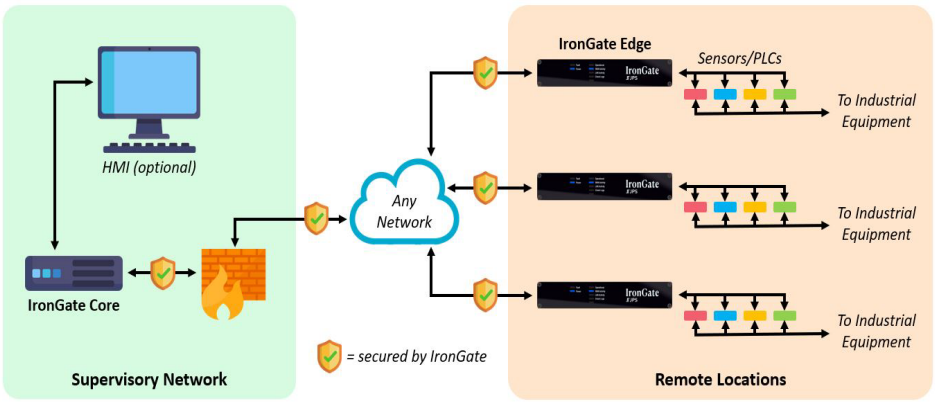
IRONGATE®

PURPOSE-BUILT SCADA SECURITY

OVERVIEW

Vast sectors of modern infrastructure rely on remote ICS/SCADA equipment, and much of it is IP-based. This built-in reliance on the Internet may come with convenience, but it also comes with the rapidly mounting risk of hacking and cyber attacks. Rather than trying to patch existing code or find other software fixes, IronGate tackles the security problem head on. By providing a hardware solution, IronGate eliminates hacking.

The IronGate system does not rely on standard networking methods for communication with SCADA equipment, nor does it rely on standard network security methods. IronGate is a purpose-built computing appliance with a custom Hardened Ethernet Interface (HEI) that is the system's only connection to the Internet cloud.



FEATURES

Until now, systems to protect IP-based SCADA communications have been expensive and only lessen, rather than eliminate, vulnerability to attack. This is because they continue to employ standard network protocols. The IronGate HEI is not a standard Ethernet Interface. It does not support any standard protocols such as SSH, FTP, TFTP, RTP, SQL, VPN, RDP, or SNMP. The HEI requires and supports only one protocol. This protocol is secure, encrypted, custom, and is used nowhere else in the world.

KEY BENEFITS

- Prevents hacking of infrastructure
- Prevents cyber sabotage by internal bad actors
- Allows two-way communication with sensors and controls
- Unique protocols change every four seconds
- If physically tampered with, Edge devices brick and signal the Core
- Red team tested by Cylance and FireEye Mandiant
- Successfully tested by an Army innovation center at Aberdeen Proving Ground

BENEFITS

- IronGate eradicates cyber attacks with proven, innovative, and cost-effective architecture. The tools and methods designed by hackers to penetrate standard networking equipment have no point of entry at any site protected by IronGate.
- With IronGate, the company's network is not extended to the remote sites, removing additional potential security breach points.
- The hardware design itself is secure; physical possession of Irongate Edge units does not expose any vulnerabilities.
- Irongate provides improved security at only a fraction of the price of existing security methods.
- IronGate carries out all communication with the SCADA sensors and controls, so users do not need to learn the many different protocols and control methodologies prevalent in the industry.

DETAILS

Congress passed the America's Water Infrastructure Act in 2018 in response to several vectors of attack against safe community drinking water. As part of the AWAI, water utilities serving more than 3,300 people have to carry out risk and resilience assessments. Despite that, it was only pure luck that a vigilant employee happened to catch a hacker in the act of logging in and manipulating SCADA data to sabotage the Oldsmar, FL town water system in 2021.

Later that same year, the Colonial Pipeline was shut down after the computerized equipment managing the pipeline was hacked. The ransomware attack forced the company to halt the gasoline and jet fuel pipeline operations and then pay the ransom.

Infrastructure is under attack every day. IronGate provides a truly unique solution. Edge devices communicate with the IronGate Core server solely via the Hardened Ethernet Interface (HEI) and its custom protocol. Edge devices are also hardened; if tampered with, they will brick themselves and reveal no data.

IronGate provides two additional unique security features. Unlike typical IP-based systems, a virus cannot migrate from point to point within the IronGate system. And once the system is up and running, usernames and passwords (or other identifiers) cannot be used as an entry vector. Even a successful phishing attack to gain these identifiers will not aid a hacker.

IronGate is:

- **Economical** - approximately half the cost of, and more secure than, competing systems
- **Secure** - physical possession of an Edge device does not expose vulnerabilities; not vulnerable to tools/methods used by hackers
- **Scalable** - each IronGate Core can serve 100+ remote Edge devices; each Edge device can handle hundreds of SCADA controls and sensors
- **Brand Agnostic** - works with a broad range of legacy and new SCADA equipment