



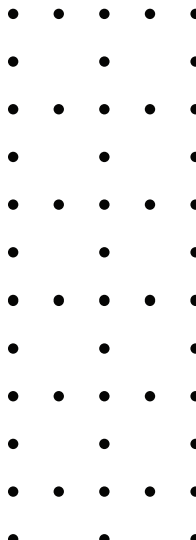
**BAYSHORE NETWORKS**  
INDUSTRIAL AND IT NETWORK SECURITY



**OTfuse™ iFIX**

INDUSTRIAL SECURITY APPLIANCE

**Datasheet**



## OTfuse iFIX

Protection for your iFIX investment by protecting its network from unauthorized and dangerous activities

OTfuse iFIX is an industrial network security appliance specifically engineered to protect your iFIX network from unauthorized communications and intrusions. It controls who, how and when updates can be implemented and augments the existing application level security of iFIX with a multi-layered security approach.

OTfuse iFIX is available in two physical form factors: DIN rail ruggedized enclosure and 1U telco rack server. It works on any iFIX 6.x deployment and no changes to the iFIX installation are required.



## Benefits

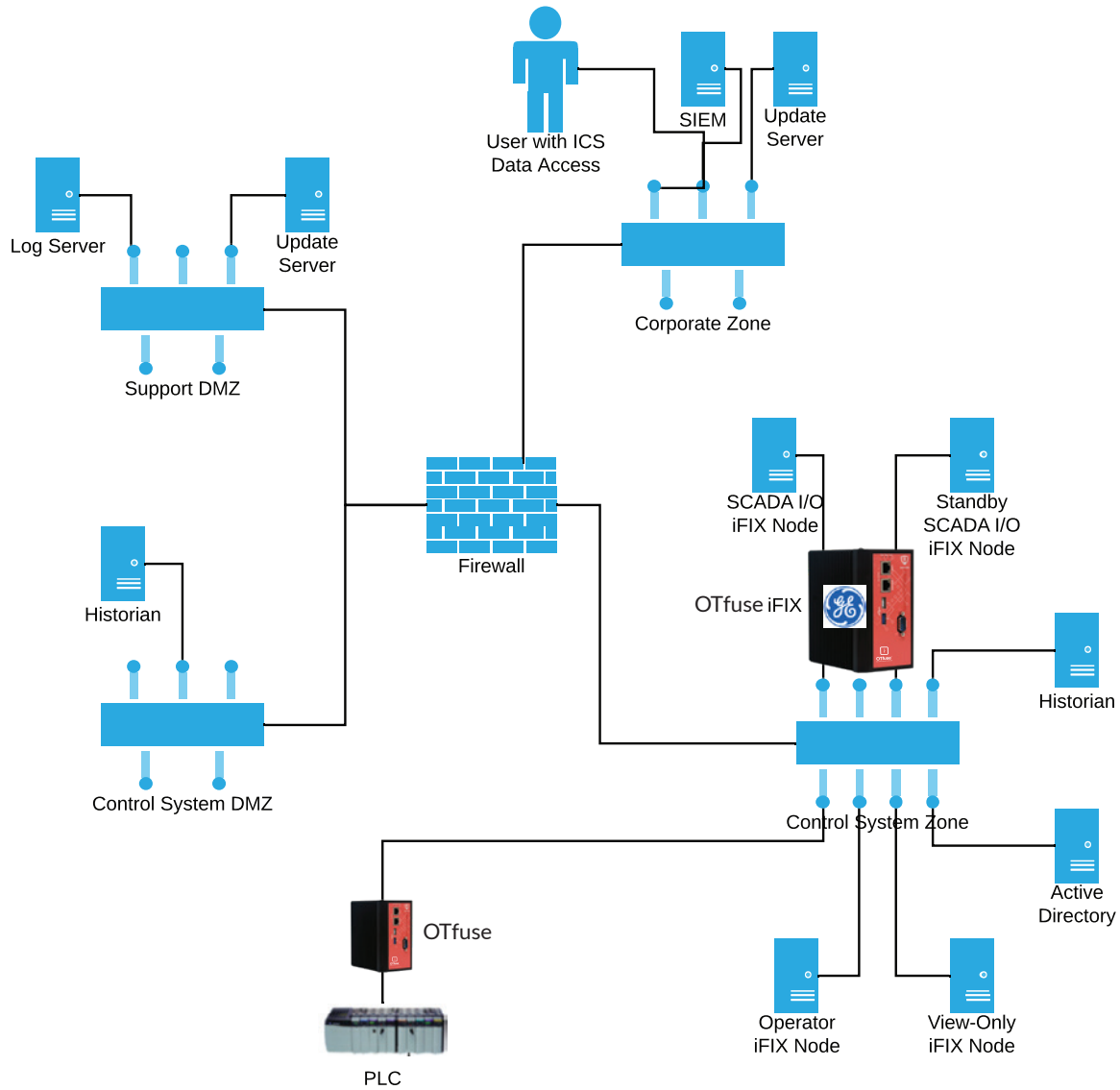
- ✦ Industrial network security appliance specifically engineered to understand iFIX protocol communication patterns and protect iFIX deployments
- ✦ Prevents unauthorized communications from reaching iFIX assets
- ✦ Allows easier protected access to iFIX 6.x systems
- ✦ Maximizes protection for the variety of iClients in use across your deployment
- ✦ Ensures unauthorized nodes cannot interact with the rest of the site
- ✦ Replacement option for Opshield products which are no longer available

## Cybersecurity Features of OTfuse iFIX

OTfuse iFIX provides five separate security controls to protect iFIX standalone, SCADA, and view nodes as they interact with each other and the broader OT/IT network.

| iFIX Network Risk                                 | OTfuse for iFIX Security Protection  | Confidentiality Control               |
|---|--|---------------------------------------|
| Risk from unknown nodes or clients                | Immediately alert and stop attempts to add a node which interacts with or modifies iFIX system behavior                                  | Rogue Node Detection                  |
| Risk from unauthorized scanning or communications | Prevent network activity from detecting protected nodes.<br>Protect nodes from revealing sensitive information about their configuration | Reconnaissance Detection & Prevention |
| Risk of accidental reconfiguration or update      | Permit only read-type function codes on native iFIX protocols except during admin-defined time ranges                                    | Scheduled Maintenance Enforcement     |
| Risk of very high message rates (DoS)             | Automatic blocking of IPs which exceed typical message rates   | DoS/DDoS Protection                   |
| Risk of fake devices                              | Direct enforcement of known IP and MAC addresses for trusted iFIX SCADA nodes and clients.   | IP Spoofing Protection                |

# OTfuse iFIX Reference Architecture



## SUPPORTED PROTOCOL FUNCTIONS

| Protocol        | Variable Access | Alarm Handling | Session Alarming | Connection Management | Data Transfer | MDBA Handshake |
|-----------------|-----------------|----------------|------------------|-----------------------|---------------|----------------|
| Read Functions  | ✓               | ✓              | ✓                | ✓                     | ✓             | ✓              |
| Write Functions | ✓               | ✓              | ✓                | ✓                     | ✓             | ✓              |

