TELOS GHOST®

Critical Infrastructure Protection

Hide your crown jewels so the cybercriminals can't see them.

The best way to ensure the security of your IT/OT networks and their resources is to hide them from view.

Organizations in critical infrastructure rely on operational technologies such as SCADA, ICS, WSANs, industrial IoT, and others to manage and optimize their industrial processes. Yet these OT systems are at greater risk now that they are increasingly connected to the internet and to enterprise IT networks. Breaches across critical infrastructure sectors are a near-weekly occurrence. When their operations have to shut down even briefly, it can jeopardize economic stability and even national security:

Energy – a ransomware attack on the IT network of the U.S.'s largest petroleum pipeline prompted them to shut down their OT network as a precaution, disrupting fuel supplies in the eastern U.S. for several days.

Water – an intruder remotely accessed a computer for a Florida city's water treatment system and attempted to raise levels of lye in the water supply by a factor of more than 100.

Dams – foreign agents broke into the SCADA system of a flood-control dam in New York, obtaining information about water levels and temperature and gaining adequate access to remotely operate its sluice gate.

Food Supply – the world's largest meat supplier closed processing plants in Australia, Canada and the U.S. following a ransomware attack that took down systems critical to the management of its global supply chain.

Communications – hacktivists broke into a leading video surveillance network, enabling them to obtain access to broader networks and hijack the cameras as a platform to launch further attacks.

Transportation – Hackers with suspected ties to a foreign government breached the transit authority of the largest city in the United States, exploiting a zero day vulnerability to gain access to their networks.

The rapid growth in always-connected controls and devices has increased the risk to critical infrastructure because they act as beacons to cyber criminals bent on exploiting vulnerabilities to gain access to "crown jewels" such as logical assets, critical data, and control interfaces. It is becoming more evident that these critical assets need to be totally hidden from the public internet and within enterprise networks. If cyber criminals cannot see the network resource, it is protected from attack.

27% of industrial sites have at least one direct connection to the public internet, and 54% have at least one remotely accessible device.
CyberX 2020 Global IoT/ICS Risk Report

By cloaking sensitive OT assets in the digital domain, critical infrastructure can keep these systems from being seen or exploited even by bad actors who have penetrated the enterprise network. And, these organizations can also mitigate risks to the OT side by using network obfuscation techniques to protect vital resources on the IT side. The harder it is to find and exploit essential assets on the enterprise network, the greater protection for a converged IT/OT environment.

Anonymity, obfuscation, cloaking — these capabilities enable you to protect your operational network and assets while also protecting users who need to access sensitive resources and systems in the course of their work.

The Solution: Telos Ghost for Critical Infrastructure Protection.

Telos Ghost® is an end-to-end security solution that addresses the complexities and performance challenges facing critical infrastructure networks. The lightweight

Key capabilities

- Web Access
- Private Networks
- Cloaked Services

Telos-patented methodologies

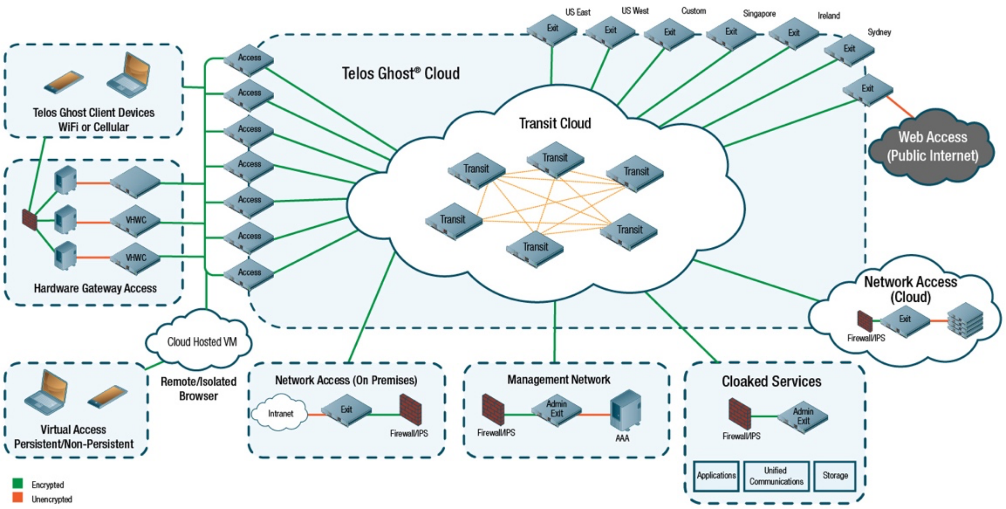
- Secure Geo-location
- Secure Obfuscation
- SIP Diverter

Key network components

- Access Methods
- Transit Cloud
- Exit Options

Offerings

- Shared Network
- Hybrid Network
- Dedicated Network



footprint of Telos Ghost and its worldwide availability and ability to secure existing communication pathways and digital resources make it the perfect solution to tackle the ever-increasing challenges facing high-risk organizations and their networks.

Telos Ghost hides OT/IT network resources, whether they are end-user devices, sensor, servers, IoT devices, or entire network enclaves. Network obfuscation techniques that eliminate cyber-attack surfaces ensure the most critical assets are hidden from the public internet.

- Offers privacy and security for worldwide communications and transactions over the internet
- Supports network segmentation to cordon off your most critical assets with end-to-end private network connectivity -- in the cloud or on-premises
- Disguises and obscures traffic with multiple layers of encryption and dynamic IP routing across hidden network nodes
- Makes connections to remote workers invisible for confidential communication from the field
- Hides secure unified communications (voice, video, text), email, storage, and applications within the network for ultimate protection

Contact us for more information about Telos Ghost.

Telos Ghost provides obfuscation and managed attribution for totally secure and anonymous communications for private network access, web access, and mobile communications.

If you would like further information or a demonstration of the capabilities of Telos Ghost, please contact Telos Sales at 1-800-70-TELOS or at sales@telos.com.

Learn more at www.telos.com/telos-ghost

Telos® Solutions that **empower** and **protect** the enterprise.™

info@telos.com | 800.70.TELOS (800.708.3567)
www.telos.com | twitter.com/telosnews
facebook.com/teloscorporation
linkedin.com/company/telos-corporation

Telos Corporation | 19886 Ashburn Road, Ashburn, VA 20147-2358 |
1.800.70.TELOS | 1.800.708.3567 | Fax 703.724.3865 | www.telos.com
Telos Ghost CIP 02-2022