TEMPERED NETWORKS

Solution Brief: Power Generation

Securing Critical Infrastructure Without Adding Operational Complexity

Increasing automation and connectivity of industrial control systems (ICS) across distributed power generation facilities is creating an increased attack surface. For cost-efficiency, network resources are often shared by multiple business users throughout the enterprise, blurring the traditional one-network, one-user model. To support the variety, complexity, and scale of various operational groups while protecting critical, revenue-generating infrastructure, power generation companies need efficient solutions that enable IT departments to solve complex network security challenges without increasing the operational burden on onsite operations teams.

Tempered Networks provides a centrally managed security appliance solution that gives power generation facilities a more secure and yet simpler approach to protecting distributed control system (DCS) networks.

Segment and Cloak the Network

The industry's best practice for protecting critical infrastructure and DCS networks is a defense-in-depth approach that starts with segmented networks. With the Tempered Networks solution, organizations can segment and isolate connectivity to and between production facilities, following the ISA-99 (IEC 62443) zone and conduits model. Unlike traditional firewalls, the solution goes beyond simple inspection to add confidentiality, integrity, and availability protection to the data as it traverses the control systems network and other untrusted networks. The Tempered Networks solution provides a private overlay network and cloaks all devices within it, leaving no configuration footprint from outside the private network. The solution leverages existing infrastructure to connect facilities without exposing device communications and without the brittleness of complex configurations.

Securely Connect and Monitor Remote Sites

By introducing an independent layer of connectivity, security, and trust management, the Tempered Networks solution enables remote device management—even across a third party's network infrastructure. Organizations can easily connect and monitor distributed generation equipment with centralized SCADA and Historian systems. The solution is transport- and topology-agnostic, supporting any mix of cellular, WiFi, wired Ethernet, or satellite communications networks.

Benefits

- **Extends the network**: IT or operations teams can easily and securely extend networks to remote locations using wired, WiFi, cellular, SatCom, and public cloud networks
- **Centralizes governance**: Facilitates administration and departmental provisioning of private overlay networks
- **Integrates with legacy and modern infrastructure**: Private overlay networks can be easily integrated with any existing IT security and network infrastructure
- **Cloaks critical assets**: Isolates and encrypts communications to cloak ICS and SCADA devices
- **Increases operational integrity and availability**: Facilitates monitoring and predictive maintenance to maximize uptime
- **Enables secure remote access**: Highly constrained remote access can be easily granted and revoked without impacting the underlying network
- **Easy to deploy and maintain**: Intuitive management user interface does not require advanced IT security expertise
- **Facilitates NERC CIP compliance:** Reduces the cost of implementing compliant network architectures

Easily Manage Third-Party Access

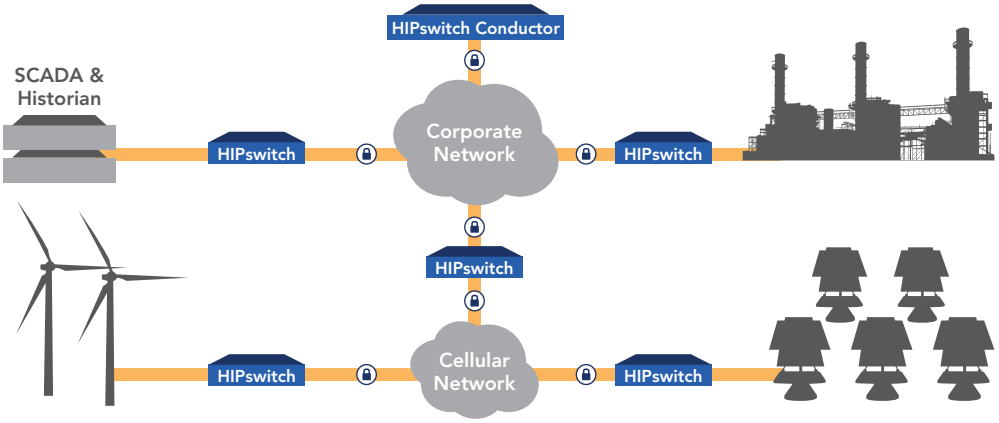
Most facilities need to give network access to vendors and contractors, but this introduces an additional security vulnerability. With the Tempered Networks solution, third-party access can be granted and revoked in just minutes. Access can be constrained to a single, isolated device or a group of devices and for a specific period of time. The solution can also be configured to require user authentication.

Tempered Networks Product Family

Military-Grade Security

- Secure channels bound to unique RSA 2048-bit cryptographic identities
- Per-peer explicit trust relationships validated up the certificate chain with SHA-256 signatures
- Secure channels protected with Diffie-Hellman exchange, AES-256 encryption, SHA-1 message authentication
- Stateful packet inspection (SPI)
- Denial of service (DoS) mitigation
- Full lifecycle identity management, including instant blacklisting and revocation
- Microsegmentation based on device whitelisting

The Tempered Networks Solution for Power Generation Facilities



The solution provides a secure overlay network among HIPswitch™ appliances that secures remote connections for SCADA systems and remote access users. The HIPswitch Conductor™ orchestration engine coordinates configuration, security policies, trust relationships, monitoring and analytics.

Take control of your critical infrastructure with Tempered Networks' proven solution for keeping industrial, commercial, and public sector systems and assets secure and resilient.

To learn more, email sales@temperednetworks.com, call 206.452.5500, or visit temperednetworks.

TEMPERED NETWORKS