Unseen is Unhacked: Network Obfuscation and Healthcare IT

Whatever security you apply to your healthcare information systems, you need more for your crown jewels.

The state of healthcare IT is split between the cutting edge and the antiquated. Internet-connected telemedicine and Internet of Medical Things (IoMT) devices uneasily coexist with legacy billing and procurement systems designed to contain large proprietary databases on-premises. Healthcare CISOs and CTOs have to run cybersecurity programs that protect against the vulnerabilities of 20 years ago and those of the next five years in one budget.

Hackers hunt for legacy systems.

The legacy billing and procurement systems that remain in use were designed before cybersecurity was the threat it is today, and before the cloud and APIs turned the world into one giant computing system. These backend systems have been integrated using third-party solutions, and while this approach improves interoperability, it does so at the expense of security. Integrating a legacy system creates holes that hackers look for as easy points of ingress.

80% of healthcare organizations are still using legacy systems vulnerable to ransomware threats.

2020 HIMMS Cybersecurity Survey

How old is your billing system?

Back-end systems aren't the only old technology endangering healthcare. Fifty-six percent of workstations on the hospital floor are using outdated operating systems, mainly Windows 7. Replacing them would be costly, but leaving them as they are could be worse. The FBI warns that hackers are developing targeted malware and malware-less techniques to specifically exploit these old systems—so just one computer running an obsolete OS makes the entire network vulnerable to a sophisticated targeted attack.

IoMT: Good for patients, good for hackers.

On the other end of the innovation spectrum are the thousands of devices in use in hospital systems today, such as patient wristbands, crash cart trackers, and wearable biosensors. Attackers have already used these devices to conduct a multitude of attacks, including rogue access attacks, in which the adversary installs a forged gateway that lets them intercept traffic undetected, denial-of-service attacks that disrupt availability, and SQL injection attacks that can introduce malware, compromise PII, or modify data. A lack of rigorous authentication practices, weak and default passwords, and embedded web servers make these devices excellent tools for malicious actors.

The number of healthcare breaches increased 55% from 2019 to 2020; the average time to recover was 236 days.

Bitglass Healthcare Breach Report 2021

One network, many vulnerabilities.

All these devices typically exist on the same unsegmented VLANs. One researcher found vending machines on the same VLANs as critical medical devices. It would certainly be feasible to hack into one of those vending machines and hop across the healthcare network to a medical device or an EHR repository. On a more mundane level, assets on these unsegmented VLANs have different patching and upgrade requirements, so managing them creates IT bottlenecks and oversights that endanger the organization and increase its operating costs.

The Eastern European ransomware group Ryuk has hit at least 235 U.S healthcare facilities, taking in more than $100 million.

The Wall Street Journal

Healthcare CTOs and CISOs are under pressure from every direction: a complex infrastructure that's hard to manage, an environment that's a prime target for attackers, and an end user population that isn't security-aware. It's enough to make a technology leader wish they could take their critical assets off the internet entirely.

And now, they can —— virtually.

If You Can't Make It Infallible, Make It Invisible with Telos Ghost.

Telos Ghost uses network obfuscation to hide critical assets from the internet, minimizing the risk of ransomware attacks, IP theft, and exfiltration of PII. So while these assets remain fully accessible to authorized users, malicious actors won't even know they exist.

Telos Ghost hides servers, applications, and unified mobile communications from the network, so even if attackers were able to enter parts of the environment through a patient wristband, stolen laptop, or firewall misconfiguration, they wouldn't be able to find the healthcare organization's crown jewels.

Proven in the toughest environments — the military and intelligence communities have been using it for years — Telos Ghost is now available to help healthcare organizations secure their most valuable information without having to harden every endpoint on their massive infrastructures.

Telos Ghost hides your crown jewels from prying eyes.

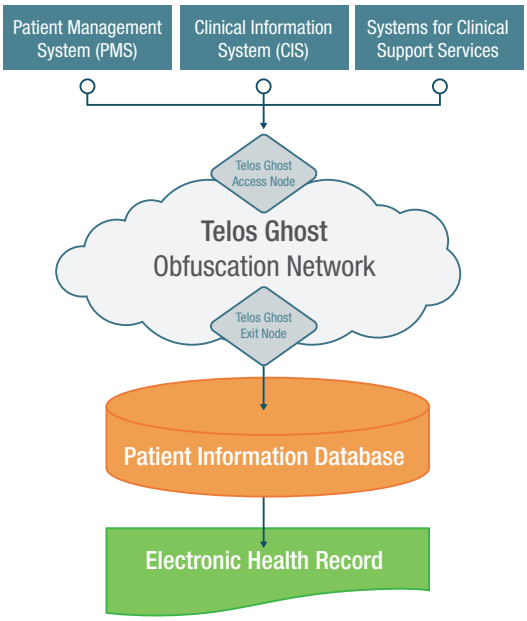
Telos Ghost is a robust, scalable, secure communications network-as-a-service that privatizes the public internet to hide network resources and masks the identity and location of users to ensure total protection as they interact with the healthcare network.

Telos Ghost uses multiple layers of encryption and proprietary mesh algorithms to dynamically route IP traffic among cloud transit nodes. Advanced managed attribution makes users and their locations completely anonymous. Together, these capabilities provide additional layers of robust security for the crown jewels in healthcare and life sciences.

Electronic health records – E-health records are composed of patient information from a variety of sources — patient management systems, clinical information systems, and clinical support service systems. Each creates attack surfaces that can be exploited for access to the connected patient systems and even the hospital information system. Telos Ghost can make the patient information database invisible and inaccessible to unauthorized users.

Connected medical devices – A 2019 report estimated there were between 10 million and 15 million connected medical devices in U.S. hospitals, creating an almost infinite number of entry points into the network. Sheathing your network of connected medical devices within the Telos Ghost network ensures that only authorized users can access them for diagnostic or maintenance purposes.

Telemedicine and remote healthcare – The rapid expansion of telemedicine in the pandemic era exponentially increased the cyber attack surface for healthcare organizations, leading to breaches of patient data and compromised privacy. Telos Ghost enables healthcare organizations to hide telemedicine communications from view, including video streams, PACS images, and other records needed for remote healthcare.



A notional view of how Telos Ghost protects critical assets such as electronic health records within its obfuscation network, making them invisible to unauthorized access.

Pharma and life sciences research – Research is the lifeblood of pharmaceutical makers, university hospitals, and related organizations. They are prime targets for hackers, whose attacks result in stolen intellectual property, loss of revenue, loss of federal contracts, and repeated clinical trials. Telos Ghost protects the researchers and their data in transit and at rest, making researchers invisible as they work online and hiding the results of their work in cloaked servers for authorized access only.

For more information about how Telos Ghost protect the critical assets for your healthcare or life sciences organization, please contact us.

Telos®

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

Telos Corporation | 19886 Ashburn Road, Ashburn, VA 20147-2358 | 1.800.70.TELOS | 1.800.708.3567 | info@telos.com | www.telos.com