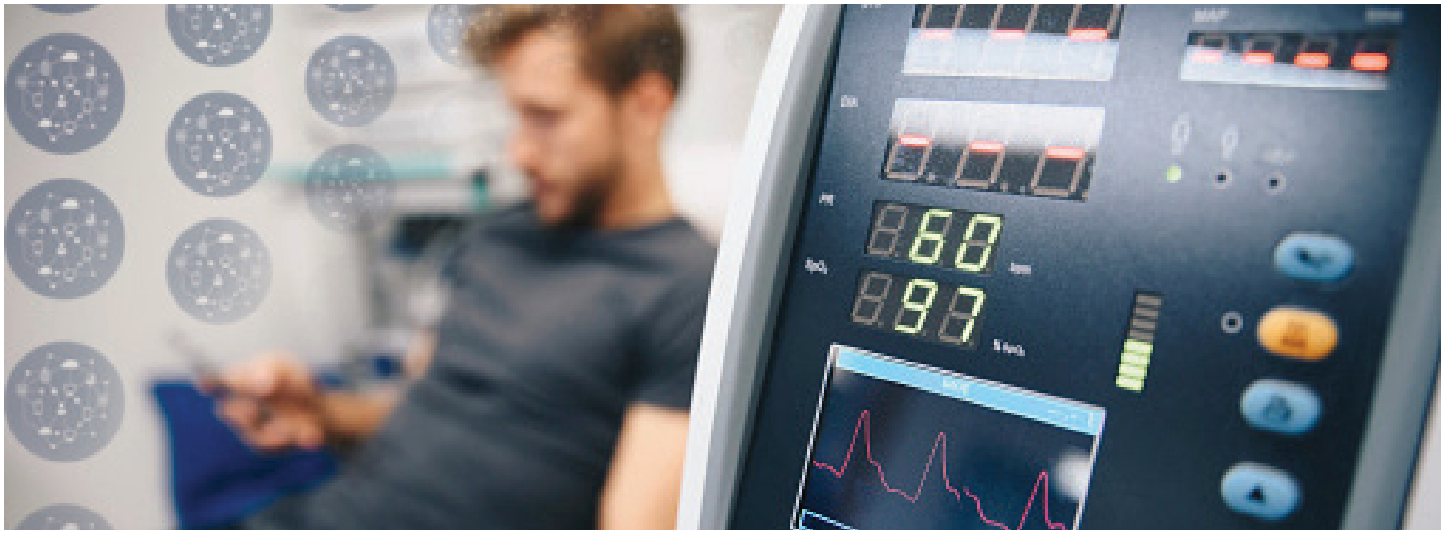
STEALTH™

Stealth(core) Smart Wire Capability for IoT

Reduce Attack Surface with Additional Security Controls



Connected Devices Create New Threat Vectors

We live in an increasingly connected world. Organizations across industries and governments are leveraging connected devices—such as surveillance cameras, baggage scanners and medical devices—to not only improve productivity and gain operational efficiency, but also collect critical data.

Like any other connected system, these devices are vulnerable to security breaches. Proprietary platforms, legacy software, lack of resources and delayed industry regulations often prohibit security changes to the devices themselves, limiting organizations to the built-in capabilities from device manufacturers. As security needs evolve or vulnerabilities are discovered, replacing non-compliant devices becomes costly and inefficient.

Organizations leveraging IoT devices need additional security controls to reduce the attack surface and contain breach impact. The solution must be scalable, cost-effective and rapidly deployed, without disrupting the network or requiring modification to existing hardware or software embedded in devices.

Unisys Stealth® offers a capability called Smart Wire for installation on a virtual machine or IoT gateway that connects to IPv4 based wired IoT devices, extending protection with microsegmentation.

Microsegmentation Secures Devices Without Modification

Stealth™ increases the security of IoT devices by isolating them with microsegmentation. The software acts as a liaison between the devices and a Stealth-protected network to prevent intrusion and remote tampering. By joining Stealth-defined secure communities of interest (COI), high-value IoT devices are shielded from unauthorized access, reducing the attack surface.

Stealth enables you to:

- Secure devices where Stealth cannot be installed
- Protect the network from compromises initiated through unsecured devices
- Seamlessly install, configure and manage Stealth with no hardware or software changes required to devices
- Encrypt data-in-motion from the IoT gateway to remote, Stealth-protected workloads

Use Case | Healthcare

Protecting patient health and information

CHALLENGE | Securing connected medical devices

Connected medical devices, such as monitoring equipment and IV pumps, deliver critical patient care and improve healthcare provider productivity through automatic data transfer to electronic health record (EHR) systems. They also increase the attack surface, as built-in security may not prevent threats from entering devices and moving throughout the network.

SOLUTION | Isolating critical assets

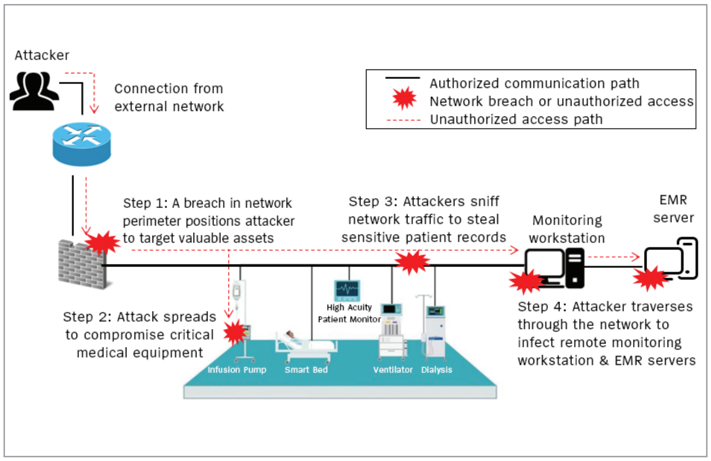
Deploying Stealth on edge gateways in patient rooms to connect medical devices enables:

- Stealth microsegmentation to isolate EHR servers
- COI among devices connected to a gateway, providing access to authorized users via remote workstations
- Encrypted data-in-motion from Stealth installed on VM or IoT gateway all the way to EHR servers

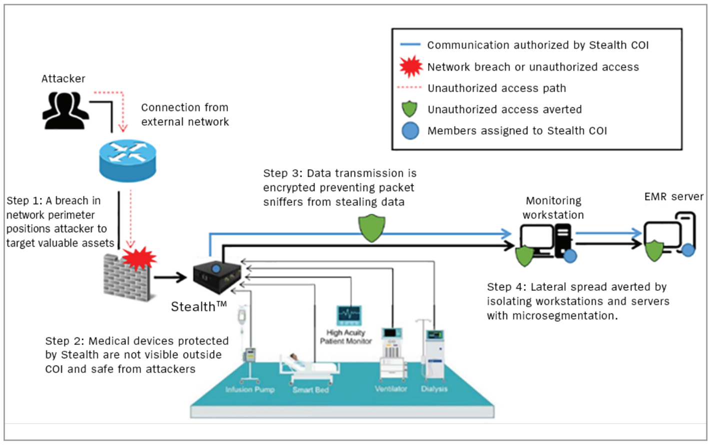
RESULT | Minimizing impact of security breaches

With Stealth microsegmentation protection, you can:

- Prevent and contain unauthorized access to medical devices and patient data
- Enable secure, real-time data flow from devices to EHR system
- Reduce cost of compliance with flexible security controls
- Protect patient care and information from security breaches


Attacker
Connection from external network
Authorized communication path
Network breach or unauthorized access
Unauthorized access path
Step 1: A breach in network perimeter positions attacker to target valuable assets
Step 3: Attackers sniff network traffic to steal sensitive patient records
Monitoring workstation
EMR server
Step 2: Attack spreads to compromise critical medical equipment
High Acuity Patient Monitor
Infusion Pump
Smart Bed
Ventilator
Dialysis
Step 4: Attacker traverses through the network to infect remote monitoring workstation & EMR servers

Before Stealth Protection


Attacker
Connection from external network
Communication authorized by Stealth COI
Network breach or unauthorized access
Unauthorized access path
Unauthorized access averted
Members assigned to Stealth COI
Step 1: A breach in network perimeter positions attacker to target valuable assets
Step 3: Data transmission is encrypted preventing packet sniffers from stealing data
Monitoring workstation
EMR server
Stealth™
Step 4: Lateral spread averted by isolating workstations and servers with microsegmentation.
High Acuity Patient Monitor
Step 2: Medical devices protected by Stealth are not visible outside COI and safe from attackers
Infusion Pump
Smart Bed
Ventilator
Dialysis

After Stealth Protection

Stealth(core) Smart Wire

	IoT Gateway Device	VMware vSphere ESXi 6.0
Stealth(core)™	Version 3.4 or higher	Version 3.4 or higher
Processor	Intel compatible x64	1 CPU core
Disk space	8 GB	8 GB
RAM	1 GB	1 GB
Network interface controller (NIC)	2 NICs or 1 NIC and 1 Wi-Fi connection Supporting drivers in 64-bit Ubuntu Server 16.04 LTS for network interfaces	2 NICs or 1 NIC and 1 Wi-Fi connection
Drives	USB or DVD drive (bootable from system BIOS)	

For more information visit www.unisys.com/Stealth or email us at stealth@unisys.com

Printed in the United States of America 04/18 18-0202