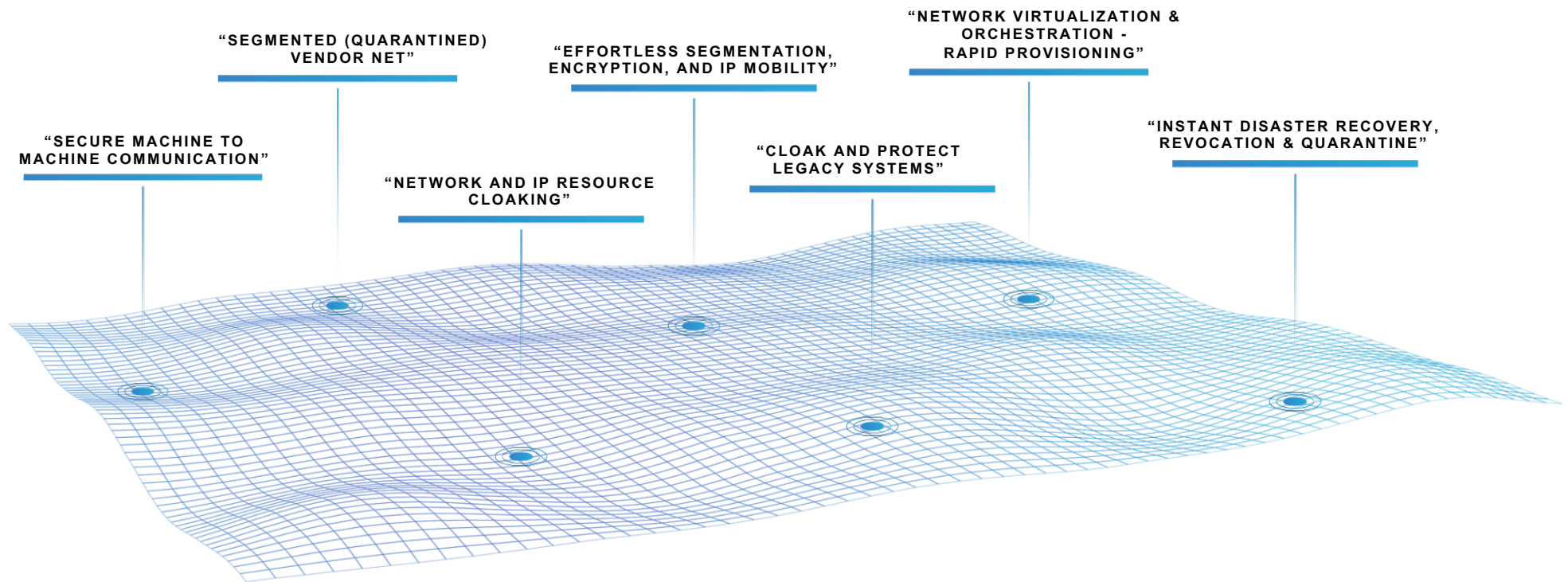


**IDENTITY-ENABLED
CLIENTS & SERVERS**



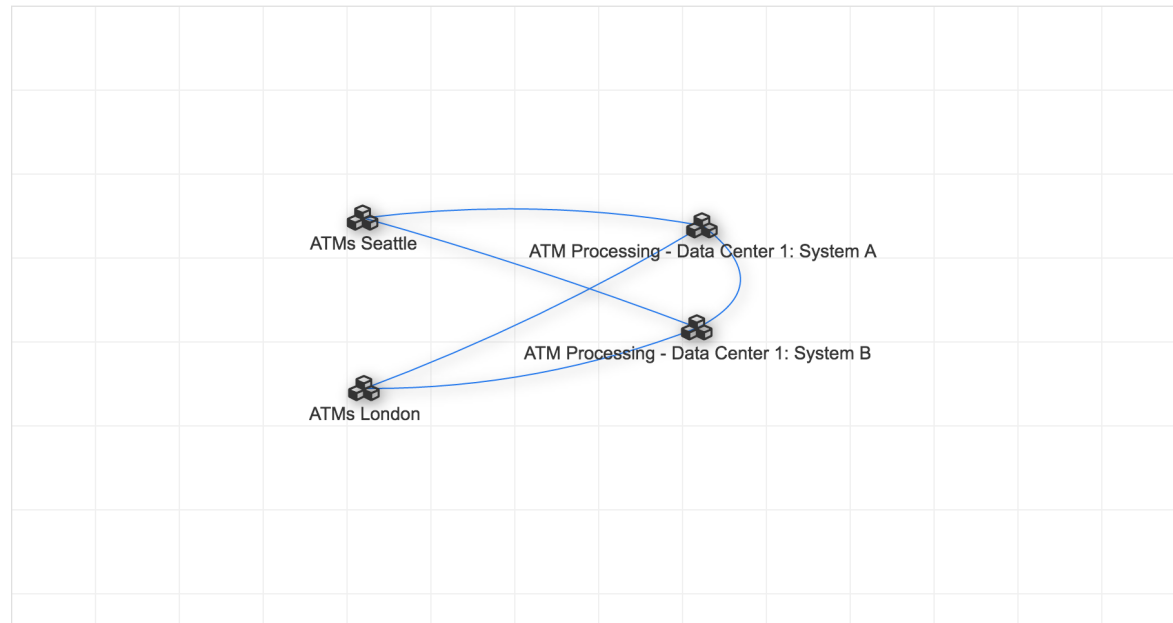
IDENTITY-EMBEDDED MODULES












Use Cases



Rapid Network Provision | Cloaking | Segmentation

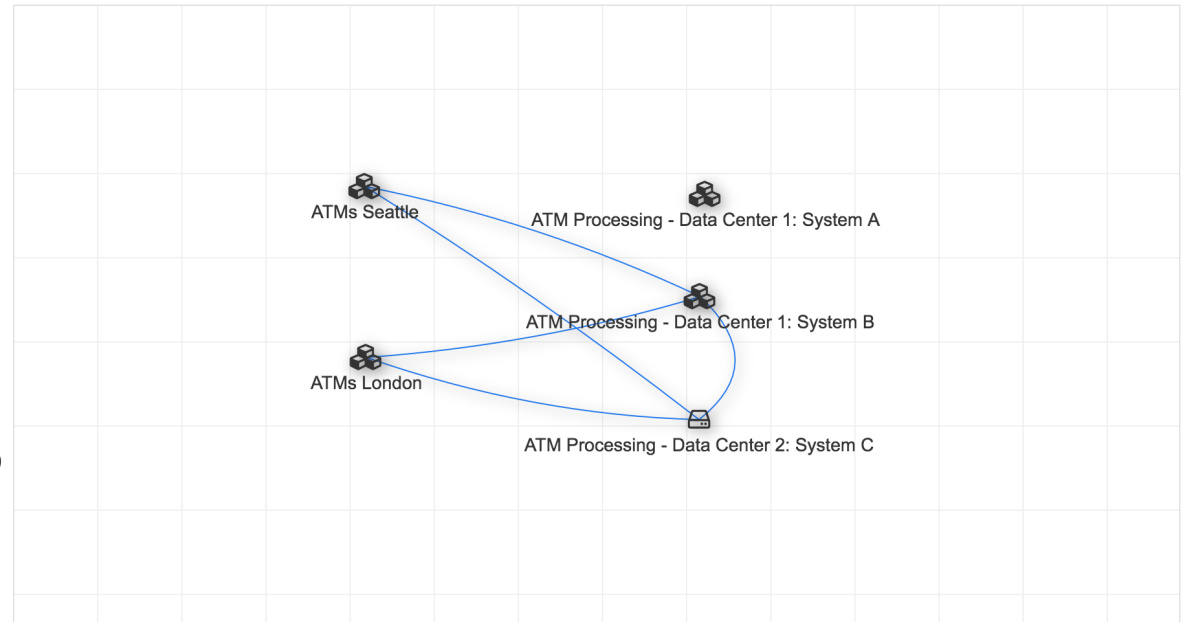
- Auto-discovered devices
- Create trust relationships
- Explicit segmentation, non-traversal
- Kiosks in Seattle are invisible to ATMs London
- No connectivity or communication between any untrusted systems in the IDO



Trust	Device name	IP address	MAC address	HIPservice
	▶  ATM Processing - Data Center 1: System A	 6		
	▶  ATM Processing - Data Center 1: System B	 6		
	▶  ATMs London	 554		
	▶  ATMs Seattle	 320		

Dynamic Networking with Failover

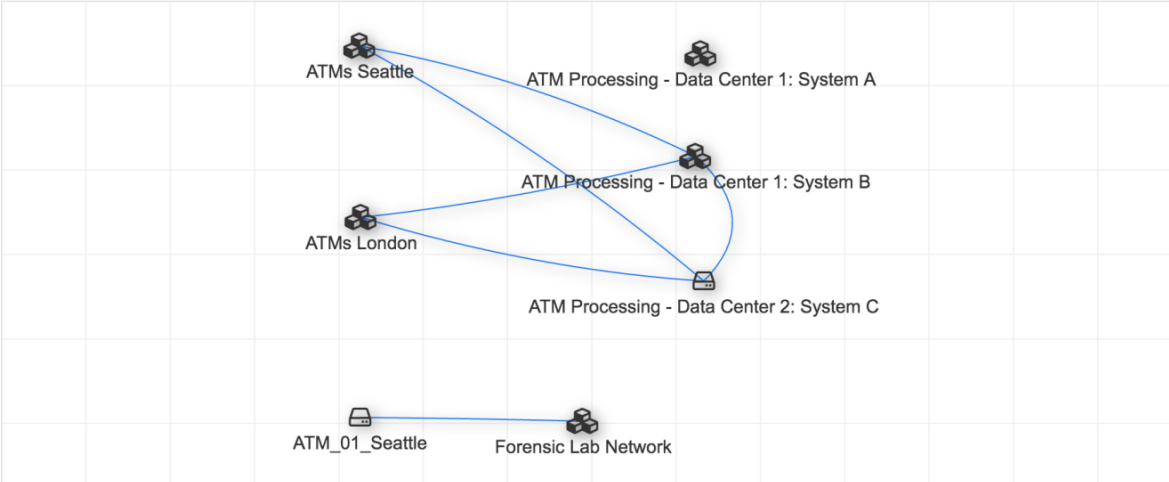
- Global or “micro” failover
- Failover can happen < 1 sec btw DCs or resources
- Overcomes DNS and routing convergence limitations
- Host Identity Tag (HIT) can be bound to IP address



Trust	Device name	IP address	MAC address	HIPservice
	▶ ATM Processing - Data Center 1: System A	6		
	▶ ATM Processing - Data Center 1: System B	6		
	ATM Processing - Data Center 2: System C	10.10.10.5		BHI@40130#B6D6D8A4AD92
	▶ ATMs London	554		
	▶ ATMs Seattle	320		

Instant Revocation and Quarantine

- Instantly isolate or revoke a device or system
- Avoid having to update VLANs, ACLs, VPN policy and cert management, FW policies



Trust	Device name	IP address	MAC address	HIPservice
<input checked="" type="radio"/>	ATM_01_Seattle	10.20.10.9		BHI@40130#B6D6D8A4AD92
<input checked="" type="radio"/>	Forensic Lab Network	2		
Trust	Device name	IP address	MAC address	HIPservice
<input type="radio"/>	ATM Processing - Data Center 1: System A	6		
<input checked="" type="radio"/>	ATM Processing - Data Center 1: System B	6		
<input checked="" type="radio"/>	ATM Processing - Data Center 2: System C	10.10.10.5		BHI@40130#B6D6D8A4AD92
<input checked="" type="radio"/>	ATMs London	554		
<input checked="" type="radio"/>	ATMs Seattle	320		

The Singular Root Defect

That affects all IP security and networking

IP Addresses are used as Network and Device Identity

- Hacker reconnaissance & fingerprinting via TCP/IP stack
- Listening TCP/UDP service ports
- All networking and security products use IP addresses for policy

Large Attack Surface

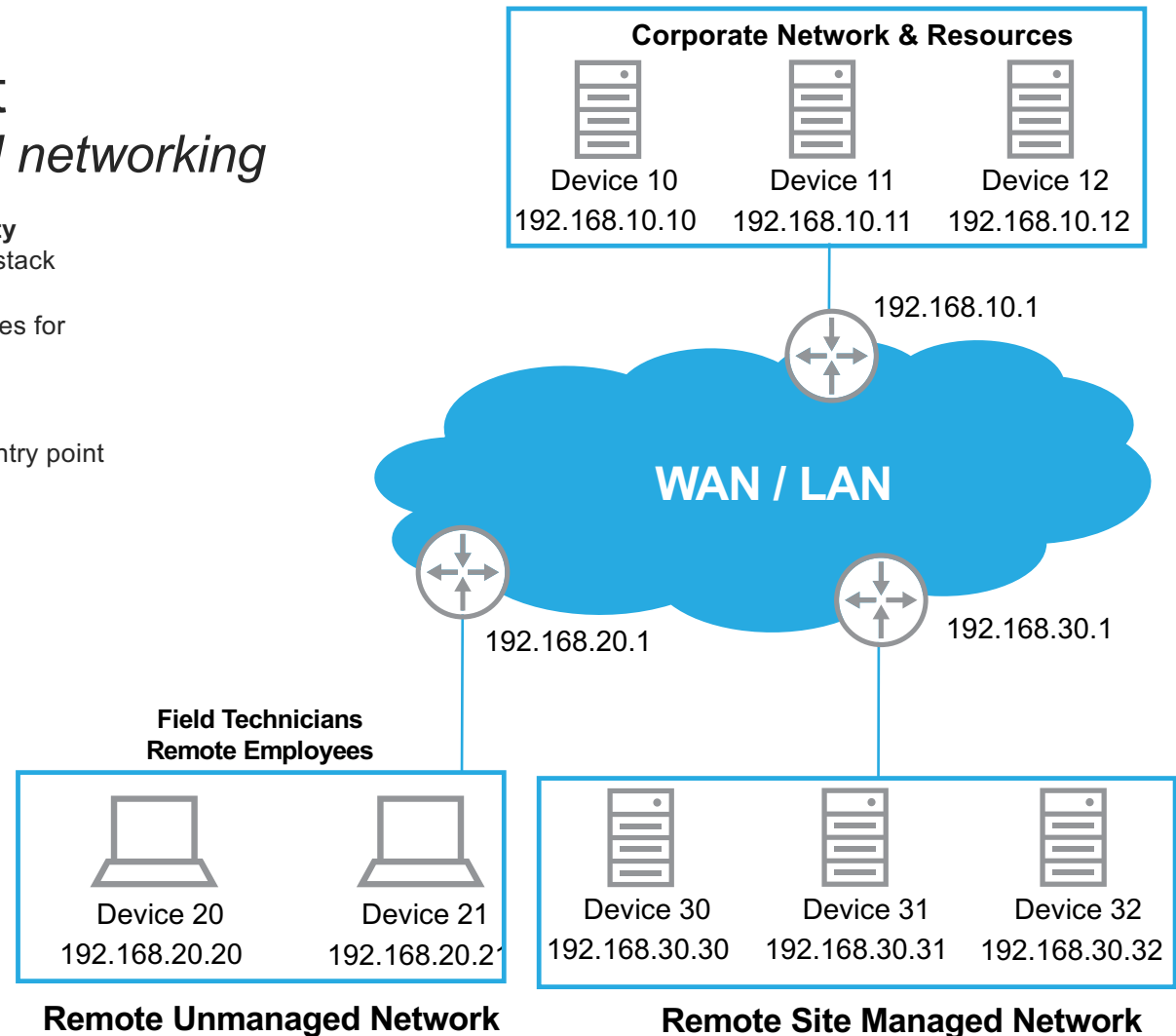
- IP, TCP/UDP Attacks: every connected thing is an entry point
- East / West lateral movement
- ACLs and VLANs ≠ segmentation

Lack of Mobility and Instant Failover

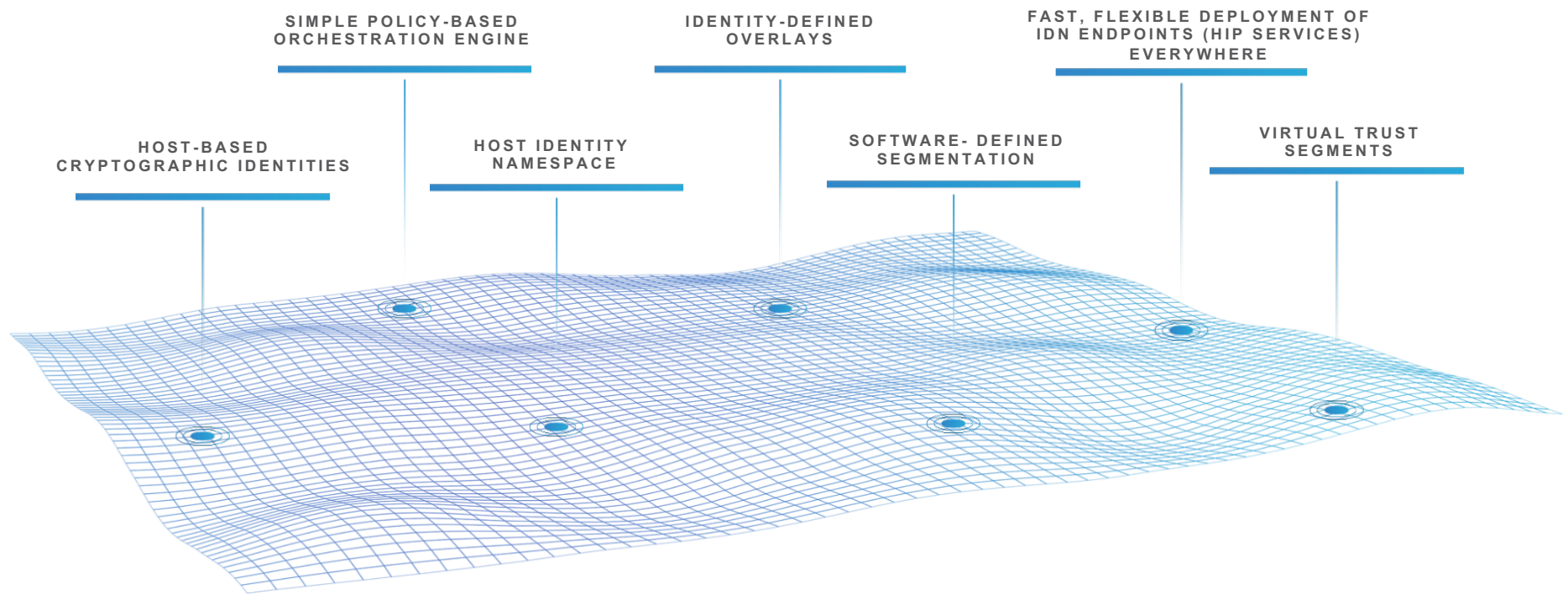
- Policies tied to IP - creates inflexible mobility
- IP conflicts
- DNS TTL and Routing Convergence Delays

Networking and Security Costs

- Many distributed, complex VLAN, ACL, VPN, firewall policies
- Controlling network routing
- IPsec VPN cert management, connection limitations, failover issues
- Expense of “next-gen” firewalls deployed on interior



How we do what we do



A New Identity Networking Paradigm

Made Simple

Unique Host Identity Approach

- Host Identity Protocol (HIP): IETF ratified April 2015
- True SDN overlay –little to no changes to network, security, or applications
- Unshackles IP from serving as identity - frees IT from complexity
- In production since 2006

Rapid Provisioning, Revocation, IP Mobility and Failover

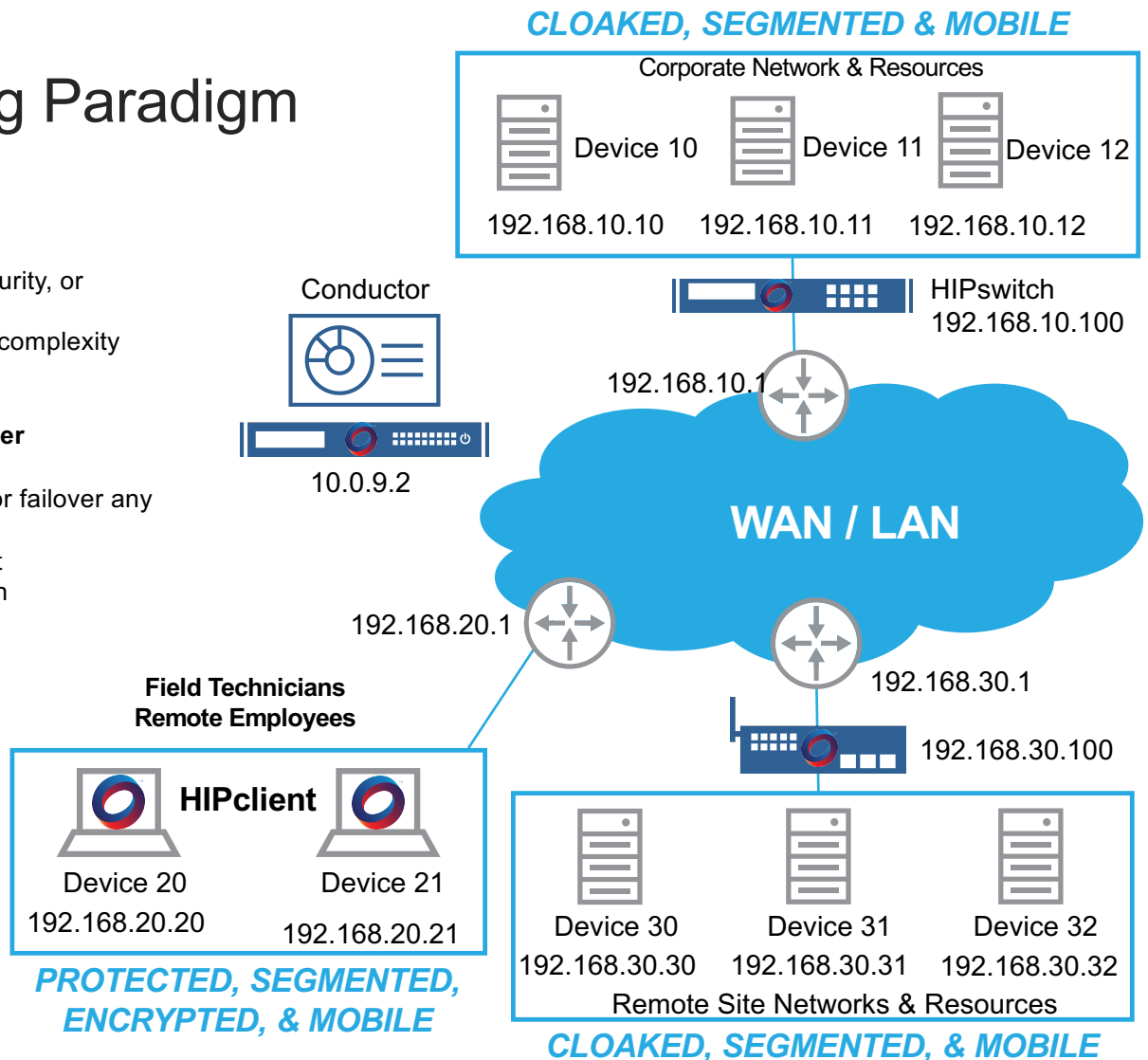
- Effortless segmentation & cloaking
- One-click orchestration to connect, disconnect, move or failover any “thing”
- Less than 1 second failover between any IDN endpoint
- Build ID overlays (IDOs) on-demand based on situation

Significantly Reduced Attack Surface

- No trust? No connectivity. No communication. No data.
- VLAN “segmentation” traversal is now impossible.
- Based on explicit device trust- all systems are invisible
- 2048 bit Identity-Based connectivity, AES 256 encryption by default

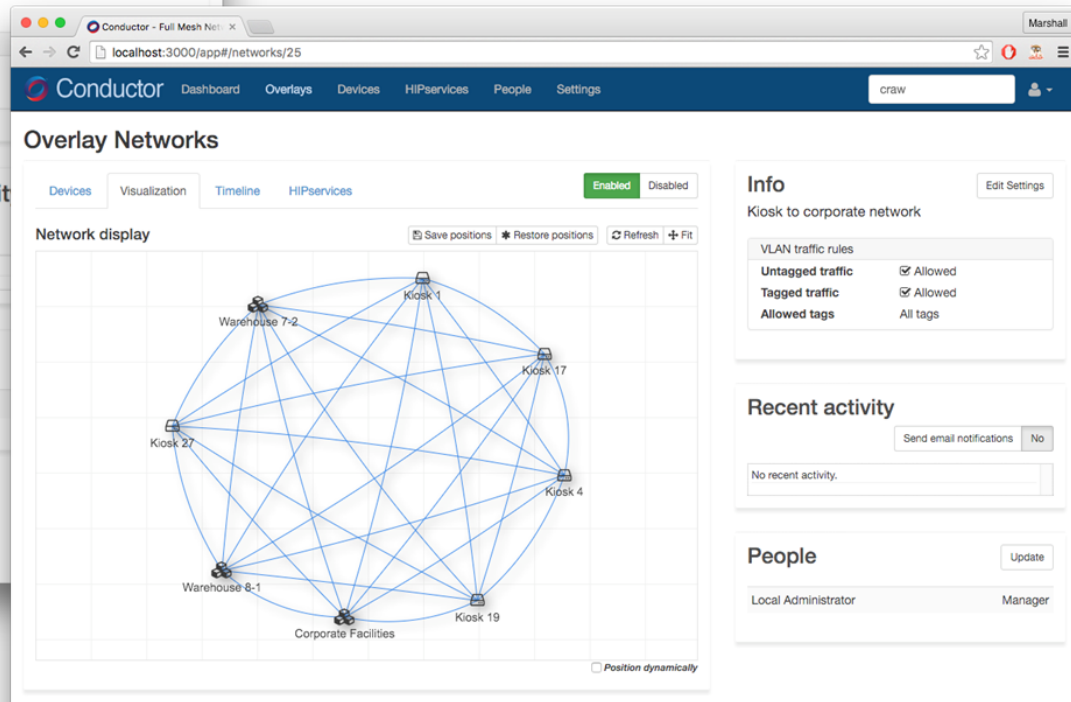
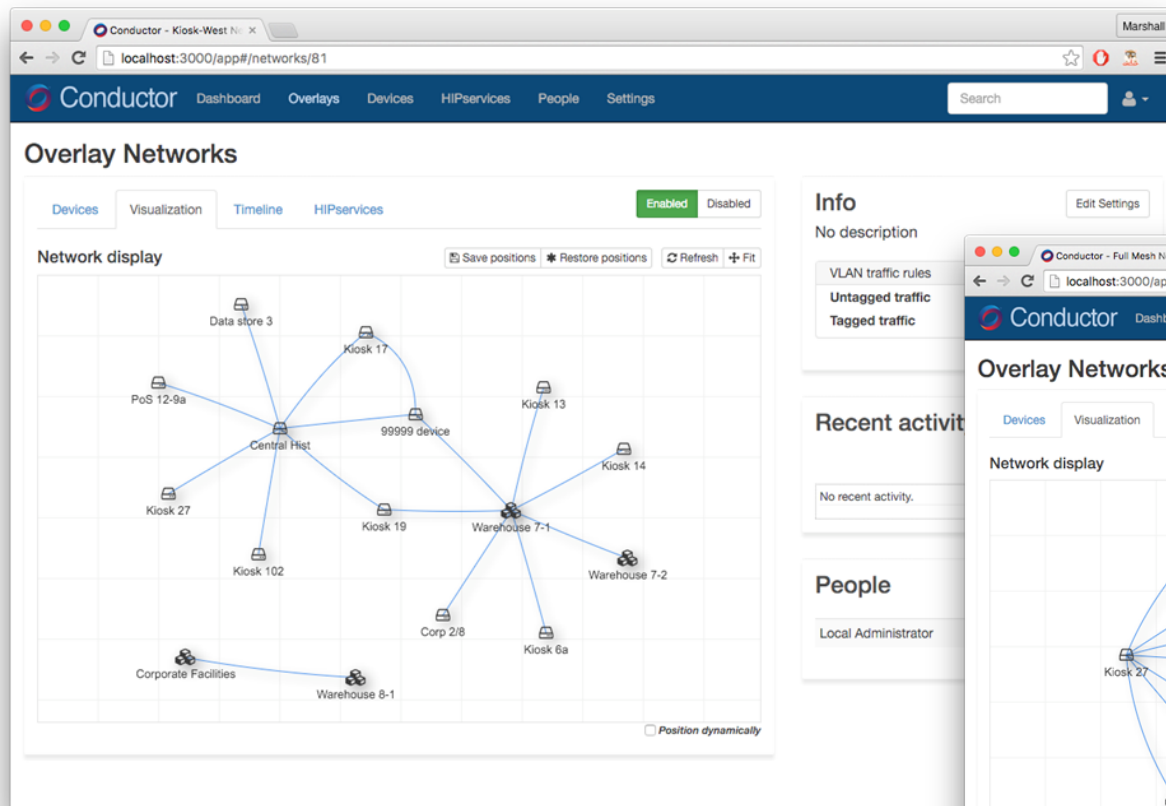
Lower Costs, Simpler Environment

- CapEx and OpEx decrease
- Eliminate or reduce interior “next-gen” firewalls, VPNs, complex policies, ACLs, VLAN complexity, cert mgmt

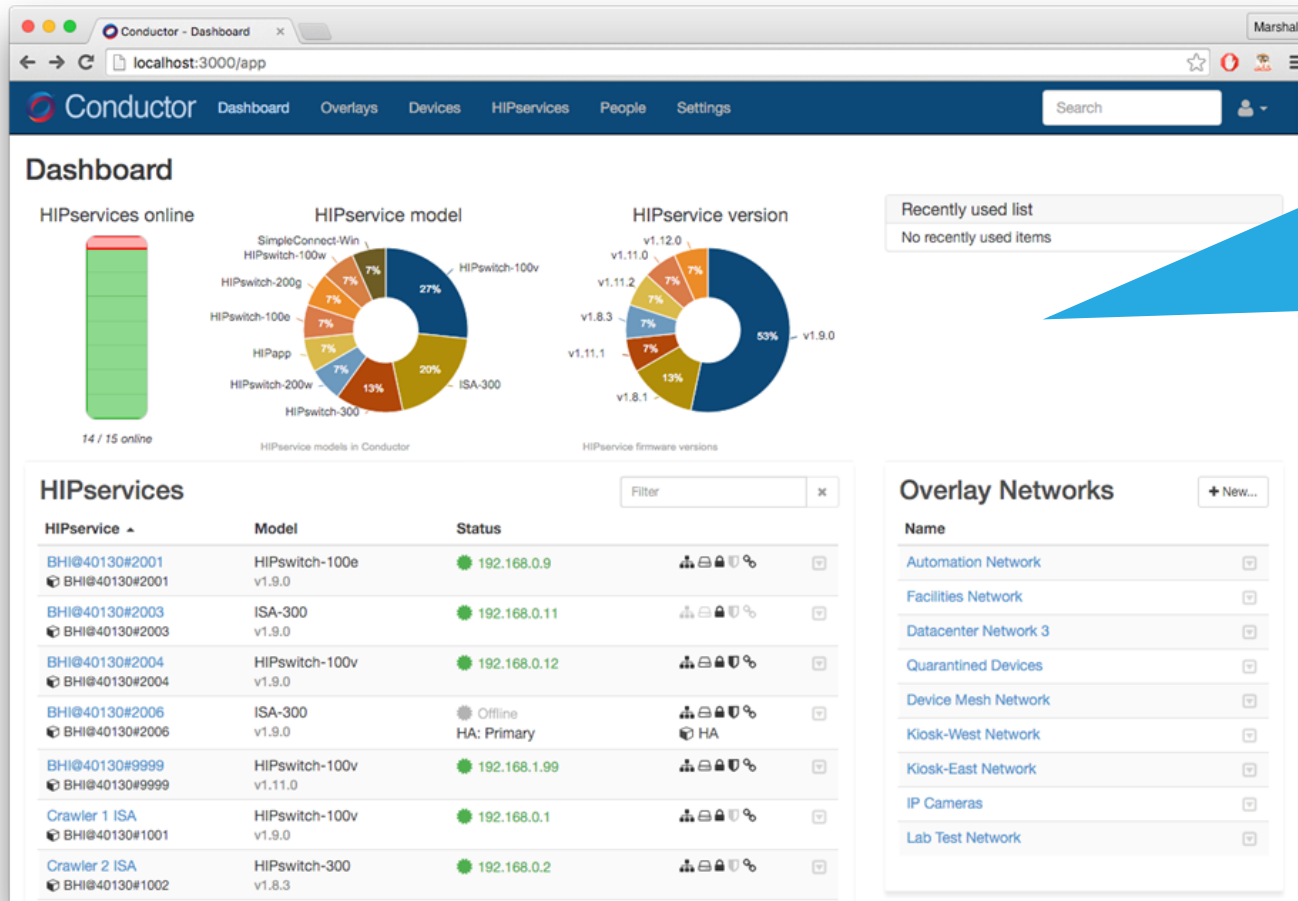


Conductor's “Visual Trust Map” – Instant Verification

Visualize trust relationships
between HIP Services and
whitelisted endpoints



Availability, Status, Configurations, Versioning – Know the State



HIP Services:

- Activity
- Models
- Versions
- Static or dynamic config
- Current IP address
- Gateway
- DNS server
- Custom routes
- Link status
- Port configuration [if available]

Users may now check which HIP associations (secure tunnels) exist on a HIPswitch and check available bandwidth as well for availability and sizing understanding.

Connectivity State –

Obtain Cellular Data, Check Availability of HIP Services

HIPswitch - 101g-A1

Navigation: [HIPswitch](#) [Local Devices](#) [Ports](#) [Reporting](#) [Diagnostics](#)

[Shared network](#) [Port assignment](#)

Port 1 (Shared network) configuration

Interface configuration:	DHCP
Current IP address:	
MAC address:	48:06:6a:02:04:a7
MTU:	Default

Cellular configuration

Provider:	AT&T
Access point name (APN):	broadband
IMEI:	359225050638451
IMSI:	310410850283617
ICCID:	89014104278502836176
MSISDN:	12062941504
Cellular modem:	sierra-mc7354
Signal strength:	
MAC address:	b2:0b:1d:d8:0a:a8
MTU:	Default

HIPswitch - SCAPI-HS100V-01

Navigation: [HIPswitch](#) [Reporting](#) [Local Devices](#) [Shared Network](#) [Diagnostics](#)

[Data capture](#) [Check connectivity](#) [Secure tunnels](#)

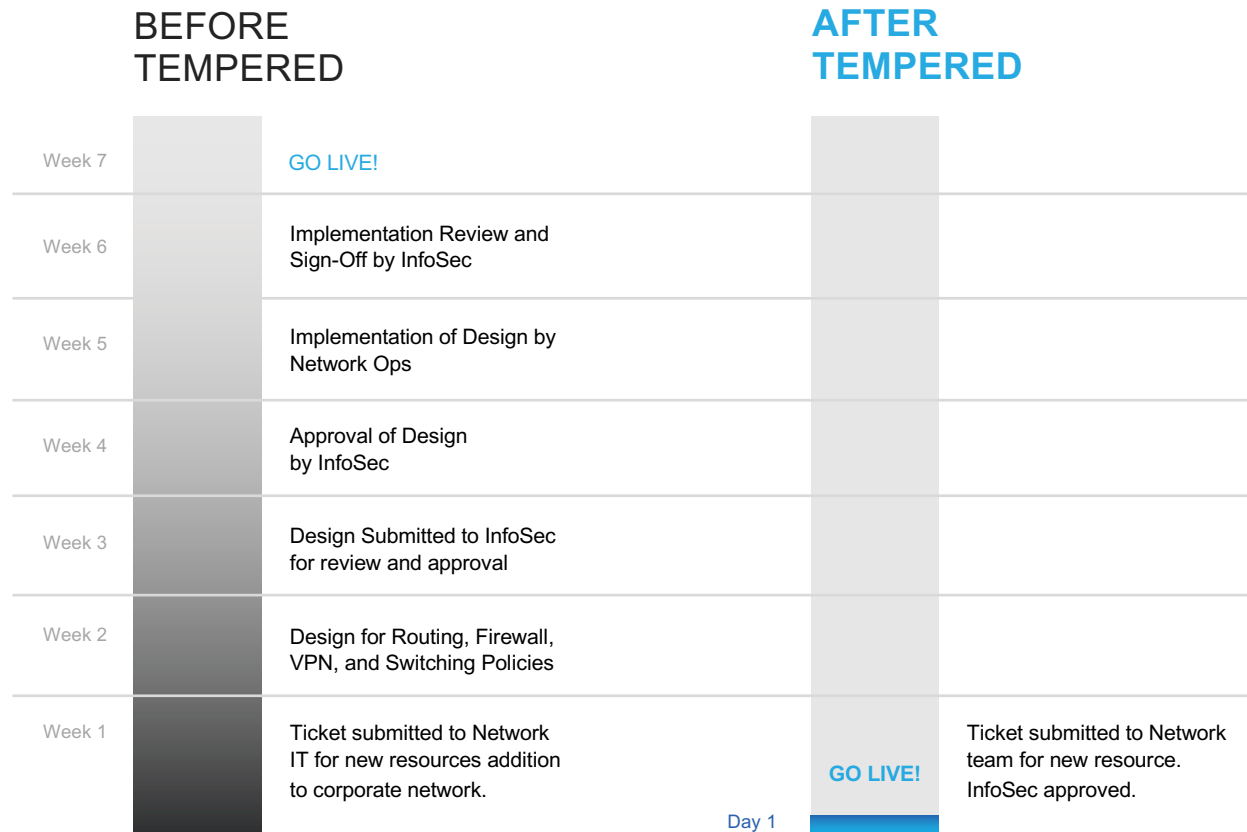
Local device connectivity

Check if devices that are protected by this HIPswitch respond to ping requests.

[Ping all Devices](#)

Device name	IP address	Ping status
10.5.9.30	10.5.9.30	✓
API TEST DEVICE 130	10.5.30.130	⚠

Reduce time to provision



Secure networking
time reduced by

97%

Resource added with explicit
trust segmentation, cloaked
and encrypted communication.

Verified by InfoSec.

Our Customers Increase Productivity

25%

**Increase in network
and security team
productivity**

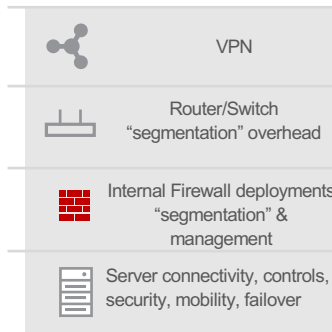
Because time to provisioning and attack surface is reduced...

- They can now focus security efforts on what else really matters instead of managing certificates, complex FW rules, ACLs, and VLAN “segmentation” playing whack a mole.
- Greater focus on new network designs and policies that improve quality of service, monitoring and uptime, not figuring out how to provision new resources.
- Simpler and faster way to test and verify disaster recovery and failover at a macro and micro-service level with minimal disruption – no more 2 am change windows thank goodness.

and Decrease IT Expenditures

Simplify, unify, replace, and reduce. Identity-defined networking (IDN) allows better offloaded segmentation, connectivity, access, and encryption **reducing capex cost** and complexity. Unconstrained provisioning, mobility, instant revocation and failover **lowers opex**.

BEFORE TEMPERED



AFTER TEMPERED



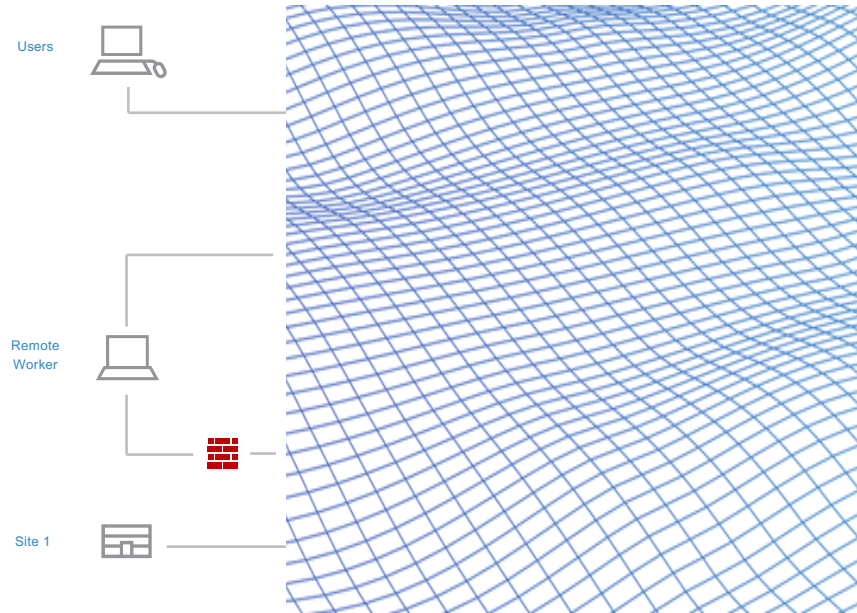
25%

Decreased IT CapEx
and OpEx costs

Cloaking makes 100% of Connected IP Resources **Invisible**

BEFORE TEMPERED

AFTER TEMPERED

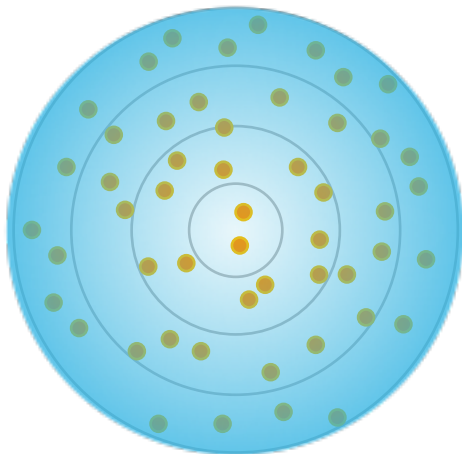


- IDN is the only technology based on the Host Identity Protocol (HIP). Unique device identity is native to networking; simple to orchestrate.
- No other solution on the market can be implemented as quickly, with little to no disruption
- Unlike others, IDN can be deployed across all environments -physical, virtual, cloud, mobile, or embedded.

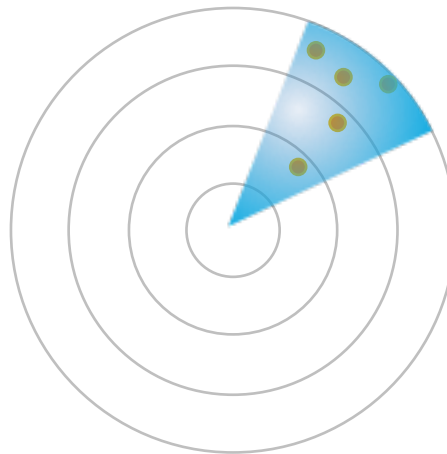
Reduce the Attack Surface

Attack surface reduction allows **greater security focus** and depth on the other areas Tempered Networks doesn't address, like endpoint or code-level security.

BEFORE TEMPERED



AFTER TEMPERED



Up to:

90%

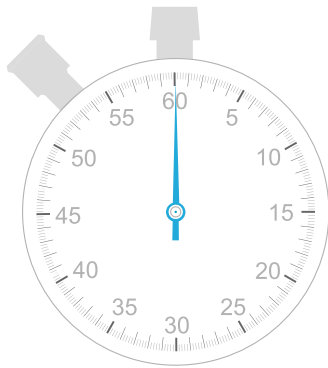
Because of cloaking,
identity-based
segmentation, non-
traversal, automatic
encryption, and instant
revocation.

Improve Time to Mitigate, Revoke, and Quarantine



- Revocation of any resource within the IDN fabric is one click or an automated API call from a security analytics system. It can happen instantly, is verifiable, and permanent - until you say otherwise.
- Even if a user's credentials were stolen and still valid, if they're not on an authorized device – no access.
- The alternative? Complexity. Check all VPNs, Firewall rules, ACLs, and directory services. Analyze other policies to ensure that system is in fact quarantined or revoked.

Decrease Failover and Disaster Recovery Time



To as
little as:

1 second

**Failover and Disaster
Recovery times
reduced to as little as
one second.**

- Every IDN endpoint or HIP Service is based on unique host identities, not an IP address or host making IP-based failover 'mobile.'
- Failover can be applied from an entire datacenter (represented as a unique host identity), down to a container (represented as a unique host identity).
- If one goes down in the IDN fabric, a simple automated API call or one-click manual update to the fabric will reconnect instantly to the designated IDN failover endpoint.

Secure Networking **Made Simple**



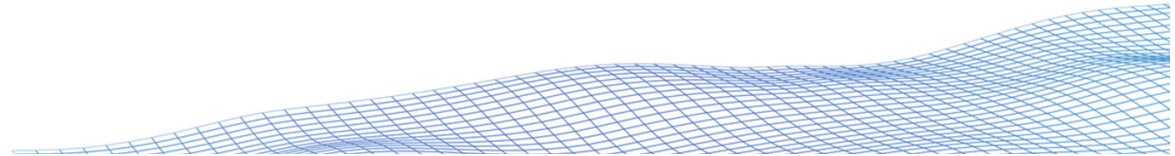
Global Orchestration and Network Provisioning

- Host Identity Namespace - Global IP Mobility
- Dynamic Device-Based Traffic Management
- Instant Failover
- Automated (API-driven) or Manual Control



Trust-Based Unique Cryptographic Identities (CID)

- Prevent IP Address Spoofing and MiTM attacks
- Assign IDN Endpoints and Networks an Identity
- Encrypted Fabric Extends all the Way to IDN Endpoints



The Cure to IT Complexity



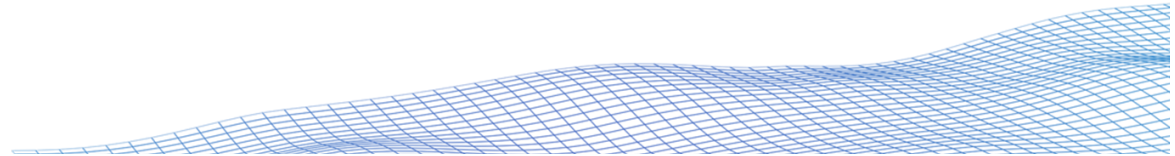
**Visual Orchestration Simplifies,
Reduces Complexity & Errors**

-
- Unified single-pane-of-glass management
 - Rapid point and click trust-based segmentation
 - Centralized governance, compliance, and policy enforcement



Reduces CapEX and OpEx as much as 25%

-
- Build secure segmented networks instantly
 - Eliminate errors caused by complexity
 - Faster and most cost-effective failover
 - Simplified auditing and access control



Tempered Networks **Solution** – control *any connected thing, anytime, anywhere*



Integrates unique device identity from the start



Instantly connect, cloak, segment, revoke, move, or failover



Fast deployment. Simple policy orchestration. Non-disruptive.



Provisions secure networks and resources rapidly

Next Steps (Examples Only. Sales People Tailor to Prospect)

Schedule a 30
minute quick
overview and
demo with
additional
stakeholders

Send IDN
Whitepaper
and slide
deck for
further
research

Schedule 30
– 60 minute
meeting to
discuss and
document
PoV Success
Criteria

Other?

Thank you!