Maintenance & Security

NOC Managed Services with Sentryx Platform

Network Operations Center

- Secure, safe, redundant storage
- 24/7 network and intrusion monitoring
- Time and cost savings
- Quick and reliable access to data
- No need for in-house servers and infrastructure
- No worries about upgrades

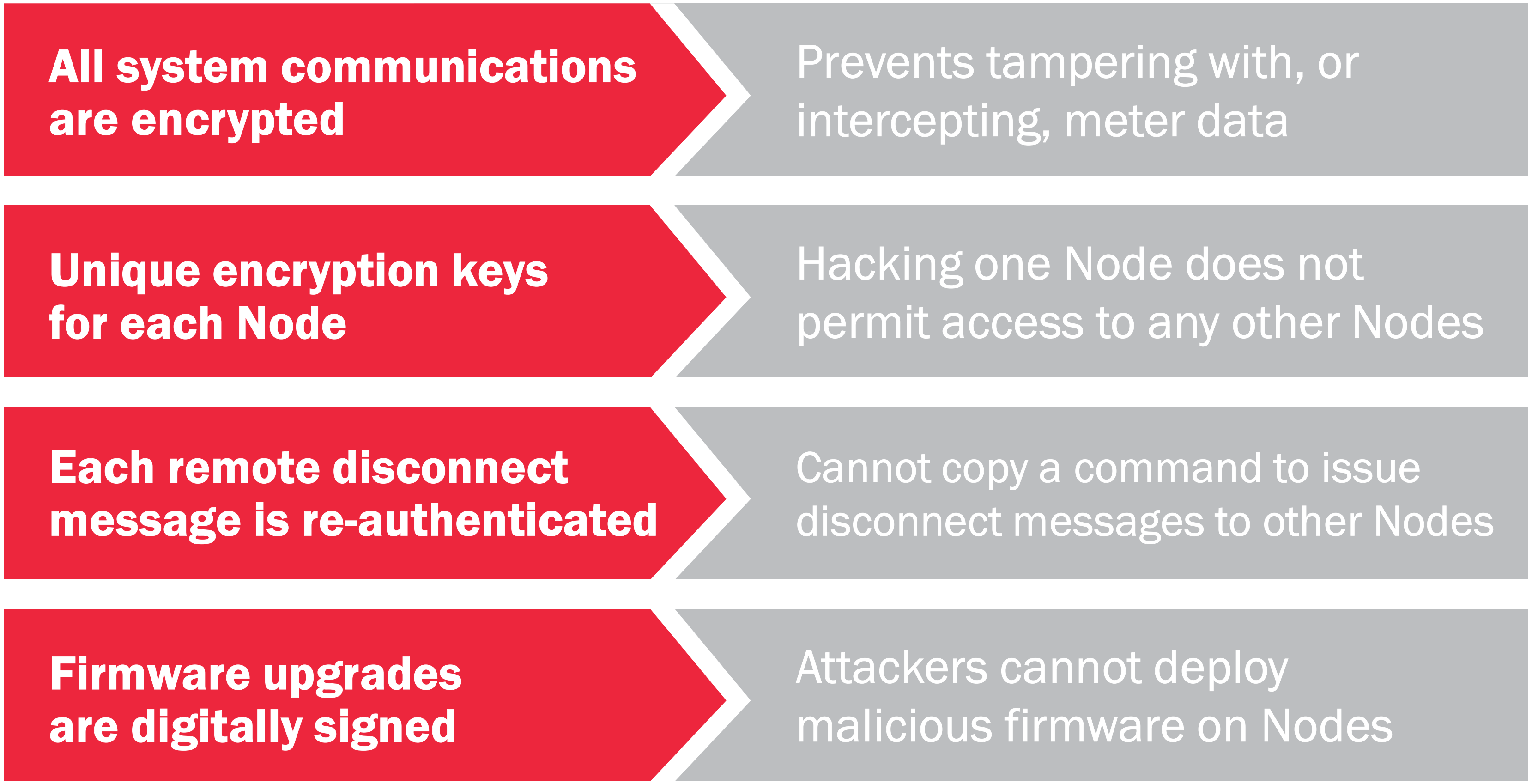
MUELLER

Holistic Approach to Security

- Data is encrypted at every point in the system
- Every endpoint is assigned a unique security key at manufacturing
- All remote disconnects have enhanced security including require re-authentication
- All remote disconnect commands are digitally signed to eliminate a “copy-cat” command
- All data applications are PII compliant with ISO-27K, all 50-states, and federal government
- Annual/quarterly security reviews with third party penetration testing
- Trained, dedicated security team, rehearsed and ready to respond and help you recover in the event of an incident

MUELLER

AMI Security Features



All system communications are encrypted	Prevents tampering with, or intercepting, meter data
Unique encryption keys for each Node	Hacking one Node does not permit access to any other Nodes
Each remote disconnect message is re-authenticated	Cannot copy a command to issue disconnect messages to other Nodes
Firmware upgrades are digitally signed	Attackers cannot deploy malicious firmware on Nodes

AMI Security Features

Permissions/Role-based Identities	Individually control permissions to system functions
Federated Identity	Utilize your existing Identity Management system (such as AD)
ISO 2700 Aligned, **PII Compliant**	Protect the personal information of your users and customers
Secure Development Lifecycle & Third Party Security Testing	Reduces security flaws

MUELLER

What Exactly is AES 128?

Why Advanced Encryption Standard (AES)

- Federally recognized standard for data encryption (NSA/NIST)
  - Approved by DOD and NSA to protect top secret data
- Why 128 bit? It's more than strong enough (3.4 x 10^{38} possible combinations)
  - Every person on the planet owns 10 computers. (There are 7 billion people on the planet)
  - Each of these computers can test 1 billion key combinations per second
  - On average, you can crack the key after testing 50% of the possibilities
  - Then the earth's population can crack one encryption key in 77,000,000,000,000,000,000,000,000 years!

At present, there is no known practical attack that would allow someone without knowledge of the key to read data encrypted by AES when correctly implemented

Enhanced RDM Security

- Federated Login to ensure access to Mi.Host and RDM function can be managed in coordination with your existing systems.
- User Access Controls let you determine who can access RDM function and what controls they have at individual user level.
- Configurable Thresholds at both the system and user level prevent flag and block potentially nefarious RDM commands.
- Re-Authentication can be provided on all RDM functions to ensure only trusted users access this control.
- Smart Alerts can be automatically be deployed on Disconnect to monitor for use/tamper and on reconnect to monitor for continuous flow.