UNISYS | Securing Your Tomorrow®

TELEHEALTH IS HERE. MAKE IT SECURE.

Unisys Stealth® for Telehealth

HIGHLIGHTS

- *Telehealth to experience massive growth with COVID-19 situation*
- *Frost & Sullivan forecasts a sevenfold growth in Telehealth by 2025 – a five-year CAGR of 38.2%*
- *Users accessing health care systems through multiple endpoints and external networks contribute to an expanding attack surface*
- *A Zero Trust Model that trusts no user or device, on the inside or outside, only granting least-privilege access upon reliable identification is the need of the hour*
- *Partner with Unisys for a start to finish roadmap to successfully develop your Zero Trust Model*
- *See, Segment and Secure with Stealth, Unisys' award-winning security solution*
- *Eliminate VPN and remote access vulnerabilities and gain operational agility fast while containing risk*

Ready or Not, Telehealth Is Here to Stay

Healthcare was already the most breached industry when the pandemic caught everyone off-guard and forced the hand of many healthcare providers, ready or not, to turn to Telehealth. Virtual doctor visits went from about 12,000 a week to more than a million a week. Demand for Telehealth is predicted to soar by 64.3% in the U.S. in 2020.

Hackers are taking full advantage of the chaos. As healthcare organizations rushed to protect the health of their workers and patients by providing remote access, security protocols sometimes went by the wayside even while the attack surface was expanding and opening gaps. With stolen medical records going for $1,000 on the dark web, and rampant insurance fraud from healthcare records theft, Telehealth providers can expect constant bombardment from cybercriminals around the world, constantly scanning the internet for an open port or a compromised device.

The explosion of Internet of Medical Things (IoMT), like at home monitors and remote-care devices, creates a target-rich environment as many IoMT devices lack embedded security and are thus vulnerable to intrusion and possibly granting intruders access to the wider healthcare network. Healthcare-related organizations are also a favorite target of ransomware attacks, with IT systems paralyzed at major hospitals, clinical testing labs, vaccine researchers, medical labs, urban care centers, and even small physician offices.

Even before the pandemic, traditional security measures were losing the battle against cyberattacks on dynamic networks. Static security controls are not only difficult to manage, update and operate, but they raise the cost of security and compliance and constrain agility. The remedy? A Zero Trust Model that trusts no user or device, on the inside or outside, only granting least-privilege access upon reliable identification.

Your Telehealth Needs Security Health Like Never Before

Stealth™, Unisys' award-winning security solution, is the only solution that can see, segment, and secure your entire infrastructure. Out of the box. In minutes. No new hardware, no disruption to your operations. Just a simple overlay of your current IT environment.

Stealth can immediately secure your network and data by:

- Reducing hackers' attempts on your organization by cloaking your endpoints
- Minimizing the impact of any intrusion by instant detection and isolation
- Securing remote access with identity management and encryption
- Assessing your cyber risk and recommending treatments
- Ensuring compliance with privacy/security regulations

Build a Zero Trust Network

Stealth reduces risk by creating dynamic, identity-based microsegments called Communities of Interest (COI), permitting communication only when COI membership is confirmed. Stealth separates trusted systems, users, and data from the untrusted. It encrypts all communication between Stealth-protected assets, cloaking them from unauthorized users and preventing ransomware attacks and IoMT security failures.

Enable Dynamic Isolation

Stealth dynamically isolate devices and users at the first sign of compromise (in less than 10 seconds) enabling immediate action in response to security incidents and stopping attacks in progress.

Decrease Network Complexity and Costs

A software-only solution, Stealth is easy to use and deploy, requires no changes to your existing network or applications and allows you to reduce complexity, expense and operation of static security controls in your dynamic organization. A reduced attack surface limits the regulatory audit footprint for lower compliance costs.

Automate Security Deployment

An expanded suite of standardized tools enables unattended automated installation. They eliminate the need for repetitive and manual operations, reducing installation time and improving management capabilities.

Adapt With Flexible Protection

Stealth enables uniform security policies across a range of endpoints and workloads, including physical servers, virtual machines, Operational Technology (OT) and purpose-built devices. You can deploy Stealth incrementally and scale it efficiently using rich APIs and automation.

Healthcare Innovator

In 2018 The Philadelphia Business Journal recognized *Stealth* and *Unisys* with its *Healthcare Innovator of the Year Award* for identity-based, encrypted microsegmentation to protect IoT and connected medical devices.

CASE STUDY

To Make Stealth Ready for Your Healthcare Enterprise, We Stealth-Secured Our Own First

We started with Stealth, transforming our network into a Zero Trust Network – so transparently that our users were unaware of it. We moved data to the cloud, cloaking our presence there with Stealth. We installed Stealth on all of our ~19,000 Unisys workstations, with the goal of eliminating VPN use. We also enabled dynamic isolation to detect and quarantine compromised users and devices in just seconds.

The value we reaped is available for your Telehealth needs:

- Your core health systems cloaked from hackers
- Your public cloud workloads hidden from other tenants
- Give users limited access to the targeted application only, without exposing the entire system
- Confidence that your network is not exposed to damage from error or malicious intrusion
- A vastly improved end user experience
- Assurance you are in full compliance with security regulations, avoiding costly fines and reputational loss
- Fully prepared for the future, whatever it brings in the way of cybersecurity threats

Contact us today at Stealth@unisys.com
Visit us at www.unisys.com/stealth