RED TRIDENT CYBER-ECP™

INTRODUCTION

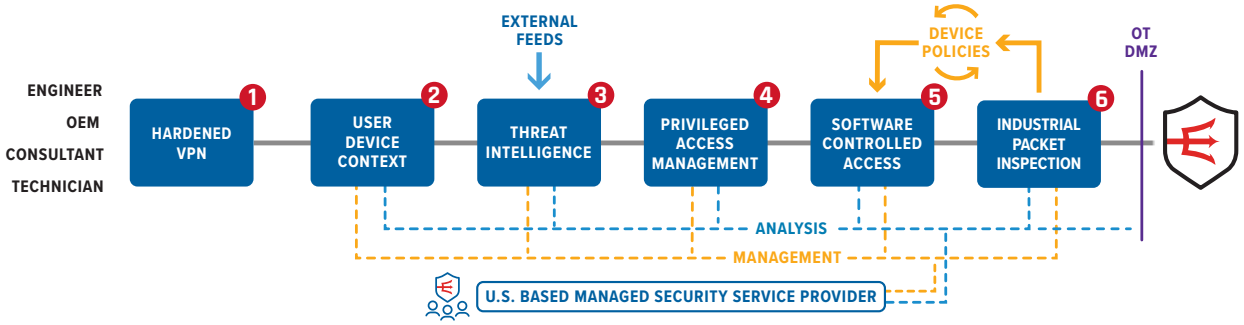
Red Trident's Cyber-ECP™ product solves the complex challenges associated with rapidly enhancing cybersecurity for Operational Technology (OT). With nearly two decades of experience working in these environments, we know how engineers, technicians, and operators work. By rethinking OT Security and understanding the detailed intricacies of Process Control environments, we developed a solution that allows you to focus on operations while we manage your OT cybersecurity for a fraction of the cost of implementing it yourself.

THE PROBLEM

In order for organizations to be competitive they are finding more ways to use the data their systems produce to make faster and more informed decisions. This means an increasing number of hardware and software solutions are being connected to networks to capture and collect the data. Additionally, organizations are allowing more access to these systems as they see the value of digital transformation and Industry 4.0 efforts.

Organizations are now finding that these systems do not have the same security capabilities as their IT counterparts and are struggling to implement cost effective and non-intrusive security controls. This leaves them open to attack, and many have already had attacks due to this issue. The industry needs a solution developed for the specific purpose of supporting Operations and Engineering teams to rapidly secure these environments.

The solution should focus on not needing to modify the network or OT environment, and to providing an easy solution for technical teams to use 24 hours a day, remote or onsite.



1. Hardened VPN leveraging the power and benefit of the cloud we are able to connect all users to a focal point for simple use of the system.

2. User/Device Context allows or denies access by user, device, device compliance status, time and purpose to the systems.

3. Threat Intelligence monitors location, user, and device behavior and continually assesses the risk a specific connection presents to an environment. When that risk exceeds permissible limits, automated actions can be taken to reduce or eliminate the risk.

4. Privileged Access Management provides just in time access and control down to the specific device a user can see or access, allowing segmentation of a flat network.

5. Entry Control Engine is an engine that manages the port, protocol, and commands that can be used by each user with a specific device.

6. Industrial Packet Inspection analyzes each packet and dissects the commands out of them. Each command is matched to a classification table where an alert can be sent back to the Entry Control Engine for action.

RED TRIDENT CYBER-ECP™

THE DIFFERENCE

The Cyber-ECP is a linear chain of security controls with each control reducing the attack surface an adversary would have to attack an environment. Each control in the chain was specifically picked based on the various Tactics, Techniques, and Procedures (TTPs) adversaries use to breach an environment, and the most effective way to detect and protect against these TTPs.

By reducing the attack surface like Cyber-ECP™ has, an adversary is unable to pivot or test out various methods of breaching an environment without being detected. This also means that trusted employees and/or contractors that turn into insider threats can be detected early and prevented from impacting operations.

Unlike other solutions that require the end user to setup and configure the system with the hope it all works right, Red Trident built a solution that can be easily deployed with Red Trident supporting you along the way.

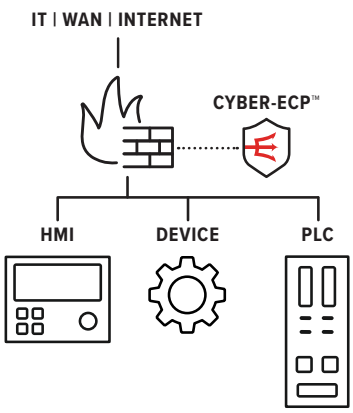
Red Trident's team of highly skilled OT Cybersecurity professionals monitor and manage the Cyber-ECP™'s operations in our Security Operations Center (SOC), so your team can focus on making your product.

HOW IT FITS

Cyber-ECP™ can easily be deployed in most OT networks to act as an OT Firewall at Purdue Levels 0-1, or to more complex routed environments at Purdue Levels 2-3. Well pads, tank batteries, electrical substations, pump and compressor stations, and remote telemetry sites are all addressable with this product.

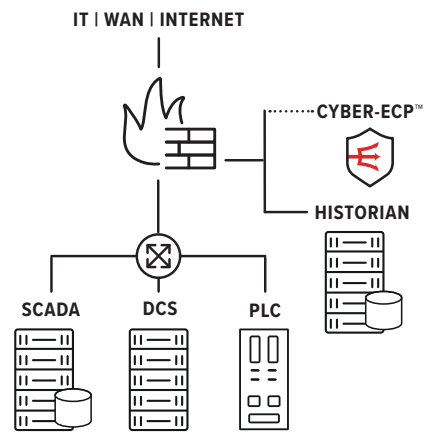
The Cyber-ECP™ appliance is a small form factor, DIN rail mounted device that is as simple to connect to the network as plugging in a laptop. Once connected, Red Trident handles the rest of the work for you. Designed by OT professionals for OT Professionals.

1 SIMPLE OT DMZ



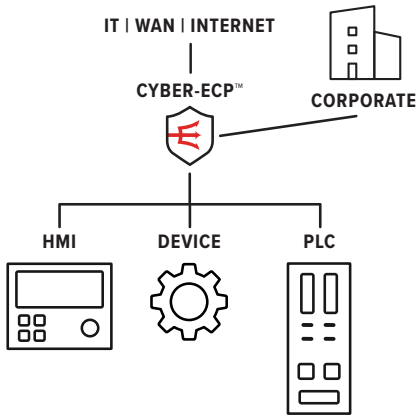
Simple OT DMZ Cyber-ECP™ can be placed in a DMZ and control access to each device downstream. This setup is good if there is an existing Firewall in place and connections need to be phased over to the Cyber-ECP™

2 COMPLEX OT DMZ



Complex OT DMZ Cyber-ECP™ can be placed above high value SCADA and DCS systems while still controlling user access to these system for both local technicians and remote workers/OEMs

3 REMOTE SITES



Remote Sites Cyber-ECP™ can act as a demarcation point for remote sites that only have a cellular modem. Allowing secure access to data from the site and secure remote support of all devices on the site without impacting dataflow

Red Trident Inc. | 5821 West Sam Houston Pkwy N, Houston, TX 77041 | 832.493.1153 | redtridentinc.com | sales@redtridentinc.com