Three Use Cases for Deception Technology in Healthcare

Black Hats vs. Top Hats

A white paper series on the use of deception technology to address industry-specific cyber risks
In healthcare sectors, security teams struggle to keep pace with the escalation of cyber risk. From care delivery to claims processing, digital transformation and data-sharing across the ecosystem is enabling precise, patient-centered service while controlling costs. However, the speed of business innovation raises risk for every entity—providers, insurers, researchers, pharmacies, and patients themselves. Investing more in traditional approaches is not likely to close the gap.

In every industry, advanced attackers evade security controls, but data-rich health systems are especially favored targets. Deception technology provides a simple, pragmatic approach to protect both the mission and the bottom line by stopping attackers before they can do significant damage—one that is easy to adopt, even for organizations without advanced cyber capabilities.

Preventing more than HIPAA fines

The recent wave of ransomware attacks aimed at healthcare organizations caused disruption that threatened patient safety. Beyond care outages, exposure of private data can risk damage to patient trust—a critical asset in an era when patients have more power to choose providers and insurance carriers, and when efficiency and effectiveness depends on their willingness to share information and use self-service applications.

Yesterday’s threat detection isn’t working

To execute an advanced, targeted attack, perpetrators must complete several phases. First, they must break in and establish presence on one or more computers—which is now easier than ever. Growing sophistication in attack tools and techniques is one factor, but a second important element is the growing complexity of the IT landscape. The explosion in mobile applications, proliferation of IoT devices, widespread M&A activity, and the dramatic increase in data-sharing across the health ecosystem dramatically increase the attack surface and make it more challenging to close security gaps and patch vulnerabilities.

In the second phase, attackers must become oriented with the environment, and figure out where coveted assets are and how to get to them. This can take weeks or months, and involves extensive information-gathering to determine how to move forward. Because advanced attackers use valid user names and passwords and access systems like a trusted user would, they don’t discernably break rules—and carefully evade traditional detection methods.

Figure 1: Stage two of the advanced attack process

Upon entry, the attacker must become oriented, understand the environment, and begin a protracted lateral movement process toward the organization’s “crown jewels.”
Finally, once within striking range of their targets, attackers manipulate various data stores, processes, or applications, depending on the nature of the quest. Most organizations, unable to catch attackers in the second stage, end up reacting to a cyber crisis once damage has been done. Illusive’s deception technology fills this critical gap. It is purpose-built to catch the attacker during lateral movement so responders can derail attackers long before they achieve their objectives.

**Preventing “code blue” and getting ahead of advanced attackers**

Illusive’s Deceptions Everywhere® approach works by planting fake information throughout the environment. Within the first few moves of the search-and-advance process, the attacker inevitably tries to use a piece of false an alarm and a forensic snapshot is captured from system where the attacker is operating. This situation requires triage but is not a “code blue.” Only an attacker can see deceptions, so Illusive creates no “noise.” Responders know an Illusive alert requires immediate attention. At the Illusive console, they can see how far the attacker is from the organization’s “crown jewels” and from systems where the attacker could find domain admin credentials. They can take immediate action, or continue to observe and analyze the attacker’s activity.

Agentless and built on intelligent automation, the Illusive solution is easy to deploy and maintain. It provides security teams with tools to make it more difficult for future attackers to move across the environment and delivers quantifiable risk metrics on business-critical systems, applications and processes. Below are three common deception use cases associated with cyber risk management objectives in healthcare organizations.

**Figure 2: A web to catch attackers moving toward critical assets**

In this diagram, blue “crown” symbols represent database, servers, and user stations that house and handle electronic health information (EHI). Deceptions planted across the IT infrastructure trick attackers into revealing themselves as they try to move toward them. Once an attacker tries to use deceptive information, an alarm is triggered and the Illusive system captures forensic data.
Use Case #1: Protecting Patient Data—from Outsiders and Insiders

Because high-volume data breaches are typically elusive, advanced attacks requiring a period of discovery and lateral movement, protecting patient data is a foundational use case for deception among healthcare providers and insurers. In the first half of 2017 alone, the healthcare industry experienced 228 breaches with 31 million records stolen—up 423% from the preceding six months. That trend continued in August and September 2017, during which 33 and 46 healthcare breaches were reported, respectively.

When Illusive detects an attacker, analysts immediately see where the attack is in relation to systems that process or store EHI, PII, or payment data. The incident record is instantly populated with a forensic snapshot from the compromised machine, presented in user-friendly language, giving responders what they need to act quickly and decisively. This method applies to any deliberate, advanced attacker, whether an outsider or a trusted insider. Illusive offers API-based integration with SIEM or common data protection technologies such as DLP or endpoint protection solutions. Incidents generated by other technologies can be configured to trigger Illusive’s forensic data collection, and the associated systems can automatically display on the Illusive Attacker View map, helping security teams correlate information and prioritize response and remediation.

When not responding to critical events, security professionals can use Illusive’s monitoring and risk visibility tools to proactively strengthen defenses and minimize the attack surface by:

- Identifying anomalous connections, compromised credentials, and users who may have unauthorized, elevated levels of access;
- Identifying areas where network segregation is not functioning as intended;
- Scanning the network for new endpoints, servers, and connection pathways to ensure there are no gaps in deception coverage.

**Figure 3: Knowing how far the attacker is from critical assets**

Illusive’s Attacker View map shows how far attackers are from critical business systems. White objects represent actual systems, and a subset of these (marked with the “crown” symbol) house domain admin credentials. Yellow objects represent deceptions. Turquoise elements have been named as risk-sensitive assets, or have been discovered to house domain admin credentials.
Three Use Cases for Deception Technology in Healthcare

Use Case #2: Guarding the Business through M&A-Driven Change

During or after an acquisition may be the time a company can least afford unauthorized data exposure or negative publicity from a cyber crisis—yet risk exposure can be much higher than usual. Extended phases of IT change and consolidation can leave dangerous security gaps. Ordinary patching and maintenance tasks may take a back seat to special convergence projects. Unless a thorough security assessment is done during due diligence, the acquiring entity may inherit dormant cyber threats along with the IT assets it acquires.

Deception provides nimble, elastic protection during these events. Not all deception technologies are up to this task, however.

The solution must rapidly discover and continuously rediscover the environment to identify newly added systems and changes to network and system usage patterns. Deceptions must be perpetually designed, tuned and tailored to the unique customer environment so they appear authentic to attackers.

Advanced automation is a baseline requirement for delivering these capabilities at speed and scale. Illusive’s AI-driven Deception Management System™ (DMS) gives business leaders the confidence that as infrastructure is being realigned, repurposed, or consolidated, advanced attackers are not able to take advantage of a high number of security gaps.

Figure 4: Deception environments require smart automation

Illusive’s DMS automates the four phases of the deception cycle to ensure that customized deceptions continuously cover the entire environment, even when the infrastructure is rapidly growing and changing.

1. Identify
   Crown Jewels and the users and systems that routinely interact with them

2. Design
   Deceptions based on knowledge of application architecture & business processes

3. Deploy
   Specialized deceptions where needed, & general deceptions broadly on all endpoints

4. Operate
   By responding to alerts and maintaining a fresh deception environment
Use Case #3: Protecting “Untouchable” Legacy Systems and Custom Applications

Although digital transformation may consume the lion’s share of cybersecurity attention, protecting critical healthcare or insurance operations can require integrated protection for legacy or proprietary technologies within a larger end-to-end service chain.

Yet mainframes, custom ERP applications, and proprietary medical technologies can be difficult to secure or monitor. Some were never designed to meet current security standards.

Others lack built-in support for IT monitoring. Zero tolerance for downtime may mean that systems rarely get patched or upgraded, that migration to newer platforms is not practical, or that installation of agents or security controls is prohibited.

Deception provides an alternative security strategy. Rather than monitoring activity on these assets directly, a specialized deception environment creates the ability to see and act against malicious actors trying to access or move toward these assets, resulting in early detection rather than reactive response once the attacker has reached critical assets. For this use case, the defined scope of “crown jewels” typically includes the essential assets themselves, and any console systems or other machines that provide access to them.

With awareness of the entire web of connectivity across the enterprise, and knowing the location of privileged credentials, Illusive can also help security teams identify unauthorized connections to these systems, and “rogue” credentials residing on systems where they don’t belong.

Figure 5: An extra ring of awareness around configuration-sensitive assets

The systems in the shaded area represent console systems, user workstations, servers and other systems that connect directly to the machines that cannot be secured directly. Specialized deceptions are deployed on them that imitate proprietary connection protocols, user interfaces, credentials, and other artifacts that mimic actual ways users engage with these devices.
In Closing

Described here are only three ways healthcare organizations can benefit from a deception approach. In today’s healthcare environments, new cyber vulnerabilities and risks open as fast as older ones get remedied. Leaders must reshape their cyber programs, acknowledging that in today’s hyper-connected world, attackers are always looking for a way in—or may already have penetrated. Without an active defense model built to counteract silent, advanced attackers, the business gains of digital transformation and innovative engagement models may be lost to the devastating impact of a successful cyberattack.

CISOs face many choices about how to keep pace with business change. But deception technology is more than just another tool in a controls-focused, layered defense model. Illusive provides attacker-centric visibility across the entire IT landscape, delivering high-fidelity alerts and the tools responders need to resolve incidents quickly and to slow the attacker’s movement through the environment. It is a lightweight, easy-to-manage solution that helps resource-constrained healthcare organizations rapidly achieve what has previously been elusive to even the most advanced cyber teams: the ability to prevent the life-and-death consequences of successful advanced attack.

Endnotes

1 The mobile healthcare app market is projected to grow 44.2% between 2014 and 2025 according to a report by Grand View Research, Inc.
2 MARKETSandMARKETS IoT Healthcare Market Global Forecast, April 2017, reports that size of the healthcare IoT market is expected to be $158 billion by 2022, based on 30.8% CAGR from 2017-2022.
3 In a report issued in October 2017, Kaufman Hall noted that the total number of mergers and acquisitions in healthcare in 2017 could outpace the record-breaking number in 2016.
4 According to the edgescan™ 2016 Vulnerability Statistics Report, it takes an average of 59 days to fix vulnerabilities associated with high-risk web applications.
5 2017 Poor Internal Security Practices Take a Toll, Breach Level Index, Findings from the first half of 2017, Gemalto
6 October 2017, Healthcare Data Breaches, HIPAA Journal
Three Use Cases for Deception Technology in Healthcare

For additional resources or to subscribe to our blog, please visit us at www.illusivenetworks.com

For more information about the Illusive’s Deceptions Everywhere® approach and the Illusive Core Solution, visit https://www.illusivenetworks.com/deceptions-everywhere

Visit our https://blog.illusivenetworks.com/ blog and our https://www.illusivenetworks.com/collateral resources page for articles on best practices for deception in the health industry

To discuss your unique business requirements, please call us or email info@illusivenetworks.com

United States and Canada
+1 844.455.8748

Outside the US
+972 73.272.4006

Follow Us:

About Illusive Networks

Illusive Networks is a pioneer of deception technology, empowering security teams to take informed action against advanced, targeted cyberattacks by detecting and disrupting lateral movement toward critical business assets early in the attack life cycle. Agentless and driven by intelligent automation, Illusive technology enables organizations to significantly increase proactive defense ability while adding almost no operational overhead. Illusive’s Deceptions Everywhere® approach was conceived by cybersecurity experts with over 50 years of combined experience in cyber warfare and cyber intelligence. With the ability to proactively intervene in the attack process, technology-dependent organizations can preempt significant operational disruption and business losses, and function with greater confidence in today’s complex, hyper-connected world.

Copyright © 2018 Illusive Networks. All rights reserved.