Cybersecurity in Heathcare Today:

Needs and Best Practices

Matthew McMahon
Product & Solution Security Professional

Richin Bhandavat
Global Lead Product Manager, POC Blood Gas

Learning Objectives

- To recognize cybersecurity issues are a growing problem in healthcare today, and present increasing risk during the COVID-19 pandemic
- To identify common cybersecurity threats and attacks
- To describe hospital security team expectations and how they can be addressed by medical device manufacturers
- To review and evaluate medical device best practice in medical device design

The Cost of Cybersecurity to the Hospital

Health data breaches cost the healthcare industry $6.2 billion in 2016[1]

- Ponemon Institute

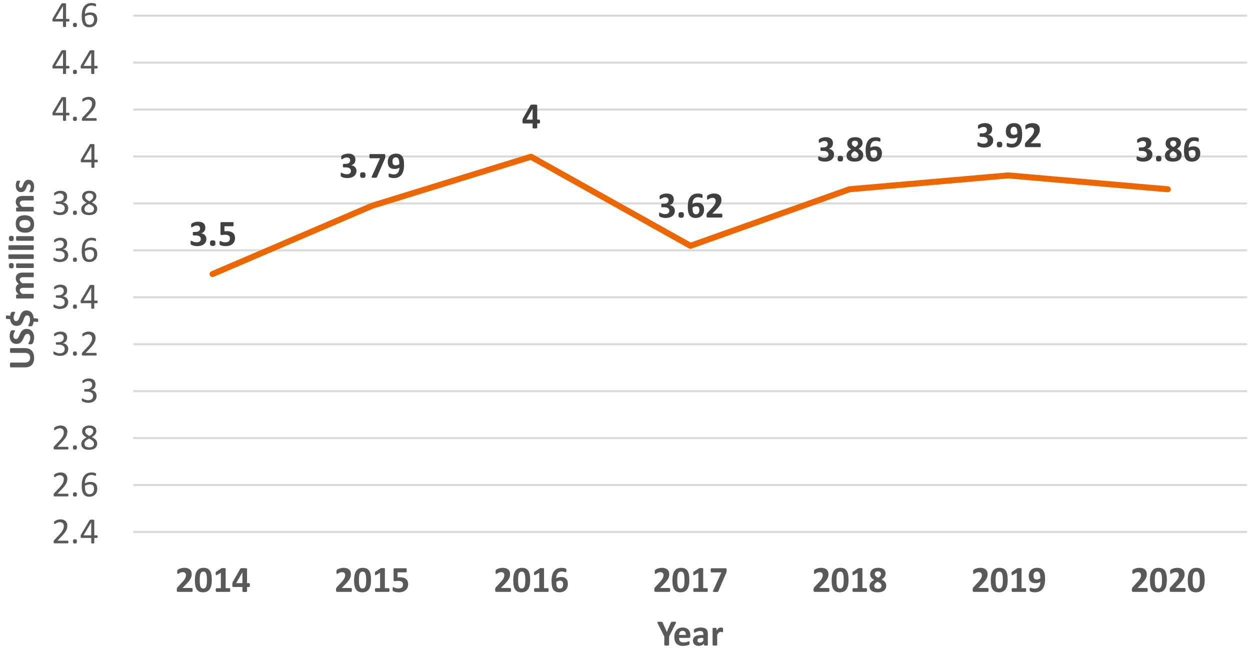
$355 – the average cost of a stolen electronic health record (EHR) [1]

- Ponemon Institute

Global healthcare cybersecurity spending will exceed $65 billion from 2017 – 2021[2]

– Healthcare Cybersecurity Report

Average Total Cost of a Data Breach[3]



[1] https://www.healthcaredive.com/news/must-know-healthcare-cybersecurity-statistics/435983/. Accessed 10-22-2020

[2] https://cybersecurityventures.com/healthcare-cybersecurity-report-2017/. Accessed 10-22-2020

[3] https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/pdf. Accessed 10-22-2020

Magnitude of the Problem

"Between 2009 and 2019 there have been 3,054 healthcare data breaches involving more than 500 records. Those breaches have resulted in the loss, theft, exposure, or impermissible disclosure of 230,954,151 healthcare records. That equates to more than 69.78% of the population of the United States. In 2019, healthcare data breaches were reported at a rate of 1.4 per day.“[1]

(emphasis added)

- *HIPAA Journal (2020)*

[1] https://www.hipaajournal.com/healthcare-data-breach-statistics/ . Accessed 10-22-2020.

Meet the Threats

Internal Factors

58% of Healthcare cyberattacks have an internal component (malicious/accidental)[1]

- Healthcare is the only industry with a higher internal than external threat likelihood
- Human error is a causal factor in just over half of the breaches that featured an internal actor.

[1] https://enterprise.verizon.com/resources/reports/protected_health_information_data_breach_report.pdf. Accessed 10-23-2020.

Meet the Threats

External Attacks

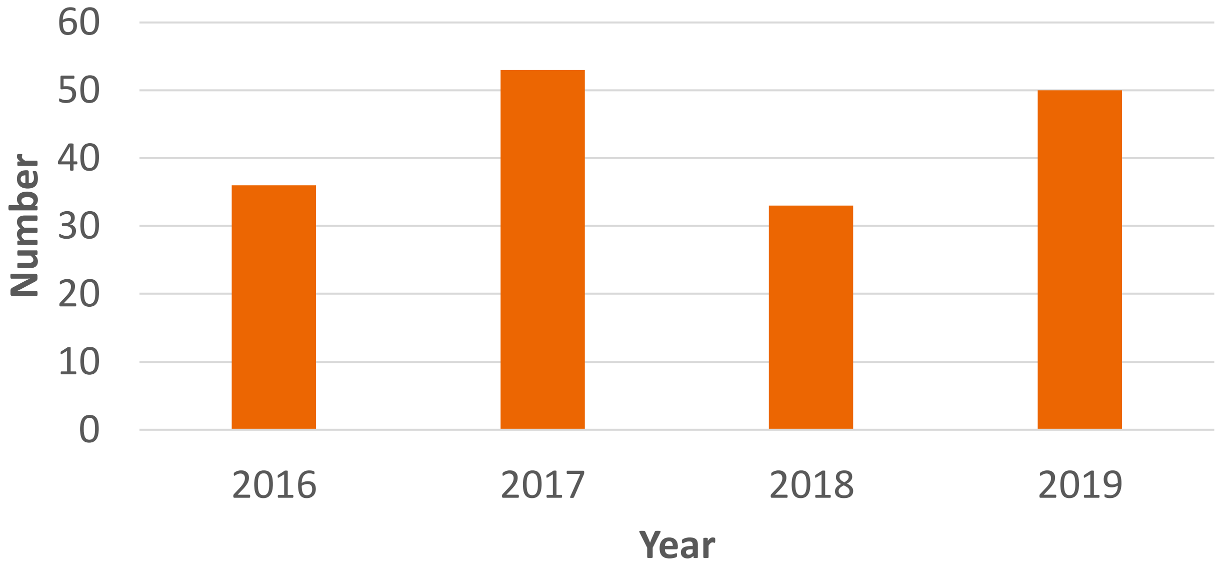
Ransomware[1]

- There were 172 ransomware attacks on US Healthcare organizations since 2016
- These attacks cost over $157 million
- 74% of organizations affected were hospitals or clinics

Malware[2]

- The WannaCry ransomware exploit affected 150 countries
- Caused $4 billion in losses across the globe
- Crippled thousands of hospitals across the UK

Number of Ransomware Attacks on US Healthcare Organizations by Year[1]



[1] https://www.comparitech.com/blog/information-security/ransomware-attacks-hospitals-data/. Accessed 10-23-2020.
[2] https://usa.kaspersky.com/resource-center/threats/ransomware-wannacry. Accessed 10-23-2020

The Growing Threat During the COVID-19 Pandemic

SIEMENS Healthineers

> ***“Cybercriminals are using the pandemic for commercial gain, deploying a variety of ransomware and other malware.”[1]***

- United States Department of Homeland Security (DHS)
Cybersecurity and Infrastructure Security Agency (CISA)
and the United Kingdom’s National Cyber Security Centre (NCSC)

Hospitals are attractive targets for cybersecurity attacks[2]

- Medical records contain valuable PHI and garner a high price on the black market
- Hospitals lag behind in technology adoption
- Patient volume is high, resources are strained, employees are distracted

Cybercriminals have exploited this dynamic with[1]:

- Phishing emails
- Malware distribution
- Registration of new COVID-19 related domain names
- Remote access attacks

1. https://us-cert.cisa.gov/ncas/alerts/aa20-099a
2. https://www.usatoday.com/story/news/health/2020/07/12/hospitals-see-rise-patient-data-hacking-attacks-during-covid-19/5403402002/

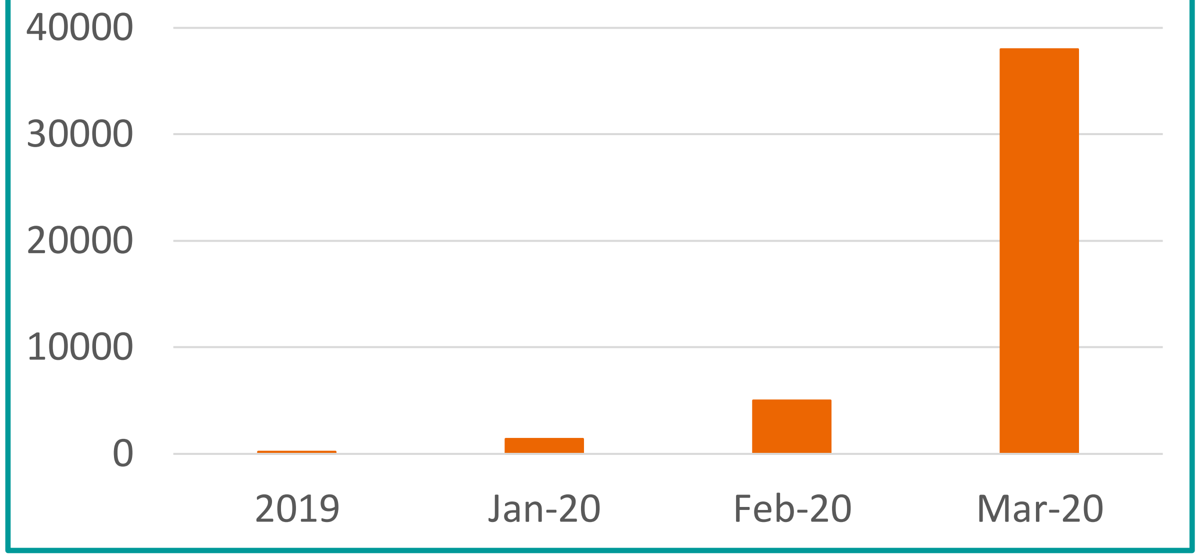
The Growing Threat During the COVID-19 Pandemic

The FBI reported the number of cyberattack complaints is up to as many as 4,000 a day: **a 400% increase** from pre-coronavirus numbers[1]

Between March and April, IBM saw **a 6,000% increase** in spam attacks on information technology systems, leveraging COVID-19, many of them at health care facilities[2]

In the first half of 2020, the Department of Health and Human Services saw a nearly **50% increase** in the number of health care-related cybersecurity breaches[4]

COVID-19 Related Phishing Domain Registrations[3]



[1] https://www.prnewswire.com/news-releases/top-cyber-security-experts-report-4-000-cyber-attacks-a-day-since-covid-19-pandemic-301110157.html. Accessed 10-26-2020.
[2] https://www.usatoday.com/story/news/health/2020/07/12/hospitals-see-rise-patient-data-hacking-attacks-during-covid-19/5403402002/ . Accessed 10-23-2020.
[3] https://wow.intsights.com/rs/071-ZWD-900/images/Cyber%20Threat%20Impact%20of%20Covid19.pdf/. Accessed 10-25-2020.
[4] https://www.medicaleconomics.com/view/covid-19-and-cybersecurity-protect-practices-and-patient-data. Accessed 10-26-2020.

Cybersecurity Breaches During COVID-19

Cyberattacks compromise healthcare operations and patient information

Magellan Health (AZ) [1]	April 2020: Ransomware attack breached 365,000 patient records
Florida Orthopaedic Institute[1]	July 2020: Ransomware attack breeched 640,000 patient records
Legacy Community Health (TX)[2]	July 2020: Phishing attack breeched 228,009 patient records
Universal Health Systems (UHS) [2]	OCT 2020: Ransomware attack took 400 US health system sites offline

[1] https://healthitsecurity.com/news/the-10-biggest-healthcare-data-breaches-of-2020-so-far. Accessed 10-25-2020.

[2] https://healthitsecurity.com/news/3-weeks-after-ransomware-attack-all-400-uhs-systems-back-online. Accessed 10-25-2020.

What the Hospital Security Team Expects
A Survey of over 300 Presale Security Questionnaires

- Active Directory Integration
- Secure by Default
- Encryption of Data at Rest and In Transit
- Secure Backups
- Secure Delete

- Easily Patchable Products
- Fully Disclosed Software Bill of Materials (SBOM)
- Unique User Groups / Roles
- Antivirus / Security Whitelisting
- The Ability to Perform Their Own Vulnerability Scans of Our Products

Easily Patchable Products

Medical Devices Can be Patched in Several Ways[1]:

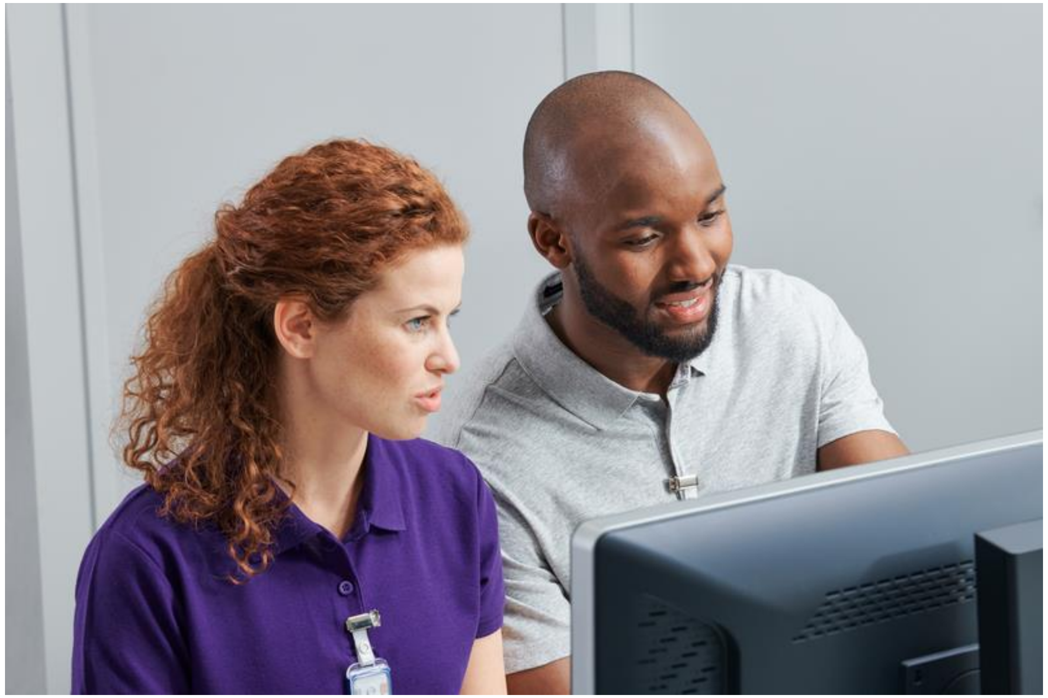
Via a customer service engineer (CSE) onsite

- Costly / Inefficient

Via a remote connection by an engineer (SRS)

- Low percentage of connected devices

Customer downloads a patch and installs themselves (Lifenet)



[1] https://www.siemens-healthineers.com/en-us/support-documentation/cybersecurity#Cybersecurity_lifecycle. Accessed 10-22-2020.

Management of Legacy Devices

- Create and offer OS upgrade kits where it is technically and economically feasible
- Utilize Microsoft's extended security support (ESU) program and continue to release patches for critical vulnerabilities
- Offer a "Security Appliance," solution for remaining medical devices: A next generation firewall with AV based on deep packet inspection, managed through an SRS connection

Fully Disclosed Software Bill of Materials (SBOM)

The Product Security Whitepaper:

- A detailed security document for each product that includes and MDS2 and an SBOM
- The document is customer facing
- Customers will not purchase a “black box,” they need to know the device components
- They need to know the “ingredients,” so they have a better understanding of whether these internal components are vulnerable

Customers ask for a detailed software bill of materials for every product that details[1]:

- The operating system
- The database
- Other key internal components

[1] https://www.meddeviceonline.com/doc/your-medical-device-software-will-need-updated-better-plan-for-it-now-0001. Accessed 10-22-2020.
https://www.flaticon.com/freeicon/insurance/smashicons. Accessed 10-25-2020

Unique User Groups / Roles

Customer medical device expectations

Unique users

- No generic users

User groups

- Administrator group
- Routine operator group

Passwords with complexity requirements

- Length, complexity, reset (90 days)

[1] https://www.fda.gov/media/119933/download. Accessed 10-19-2020.

Antivirus / Anti-malware

Blacklisting [1, 2]

Specifically blocks known threats

- **Specific Detection[2]** – Looks for known malware characteristics
- **Generic Detection[2]** – Looks for malware that are "variants" of a known malware family
- **Heuristic Detection[2]** – Scanning for suspicious activities that suggest an unidentified threat

Must be regularly updated to stay current

- Which means it must be connected

Whitelisting [1,3]

The reverse of Blacklisting

- Blocks everything except what is whitelisted

Doesn't need to be updated as often

Better option for a device that is not connected / regularly updated

[1] https://consoltech.com/blog/blacklisting-vs-whitelisting/#:~:text=Whitelisting%20is%20a%20much%20stricter,when%20using%20the%20whitelisting%20approach.. Accessed 10-2-2020.
[2] https://www.intego.com/mac-security-blog/what-does-your-antivirus-scanner-do-under-the-hood/. Accessed 10-19-2020.
[3] https://marketingland.com/b2b-marketers-care-whitelisting-204266. Accessed 10-19-2020

The Ability to Perform Their Own Product Vulnerability Scans

Vulnerability Scans

Look for known vulnerabilities

- (ex) SMB - WannaCry

Vulnerability scans can sometimes crash devices

- Could cause a reboot
- Could also require CSE onsite to fix

Run vulnerability scans on new products during the normal development lifecycle

[1] https://www.siemens-healthineers.com/en-us/support-documentation/cybersecurity#Cybersecurity_lifecycle. Accessed 10-19-2020

Active Directory Integration (by Microsoft)

SIEMENS Healthineers

- A centrally managed access management tool
- Allows hospitals to create a user and add or remove them from a user group once and push out to many devices
- Eliminates the need to manually setup user access for each user on every device they will use in the hospital
- This is a time and resource saver

1. http://download.microsoft.com/download/5/c/4/5c49d9c8-a3e9-4806-8c6d-a621b8d2402b/Windows-basedHosting_CentralizedManagement.doc. Accessed 10-19-2020.
2. File folder icon made "https://www.flaticon.com/authors/icongeek26" title="Icongeek26">Icongeek26</a

Secure by Default

Customer Expectation

- **All security related settings on a device are turned on out of the box**
  - Firewall On
  - Password Required On
  - Multifactor Authentication On
- **Service staff trained on secure installation**
- **Customers would then have to manually disable security settings themselves**

Types of Encryption

What is Encryption?

Encoding information in such a way that only authorized users have access to it

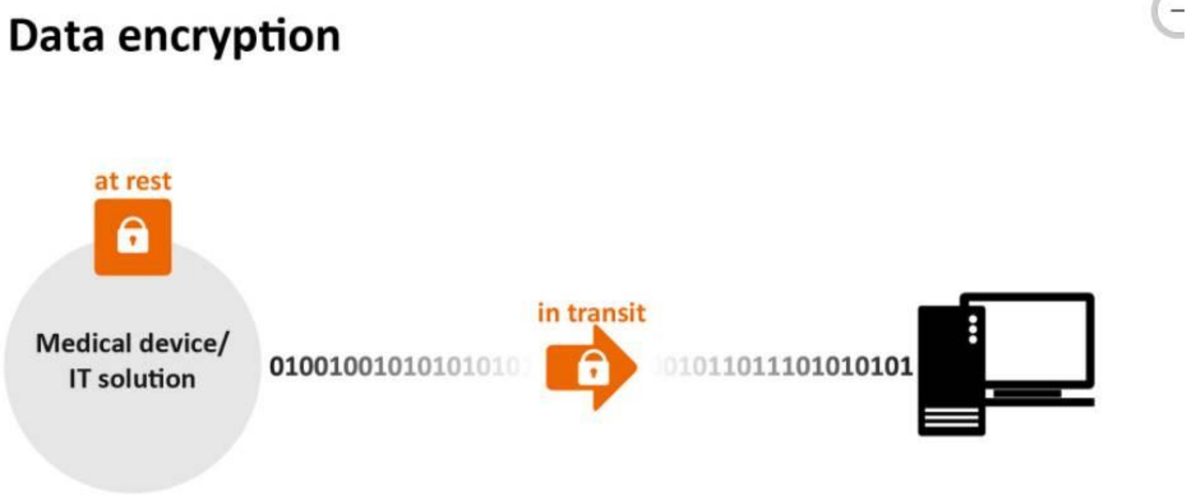
Encryption of data at rest

Protecting data stored on the medical device or within a database

Encryption of data in transit

Protecting data sent from one device to another or to a software system

- HL7 protocol is not encrypted
- Different medical devices use different programming languages



1. https://digitalguardian.com/blog/data-protection-data-in-transit-vs-data-at-rest .Accessed 10-19-2020.
2. Image: https://www.siemens-healthineers.com/en-us/supportdocumentation/cybersecurity#Cybersecurity_lifecycle

Secure Back-up & Delete

Secure Back-up[1]:

- Password protect and encrypt backup data
- Store backups off the device
- Limit access to backup data
- Checksum to assure the data hasn't been altered

Secure Delete[2]:

- When you delete a record off a device it doesn't remove the data it just marks the space the data was stored as available space to be overwritten
- To render deleted data unrecoverable the US DoD recommends copying over data at least 7 times
- A better option is special tools that overwrite ALL disc space with 1's or 0's

[1] https://www.tripwire.com/state-of-security/risk-based-security-for-executives/connecting-security-to-the-business/data-integrity-follow-ways-protect-data/. Accessed 10-19-2020..

[2] http://killdisk.com/notes.htm. Accessed 10-19-2020

A Shared Risk Model

Design Medical Devices with Security in Mind

Internal Processes

- Guidance for Secure Software Design and Implementation
- Product Cybersecurity Requirements List
- Product & Solution Security Quality Requirement

External Input

- Customers
- Evolving cybersecurity legislation from around the world
- Partnerships with security researchers actively working to improve the healthcare industries security posture

New Products Undergo

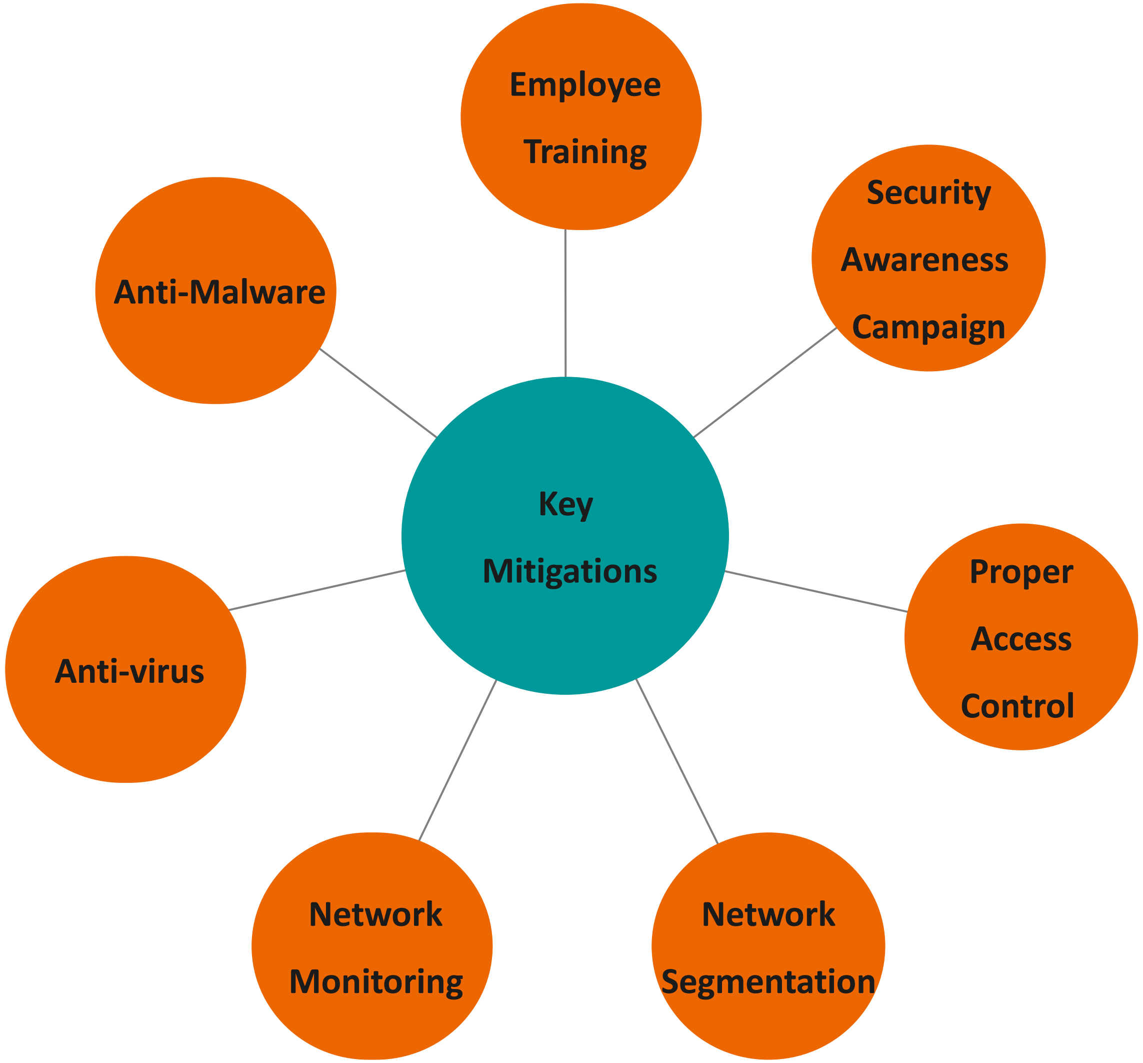
- Project Classification
- Security Requirements List
- Code Analysis
- System Hardening
- Penetration & Fuzz Testing where warranted
- Threat and Risk Analysis

1. http://www.imdrf.org/docs/imdrf/final/technical/imdrf-tech-200318-pp-mdc-n60.pdf. Accessed 10-19-2020.
2. 40-20-14530-01-76_RapidPoint_500e_SecurityWhitePaper_V5_0_1
3. Image: https://www.flaticon.com/freeicon/insurance/smashicons. Accessed 10-25-2020

Customer Responsibilities

- Reviewing the security whitepaper to assure all recommended security measures have been implemented
- Properly segmenting and securing their networks
- Physically securing devices
- Managing device access
- Properly decommissioning a device (PHI)

Key Mitigations



Summary

- Insider threats should not be underestimated as a cyber threat within healthcare
- Cyber-attacks are significantly increasing in volume during the COVID-19 pandemic
- Security solutions should be addressed in product development
- Securing medical data is a shared responsibility between the medical device companies and the end-users

Cybersecurity Medical Device Design – An example

Richin Bhandavat

Global Lead Product Manager, POC Blood Gas

Markets Are Closing to Insecure Medical Devices

A product that is not secure:

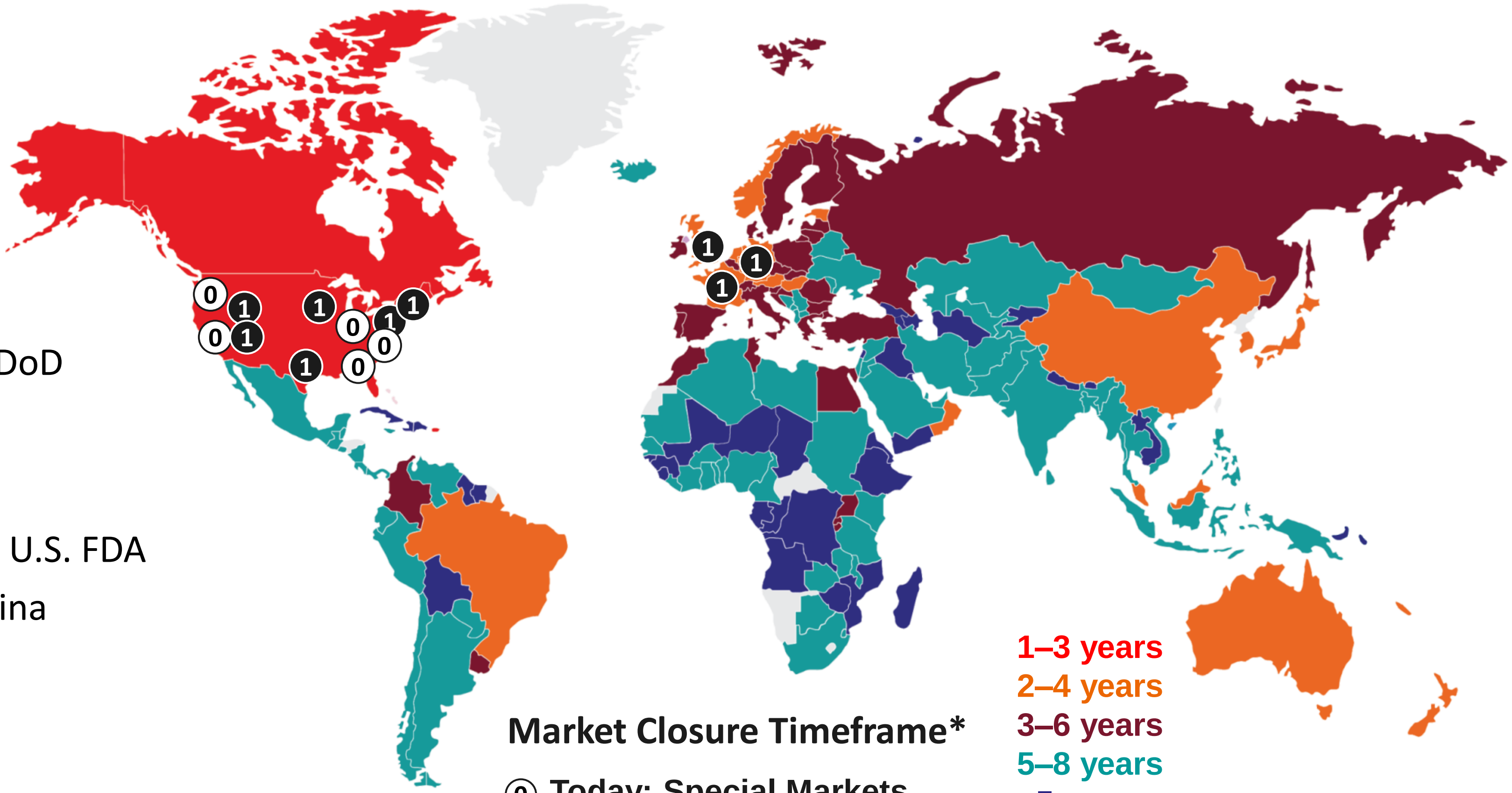
Will be unsellable*

- 5 years, globally
- 2–4 years in Europe
- 2–4 years in China
- 1–3 years in U.S.
- 0–1 years for strategic customers
- *Today* for specific markets such as U.S. VA/DoD

Will be blocked by regulators

- *Today:* unable to get 510(k) clearance from U.S. FDA
- 1–2 years: unable to get clearance from China
- 1–2 years: regulatory roadblocks in Europe

2017 Global Medical Device Cybersecurity Outlook[†]



Market Closure Timeframe*

⓪ Today: Special Markets

❶ 0–1 years: Key Accounts

1–3 years
2–4 years
3–6 years
5–8 years
>5 years
unknown

*Estimate of major impact on tenders, based on ITU 2015 Global Cybersecurity Index + regulatory activity + stated customer requirements.

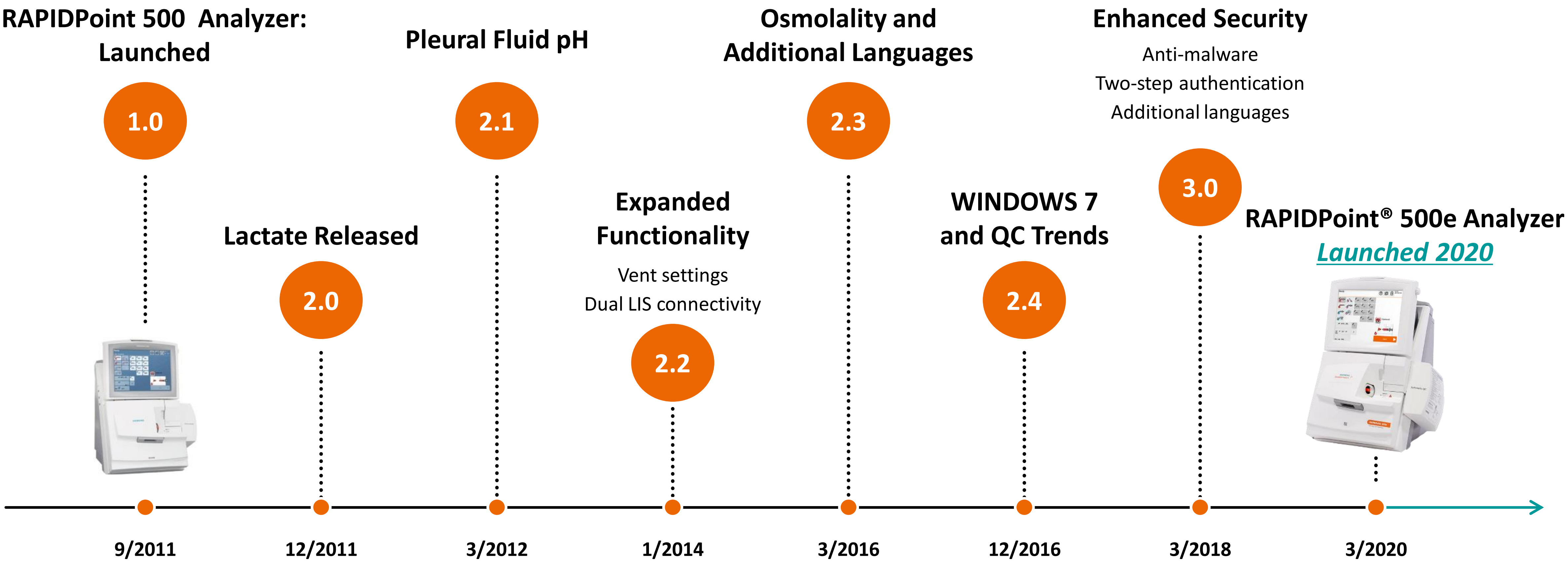
†Representative locations—do not necessarily indicate physical sites.

SIEMENS
Healthineers

RAPIDPoint® 500e
Blood Gas System

with Integri-sense™ technology

Evolution of the RAPIDPoint System



9/2011 – 1.0 – **RAPIDPoint 500 Analyzer: Launched**

12/2011 – 2.0 – **Lactate Released**

3/2012 – 2.1 – **Pleural Fluid pH**

1/2014 – 2.2 – **Expanded Functionality**

Vent settings

Dual LIS connectivity

3/2016 – 2.3 – **Osmolality and Additional Languages**

12/2016 – 2.4 – **WINDOWS 7 and QC Trends**

3/2018 – 3.0 – **Enhanced Security**

Anti-malware

Two-step authentication

Additional languages

3/2020 – **RAPIDPoint® 500e Analyzer**

Launched 2020

RAPIDPoint 500e System: An Elevated Blood Gas Solution

SIEMENS Healthineers

Integri-sense™ Technology

- Sample-to-sample integrity
- Benzalkonium flagging
- QC enhancements

Data Security

- WINDOWS 10
- Encrypted data transmission
- Capability to turn off USB port
- Full 2-step authentication
- Anti-malware
- Firewall
- No hard-coded password

Simplicity

- Modern appearance
- Refreshed user interface
- 2D bar code
- New onboard videos

RAPIDPoint 500e System: An Elevated Blood Gas Solution

SIEMENS Healthineers

Data Security

- WINDOWS 10
- Encrypted data transmission
- Capability to turn off USB port
- Full 2-step authentication
- Anti-malware
- Firewall
- No hard-coded password

RAPIDPoint System Security Roadmap

Strategy: Enhanced product security

- Patient data encryption
- Anti-malware
- Positive endpoint configuration
- Firewall
- Two-step operator authentication
- No hard-coded password

Data Security

WINDOWS 10: The Latest Operating System from MICROSOFT

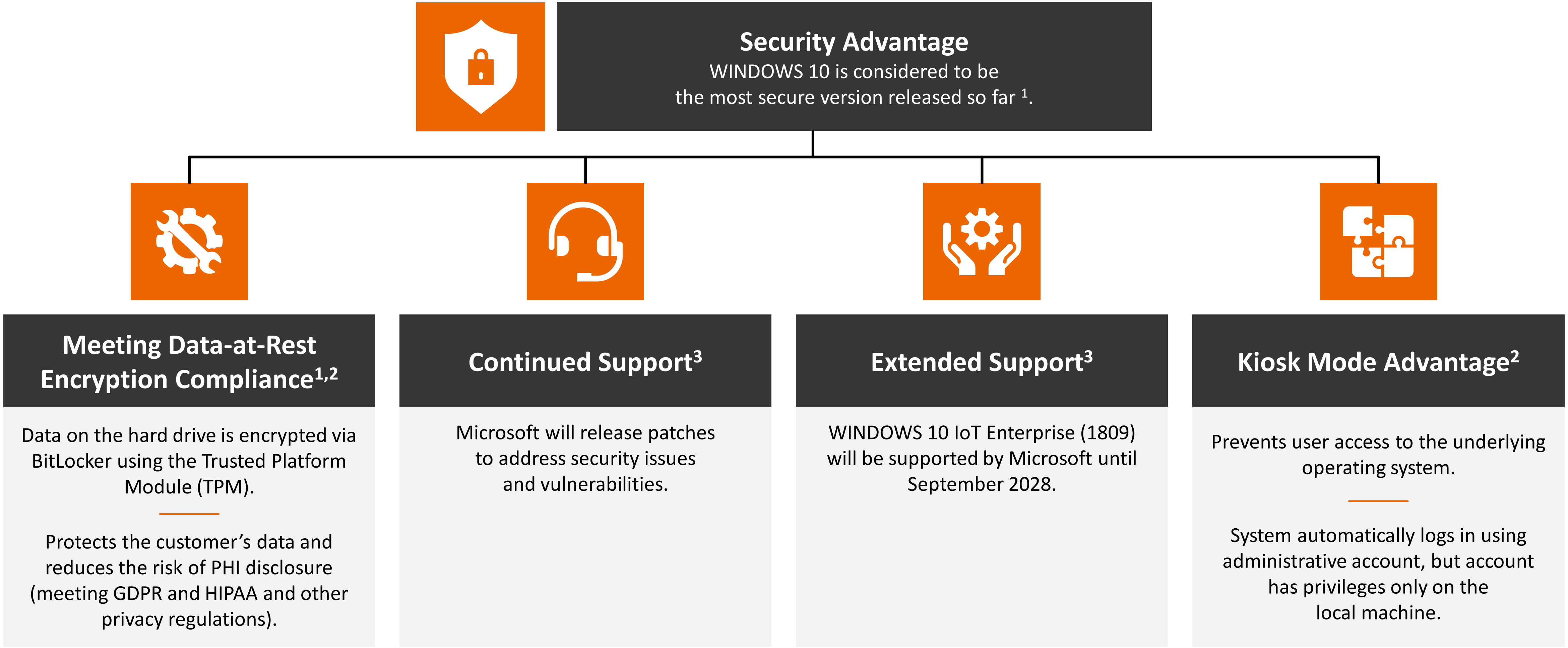
SIEMENS Healthineers

- Enhanced security with WINDOWS 10, ability to do secure installations, encrypt setup and restore
- Extended support by MICROSOFT—Sept 2028

User Benefits

- Leveraging the latest in security enhancements
- Long-term support for peace of mind
- Preventing cybersecurity threats

WINDOWS 10 Advantage from an IT Perspective



Security Advantage

WINDOWS 10 is considered to be the most secure version released so far [1].

Meeting Data-at-Rest Encryption Compliance[1,2]

Data on the hard drive is encrypted via BitLocker using the Trusted Platform Module (TPM).

Protects the customer's data and reduces the risk of PHI disclosure (meeting GDPR and HIPAA and other privacy regulations).

Continued Support[3]

Microsoft will release patches to address security issues and vulnerabilities.

Extended Support[3]

WINDOWS 10 IoT Enterprise (1809) will be supported by Microsoft until September 2028.

Kiosk Mode Advantage[2]

Prevents user access to the underlying operating system.

System automatically logs in using administrative account, but account has privileges only on the local machine.

1. https://www.infoworld.com/article/2984602/why-windows-10-is-the-most-secure-windows-ever.html. Accessed 10-21-20.
2. RAPIDPoint 500e Blood Gas SystemV5.0.1 Security White Paper and MDS. HOOD05162003111491
3. http://woshub.com/faq-windows-10-ltsc-explained/. Accessed 10-21-2020.

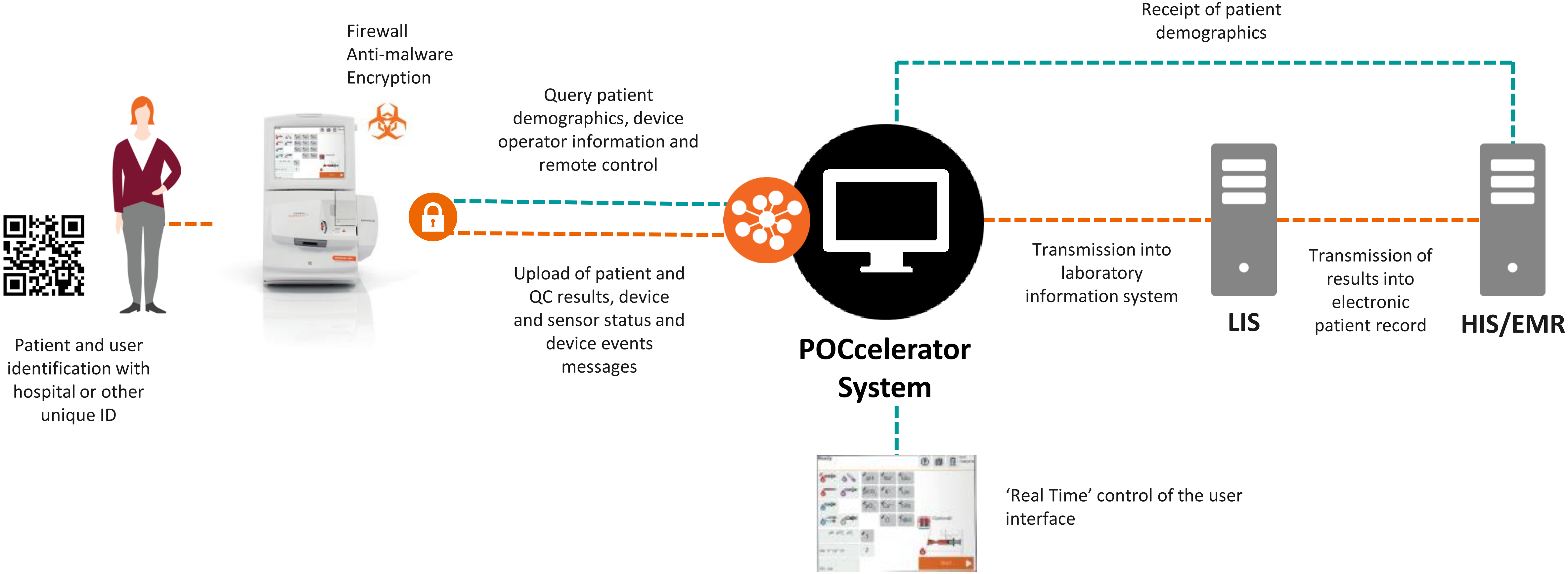
Safeguard Patient Data with Encrypted Data Transmission

Now with the power of POCcelerator™ Data Management System, customers can leverage end-to-end data encryption.

User Benefits

- Secure data transfer, safeguarding critical patient data
- Compliance with institutional requirements

RAPIDPoint 500e Connectivity Overview



Firewall
Anti-malware
Encryption

Patient and user identification with hospital or other unique ID

Query patient demographics, device operator information and remote control

Upload of patient and QC results, device and sensor status and device events messages

POCcelerator System

Receipt of patient demographics

Transmission into laboratory information system

LIS

Transmission of results into electronic patient record

HIS/EMR

‘Real Time’ control of the user interface

1. Nissen et al. Point of Care • Volume 18, Number 1, March 2019

Data Security

Improved Data Protection to Protect Confidential Data

- Configurable (on/off) USB port to meet government and hospital requirements
- Ability to encrypt data sent to USB

User Benefits

- Prevent unauthorized export of data.
- Reduce probability of software viruses entering through USB media.

McAfee Embedded Anti-Malware to Mitigate Targeted Attacks

- Whitelists allow only trusted programs necessary for daily operations to reduce the potential attack surface.[1,2]
- Blocks unauthorized programs and prevents inadvertently downloaded code from running.[1]

User Benefits[1,2]

- Prohibits the execution of unauthorized applications
- Excludes all software that has not been approved
- Protects against cybersecurity threats[2]

[1] https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-embedded-control.pdf. Accessed 10-21-2020.

[2] RAPIDPoint 500e Blood Gas SystemV5.0.1 Security White Paper and MDS. HOOD05162003111491.

Summary

- Cybersecurity threats are real and can be disruptive, costly and put patient safety at risk
- Mitigating cybersecurity threats requires addressing:
  - Physical security
  - Network security
  - Data security
  - Device security

A proactive partnership — people, processes and technology — between a hospital system and medical device manufacturers can help protect healthcare institutions against cyberthreats.

Contact

Matthew J McMahon
Product & Solution Security Expert, PSSE

Product Technology Assurance
2 Edgewater Drive
Norwood, MA 02062

Tel: +1 (781) 269 3815
Mobile: +1 (781) 856 7787
matthew.mcmahon@siemens-healthineers.com

Richin Bhandavat
Global Lead Product Manager, Benchtop Blood Gas

Point of Care Diagnostics
2 Edgewater Drive
Norwood, MA 02062, USA

Tel : +1 781 856 9459

richin.bhandavat@siemens-healthineers.com

Siemens Healthineers
Point of Care
Siemens Healthcare Diagnostics Inc.
2 Edgewater Drive, Norwood, USA
siemens-healthineers.com

Inspired by patients. Empowered by technology.

Transforming care delivery by elevating your blood gas solution.

RAPIDPoint and all associated marks are trademarks of Siemens Healthcare Diagnostics Inc., or its affiliates.