Forcepoint Critical Infrastructure Security

Securing the OT/IT boundary and beyond

Forcepoint

Brochure

forcepoint.com

Organizations that deliver the critical infrastructural services on which we all depend are constantly seeking ways to increase productivity, become more agile, accelerate innovation, and ultimately decrease cost and increase profits. But one of the biggest challenges they face in pursuing these goals is how best to defend against cyberattacks while still maintaining the system availability and integrity on which the business depends.

Cyberattacks on critical infrastructure are growing in frequency and potential severity. Whether it's Stuxnet using a combination of zero-day attacks on systems, or targeting industrial safety technology from automation and HVAC vendors, or Shamoon 3 targeting the oil, gas, energy, and telecom sectors across the Middle East and beyond. Defending against cyberattacks is a persistent challenge. Effective protection against these attacks requires flexible solutions that can adapt to their unique industrial contexts and challenges while being strong enough to keep out even the most persistent or advanced adversary.

Challenges for Secure Data Transfer

Critical infrastructure providers looking to ensure data integrity across distributed, air-gapped sites, meet regulatory/governance requirements, and deliver scalability by collapsing and simplifying the security infrastructure must find solutions to the following secure data transfer challenges:

Extracting data

One of the most common requirements at the IT/OT boundary is the need to extract historical data or logging information from the OT network for analysis in the IT network. Data travelling in this direction can be assumed to be "safe" and therefore the primary concern is to ensure that the communication channel itself cannot be used by an attacker to jump the electronic air gap and cross from the IT to the OT network.

Importing Software Updates

Another common requirement at the IT/OT boundary is the need to import software updates such as Windows/Linux updates and antivirus signature updates. A unidirectional gateway can provide an effective solution, ensuring that traffic can only flow in one direction between pre-configured update servers residing either side of the boundary.

Importing IT Files

The challenge of managing security at the IT/OT boundary becomes much more complex and nuanced when it comes to importing IT files (rich content of the kind used every day in the enterprise network) from IT to OT. Manuals, maintenance, and compliance documents contained in Office files, PDFs, and diagrams are all essential to the smooth operation of plant and machinery. However, this type of complex data is the carrier of choice for cyberattackers intent on getting malware in and establishing remote command and control channels.

Secure Monitoring in the Cloud

Managing OT networks and assets from the cloud, whether for the purpose of viewing historical data, or monitoring those assets in real-time or even remotely controlling them, delivers big business benefits. However, to enjoy these benefits, providers of critical infrastructure need to be certain the links between the OT network and the cloud monitoring platform cannot be used by an attacker to compromise the OT network and assets.

Ring Fencing the Enterprise

With the convergence of IT and OT, critical infrastructures is now a prime target for cyber attackers. The use of networked machines, automation, and IoT devices continues to grow but many of these devices were not designed with security as a key characteristic. Cybercriminals are keenly aware of this. Malware delivered into the IT network via Office documents, PDFs and images in email or web downloads is designed to compromise not only enterprise workstations but also to move laterally and "jump" the IT/OT boundary.

Forcepoint Critical Infrastructure Product Portfolio

Forcepoint provides a comprehensive portfolio of products designed to help providers of critical infrastructure meet these challenges:

Next-Generation Firewall

Forcepoint Next-Generation Firewall (NGFW), combines fast, flexible networking (SD-WAN and LAN) with industry-leading security to connect and protect people and the data they use throughout diverse, evolving enterprise networks. Forcepoint NGFW provides consistent security, performance, and operations across physical, virtual, and cloud systems. It's designed from the ground up for high availability and scalability, as well as centralized management with full 360° visibility.

Forcepoint Data Diode/ Unidirectional Gateway

Data Diode ensures secure one-way transfer with optical isolation, enabling organizations to create boundaries between trusted and untrusted networks by creating a physically secure one-way communication channel. Ideally suited to unidirectional protocols, Data diodes enable you to send data from one secure network to another; data is transferred using light instead of electrical signals, ensuring that data can enter but never exit.

Data Guard

Forcepoint Data Guard enables the bidirectional, automated transfer of highly complex data—including real-time streaming video across segregated networks. With deep content inspection and highly granular policy-based control over source, destination, and content, Data Guard is ideally suited to cross-domain data transfer and targets specific high assurance security requirements found in government environments.

High Speed Verifier

The Forcepoint High Speed Verifier (HSV) is a diode-based hardware solution designed for environments where bidirectional applications need to securely transfer data, such as OT monitoring in the cloud. The HSV combines multiple unidirectional diodes, protocol breaks, and integrity checks in a single unit. Data verification is enforced using hardware Field Programmable Gate Arrays (FPGAs) meaning the HSV cannot be remotely compromised by an attacker and Content Disarm and Reconstruction (CDR) can be optionally enabled. The HSV can be deployed to secure data transfer between OT and IT, IT and OT, and OT and the cloud.

Zero Trust Content Disarm and Reconstruction (CDR)

Forcepoint Zero Trust CDR works with the High Speed Verifier (HSV) to deliver 100% malware-free data without using detection. It works by extracting the valid business information from files, verifying the extracted information is well-structured and then building brand new files to carry the information to its destination. This unique zero trust approach is applied to all data, irrespective of whether it contains a threat or not. It renders IT files such as Office and PDF documents and images threat-free. It can also be applied to the web application traffic typically used to monitor OT networks in the cloud.

Forcepoint Insider Threat (FIT)

Forcepoint Insider Threat has been identifying and stopping threats from within for government and Fortune 100 customers for more than 15 years. With more than 1 million endpoints deployed, Forcepoint Insider Threat's proven solution protects some of the most sensitive organizations on the planet. One Fortune 100 retail client realized 60% ROI in the first year of deployment. Insider Threat empowers your organization, saving your team time and effort by automatically scoring and prioritizing your riskiest users, reducing the need to dig through thousands of alerts. This frees your team to focus on high-priority tasks and improves efficiencies. Forcepoint Insider Threat also provides the context and forensic evidence needed for undeniable attribution and chain of custody–simplifying investigations, prosecution, and compliance.

Solution Summary

SCENARIO	REQUIREMENTS	CONSIDER THESE SOLUTIONS
Extracting data from OT into IT	Secure and reliable data transfer with no data loss. Communication channel cannot be used by an attacker as a back link into the OT network.	• Data Diode or High Speed Verifier with Zero Trust CDR • NGFW
Importing software updates from IT into OT	Secure and reliable data transfer with no data loss. Communication channel cannot be used by an attacker to get malware into the OT network or exfiltrate data out.	• Data Diode or High Speed Verifier with Zero Trust CDR • NGFW
Importing IT files into the OT network	High assurance that files coming into the OT environment are malware-free and cannot be used as a vector for attacking the OT network, plant, and assets.	• High Speed Verifier with Zero Trust CDR or Data Guard • NGFW
Monitoring OT networks from the cloud	Secure and reliable data transfer with no data loss. Support for bidirectional Web application protocols with the same levels of assurance as if the communication channel was unidirectional and enforced in hardware. Constraint of the application data to pre-defined schemas to ensure it cannot be used to attack the OT network, plant, and assets.	• High Speed Verifier with Zero Trust CDR • NGFW
Ring-fencing the enterprise	A zero-trust security posture for all inbound content arriving at the enterprise network.	• High Speed Verifier with Zero Trust CDR • NGFW

forcepoint.com/contact

About Forcepoint

Forcepoint simplifies security for global businesses and governments. Forcepoint's all-in-one, truly cloud-native platform makes it easy to adopt Zero Trust and prevent the theft or loss of sensitive data and intellectual property no matter where people are working. Based in Austin, Texas, Forcepoint creates safe, trusted environments for customers and their employees in more than 150 countries. Engage with Forcepoint on www.forcepoint.com, Twitter and LinkedIn.