30 DAYS

TO OT ZERO TRUST PROTECTION

A practical roadmap for deploying Zero Trust Protection in your Operational Technology Network

DAY 1

REGISTRATION

Register your Gateway to your Orchestrator and overlay your existing OT Cybersecurity solution without impacting any network operations.

DAY 2

ADD USERS

Use Orchestrator to cryptographically invite initial administrators to least privilege access to OT network

DAY 3

IMPORT DEVICES

Import via API or manually add OT devices for zero trust policy creation

DAY 4-6

CREATE POLICIES

Create initial policies, creating a virtual air gap for vulnerable devices , device-to-device communications, and groupings

DAY 7-11

GO LIVE

Go live by enabling access through BlastShield and fine-tune policies to minimize allowed protocols in OT network

DAY 12-18

MIGRATE USERS

Continue to migrate users to from legacy Secure Remote Access Solution until all users access the OT network through BlastShield

DAY 19+

MICROSEGMENT

Create device-level segmentation policies until you reach maximum microsegmentation security

DAY 30

ZERO TRUST PROTECTION ACHIEVED

In 30 Days or less, achieve Zero Trust Protection from Phishing, Reconaissance, and Lateral Movement Tactics

BlastWave

www.blastwave.com