Acalvio Advanced Threat Defense and Identity Protection for Healthcare Organizations

How healthcare organizations can use deception technology to protect medical devices and sensitive patient data from advanced cyber threats

Healthcare security is marked by an escalation of cyber threats, which contain a diverse range of challenges. These include financial impacts from cyberattacks, organizational and reputational damage, and personal bearings on individuals whose data is compromised. The economic toll of healthcare cyberattacks can be significant, with breaches costing organizations millions, alongside the potential for litigation from affected parties. Healthcare leaders are increasing their cybersecurity investments to counter these threats, focusing on internal and external threat environments.

The rise in attacks on these entities highlights the need for an active defense across all levels of healthcare providers, regardless of their business maturity or breadth. These strategies include exploring new protections against evolving cyberattacks, leveraging AI to balance cybersecurity with user experience, and moving beyond traditional security frameworks to drive collaborative innovation. The importance of securing IoT and IoMT devices is also emphasized and now carries additional regulatory compliance expectations.

Active defense solutions are proactive versus reactive and serve to identify vulnerabilities, alert on attacker engagement, and divert attacks before an exploit or breach occurs. Cyber deception is a favored mechanism for an active defense. It works by populating an organization's computing environment with a wide range of decoys and deception elements that attract the attention of attackers, lead them away from real data and systems, and alert security teams to their every step.

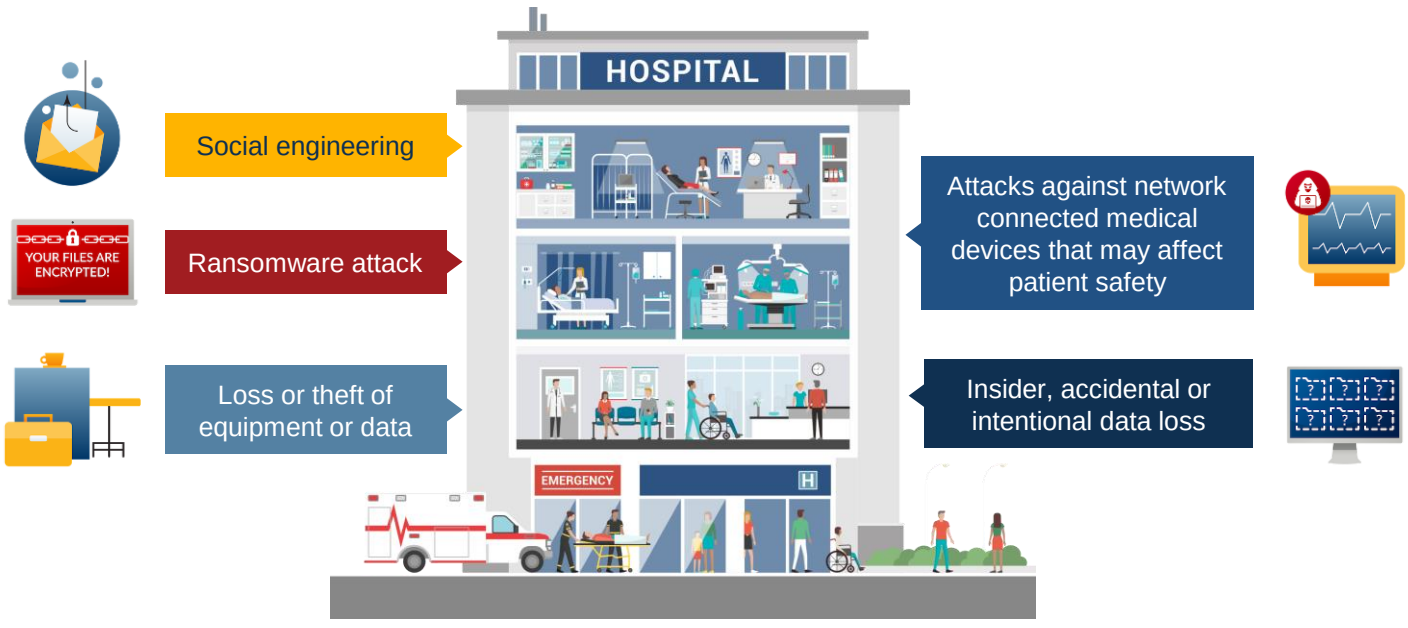
Deception is a recommended cybersecurity practice for healthcare

The Health Industry Cybersecurity Practices (HICP) Technical Volume 2: Cybersecurity Practices for Medium and Large Healthcare Organizations released by the Healthcare and Public Health Sector Coordinating Council provides an overview of cybersecurity practices the industry has outlined as highly effective at mitigating risks in the healthcare industry. It also provides guidance on why cyber deception is critical to a comprehensive security posture.

The tech volume details how Healthcare Delivery Organizations (HDOs) can implement cyber deception techniques, such as deploying honeypots, honeytokens, and other decoys, to create a layered defense and make it more difficult for attackers to access sensitive data.

These provisions and several others demonstrate a significant commitment to advancing cybersecurity defenses for healthcare through proactive measures, including cyber deception and active defense, to protect HDO interests and counter evolving cyber threats.

HHS identifies the top threats targeting healthcare in the figure below.



Source: Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients
https://405d.hhs.gov/knowledgeondemand

Use Cases for Deception-based Active Defense in Healthcare

Medical device attacks: Network-connected medical devices such as IV devices, fusion pumps, imaging devices, and IoT devices are increasingly subjected to attacks. Medical devices are often not updated with the latest patches, providing opportunities for attackers to perform vulnerability exploits. Medical devices are also not compatible with agent-based security solutions such as EDR, making them particularly vulnerable. Defense teams can deploy decoys that represent medical devices and detect threats to prevent attack propagation and protect the real devices.

Ransomware: A wide variety of ransomware threat actors target healthcare, with ransomware-as-a-service (RaaS) affiliates generating novel ransomware variants to evade detection by traditional security solutions. Ransomware threats employ double extortion techniques to exfiltrate sensitive Protected Health Information (PHI) data in healthcare. Acalvio ShadowPlex provides a unique and proven approach based on deception technology and AI to detect known and unknown ransomware variants with precision and speed. Acalvio's ransomware detection is based on a carefully optimized combination of deceptions (decoys, breadcrumbs, specially crafted baits) that detect ransomware activity with precision. Acalvio's approach does not depend on signatures or anomaly-based detection and is a proven approach for detecting evolving and zero-day ransomware variants.

Loss or theft of equipment or data: Healthcare organizations have critical assets and sensitive data, such as PHI data. Adversaries leverage identity-driven attacks and data exfiltration techniques to gain trusted access to critical assets and sensitive data.

Identity-driven attacks: Adversaries target identity architecture in healthcare organizations to gain access to credentials for privilege escalation and lateral movement. Credential access is gained through identity stores such as Active Directory (AD), Cloud identity stores, credential caches on endpoints, and application caches. Readily available offensive tooling is easily used to access privileged user accounts and service accounts. Adversaries leverage the stolen credentials to compromise critical assets in healthcare, such as medical systems and servers that store patient records. Traditional security solutions are unable to differentiate between legitimate and malicious use of credentials. Healthcare organizations can deploy identity honeytokens based on deception technology to detect identity-driven attacks with precision. This provides an effective deception-based identity threat detection and response (ITDR) layer to detect identity threats, including current and evolving threats. Healthcare organizations can mature their Zero Trust Architecture (ZTA) by deploying identity honeytokens across the identity stores and endpoints.

Data exfiltration: Data loss is the primary threat vector for healthcare, with PHI data being the top target. Adversaries leverage stealthy and evasive offensive techniques such as living-off-the-land (LotL) techniques and AI-fueled polymorphic malware variants to evade detection and gain access to the data. Embedding data deceptions in the data and deploying baits on attack pathways provides an effective approach for the early detection of threats targeting sensitive data.

Insider threats: Insider threats are of particular consequence for healthcare organizations. Insiders can represent malicious insiders, negligent insiders, or third parties. Insiders have trusted access to medical data and files containing sensitive healthcare information. Insider threat risk from third parties is a critical risk factor for healthcare, with healthcare organizations providing third parties with access to their systems. Defense teams find it challenging to detect insider threats using traditional security solutions because the trusted access does not trigger anomaly-based alerts and leaves no clear signal in the logs. Cybersecurity recommendations for mitigating insider threat risk include goals for deterring the individuals, detecting the activity, and disrupting the effort. Deception-based Active Defense is the only approach that can help defense achieve these goals, providing a critical capability to protect healthcare organizations from the risk of insider threats.

Advanced Threat Defense and Identity Protection for Healthcare Organizations

Acalvio ShadowPlex Advanced Threat Defense and Identity Protection offerings provide a proven approach for protecting healthcare organizations from cyberattacks. ShadowPlex is an agentless solution, ensuring ease of deployment in healthcare. ShadowPlex is pre-integrated with security platforms such as EDR, SIEM, and SOAR, covering interoperability with the enterprise ecosystem. ShadowPlex provides healthcare-specific deception templates and strategies, providing immediate time to value in healthcare.

Healthcare frameworks and advisories include:

- The Health Industry Cybersecurity Practices (HICP) Technical Volume 2: Cybersecurity Practices for Medium and Large Healthcare Organizations document (https://405d.hhs.gov/Documents/tech-vol2-508.pdf). The document specifically cites reduced dwell time, improvement in threat intelligence, and increased situational awareness as key benefits.
- Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP)," published by the U.S. Department of Health and Human Services (HHS) in partnership with the healthcare industry. This publication is a crucial outcome of the Cybersecurity Act of 2015, Section 405(d), aimed at providing guidance and best practices to enhance cybersecurity across the healthcare sector. The HICP document primarily addresses the most pertinent cybersecurity threats to the healthcare sector and outlines best practices to mitigate these risks. It covers aspects such as protecting against ransomware, securing network-connected medical devices.

Summary

Cybercriminals are actively targeting HDOs of all sizes, with smaller regional providers, specialty clinics, and medical imaging facilities serving as increasingly attractive targets due to their sensitive data. HDOs can implement cyber deception techniques, such as deploying honeypots, honeytokens, and other decoys, to create a layered defense and make it more difficult for attackers to access sensitive data. Cyber deception has become the foundation for an Active Defense and is rewarding HDOs with efficient attack disruption, early warning of intrusions, and the impact reduction of a successful attack.

Visit www.acalvio.com/schedule-a-demo to request a consultation or for insights into what's new in cyber deception in 2024.

LEARN MORE

ACALVIO

Acalvio is the leader in autonomous cyber deception technologies, arming enterprises against sophisticated cyber threats including APTs, insider threats and ransomware. Its AI-powered Active Defense Platform, backed by 25 patents, enables advanced threat defense across IT, OT, and Cloud environments. Additionally, the Identity Threat Detection and Response (ITDR) solutions with Honeytokens enable Zero Trust security models. Based in Silicon Valley, Acalvio serves midsize to Fortune 500 companies and government agencies, offering flexible deployment from Cloud, on-premises, or through managed service providers. For more information, please visit www.acalvio.com