CyberFence : Enhancing security for critical infrastructure

Executive summary

As the digital landscape evolves, securing critical infrastructure has become more crucial than ever. Operational Technology (OT) networks face significant cybersecurity challenges because of their standard communication protocol usage and exposure to diverse environments. Ultra Intelligence & Communication's (Ultra I&C) CyberFence product addresses these challenges by providing a multi-layered security solution specifically designed for OT networks.

With advanced features such as FIPS 140-3 certified encryption, comprehensive firewall protections, and deep packet inspection (DPI), CyberFence ensures the integrity and security of critical infrastructure devices. With a compact design and power over Ethernet (PoE) capability, it's an ideal choice for space-constrained industrial settings. By segmenting networks, managing communication, and inspecting data at a packet level, CyberFence mitigates both current and emerging threats —offering robust defense against cyber threats. Its seamless integration and user-friendly management interfaces facilitate enhanced security and operational efficiency.

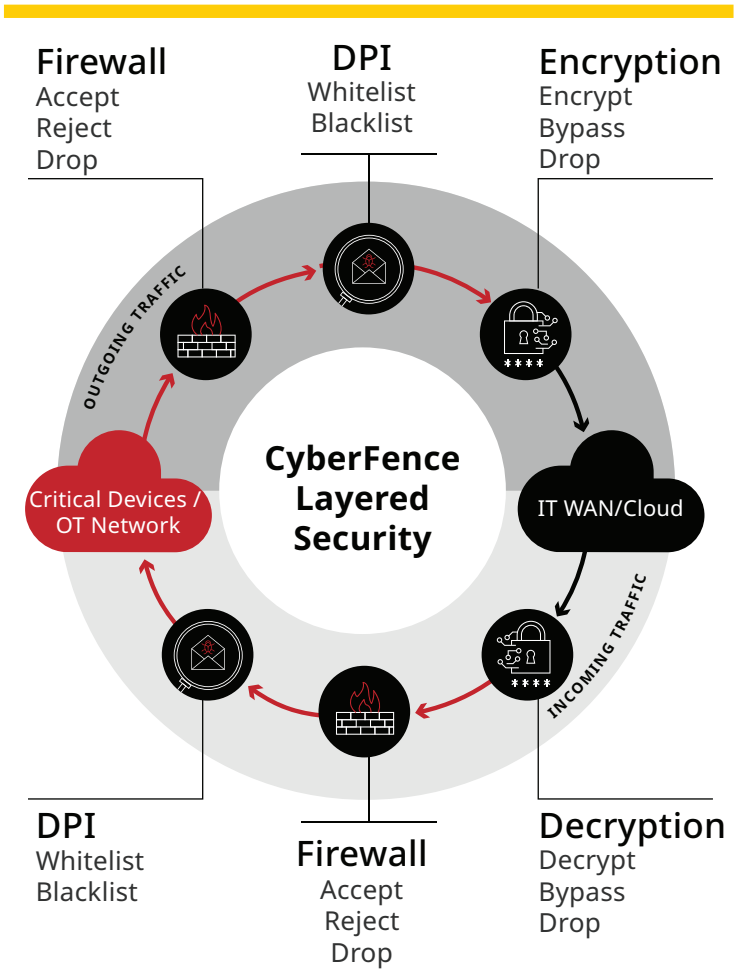
CyberFence: Enhancing security for critical infrastructure

As our world grows increasingly interconnected, preserving trust in the critical infrastructure systems that underpin modern society has become paramount. Operation technology (OT) networks often use standard protocols, such as BACNet, to communicate with other devices from different suppliers. These devices are often installed outside locked servers, outside buildings, and sometimes on poles — unsecured in remote areas that must withstand all weather environmental conditions. These physical security vulnerabilities are compounded by the real threat of a zero-day attack where small, latent defects within millions of lines of completely valid software code are exploited to inject malicious code, compromising data or operations. Despite the best security design, OT devices are still vulnerable and susceptible to exploitation from nefarious actors.

Ultra Intelligence & Communication's CyberFence solution provides sophisticated, layered security for critical infrastructure devices and their OT networks, incorporating the latest FIPS 140-3 standards. The device features robust encryption, firewall, and deep packet inspection (DPI) in a compact form factor. With power over ethernet (PoE) support, CyberFence is especially suited for use within industrial enclosures and network closets where space is at a premium.

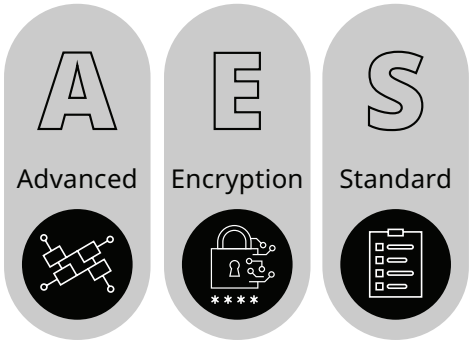
CyberFence detects and contains the impact of a compromised device through the following capabilities:

1. VPN/VLAN Encryption: CyberFence segments devices into separate networks or private clouds using encryption tunnels to guard against data compromise, as well as other computing resources from being monitored by pivot attacks.
2. Firewall: CyberFence's firewall detects and controls incoming commands and outgoing messages to only authorized source and destinations. Robust event reporting enables administrators to detect and respond.
3. Deep Packet Inspection (DPI): CyberFence inspects each message exchanged between authorized sources to ensure proper protocol usage and valid data.



Unlike IT environments with varied networking protocols, OT networks typically involve consistent communication between controllers and servers. Controllers generally complete the same commands daily, with changes only coming during special situations or specific operational goals. This behavior allows operators to effectively create endpoint and command whitelists that are relevant to their specific and respective process. Any manipulation of packet data by a compromised device is then detected and immediately reported. By understanding the nature of critical infrastructure devices, CyberFence independently locks down and secures the device communication channel —ulitmately limiting the impact of potential cybersecurity attacks.

Advanced security techniques



CyberFence protects data between the OT and IT network with layer 3 encryption using standard quantum-resistant, AES-256, IPSEC protocols to link to standard core and cloud VPNs. This ensures confidentiality as data is routed over untrusted public networks.

CyberFence also provides layer 2 encryption to ensure confidential communication within a local area network (LAN). This supports the benefits of dynamic discovery, broadcast messages, and non-standard IP messages to securely expand the LAN into multiple physical locations. When encrypting in layer 2 mode, CyberFence behaves as a “bump in the wire” for line rate encryption speeds and low latency. Without an assigned IP address, the device behaves like a layer 2 switch. Attackers monitoring the network cannot discover the device because it does not respond to network queries. The result is having security devices “hidden” in the network, making it much more difficult for would-be attackers to thwart the device.

In combination with deep packet inspection, (DPI), CyberFence’s firewall protects against new threats and zero-day vulnerabilities. The firewall filters communication by port, IP address and MAC address, allowing operators to limit which devices on either side of the encrypted tunnel may communicate. Prior to encryption, packets are inspected to ensure compliance with configured whitelist criteria. Violations are detected, blocked and reported. In combination with deep packet inspection (DPI), CyberFence’s stateful firewall protects against new threats and zero-day vulnerabilities.

CyberFence provides DPI for BACnet, Modbus TCP, OPC, EtherNet/IP and DNP3. Without DPI, any command conforming to the protocol’s standards can be sent to the controller, which will attempt to execute the received instructions. This vulnerability is particularly concerning in scenarios where malware transmits commands to upload new and potentially corrupted firmware, such as what occurred in the Hatman/TRISIS attack. Because firmware update commands are infrequently used, deploying solutions like CyberFence can effectively block such commands from being transmitted during regular operations. Consequently, operators would be promptly alerted if such a command is detected — enabling timely responses and mitigating potential security risks.

In addition, CyberFence monitors and records all unique commands in learning mode, bridging the knowledge gap for operators unfamiliar with packet-level commands. This automated process facilitates creation of a tailored ruleset for the industrial protocol, ensuring only validated commands are allowed, significantly enhancing security against protocol-specific attacks such as firmware manipulation. Learning mode alleviates operator burden of understanding commands at a packet level by automating the process and presenting a suggested command whitelist based on the traffic observed.

Integration and management

CyberFence is easily managed via web UI, SNMP, or Ultra I&C's Situational Awareness Management Software (SAMS). Alerts are sent via syslog for integration with any SIEM or syslog manager and are also available through SNMP v2/v3. Separate encrypted management tunnels may be configured to connect to a provisioning or management server, following manufacturing reset and power on allowing configuration and management from a single location. Additional management tunnels may be configured for timer server synchronization, LDAP certificate authentication, and SYSLOG ensuring CyberFence is ready to manage within any network infrastructure.

OT security solutions have traditionally concentrated on perimeter protection. Firewalls, data diodes and airgaps are great ways to thwart attacks on external-facing systems. However, the greatest and more frequent method of attacks come from within the network. A lack of monitoring and control, combined with social engineering, are the primary causes of attacks in critical infrastructure today. CyberFence affords operators the ability to be vigilant and monitor commands at the edge while providing a critical line of defense against potentially dangerous situations.

Conclusion

CyberFence stands out as a comprehensive security solution for OT networks, addressing both external and internal cybersecurity threats. Its sophisticated features, including advanced encryption, stateful firewall, and deep packet inspection, ensure robust protection of critical infrastructure. By facilitating seamless integration with existing systems and simplifying management, CyberFence significantly enhances the security and operational resilience of OT networks against evolving cyber threats.

ULTRA Intelligence & Communications

1094.1-REV0524