CRYPTONITE NXT

MDISS
MEDICAL DEVICE INNOVATION, SAFETY & SECURITY CONSORTIUM

Health Care Cybersecurity Best Practices

Zero Trust Networks Bring Benefits to Patient Safety, Privacy and Business Operations

CryptoniteNXT Special Report

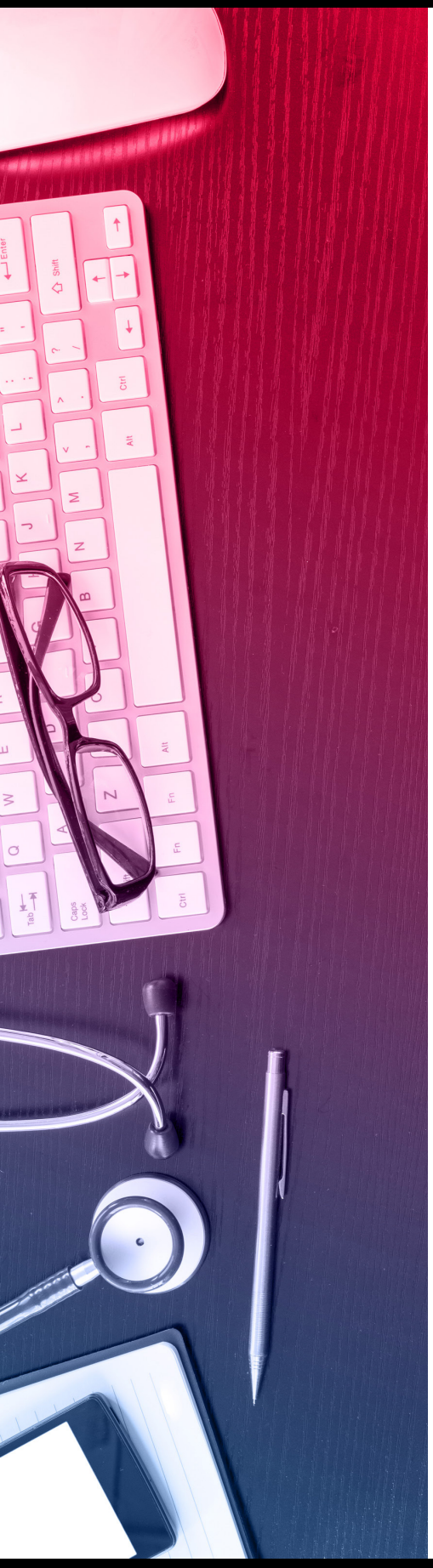
Contents

March 26, 2018 | This report has been sponsored by the Medical Device, Innovation, Safety & Security Consortium and Cryptonite, LLC

Notice

This publication is made available for information purposes only. At the time of publication, all information referenced in this publication is as current and accurate as we could determine. Any additional developments or research since publication, will not be reflected in this report. Please note that this publication may be changed, improved, or updated without notice.

The sponsors (Cryptonite, LLC and the Medical Device Innovation, Safety & Security Consortium (MDISS)) are not responsible for any errors or omissions in the content of this report or for damages arising from the use of this report under any circumstances.



Foreword by MDISS

The Medical Device, Innovation, Safety & Security Consortium (MDISS) is a 501(c)3 non-profit public health and patient safety organization focused on medical device cybersecurity. MDISS, a public health initiative based on Center for Disease Control (CDC) best practices, helps organizations develop practical technologies, best practices-based programs for cyber risk surveillance and response, patient safety programs, and policy solutions for making devices and medical device associated networks safer and more secure. MDISS public health programs promote patient safety based on the CSC's National Health Safety Network (NHSN) model. Specifically, the MDISS National Cyber Safety Network is a community of practice that combines deep embedded vulnerability and regulatory expertise with patient-centered security, epidemiological methods, and a public-private partnership model to effect meaningful public health impact.

MDISS continues to expand its applied operations research agenda with industry partners, develop, and identify new best practices and the underlying technologies that support them to address cybersecurity mediated public health challenges in the current health care delivery environment. The security of medical device networks is both a function of their internal designs, architectures, and security mechanisms, as well as the information technology environment and the network infrastructure into which these medical devices are integrated and operated.

MDISS programs are designed to support medical device manufacturers, healthcare delivery organizations, public sector stakeholders and the broader technology community. This report is an example of an MDISS collaboration. The report provides a snapshot of some of the current cybersecurity environments in health care, shares important insights into cyberthreat related trends in these environments, and identifies recent technology solutions that can help maintain the integrity of medical devices that are installed and connected in health care network environments.

Our partnership and cooperation with the medical device health care delivery, and the greater information technology and communications (ITC) industries helps foster more reliable and secure health care solutions. MDISS programs are designed to strengthen the capabilities of the health care information technology and security operations teams that mitigate cyber risk and contribute to safe patient care environments in the near term.

Dale Nordenberg, M.D.

Executive Director and Co-Founder of MDISS

MDISS
MEDICAL DEVICE INNOVATION, SAFETY & SECURITY CONSORTIUM

Executive Summary

Health care networks remain under sustained attack by cybercriminals who intentionally target health care networks for two primary reasons - to steal the medical records they contain and to extort ransom payments. Medical records are prime targets, as this data is highly prized to support identity theft and financial fraud. Medical records also rival those records stored within credit bureaus for completeness and criminal utility. For these reasons, medical records are an attractive commodity on the dark web where they demand high premiums from criminal purchasers. Hostile nation states also acquire medical records, amongst other stolen records and databases, to assemble profiles on our citizens for future use. In contrast, ransomware and other forms of crypto malware provide more immediate financial rewards by preventing access to essential health care network data until ransom in the form of digital currency is disbursed.

The solution for immediately addressing high vulnerability use cases lies in embracing the concept and new best practice of Zero Trust. The term Zero Trust was originated in 2009 by the industry analyst firm Forrester Research. Forrester's position was that the notion of treating the internal network as trusted and the external networks as untrusted was inherently flawed. Forrester's conclusion was that every network should be considered untrusted.

A Zero Trust health care environment is architected to stop the cyberattackers, ransomware, and insider threats within your internal health care networks. New best practices enable you to implement Zero Trust environments to directly address and defeat attempts to exploit the multiple areas of vulnerability common to health care institutions of all sizes.

New technologies such as next-generation firewalls, moving target cyber defense (MTD), micro-segmentation, deception technology, and 802.1x compliant 2-factor user and device authentication combine to enable a powerful Zero Trust environment, designed and optimized for health care institutions of all sizes.

Why should health systems assume a Zero Trust approach to their networks when designing cyber strategies?

- The high vulnerability network environments commonly found among health care networks are exactly those environments in which an attacker has a high probability of success.
- These high vulnerability environments are easy prey for the cyberattacker using commonly available hacker tools and publicly known and available exploits.
- Vulnerability becomes common, especially among medical devices, due to failures in systems updates and patching.
- The diversity of device types creates significant risk because it is difficult to implement update and patching standard operating procedures at scale.
- Device diversity includes:
  - Workstations and servers.
  - Internet of things (IoT) devices typical of intensive care environments.
  - Embedded Windows XP and Windows 7 processors in FDA approved medical devices.
  - Mobile devices that must interconnect with health care networks, especially those used by ambulatory clinicians.
- Regulatory oversight and safety concerns for medical device modifications require specific processes for update/patch verification prior to administration.

Current cyber defense best practices, already deployed in many health care institutions, are important but no longer enough to keep out determined cyberattackers. This defense in depth strategy is focused on maintaining a secure perimeter around the health care institution but does not provide sufficient visibility into movement once a user has gained access to the internal network. Once this perimeter is broken and the cyberattacker is inside the network, they can move freely, often undetected for months, to compromise the network, threaten operations, and exfiltrate patient data. Today, perimeters are being breached frequently by cyberattackers. For these reasons, a strategy based solely on perimeter defense appears no longer sufficient to protect the health care enterprise.

New technologies such as new next-generation firewalls, moving target cyber defense (MTD), micro-segmentation, deception technology, and 802.1x compliant 2-factor user and device authentication combine to enable a powerful Zero Trust environment, designed and optimized for health care institutions of all sizes. These technologies bring a high degree of automation that can mitigate active attackers already embedded and previously not detected within your medical devices.

In summary, health care enterprises that adopt a Zero Trust network best practice will further harden their cybersecurity posture to protect patients, patient data, and business operations. This report will share how these technologies can help support new best practices and how they address common and unprotected vulnerabilities within your organization.

Health Care Vulnerability in Context

Health care networks are highly complex. They include all of the standard information technology platforms, servers, and communications devices in addition to the large number of specialized devices common only to health care delivery organizations. Connected health is dependent on technical interoperability across ambulatory practice-based EMR/EHR systems, mobile devices, hospital networks and their EMR/EHR systems, diagnostic labs, and a large variety of other institutions such as skilled nursing facilities, surgical centers, urology (dialysis) centers, vision care centers, and MRI/CT scan centers, among many others. Connected health brings substantial challenges to the security operations and information technology teams.

Health care networks also have all of the vulnerabilities evidenced in other industries. Failure to install updates and patches is a primary source of exploits attackers can use within the health care networks. This may include any of the workstations used throughout the institution or portable devices such as laptops used by ambulatory physicians. Network printers, scanners, and fax machines also represent a similar liability and often contain embedded processors with operating systems which are no longer supported by the operating system manufacturers.

There are many vulnerabilities unique to health care delivery organizations due to the vast network of medical devices, including portable computing devices and network connected Internet of Things (IoT) devices. Cyberattackers target medical devices and use them to establish a "backdoor" which can then support extended cyberattacker activity to perform reconnaissance, discover valuable sources of data, and then move laterally through the networks. Medical devices themselves may exhibit good security practices in their design and architecture, but when placed within networks without adequate internal security, they are rapidly compromised by sophisticated and highly persistent cyberattackers.

Cyberattackers use a variety of attack vectors to gain access to health care networks. These include but are not limited to phishing attacks, corrupted websites, and malware-laden emails and memory sticks, all of which enable the loading of attacker tools into the network. Even when these attacks are identified and defeated in the standard information technology platforms, they cannot be easily found within medical devices.

In cases in which breaches are detected within medical devices, the cost and time for remediation through rebuild or replacement of the embedded software is high, and the remediation must be done by the medical device manufacturer's certified personnel. Without network defense best practices in place, even these remediated medical devices can be reinfected and compromised almost immediately as the same attacker tools propagate through the network again, perhaps emanating from an unremediated medical device elsewhere within the network. The cost for all of this continues to climb as health care institutions and medical device manufacturers partner on the best ways to identify and address these problems.

Medical Device Updates: Compensating for Overdue Software Updates and Patches

Data shows that unpatched software remains the #1 source of exploits for cyberattackers. This common source of exploit is overviewed in an earlier authoritative publication by IHE International, Inc. and the MDISS consortium. This data is confirmed by the United States Computer Emergency Readiness Team (US-CERT), which attributes approximately 85% of all cyberattacks to this problem.

As cyberattackers perform reconnaissance within your network, they enumerate the network, determine the versions of software you are running, identify vulnerabilities, and then map and target the exploits. Operating systems and applications within the network that are missing patches and updates provide attackers an almost endless list of attack vectors. Yet despite a clear understanding of the vulnerability, most health care teams cannot keep up with required patches and updates. One of the major reasons for this is that there are just too many. In addition, patching medical devices usually requires manufacturer testing and approval prior to patch updating. According to the Microsoft Security Intelligence Report, many thousands of vulnerabilities are found each year. Each operating system and software application has hundreds of issues that need attention and patches and updates should be applied immediately. Most patches and updates can take weeks or months to apply or, in some cases, are never applied at all because of negligence or the fear of introducing instability within the network.

Information technology teams know that patches and updates might destabilize production systems such as EMR/EHR systems and their interconnections with other health care infrastructure systems. Patches and updates may bring new problems and, in some rare cases, can totally stop ongoing operations. Information technology practitioners may also have personal experiences with updates bringing instability to otherwise stable systems. As a result, enterprise teams may try to delay patch installation for weeks or months in order to let other organizations flush out hidden problems with the update. Then, if no major problems surface after a period of time, they will go ahead and roll out the updates within their own networks.

Unfortunately, cyberattackers work to take advantage of these unpatched "gaps" to execute exploits in health care networks in real time. They watch for the announcement of new exploits and then immediately test targeted networks to see if the exploit is available. Cyberattackers are faster at finding these open unpatched "gaps" in security than the security and information technology staff is at resolving them. This approach by cyberattackers has been responsible for many successful recent attacks.

Recent ransomware attacks by WannaCry, a variation on WanaCryptor, utilized an exploit called EternalBlue. EternalBlue is a vulnerability in the Microsoft implementation of Server Message Block (SMB) which allowed attackers to execute code in the targeted computer. In many cases, even after the patch was available, the exploit was still used successfully since the patch was not installed. In other cases, such as in the use of older XP systems which are often found in health care, there was initially a window during which no patch or protection was available. Microsoft then took the unusual step of providing a patch to stop the EternalBlue enabled WannaCry from executing on unsupported XP systems.

Diversity, Specialization, and Complexity: Embedded Processors and IoT Devices in Health Care

Medical device networks are highly complex environments. Network architectures are highly heterogeneous, including a wide variety of devices from small mobile devices running real-time operating systems to large bolted down devices that are multi-component and run more complex operating systems. These devices generally contain embedded processors and a wide variety of operating system software.

Medical devices are turnkey and purpose built - they are not general purpose computing platforms. They are regulated by the Food and Drug Administration (FDA), which influences the modification process for medical devices, including but not limited to routine patching of third-party software components. This makes it difficult for standard cyber defense software to provide adequate protection. There is almost no visibility into the internal software bill of materials for a given medical device. There is a huge gap in cybersecurity and interoperability specifications of medical devices at the point of care where health delivery organizations' (HDO) IT professionals use the information to optimally configure medical devices and associated networks in health care delivery organizations. This creates a perfect environment from which a cyberattacker can conduct clandestine activities.

The list of medical devices that cyberattackers target for compromise includes CT scanners, MRI scanners, medical lasers, infusion pumps, heart-lung machines, dialysis machines, blood gas analyzers, and hundreds of other pieces of equipment commonly found within health care institution networks. Even portable X-ray machines can be compromised in the few moments when they are connected to the network, and, once compromised, they can continue to be a source of attacker tool propagation and compromised with each additional connection to the network.

Internet of Things (IoT) devices represent a new and rapidly expanding area of risk and vulnerability to health care networks. Health care has been an early adopter of

IoT devices. There are dozens of simplified medical devices that are wirelessly connected and IoT enabled. Many of these IoT platforms have limited purpose-built operating systems and board processors, which, as mentioned above, are difficult to monitor and provide attractive targets for compromise by cyberattackers.

As before, standard health care cybersecurity software does not protect IoT devices. You cannot load standard cyber defense software in IoT devices or have visibility to what is happening inside of them. When attackers find IoT devices that they can exploit, they know that the enterprise cyber defense is unlikely to have protection for these devices, nor any visibility into their operations.

Security solutions specifically targeted to IoT devices are highly fragmented and very new. While multitudes of schemes for embedding trust and identifying and credentialing IoT devices on the network have emerged, most will take considerable time to roll out, and these solutions are unlikely to help to protect the existing and growing installed base of devices within your networks anytime soon.

The cost of medical devices makes replacement unlikely. You cannot simply throw out a network connected blood gas analyzer IoT medical device. These devices are expensive and they have long system lives during which the financial payback on the equipment must be achieved by the health care institution. Any solution must address the challenges within health care by protecting both the installed base of IoT devices, as well as new devices that will be brought into the network on an ongoing basis.

Connected Mobile Devices: Medical and Non-Medical

Smartphones and tablet computing devices add to the risk of health care networks being targeted by cyberattackers. Ambulatory clinicians rely on these devices as they move between their practice EMR/EHR and the variety of other IT systems to which they must connect. Mobile devices are particularly attractive to cyberattackers because of their high volumes of use and because they present a wealth of attack vectors. The constant movement of clinicians and their administrative support non-clinicians between their practices, hospitals, and other health care entities creates an ever-expanding opportunity for cyberattackers to compromise these connected systems.

As smartphone and tablet computing device use grows, hackers are discovering and documenting every possible way to break through mobile security. Attackers need little time to gain access to a mobile phone or an iPad and install the malware tools that will enable them to siphon data from these devices at their leisure. Browser-based attacks, targeted use of buffer overflow, and SMS/MMS are a few of the many ways basic mobile device security can be compromised and defeated.

The greatest threat is that once these devices are compromised, they can be used to gain access to networks. In early 2017, Dimensional Research did a survey on mobile security for CheckPoint Security that included over 400 security professionals. They revealed that 20% of companies' mobile devices have been found to be breached, and 24% don't know whether they've experienced an attack.

Mission at Risk: Implementing a Zero Trust Health Care Network

As we noted in our executive summary, one best practice solution for addressing all of these vulnerability use cases lies in embracing the concept and new best practice of Zero Trust. Zero Trust network best practices require reducing access to resources and visibility within the network to the absolute minimal subset you need to perform your job - no more. Traditional defense in depth cyber defense software and network security equipment cannot implement Zero Trust. You must combine your existing resources with new emerging technologies to build out the strongest defense to stop and defeat cyberattackers.

A Zero Trust environment may be constructed by combining cyber defense technologies such as moving target cyber defense (MTD), network micro-segmentation, deception technology, and 802.1x compliant user and device authentication. These can enable health care defenders to leapfrog the tactics of cyberattackers' tools and the ransomware they deploy.

MTD reduces the attacker's visibility within the health care network. They can no longer conduct reconnaissance, so IP addresses can no longer be used to map out and enumerate an attack. In fact, using both MTD and micro-segmentation to build out a Zero Trust environment renders most classic attacker tools inoperable. Lateral east-west movement in the network is similarly restricted and limited by role and policy. Cyberattackers cannot target health care servers or medical devices that they cannot see, and they cannot attack without a target. Micro-segmentation is also supported and advocated by NIST for use with health care, manufacturing, and other industry networks.

Deception technology adds additional layers of protection to build out a resilient Zero Trust environment. Deception technology creates a virtual deployment of fake devices which look like standard IT infrastructure, and in some cases, actual medical devices. This deceives and attracts the attackers, enabling their potential detection early in the attack.

802.1x compliant user and device authentication allows for the very strong authentication of users, computers, and mobile devices within the network. One

time password and pin authentication technologies, such as OKTA multifactor authentication, combined with machine authentication (embedded digital certificates), make it much more difficult for intruders to gain access to your network. Credentialed and authorized users can only access network resources from a similarly credentialed and authorized machines.

A Next-Generation Firewall (NGFW) is the latest generation of firewall technology. NGFW's combine legacy firewall technology with other advanced network device filtering functionalities including application firewall with deep packet inspection (DPI), and an intrusion prevention system (IPS). NGFW's may also include integration with other indentity management technologies such as Radius, LDAP and Active Directory. NGFW's perform the deepest levels of inspection going deeper into the various network layers to provide comprehensive awareness over applications and network activity.

A Zero Trust environment allows health care networks to stop and defeat attackers, ransomware, and insider threats. A Zero Trust network brings together new technologies to supplement standard defense in depth so that attackers are kept out of the network to the greatest extent possible, as well as promptly identified and stopped from movement or acquiring resources when attackers do successfully breach the network.

Stopping Reconnaissance in Health Care Networks

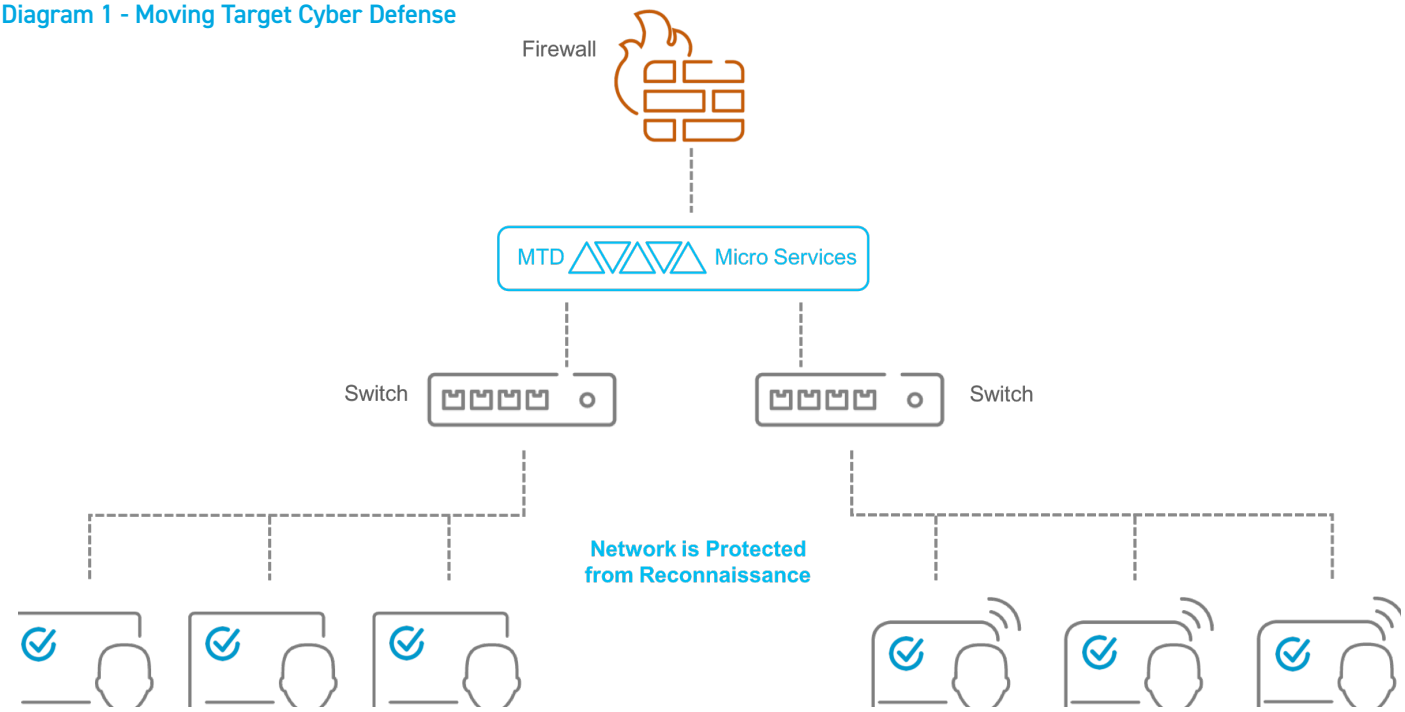
Technology Set 1 - Moving Target Cyber Defense (MTD)

Moving target cyber defense (MTD) deceives and contains cyberattackers at the very beginning of the attack and makes their targets invisible. Reconnaissance is completely shut down. Without visibility into the network, it is impossible for cyberattackers to map the network, identify targets, access unpatched vulnerabilities, and proceed with an attack.

MTD does this by transforming the endpoint's view of the network into a dynamic, abstract structure, in effect making the once static network into a dynamic moving target. MTD (see Diagram 1) creates a mapping from the obfuscated network to the

real network to enable the flow of traffic across the traditional network infrastructure. Normal legitimate traffic is unaffected by MTD, but an attacker cannot collect actionable information about the network or masquerade as another legitimate endpoint. All of this is done without sacrificing performance or transparency to users on the health care network. MTD also protects against attackers or insiders that have been resident in your network prior to installation; network mapping done by attackers prior to the installation of MTD is not actionable. All of this existing sensitive information is rendered useless for continued cyberattack planning.

Diagram 1 - Moving Target Cyber Defense



Restricting Lateral Movement by Policy in Health Care Networks

Technology Set 2 - Network Micro-Segmentation

Network micro-segmentation significantly reduces attack surfaces accessible via lateral movement. Users only have visibility to the servers and other devices necessary to support their daily work; attackers and malicious insiders are denied access to lateral movement beyond a very narrowly defined set of resources. Vendor automation generally identifies every specific device, the approved access to resources, and the user authenticated and authorized to use it.

Network micro-segmentation can easily be deployed within hospitals and health care networks. IT staff can define policies within the micro-segmentation platform to control network access based on device types, user profiles, applications, or numerous role-based characteristics shared via Active Directory or a Lightweight Directory Access Protocol (LDAP)-based directory service use by the great majority of health

care institutions. Micro-segmentation can also support all of the health care institution's existing routers, switches, and network infrastructure.

Deceiving and Detecting Attackers Moving Inside the Network

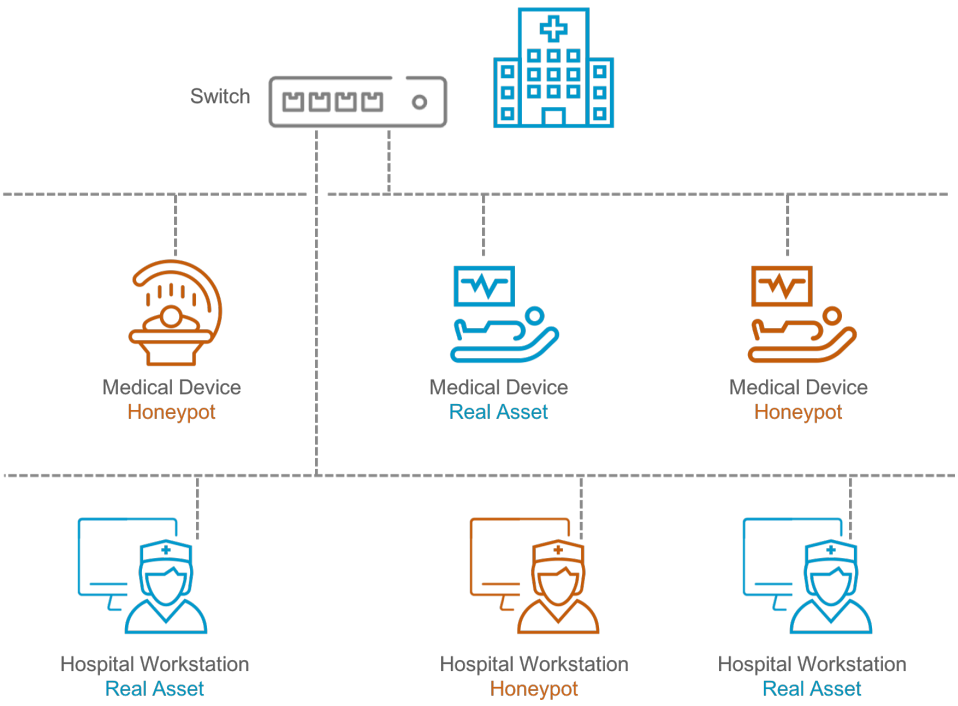
Technology Set 3 - Deception Technology

Deception technology provides for lures (decoys) and honeypots (traps) that entice and distract attackers that have penetrated your network. Once they access a lure or honeypot, you are provided with a high integrity alert.

Deception lures appear as real documents stored within the health care infrastructure. These document lures list passwords and offer access to production and development servers. Once an attacker uses this false information, they will be immediately detected and identified.

Deception honeypots (see Diagram 2) appear as real health care IT infrastructure and medical devices to lure attackers and purpose-built malware. Deception honeypots may appear as servers, switches, workstations, EMR/EHR systems, X-Ray machines, and even devices such as a blood gas analyzer. One touch of the deception honeypot creates a high integrity alert which may be used to rapidly identify and isolate the attacker. The integrity of the alert is high because no one should be accessing the honeypot for any reason. Deception technology may use emulated devices, or, in the case of some vendors, utilize complete and fully deployed operating systems which make it very difficult for attackers to discern traps.

Diagram 2 - Deception Technology



Deception technology can add additional layers of protection to build out a resilient Zero Trust environment. This deceives and attracts the attackers, enabling their potential detection early in the attack.

Securely Identifying Users and Their Computing Platforms Using 802.1X Authentication

Technology Set 4 - 802.1X Authentication

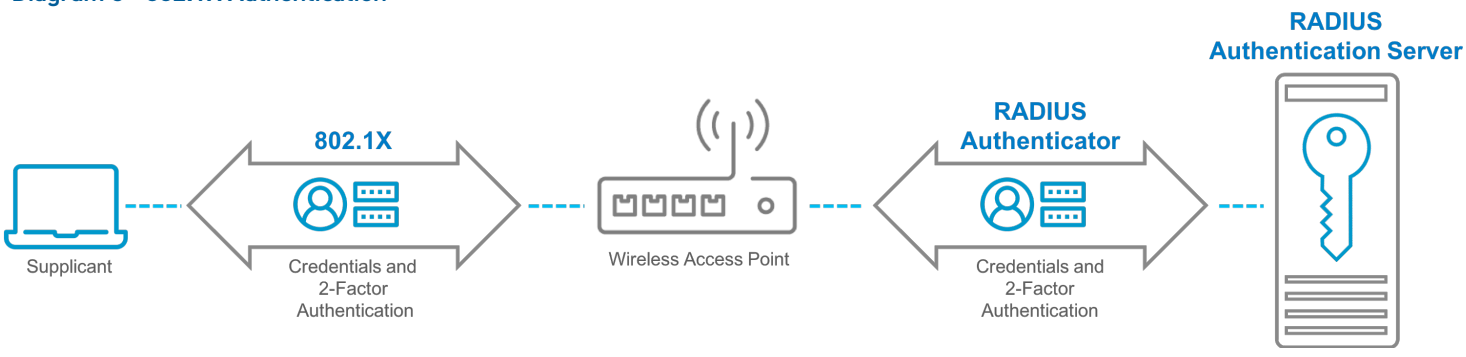
802.1X (see Diagram 3) defines Port-Based Network Access Control, which allows devices to authenticate to the network using a protocol known as Extensible Authentication Protocol (EAP). 802.1x only allows both properly credentialed users and properly credentialed devices access resources within the network. This powerful authentication makes it much more difficult for cyberattackers to gain unauthorized access to your health care networks.

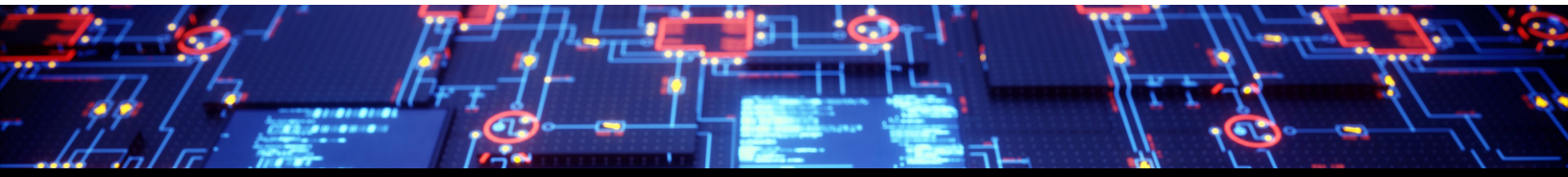
802.1x compliant 2-factor authentication generally requires both a one-time password and a single-use PIN prior to authenticating any users. 802.1x also requires that the computer or mobile device through which that authorized user is requesting access is similarly authenticated. All of this makes it much difficult for attackers to compromise and exploit your health care networks.

EAP defines the format for messages sent between three different entities:

- The supplicant, or client, is the device that wants to gain access to the 802.1x network.
- The authenticating server could be a Radius server providing 802.1x authentication for both wired and wireless users. The authentication server also provides a database of information required for authentication and directs the authenticator to deny or permit access to the supplicant.
- The authenticator permits or denies access to the supplicants.

Diagram 3 - 802.1X Authentication





Enforce Security Policies at the Application Level

Technology Set 5 - Next Generation Firewalls

A next-generation firewall classifies traffic, including encrypted traffic, based on application, application function, user, and content. This supports the creation of comprehensive, precise security policies, resulting in safe enablement of applications. Only authorized users can run sanctioned applications, greatly reducing the surface area of cyber attacks across the organization.

Mitigating Vulnerabilities in Health Care Networks

Updates and Patches

The key to exploiting missing updates and security patches is to first find them. Attackers must navigate the network, move laterally, and discover out of date software to exploit it. 802.1x authentication makes it much more difficult for an attacker to find an entry point to the network. Once inside, MTD technology does not allow reconnaissance and micro-segmentation severely restricts attacker lateral movement. Instead of being exposed to potentially dozens of vulnerabilities, the attacker is contained at the originally infected endpoint without the visibility to see unpatched vulnerabilities. The attackers cannot enumerate the network, cannot lookup vulnerabilities, and cannot identify the corresponding exploits.

In the unlikely event that the cyberattacker can determine movement through the network, various deception lures and traps make it impossible for the attackers to identify real resources without discovery. The risks created by overdue software updates and missing patches are thus substantially reduced.

Embedded Processors and IoT Devices

IoT and embedded processor based medical devices security architectures are improving all the time. That said, millions of IoT devices have already been installed. The life cycle of this installed base is as many as 10 years without replacement. A Zero Trust environment enables you to bring in new medical devices while managing the liability inherent in your installed base. If the attacker cannot find these targets, see the network, and move laterally within it, the attack is effectively over.

A Zero Trust environment no longer allows the discovery of embedded processors with older operating systems. They are effectively invisible. Even if an attacker has enumerated the network prior to the installation of MTD and micro-segmentation and has obtained the specific IP of the target, that IP address will not work in a Zero Trust environment and the device will remain safe.

This is particularly useful for environments with a large number of medical devices and embedded processors in which the cost and process of replacement are prohibitively high, including all of the medical devices commonly installed within hospitals and health care networks. With a Zero Trust environment, all of these networks now have additional protection.

Mobile Devices

In cooperation with mobile security solutions, specific MTD and network micro-segmentation solutions can take authenticated mobile security at the edge of networks and securely extend them across the entire network while also preventing adversary reconnaissance and lateral movement. In the event that a wireless device is compromised, it is brought into the network with the policies defined by network micro-segmentation so that lateral movement from the device is reduced to the absolute minimum. As before, attackers cannot perform reconnaissance, and, thus, cannot move laterally between other mobile or wired endpoints and servers. Further, 802.1x allows you to authenticate both the user and the mobile device uniquely. 802.1x implementations are often vendor specific and depend on integration between the network and vendor products.

Deception technology and strong 802.1x authentication provide additional layers of protection for these vulnerable internal networks. Deception can lure and identify cyberattackers by their movement early in the attack cycle before they can exfiltrate data. 802.1x authentication can enable you to validate both the user and their computing platform prior to granting access to the network.

Finally, as noted earlier, next-generation firewalls manage traffic based upon the application deployed, user and content. Only authorized user can run sanctioned applications, greatly reducing the number of cyber attacks across the enterprise. Deployed in combination with MTD, micro-segmentation, deception technology and 802.1x authentication, next-generation firewalls present a formidable and highly effective defense to network cyberthreats.

Automation Meets the Challenge of Rapid Response

The speed of detection and response is critical to reducing the time to breach detection and the risk of data breach. Depending on the technology set, there can be minimal to no alerts to resolve to action - the system infrastructure supported by vendor interoperability can be enabled to do that automatically. Cyberattackers that seek to perform reconnaissance and enumerate the health care network are logged and alerted to the SIEM, and, most importantly, they can be immediately shut down and stopped through automation. Lateral movement out of policy is logged and alerted to the SIEM, but at the same time the attacker or insider threat is restricted and shut down.

For More Information

To learn more about Cryptonite, LLC and CryptoniteNXT, please email **info@cryptonitenxt.com**

This document is current as of the initial date of publication and may be changed by Cryptonite at any time.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NONINFRINGEMENT.

Cryptonite products are warranted according to the terms and conditions of the agreements under which they are provided. The client is responsible for ensuring compliance with laws and regulations applicable to it. Cryptonite does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security mea- sure can be completely effective in preventing improper use or access.

CRYPTONITE DOES NOT WARRANT THAT ITS PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

About Cryptonite, LLC

Cryptonite is a leader in moving target cyber defense. CryptoniteNXT enables any network to actively shield itself from cyberattacks by preventing all attacker reconnaissance and lateral movement. Patent pending moving target cyber defense and micro-segmentation technologies protect enterprise networks from an advanced cyberattacker, insider threats and ransomware. The Cryptonite customer base includes leading commercial and government customers around the world. Learn more at **www.cryptonitenxt.com.**

Cryptonite, 2275 Research Blvd. Suite 750, Rockville, Maryland 20850