TEMPERED NETWORKS®

Product Datasheet

HIPswitch 100 Series

Zero Trust Identity Defined Networking (IDN) for Commercial and Industrial Deployments

IDN Overview

IDN eliminates the complexity, cost, and exposure of traditional IP networks. With IDN, our customers accelerate resource provisioning and eliminate the network attack surface by enabling peer-to-peer, zero trust overlay networks that are remarkably simple to deploy and maintain.

All devices in an IDN overlay transparently authenticate and authorize network connections before data transport, making the network invisible and inaccessible by any unauthorized devices. Segmentation is made simple, and administrators can easily connect, encrypt, failover, and disconnect device communications across any network without disrupting or changing existing infrastructure.

- **50% Lower CapEx and OpEx**
- **97% Faster Resource Provisioning Time**
- **90% Reduced Attack Surface**

HIPswitch 100 Overview

The HIPswitch 100 is a purpose-built industrial IoT edge gateway that makes it remarkably simple to connect and protect IoT endpoints, while securely collecting data. Unlike traditional IT alternatives, the HIPswitch is very easy to deploy and manage, is network and transport agnostic, and requires little to no change to existing infrastructure. Our customers can now rapidly join all ICS/SCADA, BACnet, payment systems, and other endpoints to a private and segmented overlay network in minutes.

Like all IDN enforcement points, the HIPswitch 100 serves as the network boundary and security perimeter for IoT endpoints, which removes the complexity associated with traditional network and security methods. All connected and protected devices behind the HIPswitch 100 are cloaked and can't be discovered or reached by unauthorized devices, eliminating the network attack surface. Our customers now have a plug and play design with an optional cellular modem configuration that makes universal connectivity and segmentation across all networks simple, fast, and extremely cost-effective.

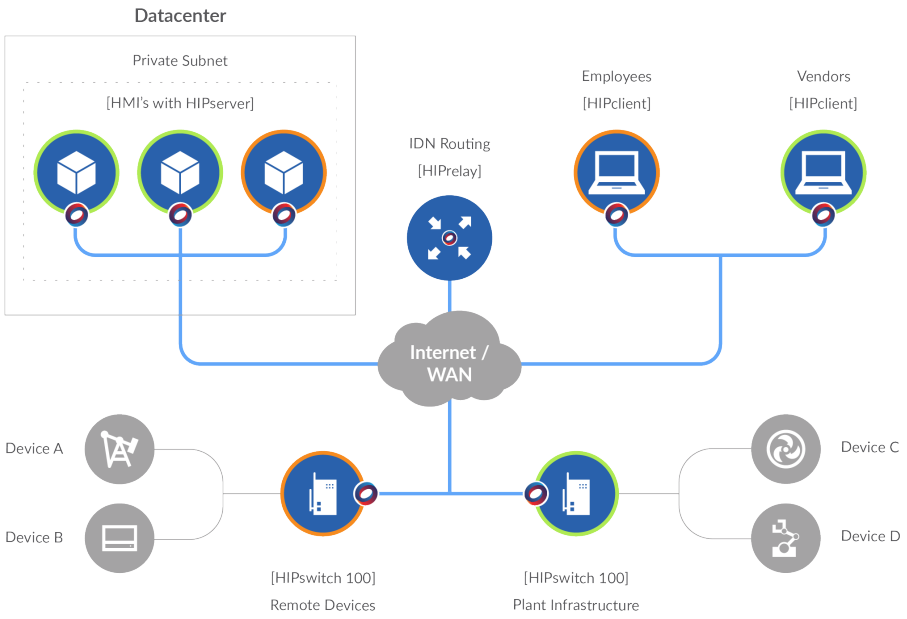
FEATURES	BENEFITS
Zero Trust Policy Enforcement	The HIPswitch enforces whitelisted network and security policy for trusted and protected endpoints in the IDN overlay, making it simple to connect and protect any IP-enabled device. Revocation of device access is instant.
Plug and Play Deployment	Provisioning the HIPswitch takes less than a minute and requires little to no changes to existing infrastructure. It can also be pre-provisioned for deployment by non-technical staff to accelerate the time to connect, protect, and segment.
Software Defined Perimeter	As a software defined gateway for protected devices, the HIPswitch becomes both the network boundary and security perimeter. This eliminates the complex, error-prone, and ineffective network and security controls of traditional IT solutions.
Cloaking	Cloaked endpoints and networks have no visible TCP/IP footprint and are invisible to the underlying network and any untrusted devices or systems, meaning attackers cannot discover or hack protected endpoints.
Universal Connectivity and Peer-to-Peer Encryption	IDN delivers private wide-area overlay networks that makes it simple to connect privately-addressed devices on separate Layer 2 and Layer 3 networks. AES-256 encryption for all sessions is on by default.
Network Resiliency and Availability	Traffic flows between distributed HIP Services can be moved instantly without disrupting application sessions to enable fast and predictable failover, disaster recovery, and quarantine.
LAN and WAN Micro-Segmentation	Secures north-south and east-west traffic in any environment - physical, virtual, and cloud - across Wi-Fi, cellular, and Ethernet networks. Provides authenticated and verifiable device-level access control that can't be spoofed or violated.
Autonomous Operation	Ensuring the highest level of security, the HIPswitch is managed only by Conductor with no local administration. No network traffic flows through the Conductor, allowing for autonomous and continuous operation.

 |

TEMPERED NETWORKS®

Deployment

- Enables simple policy orchestration of enforcement points within a unified overlay architecture that's network, platform, and transport agnostic.
- Simplify your network. Organizations use IDN for secure peer-to-peer connectivity and segmentation that traverses existing switching and routing infrastructure across all LAN WAN, and Internet environments.
- Central policy orchestration is non-persistent, so all enforcement points can run autonomously for superior network resiliency and availability
- Simple and cost-effective to acquire, deploy, and maintain to save time, money, and personnel resources.



Value Licensing

- Uniform software pricing regardless of platform or environment creates predictability
- No-charge software portability delivers agility to adapt to changing requirements
- HIPswitch throughput 'bursting' without penalty eliminates surprise costs

"Tempered Networks gave us a simple way to achieve rapid segmentation 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 systems or involve IT."

Tom Walker

Facility Automation Services,
Penn State University

Summary

IDN enables borderless, zero trust overlay networks with point-and-click simplicity. It's now simple to create segmented and private networks spanning on-premises, remote, and cloud environments, with granular access control for each connected resource. With IDN's unique overlay technology, our customers can start small and quickly scale and automate their segmentation architecture, without having to change their existing networking infrastructure. The results? Provision, segment, and revoke endpoints 97% faster than alternatives, while reducing the attack surface by up to 90%. With simple segmentation, built-in peer-to-peer encryption, cloaking, and universal connectivity and mobility, IDN delivers a more resilient, flexible, and extremely secure architecture.

Contact us at sales@temperednetworks.com to learn more.

