DEFENDING HEALTHCARE ORGANIZATIONS WITH THE THREATDEFEND® PLATFORM
INTRODUCTION

Healthcare organizations face unrelenting attacks as criminals seek to access the personal data they store for fraudulent purposes. While they deploy security controls for compliance reasons and to protect their networks, their security priorities also include protecting medical equipment that provides care for their patients. Recent high-profile breaches and the increasing number of lost health records underscore the healthcare industry’s need for an efficient and effective solution to address advanced cyber threats that reliably protect their data, infrastructure, and patients’ well-being (and even lives) from an attack. The Attivo ThreatDefend platform gives them effective and efficient solutions to defend their business, medical networks, and the data they must safeguard. Through early detection, attack misdirection, and conditional access management, the platform detects attackers, denies them access to sensitive or critical data and accounts, and deflects their attacks away from production systems.

CYBERSECURITY IN HEALTHCARE ORGANIZATIONS

Cybersecurity requirements continue to grow more complex in today’s world of connected health. Healthcare providers, device manufacturers, biotech companies, and pharmaceutical organizations are transforming their IT infrastructures to support electronic health data information sharing and to facilitate new trends in remote working. These demands are outpacing their abilities to protect their electronic health record (EHR) systems, databases, connected medical and personal devices reliably. Today’s world of connected health requires clinical staff and equipment to share personal health information securely while maintaining compliance with HIPAA, HITECH, and Meaningful Use requirements that healthcare organizations must also consider. With this complexity and the investment prioritization of patient services over robust security infrastructures, these organizations have become rich targets for attackers.

Healthcare providers are now a primary focus of cybercriminals as they seek to steal and monetize healthcare information, extort for financial gain, and compromise networks and data for state-sponsored cyber espionage and hacktivism. Ransomware has become a top method of attack. However, medical record theft also continues to be a target because of its ability to command a premium over credit card and other information based upon the social security numbers, addresses, and other claims and medical information, known as personal health information (PHI) that they contain. Criminals prize PHI data because some of the data seldom changes, and their fraudulent use can go months without detection, unlike credit card numbers that trigger fraud alerts and get deactivated. These attacks are often driven by an external threat actor, though many breaches continue to occur via insider access, driven by a disgruntled or financially motivated employee, supplier, temporary worker, or trusted third party.
Healthcare organizations operate in a highly distributed fashion with a very mobile workforce. This can create challenges for security teams to find and secure devices. Devices are often hard to find, and taking them out of service for patching can problematic as they are typically in constant use. Some devices are also used well beyond the software support periods, which then leave them at risk, while others simply cannot be patched in the field as any change to operations must be done by the vendors. Collectively, these all create opportunities for attackers to get onto a network. Once the attackers have established a beachhead onto the network, they will seek to move laterally around to different devices and systems to execute their attack. Their actions include discovery, credential theft, privilege escalation, lateral movement, and data collection activities, using the information to connect and jump to other systems until they find sensitive data they can steal or encrypt for ransom. To remain undetected as long as possible, they use tactics and techniques that are difficult for traditional security controls to detect.

The ThreatDefend platform protects healthcare organizations from adversaries who seek to steal healthcare data for criminal purposes by detecting these tactics and techniques early in the attack lifecycle as they try to break out of their beachhead.

THE ATTIVO NETWORKS THREATDEFEND PLATFORM

The Attivo Networks ThreatDefend platform provides early and accurate detection of in-network threats, regardless of attack method or surface, using deception, deflection, and concealment technologies. It provides a comprehensive protection fabric that blankets the network and detects credential theft, protects Active Directory, and hides and denies access to shares and network assets. This fabric will bait and add misdirections that will derail adversaries early in the attack lifecycle. The solution also provides the ability to automate intelligence collection, attack analysis, and third-party integrations for accelerating incident response. The platform’s components include the BOTsink deception server, the Endpoint Detection Net suite, and ADSecure for Active Directory (AD) protection.

The ThreatDefend Deception Platform creates a threat-informed defense against attackers using its many modular components.

- The Attivo BOTsink® deception servers provide decoys, the Informer dashboard for displaying gathered threat intelligence, as well as the ThreatOps® incident response orchestration playbooks.

- The Endpoint Detection Net suite includes the ThreatStrike® endpoint module, ThreatPath® for attack path visibility, ADSecure for Active Directory defense, the DataCloak function to hide and deny access to data, and the Deflect function to redirect malicious connection attempts to decoys for engagement.
• The ThreatDirect deception forwarders support remote and segmented networks,

• The Attivo Central Manager (ACM) for BOTsink and the EDN Manager for standalone EDN deployments add enterprise-wide deception fabric management.

The ThreatDefend platform enhances existing security controls to give the organization internal network visibility, prevention, and detection for those tactics that attackers use to bypass traditional controls. With native integration to over 40 security controls, the platform accelerates incident response and enables efficient information sharing.

PROTECTING HEALTHCARE ORGANIZATIONS WITH THE THREATDEFEND PLATFORM

The ThreatDefend platform provides credential protection and conditional access control capabilities, which complement existing security controls by providing in-network threat visibility and prevention for discovery, lateral movement, credential theft, privilege escalation, and data collection activities that would typically evade detection. The platform deploys on-premises, in the cloud, and at remote work sites like clinics or remote worksites, defending the organization no matter the network size.

To mitigate the risk of a successful attack, the platform:

• Reduces the attack surface by pre-emptively identifying and remediating credential exposures and misconfigurations that attackers use to move between systems.

• Obscures the attack surface by deploying these decoys and concealing data at the network, endpoint, and AD layers within the enterprise. It uses machine learning to profile the environment, customizing the decoy systems and credentials to match the production servers, endpoints, IoT, and medical IoT devices.

• Projects decoys to misinform and misdirect attackers, then deploys fake credentials that point to these decoys (including ones for medical devices), leading attackers to the engagement environment. The platform includes decoys for many different IoT devices, including drug infusion pumps, and they record all attack activity as forensic evidence for threat intelligence development.

• Hides any user-configured sensitive or critical local and network accounts, files, folders, mapped shares, removable storage, and AD objects, restricting unauthorized access so attackers can’t steal or encrypt them for ransom.

• Identifies illegitimate AD queries and hides sensitive results while inserting fake objects that lead to decoys for engagement. These functions conceal the sensitive data and alert when attackers attempt to enumerate them, giving security teams early warning of the activity, which is particularly useful against targeted ransomware attacks where the attackers use APT-like tactics to find critical data for encryption.
• Further protects against ransomware by creating fake file servers that map hidden shares to endpoints for the ransomware to find. As the malware encrypts the data on these servers, the platform generates alerts on the activity while simultaneously feeding it with unlimited data to stall the attack, giving responders time to remediate the infection.

• Provides the means to load any application, software, or fake data to customize their decoys and match the production environment more closely. They can even set up phony databases filled with fake customer records that alert security teams and record all activity when attackers attempt to access them.

• Creates DecoyDocs that can are used to create fake documents and data for the attackers to steal, alerting when they get opened from inside the network or after exfiltration. These DecoyDocs will send details of each internal system and the geolocation and IPs of external systems that open them.

• Identifies discovery attempts, alerting on any host, port, and service reconnaissance while redirecting inbound or outbound connection attempts that touch closed ports to decoys for engagement. This function further obscures the attack surface as it renders any fingerprinting attempts moot, giving attackers a false understanding of the environment. It also derails lateral movement attempts since every connection attempt that touches a closed port on a host gets redirected to the decoys and can natively quarantine the attacking IP by limiting all inbound and outbound traffic to the decoy environment.

CONCLUSION

Healthcare organizations face numerous threats in today’s cybersecurity environment. Whether it is data theft for fraud or ransomware attacks, they store PHI that criminals desperately want. The penalties for data breaches that involve PHI are severe, as is the potential loss of patient confidence and reputation damage. The ThreatDefend platform provides a much-needed defense against advanced attackers that delivers its value early in the attack process. Its comprehensive functions enhance existing security solutions by providing visibility into attack activities that elude them, giving healthcare organizations the critical tools they need to derail attacks before they become data breaches or ransom situations. To learn more, visit www.attivonetworks.com.

ABOUT ATTIVO NETWORKS®

Attivo Networks®, the leader in cyber deception and lateral movement attack detection, delivers a superior defense for revealing and preventing unauthorized insider and external threat activity. The customer-proven Attivo ThreatDefend® Platform provides a scalable solution for derailing attackers and reducing the attack surface within user networks, data centers, clouds, remote worksites, and specialized attack surfaces. The portfolio defends at the endpoint, Active Directory and throughout the network with ground-breaking innovations for preventing and misdirecting lateral attack activity. Forensics, automated attack analysis, and third-party native integrations streamline incident response. The company has won over 130 awards for its technology innovation and leadership. For more information, visit www.attivonetworks.com.