An Adaptive Cyber Security Threat Defense for Healthcare Organizations

Deception-Based Threat Detection
Protecting Patient Data, Company Assets, and Patient Lives

In today’s world of connected health, the complexities around cybersecurity continue to grow at staggering rates. Healthcare providers, device manufacturers, biotech companies, and pharmaceutical organizations are all working to transform their IT infrastructure to ensure access and support information sharing so that they can send and receive electronic health data. The demand to share information is outpacing many organization’s abilities to reliably protect their electronic health systems (EHR), databases, connected medical and personal devices.

Given the complexity and that many organizations have not made the investment in a robust security infrastructure, they have become rich targets for cyber attackers. Medical records command a premium over credit card and other forms of information since they contain a wealth of information, which can be used for identity theft and fraud. A typical medical file will include social security numbers, addresses, and other claim and medical information. This information, known as personal health information (PHI), commands a strong premium on the black market and has been known to average a payout of $20 per record. PHI is also prized because unlike a credit card that can be deactivated, PHI can be used for extended periods of time without the individual ever knowing.

Based upon data collected by the HHS Office for Civil Rights, as of February 1, 2016, protected health information breaches affected over 113 million individuals in 2015. In 2015, hacking incidents comprised nearly 99% of all individuals affected by breaches, and the number of reported hacking incidents, 57, comprised over 20% of all reported breaches. From 2011 to 2014, 97 hacking incidents affected less than 4 million individuals - less than 10% of all reported breaches and affected individuals during this time.
Healthcare organizations are under attack by cyber criminals on a mission to steal and monetize its information, extort it for financial gain, and compromise its networks and data for state-sponsored cyber espionage and hacktivism. The attacks are getting more aggressive with phishing campaigns, ransomware demands, and the latest tactic which is now being used to extort organizations for financial gain with the threat to sell PHI on the black market if payment is not made. Prior ransom demands may have been avoided with backups but this new tactic and the risk of failed restores have upped the stakes and the game in cyber healthcare warfare.

This paper will focus on changing the game on cyber attackers and turning the hunters into the hunted. As a healthcare cyber security leader, you need an efficient and effective solution to address advanced cyber threats, one that will reliably protect your organization’s data and patient’s well-being from an attack. This infrastructure must share a balance between technological and operational strategies and provide strong security without impacting employee productivity. It is no longer reasonable to expect patient information to be isolated from sharing. In today’s world of connected health, clinical staff and devices must all be able to securely share information. The HIPAA, HITECH, and Meaningful Use requirements that your organization is constantly being measured against, must also be factored in, but in ways that minimize frustration and time-wasting barriers to access.
An Adaptive Cyber Security Threat Defense for Healthcare Organizations

Know Your Enemy. He Will Know You

Understand the Battlefield

Building an Adaptive Defense

Changing the Game with Deception-based Threat Detection

Healthcare Customer Feedback on Investment Benefits and ROI

Attivo Healthcare Use Cases

Ransomware

Email Phishing Management

Bring Your Own Device (BYOD) Network Monitoring

Internet of Things (IoT) Revolutionizing Healthcare

Medical Device Segment Monitoring

Workstations on Wheels (WOW) and Other In-ward Units

Public Web Presence

PCI Compliance Assurance

Winning the Cyber Security War
Know Your Enemy. He Will Know You.

Cybercrime used to be limited to stolen laptops and USB drives, but with today’s connected health systems, an attacker can find the right vulnerability to exploit and has proven their ability to exfiltrate thousands of PHI records. In June of 2016 alone, a hacker was reported to be selling upwards of 655,000 healthcare records on the dark web allegedly obtained after exploiting a vulnerability in how companies implement remote desktop protocol, or RDP, functionality.

Financial and retail organizations where hit heavily with breaches over the last couple of years. It has not gone unnoticed by attackers that healthcare has not kept up with the same security investments, plus the value of a healthcare record is far greater and of longer lasting value than a credit card. The recent trend in ransomware is also quite troubling and demands the question to what a provider would pay if drug dispensation systems or other devices that control a person’s well-being were to be held hostage.

Healthcare is unquestionably a target rich environment for hackers and in addition to meeting compliance, the C-suite should be taking non-traditional measures to protect and defend their organizations. The stakes are high and the environment complex. The attacker knows that there are vulnerabilities with XP-based systems, less secure medical devices, and an intense pressure to share information, which creates opportunities related to connecting systems and devices that may not always be maintained at ideal security standards.

It is now time to change the game on the enemy. The enemy is aware that prevention alone is unreliable, and they believe that once they are inside the network if they work low and slow that they can go undetected. It is now time for organizations to go beyond just prevention with an adaptive defense that includes 1) measures to understand vulnerabilities and predict attack paths that would be taken to reach their target assets. 2) detection of threats as they scan for targets, attempt to use stolen credentials or move laterally through the network 3) continuous threat management programs that can accelerate the response to incidents and prevent attackers from completing their mission or causing wide-spread harm. Prevention is core to creating a barrier to protect against the known attacker. Systems across vulnerability assessment, detection, attack analysis, and threat intelligence solutions should all also tie together to simplify and accelerate the response to an incident and strengthen prevention solutions to protect against repeat incidents.

If your enemy is secure at all points, be prepared for him. If he is in superior strength, evade him. If your opponent is temperamental, seek to irritate him. Pretend to be weak, that he may grow arrogant. If he is taking his ease, give him no rest. If his forces are united, separate them. Attack him where he is unprepared, appear where you are not expected.

Sun Tzu
Understand the Battlefield

Whether you are a healthcare provider, insurance, pharmaceutical, or device manufacturer, there is a critical need for early threat detection and to know whether your organization has been breached or worse and if sensitive information is being exfiltrated or medical devices are being tampered with. Healthcare organizations have increased information security as a business priority, however the majority agree that there are still many vulnerabilities in their network infrastructure that have not been adequately addressed.

In a study of 297 individuals employed in healthcare, sixty-eight percent shared that there had been a cyber-attack on their facility recently and carried a low degree of confidence (3.82) in their organization’s ability to detect zero-day attacks, defined as the exploitation of vulnerabilities not known to the software vendor/manufacturer.

The best way to protect your healthcare organization from a cyberattack is to think like a military attacker or hacker. An attacker will start with the targeting and social engineering of an attack, identifying the company and targets within the company that best align with their ability to compromise an organization. They can spend weeks, months, and even years observing behaviors, planting malware, and escalating their attack. Common ways for attackers to penetrate an organization include man-in-the-middle attacks with a close second of content manipulation attacks, in which hackers alter data to cause a victim to perform desired actions through a manipulated interface or in a third-party system. Common threat vectors used are:

• **Reconnaissance Attacks**: Begin with a scan of the network from the infected endpoint to locate the asset and services an attacker wants to target.

• **Stolen Credential Attacks**: Exploit the infected endpoint to extract credentials and the location of the assets that it wants to target.

• **Phishing Attacks**: Will use deceptive techniques to trick a user into revealing credentials or confidential information or to take actions that grant attacker access or privilege.

• **Ransomware Attacks**: Are designed to erase or encrypt networked files with the intent to provide recovery based on payment of ransomware typically paid in Bitcoin. New tactics now include exfiltrating the data as an additional measure to ensure payment. If payment is not made the information is sold on the black market.

• **Insider Threats**: Include employees and 3rd parties with network access. Being on the inside, these individuals circumvent traditional prevention systems and are much harder to detect.
Traditional prevention solutions are designed to block based on known signatures and attack patterns and proven unreliable in detecting the advanced cyber attacker using a zero-day attack, stolen employee credentials, spear phishing campaigns, ransomware, and insider threats. Bring your own device (BYOD) and zero-day web services exploitation has also proven to be highly challenging for traditional security solutions to quickly identify and stop the threat actor.

Building an Adaptive Defense

Understand the most common battle plans and attack paths

The onramp onto your organization’s network starts with exploiting misconfigurations and weak or misapplied policies. Organizations should assess both end-point and the paths to critical company assets. Understanding where an attacker can gain a foothold and how they can escalate to get their target can help predict and prevent attacks from occurring.

All warfare is based on deception

Turn the hunter into the hunted. Deception can change the game by confusing and misdirecting an attacker into revealing themselves and being detected. As used time and again in warfare, setting up deceptions and decoys will distract an attacker and provide insight into attacker’s intent, tools, and methodologies. Deception provides a highly efficient and effective way to detect attackers conducting reconnaissance and attempting to use stolen credentials. Deception lures and bait are planted to trick an attacker into thinking they have found something of value, where instead they are being lead to an engagement server for attack analysis and the revealing of their presence.

Deception solutions now provide real operating systems and services and with advanced providers, can also be set up with a golden image of the production environment, making the decoy indistinguishable to the company asset. Early detection reduces the attacker dwell time, dramatically reducing their ability to mount a successful attack.

Continuous Incident Response

Healthcare organizations should be prepared at all times for a cyber incident and should assume that they can and will be infected if not breached. 2 out of 3 healthcare organizations have stated that they will experience a cyberattack within the next year. Readiness will come in the form of an incident response plan that outlines actions and procedure. It should also come in understanding your detection systems and the depth and organization of information

All warfare is based on deception. Hence, when we are able to attack, we must seem unable; when using our forces, we must appear inactive; when we are near, we must make the enemy believe we are far away; when far away, we must make him believe we are near.

Sun Tzu
that they can provide once an attack is detected. Forensic reporting of attack information with the substantiated detail to quarantine an infected endpoint and to block further contamination or exfiltration should be seen as required information that comes with every alert. Advanced incident response will include the automatic creation of signatures for blocking and should offer to automate the updates for prevention systems for high alert attacks. Sharing of information with threat intelligence databases will also help with understanding the characteristics and history of an attack or enable you to update other organizations to new threats.

**Prevention**

Always prevent what you can, but also admit when there is a weak flank. Prevention systems are great for known threats, however advanced threats find ways to punch through even the best prevention systems. An adaptive solution has prevention and detection working together for the strongest defense.

**Changing the Game with Deception-based Threat Detection**

Many healthcare organizations have made reasonable investments in firewall, IPS, sandbox, and end-point security solutions. However, even the best-of-breed for these security solutions cannot reliably detect sophisticated attacks that are zero-day, come in through the use of stolen credentials or originate from an insider. They have also repeatedly failed in the prevention of ransomware attacks.

- It is estimated that in 2015 alone, there has been over $6 billion in costs and damages associated with cyberattacks and over $8.6 million reported in HIPPA settlements.*
- Unlike an actual data breach, there’s currently no reporting obligation for ransomware attacks. Though attacks on Hollywood Presbyterian Medical Center, MedstarHealth, and Alvarado Hospital Medical Center have been reported as recent ransomware attacks.
- In 2015 it was also reported that a security researcher was able to hack into multiple IV drug pumps from the manufacturer Hospira and alter the administered dosage.

*OCR HIPAA Enforcement: hhs.gov/ocr/privacy/hipaa/enforcement/

The ability to enter networks undetected and evade traditional security measures has driven a shift from a defensive only posture to one of a modern-day adaptive defense that adds offensive strategies to its war against hackers.

Deception as an automated responsive mechanism represents a sea change in the capabilities of the future of IT security that product managers or security programs should not take lightly.

Lawrence Pingree
Research Director at Gartner
By adopting a modern day adaptive defense, organizations are now taking an assumed breached security posture and now going on the offense to proactively predict and detect the presence of attackers. Deception has been recognized by Gartner Vice President, Peter Firstbrook as “the most advanced approach for detecting threats that are inside the network" and has being rapidly deployed within healthcare organizations of all types.

How Deception Works

- Lures attackers into revealing themselves as soon as they start to look for high-value assets in network services across multiple virtual machines, IP services, and subnets.
- Catches the known and unknown attackers. Uses deception to detect an attacker vs. relying on known signatures or attack patterns.
- Reduces attack time-to-detection by accurately identifying infected clients, including sleeper, and time-triggered agents.
- Provides substantiated engagement-based alerts; No false positives.
- Attack analysis is captured by identifying infected systems and by collecting and analyzing information on the time, type, and anatomy of an attack.
- Attack forensics catalog all attack activity in order to understand an attack’s anatomy and objectives and can create Indicators of Compromise (IOC) PCAP files, Syslog, IOC, and CSV reports.
- Includes a comprehensive threat intelligence dashboard with UI drill downs to better understand top attacks, severity levels, and attacker actions. Containment actions can be activated from the console or can be set to automatically apply.
- Attack threat path analysis can also be run for ongoing vulnerability assessment of attacker paths to critical assets.

Attivo Solutions for Protecting Healthcare Organizations and Patient Records

Attivo ThreatDefend™ solutions empower organizations with an advanced deception and response platform that delivers early detection, insight into attacker threat path vulnerabilities, in-depth analysis, forensic reporting, and automations that can dramatically improve a organizations incident response time.

The ThreatDefend Deception and Response Platform is designed for user networks, data centers, cloud, IoT, and SCADA environments and will turn the entire network into a mirror of deceptions and traps for attackers. The ThreatDefend solution provides early detection of attackers that are inside the network, improving an organization’s time to detection (TTD) and the overall time to respond (TTR). Attacker dwell time within a network before detection averages 6 months and time to remediate an attack is shown to on average take another 5+ months.
Attivo Benefits for Protecting Healthcare Organizations

Attivo active deception solutions are an effective, efficient, and scalable way to catch attackers from all threat vectors: advanced persistent threats, stolen credential, ransomware, man in the middle, and insider.

- Real-time luring, detection, and identification of cyberattacks provides an additional layer of security protection for networks, data centers, and medical devices
- Mitigates delayed detection of breaches and additional risks associated with BYOD, workstations, and medical devices
- Effectively identify targeted attacks on end-point devices with the intent to steal credentials to infiltrate company data or patient records or tamper with devices
- Provides authentic, believable deception solutions that are built on real operating systems and services that can be customized to a customer’s environment
- eMail ribbon bar and direct submission of phishing emails to the ThreatDefend BOTsink analysis engine provides hacker intent for phishing emails, thwarting a hacker’s intent to exfiltrate business data and sensitive information or to download malware through phishing campaigns
- Available as an appliance or virtual machine, the solution installs seamlessly and non-disruptively with current security infrastructure including automations for attack blocking and quarantine
- Scalable, non-inline architecture provides friction-less deployment and can be operational within 1 hour
- No false positive design improves effectiveness of the security staff
- Helps satisfy HIPAA privacy rules.
Healthcare Customer Feedback on Investment Benefits and ROI

Healthcare organizations are turning to Attivo Networks for a comprehensive threat detection and response system:

- Real-time, accurate visibility into the existence of in-network threats
- Fast and in-depth analysis of attacker intent with zero false positives
- Updating of anti-incursion systems to shut down actual attacks and prevent future attacks

The Attivo ThreatDefend Deception and Response Platform is the most authentic and accurate way to identify cyber threats before they steal critical data or are able to tamper with medical devices. Attivo ThreatDefend solutions provide organizations shifting from a defensive security posture to an offensive posture; a critical tool in the war against cyber attackers

Real-time Attack Detection (Breach Avoidance)

- Healthcare provider was able to detect and stop a breach from the new variant of Pinkslip, which is now being referred to as Qakbot, which had targeted its 32-bit windows PCs.
- Biotech provider uses deception to alert on attacks on its medical imaging systems and files. Detailed alerts enable them to quickly detect and contain attacks. Reporting is also used to demonstrate to their BOD that vulnerabilities and threats are continuously addressed.

Ransomware

- Healthcare provider detected a CryptoLocker attack with a virus attached; immediate detection provided visibility, thwarted attack, and prevented a major incident.
- Healthcare provider had a Locky attack: Attivo helped contain infection to 3% of systems, preventing a widespread outbreak.

Phishing

- Healthcare device manufacturer uses the ThreatDefend BOTsink analysis engine to analyze daily phishing emails. This saves them hours daily in analyzing emails and updating prevention and detection systems.

Device

- Healthcare device manufacturer to provide the Attivo ThreatDefend deception solution as part of the device management of its drug dispensation systems. This provides additional compliance and responds to recent FDA requests for stronger detection and prevention capabilities on medical devices.

Insider

- Healthcare provider was able to detect an insider who was scanning the network using Powershell in an attempt to break into the backdoor of their Wi-Fi network.
Attivo Healthcare Use Cases

Attivo has created solutions that address many of the greatest cyber vulnerabilities facing healthcare organizations today, including:

- Ransomware
- Phishing
- BYOD Network Monitoring
- Medical Device Segment Monitoring

- Workstations on Wheels and Other In-ward Units
- Public Web Presence
- PCI Compliance Assurance
- Email Phishing Risk Management

Ransomware

Ransomware is a form of malware that typically seeks to encrypt, deny access, or erase files with return access granted upon a Bitcoin ransomware payment. A target could be Electronic Healthcare Records (EHR) in which the entity could be locked out from critical systems and be unable to get access, causing problems for an organization’s hospital data security and HIPPA compliance.

Forms of ransomware including Crypto ransomware (CryptoLocker) will encrypt the data, while locker (Locky, Dridex) ransomware prevents users from accessing the information. There is also a new practice, where hackers are threatening to sell PHI information if ransomware payments are not made. It is important to note that just because an organization has paid the demanded fee, it is not guaranteed that the data will be made accessible again. The Institute of Critical Infrastructure Technology (ICIT) called 2016 the year of ransomware in a report released earlier this year. ICIT added that ransomware will “wreak havoc” on America’s infrastructure.

The Attivo Solution

1. The Attivo ThreatStrike™ End-point Deception Suite provides an agentless solution designed to deceive attackers with deception SMB shares in addition to deception credentials and lures.
2. As the attacker seeks to infect the next networked drive they will be led to the ThreatDefend BOTsink® deception engagement server, which will immediately raise an alert with details on the infected end-point and attack forensic analysis.
3. Manual or automated blocking of attack and quarantine of infected systems through 3rd party prevention system integrations accelerate incident response.
Email Phishing Management

Phishing campaigns typically occur through the use of fraudulent emails which pretend to be legitimate services or companies in order to lure individuals to provide sensitive information or to click on a malicious link where malware is downloaded or account details handed over. Hackers can quickly infiltrate corporate networks and find ways to exfiltrate business data and sensitive information through phishing campaigns.

The Attivo Solution

1. Emails with phishing intent can be sent to the Attivo BOTSink® where the email is sandboxed and the email safely expanded to understand the intent of the attacker.

2. Once the analysis has completed, a detailed report is generated explaining whether the email was malicious and providing the attack detail that can be used to update prevention and detection systems.

3. Organizations cite the hours of time saved by automating phishing analysis.

Bring Your Own Device (BYOD) Network Monitoring

BYOD represents one of the most serious threats to an organization’s network security. Employee-owned devices often attach to unsecured networks outside the work environment and outside of any perimeter security protection, making them vulnerable to threats that may have otherwise been contained as part of a corporate security policy.

Once connected back to the corporate network, such devices are often used to access medical data (e.g. PACS images), creating backdoor for the attacker. Through backdoor, the attacker bypasses all North-South security solutions as the malware uses encrypted communications to communicate with C&C server. The wide variety of BYOD devices many times results in limitations in the effectiveness of end-point security solutions and often to the depth of network access security that can be configured.

The Attivo Solution

1. The Attivo ThreatStrike™ End-point Deception Suite provides an agentless solution designed to deceive attackers with deception SMB shares in addition to deception credentials and lures.

2. As the attacker seeks to infect the next networked drive they will be led to the ThreatDefend BOTsink® deception engagement server, which will immediately raise an alert with details on the infected end-point and attack forensic analysis.

3. Manual or automated blocking of attack and quarantine of infected systems through 3rd party prevention system integrations accelerate incident response.

McAfee Phishing Quiz results indicate that 80% of the 16,000 business users they targeted with fake phishing schemes succumbed to at least one phishing attempt.
Internet of Things (IoT) Revolutionizing Healthcare

The Internet of Things (IoT) is revolutionizing the healthcare industry by changing the way professionals deliver care to patients and how patient data is collected, shared and stored. This new innovation comes with many benefits, however with the increased use of internet connected devices, comes additional security risks. These connected devices can become the target for medical device tampering and become a primary target for ransomware attacks as threat actors seek monetary gain in return for restoring services. Additionally, medical device networks are often overlooked in the IT security monitoring infrastructure providing attackers opportunities to infiltrate and persist in the network undetected.

In a survey of 370 professionals in the medical device/IoT field, over one-third experienced a cybersecurity incident in the past year. If the medical device/IoT field mimics other industry trends, the number of incidents is only going to increase. What is particularly alarming, though, is that since medical devices are built to last longer than most technology, the devices weren’t initially built to cope with the 2018 threat landscape. To combat the evolving attack surface, organizations need tools that stay one step ahead of attackers by not only preventing attacks but also detecting and responding to them early.

To address these challenges, Attivo Networks has collaborated with BD (Becton, Dickinson and Company) to provide visibility and improve detection capabilities against potential cyber threats that can impact medical devices. The Attivo BOTsink® deception-based threat detection solution provides decoys and lures to misdirect potential attackers away from production assets and, through this collaboration, Attivo decoys now provide preloaded software to mirror-match decoy authenticity of certain BD products. This authenticity creates an environment in which a potential attacker cannot discern between real and fake assets; ultimately, revealing an attacker’s activities as they try to scan systems or attempt to download malware onto these devices.

The Attivo BOTsink® deception solution complements protections for certain BD products by placing decoys that appear as production IoT devices to confuse, trip up, and detect potential attackers. BD employed a rigorous evaluation of the Attivo BOTsink technology to ensure it is compatible with certain BD products and performs as indicated. Additionally, the Attivo solution provides attack analysis with indicators of compromise (IOC) and attacker tools, techniques, and processes along with actionable forensics that may be leveraged for remediation.
Medical Device Segment Monitoring

One of the greatest concerns in healthcare is the security of embedded systems providing critical medical care (e.g., IV Pumps, patient monitors, medical x-ray scanners, blood gas analyzers, etc.). These products often utilize embedded popular operating systems, such as Windows, that, due to the nature of the application and FDA certification, are notoriously difficult to maintain via patch strategies.

The application of security patches is often dependent on equipment manufacturers and is outside the control of IT departments. This dependency can make these life-critical devices more vulnerable than typical end-point devices, with limited options on the part of IT to address.

The Attivo Solution

1. By placing Attivo ThreatDefend deceptions and decoys on the same network segments as the medical devices, the network is turned into a trap that will detect potential attacker activity during reconnaissance and lateral movement. The attacker is deceived away from production assets and lured into engaging with the engagement server for early detection and identification.

2. The ability to run real operating systems and to customize the services and applications within the deception platform provides the ability assume the network configuration characteristics of medical devices, making them appear authentic and indistinguishable from production devices.

3. Users can customize the ThreatDefend BOTsink VM’s using medical devices protocols or golden images can be loaded for ideal matching to networked environments of respiratory systems, drug infusion pumps and other medical devices.

Workstations on Wheels (WOW) and Other In-ward Units

In many hospital wards, critical patient information is accessed through the use of workstations deployed around the ward, often on mobile carts. The mobile nature of these devices leads to leveraging Wi-Fi to gain access to network resources. The stations often run specific versions of operating systems supporting specific healthcare applications. Patch management issues and the need for ease of access for healthcare providers can result in these workstations not being in an ideal secure state, making them a high-risk target for malware attacks. Additionally, malware is becoming more sophisticated and navigates around AV or end-point security solutions.

The Attivo Solution

1. Placing the Attivo ThreatDefend deception platform on the same subnet as these workstations provides an enticing target for malware, and real-time detection of the threats, enabling prompt blocking and quarantine, preventing additional systems from becoming infected.

2. The deception engagement server can also be configured to allow communications with the command and control (C&C) providing higher-quality understanding of the vulnerabilities and hacker intent.

3. Configuring the deception decoys to appear as a WOW will deceive an attacker by appearing as an enticing target for malware.
Public Web Presence

In many healthcare organizations, public web presence is hosted outside the firewall using public IP addressing or in a DMZ. The level of threat protection available in these scenarios is often limited when compared with the levels designed for corporate internal networks.

The data throughput requirements of web server farm environments make packet inspection malware detection solutions a problematic approach and potential bottleneck. Additionally, these segments are on more public segments often result in a high number of probes and attempted infections. The volume of logs generated, along with the high level of “noise”, makes analysis and response a labor and process-intensive task.

The Attivo Solution

1. Placing the Attivo ThreatDefend deception solution on these segments will result in a higher quality understanding of the vulnerabilities. Logs generated will be specific to potential malicious activity and lack the usual “noise”
2. Configuring an engagement server to appear as a production web server will make it an enticing non-production target for malware. For the highest levels of authenticity, the environment can be customized, or the golden image of a production server can be loaded.
3. Installing deception lures on production servers and end-points will deceive attackers into attacking the engagement server over other assets.
4. In the event of threat activity, the ThreatDefend engagement server will analyze the attack, report the actions, or automate the threat blocking and quarantine through integrations with prevention systems.

PCI Compliance Assurance

As with many organizations today, PCI compliance is important for credit card processing in Healthcare. PCI function and devices are often placed on their own network segments with compliant security measures implemented.

The Attivo Solution

1. Deploying the ThreatDefend deception platform on PCI subnets adds an additional layer of visibility and assurance.
2. By monitoring your PCI segments and devices with the ThreatDefend platform, a healthcare organization is:
   a. Providing an early warning capability should those subnets become compromised
   b. Adding assurance that the border and other security measures installed are keeping the subnets secure and compliant
Winning the Cyber Security War

The key to an adaptive defensive strategy lies in being able to accept that your healthcare network can and will be infiltrated. The choice to be a sitting duck or to take an offensive posture is within your control with modern day security solutions. Tools are available today that provide insight into vulnerabilities that provide attacker onramps on to your network. Advanced deception is available to deceive and misdirect an attacker’s efforts, which provides early detection and removes the dwell time needed to launch a full-fledged attack. Continuous threat management can also be achieved by having decoys lay in wait for the attacker and then upon engagement can analyze, alert, report, and automate incident response handling, dramatically simplifying and reducing the resources required to shut down an attack.

Tip the battle in your favor and actively consider the vulnerabilities of a prevention only based defense. Know your weakest links and change the battlefield by turning the hunters into the hunted. Deception is the secret weapon of success and will put the control back in your hands, in the same way it has time in again in historical warfare.

About Attivo Networks

Attivo Networks® provides the real-time detection and analysis of inside-the-network threats. The Attivo ThreatDefend™ Deception and Response Platform detects stolen credentials, ransomware, and targeted attacks within user networks, data centers, clouds, SCADA, and IoT environments by deceiving an attacker into revealing themselves. Comprehensive attack analysis and actionable alerts empower accelerated incident response. www.attivonetworks.com