BAYSHORE NETWORKS
INDUSTRIAL AND IT NETWORK SECURITY

OTfuse Cimplicity

INDUSTRIAL SECURITY APPLIANCE

Datasheet

OTfuse Cimplicity

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

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

OTfuse Cimplicity is available in two physical form factors: DIN rail ruggedized enclosure and 1U telco rack server.

#1: DIN rail ruggedized enclosure

#2: 1U telco-rack server

Benefits

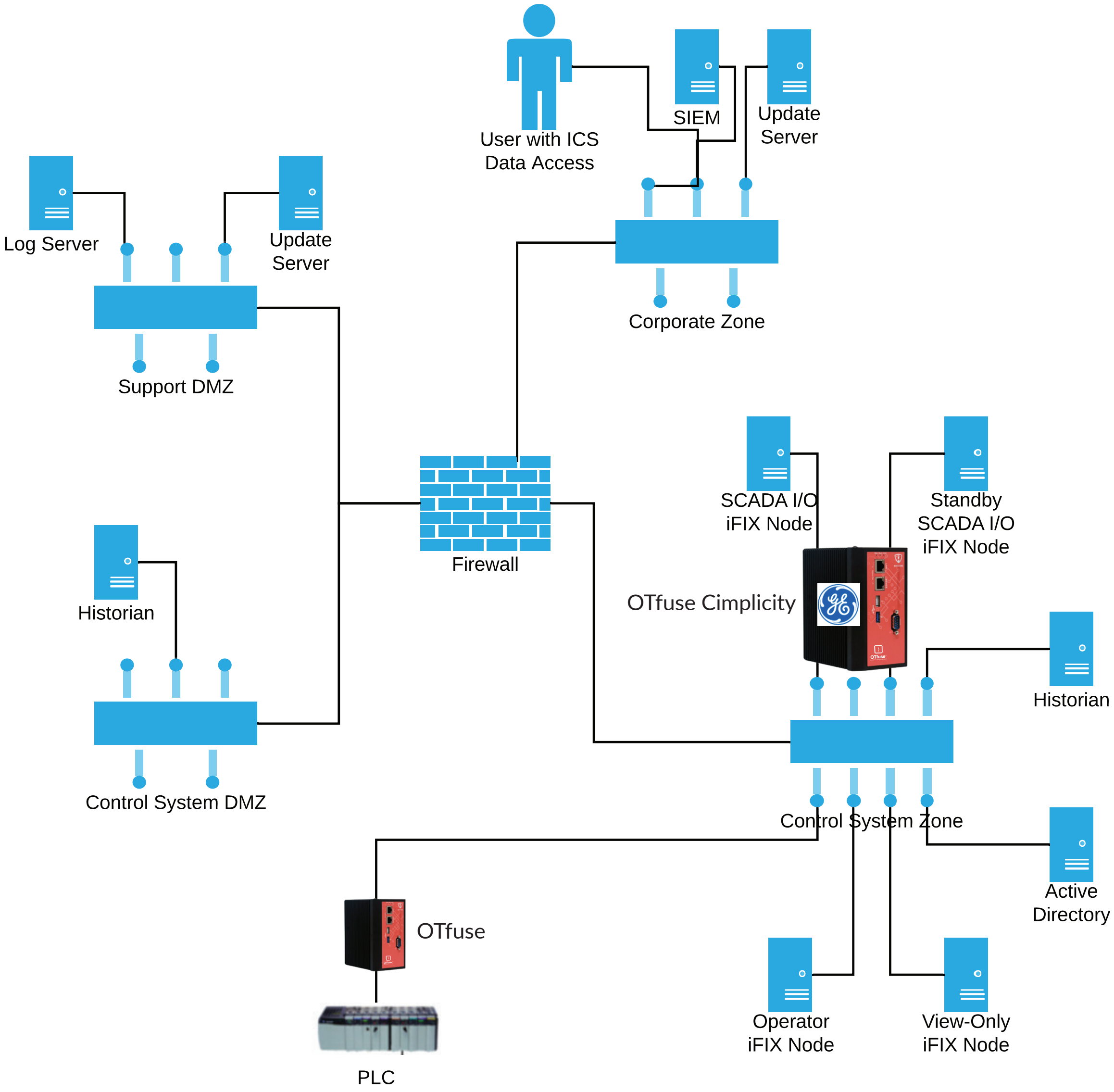
- *Industrial network security appliance specifically engineered to understand Cimplicity protocol communication patterns and protect Cimplicity deployments*
- *Prevents unauthorized communications from reaching Cimplicity assets*
- *Maximizes protection for the variety of iClients in use across your 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 Cimplicity

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

Cimplicity Network Risk	OTfuse for Cimplicity Security Protection	Confidentiality Control
Risk from unknown nodes or clients	Immediately alert and stop attempts to add a node which interacts with or modifies Cimplicity system behavior	Rogue Node Detection
Risk from unauthorized communications	Prevent network activity from detecting protected nodes. 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 Cimplicity 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 Cimplicity SCADA nodes and clients.	IP Spoofing Protection

OTfuse Cimplicity Reference Architecture



SUPPORTED PROTOCOL FUNCTIONS

Protocol	Variable Access	Alarm Handling	Connection Management	Data Transfer	Session Handshake
Read Functions	✓	✓	✓	✓	✓
Write Functions	✓	✓	✓	✓	✓

BAYSHORE
NETWORKS