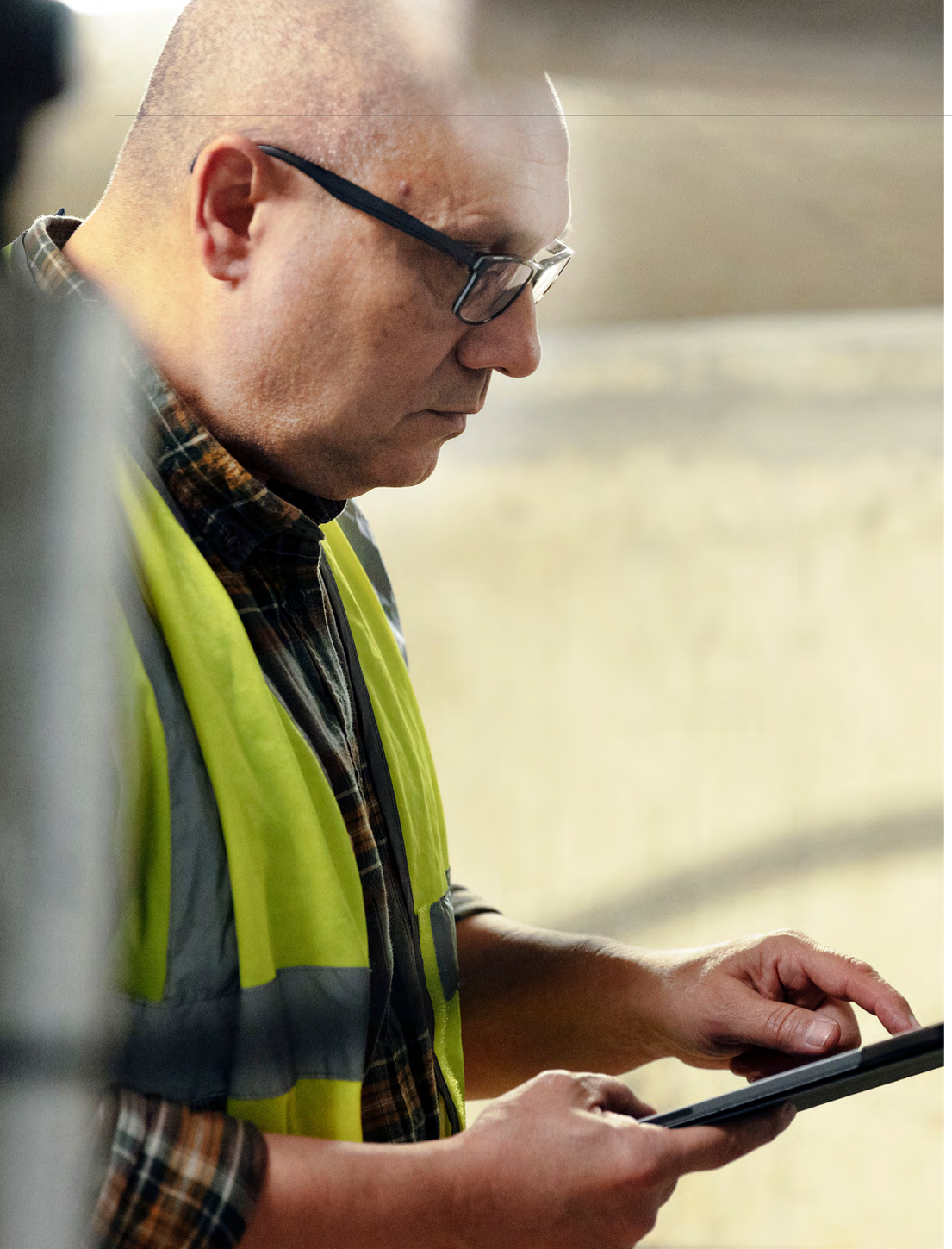


Forcepoint

Securing Critical Infrastructure from Cyber Attack

Implementing Zero Trust Security at the IT/OT Boundary and Beyond

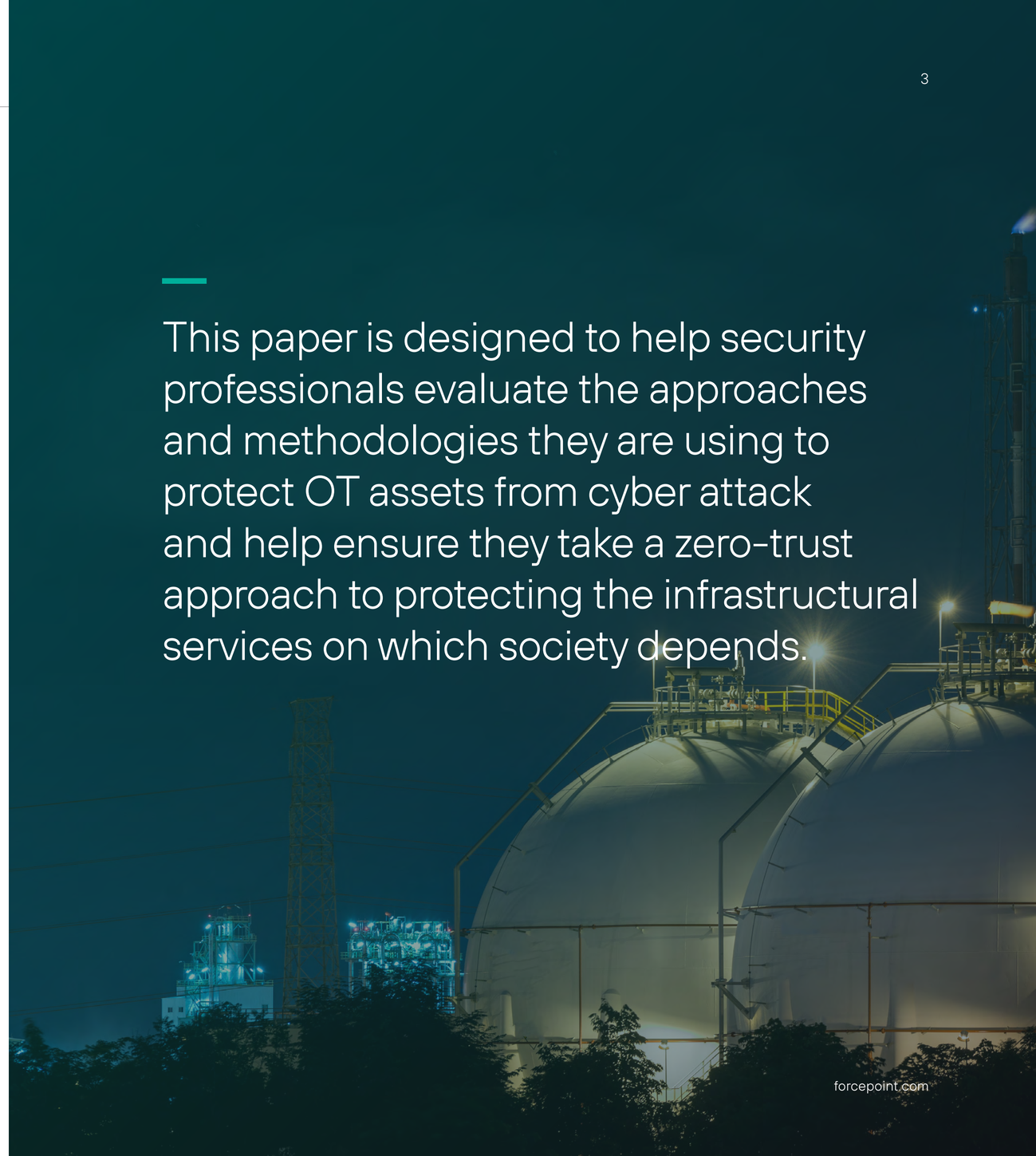
Table of Contents

Executive Summary

Like all other industries, critical infrastructure has benefited from digital transformation and the move to Industry 4.0. The benefits of this interconnectivity are game-changing. However, with benefits come risks.

There is a long history of attacks against organizations that deliver critical infrastructural services, and these are becoming more frequent, sophisticated, and targeted. Barely a week passes without news of a new attempt by cyber attackers to compromise critical infrastructure. From major ransomware attacks to attempts to penetrate industrial networks and directly target operational technology (OT), critical infrastructure is in the cross hairs.

This paper is designed to help security professionals evaluate the approaches and methodologies they are using to protect OT assets from cyber attack and help ensure they take a zero-trust approach to protecting the infrastructural services on which society depends.

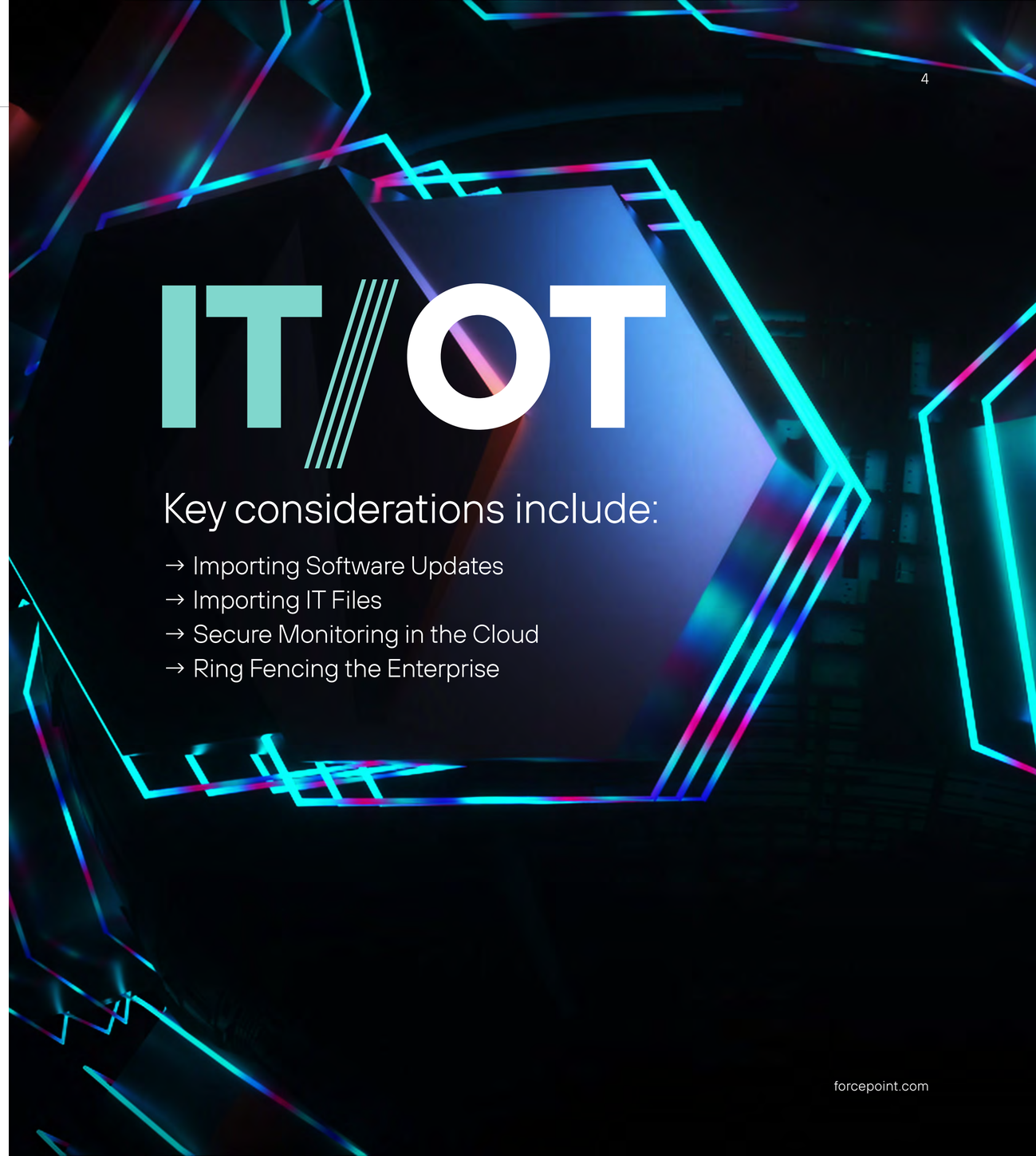


Key Considerations

Traditionally, the communications channel between the enterprise network (IT) and the operational network (OT) has been seen in cyber security terms as the organizational Achilles Heel.

In times past, a physical air gap was considered the only way to mitigate the risk of an attack crossing the zone from the Enterprise or IT network, penetrating the operational technology (OT) network and threatening the availability of critical service provision.

Today, a number of different approaches can be used to defend this boundary and deal with the increasing requirement to protect the OT network.



Importing Software Updates

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

However, this approach comes with a particular set of challenges. Using a traditional data diode to enforce a unidirectional data flow in hardware, how can you be certain that all the software updates downloaded onto the IT network update server arrive—intact and in order—onto the corresponding update server on the OT network?

A further concern with importing files from IT into OT is that a traditional data diode does nothing to check the content being imported is threat-free, it merely stops the path being used by an attacker to get reconnaissance information back out.

REQUIREMENT

Import updates reliably from IT into OT with high assurance that the import mechanism cannot be used by an attacker to get malware in to the OT network or exfiltrate data out.

Targeting ICS

EKANS encrypts files in IT systems and demands a ransom from the victim. The malware also can kill Industrial Control System (ICS) processes on infected hosts. It is thought to be the first public example of ransomware that can target ICS operations.

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 plants and machinery. However, this type of complex data is the carrier of choice for cyber attackers intent on getting malware in and establishing remote command and control channels. Sadly, detection-based antivirus all too often fails to detect malware concealed in this way, and for providers of critical infrastructural services, another solution—one that provides very high levels of assurance that there is no malware present—must be found.

This challenge is further compounded by the fact that most modern application protocols are inherently bidirectional, a characteristic that makes it difficult to implement reliably over a traditional unidirectional communication link such as a data diode.

REQUIREMENT

Ultra-high levels of assurance that IT files are malware-free and cannot be used as a vector for attacking the OT network, plant and assets.

Support for bidirectional protocols with the same levels of assurance as if the communication channel was unidirectional and enforced in hardware.

Power Outages

An attack on the Ukrainian electric grid in 2015 resulted in power outages for over 225,000 people and forced systems to failover to manual operation following the delivery of malware via macro-embedded Microsoft Office documents delivered via email into the IT network.

Secure Monitoring in the Cloud

Managing OT networks and assets from the cloud, whether for the purpose of viewing historical data, monitoring those assets in near 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.

Many modern monitoring applications use bidirectional IT and OT protocols such as HTTPs, OPC and MQTT to communicate between the OT network and the cloud monitoring platform. These protocols carry monitoring data encoded in a format such as xml or json.

On its own, a data diode won't check or constrain this data leaving the OT network open to attack if a threat actor is able to compromise the communications channel.

REQUIREMENT

Ultra-high levels of assurance that Web application data being carried between OT network and cloud monitoring platform cannot be used as a vector for attacking the OT network, plant and assets.

Support for bidirectional protocols with the same levels of assurance as if the communication channel was unidirectional and enforced hardware.

Water Woes

A hacker used a remote management tool to gain access to the Oldsmar water supply OT network and only vigilance on the part of personnel at the site prevented the supply being contaminated with potentially lethal levels of caustic soda.

Ring Fencing the Enterprise

With the convergence of IT and OT, critical infrastructure 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. Indeed, by 2025, Gartner predicts that cybercriminals will be able to weaponize OT environments to successfully harm or even kill people.

Traditionally, attacks on critical infrastructure and specifically on industrial control systems were delivered via removable media such as USB drives, in acknowledgement of the fact that most of these environments were "air gapped" from IT networks.

IT/OT convergence has changed the rules of engagement. 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 to move laterally and "jump" the IT/OT boundary.

REQUIREMENT

A zero-trust security posture for all inbound content arriving at the enterprise network, whether via email, Web, file upload, removable drives, or social media.

Ransomware

Colonial Pipeline paid $4.4m to a gang of hackers who broke into its computer systems. After it learned of the ransomware attack, the company took its pipeline system offline and needed to do everything in its power to restart it quickly and safely.

Forcepoint's Critical Infrastructure Advantages

Forcepoint technologies enable the sharing of information between OT and IT as well as between OT and the cloud, without creating untenable, unnecessary risk.

Network Segmentation and NGFWs

Forcepoint employs network segmentation to make it difficult for adversaries to gain access to networks and steal critical data. Network segmentation physically separates computer networks, so that each network is visible only to users who have the appropriate access rights and is not visible to unauthorized users.

The 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.

Unidirectional Gateways (Data Diodes)

The Forcepoint Data Diode ensures secure one-way transfer with optical isolation, enabling organisations 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.

High Speed Verifiers (HSVs)

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 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.

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.

At a Glance

Scenario	Requirements	Consider These Solutions
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 Guard → 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.	→ Data Guard → High Speed Verifier with Zero Trust CDR → 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.	→ Data Guard → 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.	→ Data Guard → High Speed Verifier with Zero Trust CDR → NGFW

Forcepoint

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.