The Chicken or the Egg: Securing converged IT/OT in critical infrastructure

The convergence of IT and OT means that critical infrastructure organizations have to solve for two distinct security problems at once. How can they maintain security and availability in both technology environments?

Over the past decade, as information technology (IT) and operational technology (OT) have converged, critical infrastructures has been left more vulnerable to attackers than ever before. The emergence of digital transformation hastened this trend, and today it would be difficult to assert that an organization's OT systems are air-gapped or otherwise secure against connectivity to the public internet.

This puts infrastructure operators in a difficult situation. They have two completely different types of technology to protect, each with its own business priorities and security vulnerabilities. And while it's hard to hire good cybersecurity staff for IT and even harder to hire experts in OT security, finding people who are knowledgeable in both is a unicorn hunt. With hyper-connected IT offering new points of entry to attackers while OT security trails its enterprise counterpart by a decade or more, critical infrastructure operators need to understand the vulnerabilities introduced by convergence and look beyond traditional cybersecurity to protect their operations.

71%

of cybersecurity professionals won't work on industrial networks.

— Security Magazine

The perception of safety is a vulnerability.

Organizations have done what they can to secure their environments, and that usually means they've segmented the networks with firewalls. But segmentation is not a one-and-done effort — it atrophies over time as new devices and connections are stood up and as misconfigurations and conflicting policies are unknowingly introduced. Critical infrastructure operators can patch their IT systems, but they can't shut down their plants to upgrade their OT — and few could say with confidence that they even have the ability to discover and secure every sensor or other device on their infrastructure in order to secure it.

Top Cybersecurity Challenges for Critical Infrastructure

- Exposure of legacy technology to internet
- Lack of holistic security that covers OT and IT
- Traditional cybersecurity tools do not protect OT

63%

of US IT security professionals expect a major cyberattack to be successfully carried out on national infrastructure within the next five years.

— Security Magazine

Half-secure is not secure.

CISOs are not usually responsible for implementing OT security or making sure security standards are being met at the plant level. That leaves the plant vulnerable, as the people who implement and manage OT security controls are not accountable to the CISO and may not be aware of what's happening in the IT estate. OT technologists should know about every new device, API, third-party software, or vendor that's being added to the network and what possible vulnerabilities each change might introduce. But since it can be difficult to gain total visibility into and management over the asset inventory of OT/IoT environments, many are unable to take the actions needed to harden OT against possible threats incoming from the IT estate.

A different way to secure your IT and OT environments: Network obfuscation from Telos Ghost.

Network obfuscation hides your assets from the internet. Attackers who are seeking a way into your network can't find your weak spots because they can't find you at all.

Proven in the toughest environments — the military and intelligence communities have been using its network obfuscation capabilities for years — Telos Ghost is now available to critical infrastructure organizations to help them secure their most valuable assets without having to harden every device or connection on their massive infrastructures.

How network obfuscation works.

Network obfuscation hides servers, applications, and unified mobile communications from the network and erases digital footprints so attackers can't follow them back to the targeted organization.

This is a different approach from traditional cybersecurity, which focuses on protecting the enterprise and its endpoints, firewalls, and applications. Instead, network obfuscation focuses on the internet itself.

Network obfuscation protects traffic with multiple layers of encryption, eliminates source and destination IP address information, sends traffic through complicated routes, and conceals details associated with users, devices, files, locations, network pathways, and more.

As a result, unauthorized users cannot identify a target based on network-defined or static identity information or understand the nature of the organization's communications. Your environment remains invisible, even to those who are actively trying to find your specific network.

Security without downtime is a reality with Telos Ghost.

Telos Ghost is a robust, scalable, secure communications network-as-a-service that privatizes the public internet to hide network resources and mask the identity and location of users to ensure total protection as they interact with the operator's network.

Telos Ghost uses network obfuscation, multiple layers of encryption, and proprietary-based mesh algorithms to dynamically route IP traffic among cloud transit nodes. Advanced managed attribution makes users and their locations completely anonymous, which is a particularly compelling case for critical infrastructure operators conducting energy exploration, interacting with third-party suppliers and distributors, or communicating with remote workers.

To learn more, please contact us.

Ken Michaels
ken.michaels@kttechnologies.net
https://www.kttechnologies.net

publication number: 5690-0622-B