



The Top Threats Targeting Healthcare

Five key cyber threats impacting health providers and how to protect against them



Foreword

Healthcare Was Once Off-Limits for Hackers. But Those Days Are Long Gone.

Healthcare used to be the ethical line hackers wouldn't cross. Sadly, things have changed. The entire industry—from hospitals to medical labs to pharmacies to rehab centers and beyond—is now a lucrative target. Cybercriminals are clamoring to get their hands on your data, and they couldn't care less about who they hurt in the process. They'll crash your systems. Force you to reroute ambulances. And even delay life-saving surgeries.

Worse yet, these aren't isolated incidents anymore. They're the new norm. In fact, the U.S. Department of Health and Human Services (HHS)* has even shot off the warning flare, calling out five of the most dangerous threats currently hurting the health sector.

* To learn more about HHS' guidance on cyber threats, you can [read their full report](#), *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients*.

Top Five Threats Targeting Healthcare:



Social Engineering

Phishing and other manipulative tactics are designed to trick you and your team into making moves that serve the attackers and hurt your organization.



Ransomware

Malware that locks up your sensitive data and holds it hostage until you pay up—often at a devastating cost.



Attacks Against Interconnected Medical Devices

Hackers can now infiltrate your network, seize control of medical devices, and put patient lives on the line.



Loss or Theft of Equipment and Data

Sensitive patient data can potentially fall into the wrong hands when a device is lost or stolen.



Insider, Accidental, or Malicious Data Loss

Data loss—whether caused by a careless mistake or malicious intent—can wreak havoc on your healthcare organization.

Table of Contents

Introduction: Healthcare Is Now a Gold Mine for Hackers	4
Navigating Human Error and Social Engineering in Healthcare.....	5
Three-Letter Solutions, One Objective: How MFA, MDR, and SAT Can Outwit Social Engineering	10
Real-World Incident: An Email-Based Attack Uncovers Larger Crimes	14
Fighting the Plague of Ransomware	15
Leveraging Managed EDR Solutions to Protect Against Ransomware	18
Real-World Incidents: An Ounce of Prevention is Worth a Pound of Cure	19
Interconnected Devices Inject Risk Into Patient Safety.....	20
The Physical and Digital Realms are Now Interwoven	21
Interconnected Devices Are a Double-Edged Sword	22
Scenario: Breaching a Nurse Call System	24
Accidental or Intentional Data Loss Can Be Debilitating for Healthcare	26
Scenario: Hot Data and Cold Coffee	28
Scenario: One Good Nurse. One Crooked Nurse. Two Bad Outcomes.....	29
How to Protect Against Data Loss and Theft	30
Make Security Awareness Second Nature for Your Organization	31
Your Prescription for Cybersecurity Success.....	32

Introduction

Healthcare Is Now a Gold Mine for Hackers

Across healthcare organizations, there's an endless amount of data. And data is how hackers get paid. Whether they hold it hostage through ransomware or simply sell it on the black market, data is valuable. In 2024, UnitedHealth learned this the hard way, paying a ransom of roughly \$22 million. Though hackers once had an unwritten code that life-saving institutions were off limits, this payment only incentivized the worst threat actors to set their sights on health providers of all sizes.

This is unfortunate because one thing's always been clear—healthcare is an “easy target.” Doctors, nurses, and other medical staff are always on the move, multi-tasking at all hours of the day. In this high-pressure, fast-paced environment, it's easy to lose focus for a moment and click on an email without a second thought. But there are plenty of potential consequences from that seemingly harmless click, including:

- Your organization's reputation suffers
- Patients' data gets exposed, increasing the risk of identity theft
- Critical systems are disrupted, compromising patient care
- Trust in your services erodes, leaving patients anxious and fearful
- IT and security resources are overwhelmed and overstretched
- Doctors and nurses are unable to access vital information
- Financial losses escalate through legal fees, compliance penalties, and lost revenue

These are repercussions neither you nor your patients should ever have to face. Let's explore the most prevalent threats targeting healthcare, gain insights into their tactics, and learn how to effectively counter these malicious attacks.

Navigating Human Error and Social Engineering in Healthcare

Threat: Social Engineering

Nobody's perfect. Even the sharpest among us makes the occasional mistake. Cybercriminals know that. And that's precisely why they love social engineering.

Social engineering is the deceitful art of tricking people into handing over valuable data. Across healthcare organizations—hospitals, pharmacies, regional clinics—cybercriminals will attempt to communicate with countless individuals to gain unauthorized access to sensitive information. The most common tactics are:

- Phishing
- Business email compromise (BEC)
- Vishing

Usually starting as an unsolicited message, social engineering attacks can lead to severe breaches, jeopardizing protected health information (PHI) and financial records. And even disrupting vital medical services. Hackers favor social engineering methods for their simplicity—whether they're sending 100 or 1,000 emails, the effort is minimal, and all it takes is one recipient caught off guard to succeed.



Phishing

Phishing is the [leading cause of healthcare data breaches](#) today. Phishing emails—and the texting equivalent SMSishing (or smishing)—appear to be from a trusted source, usually urging immediate action. In healthcare, threat actors rely on phishing to either steal data or access networks to initiate ransomware attacks. Once ransomware encrypts your data, your ability to conduct business and treat patients is compromised. Because PHI primarily lives digitally, in the midst of a ransomware attack, medical practitioners can't access patients' records, and in the ensuing chaos, must rely on pen, paper, and guesswork to provide treatments.

A common phishing scam you've likely seen involves an email appearing to be from PayPal. It cites unusual activity on your account and demands you click a malicious link to reset your password. Exploiting your trust in this recognizable company, the hackers are provoking you into performing a harmful task such as providing your credentials or, worse, running a malicious payload.

The [FBI recently alerted the American Dental Association \(ADA\)](#) of a phishing threat targeting oral surgeons. Threat actors are posing as people seeking to register as new patients. Once they receive their new patient forms online, they'll contact the practice and claim they're having trouble submitting them online and request to scan and email them instead. The threat actors then email the "forms" as an attachment, which, when opened, deploy malware.

Gone are the days, however, when a closer look at a message could reveal obvious red flags—grammatical errors, aggressive language, and mysterious links or attachments. Hackers are doing their due diligence on you and your organization. And with the increasing adoption of generative AI tools, they're getting far better at creating [deceptive emails and websites](#) that appear nearly identical to the sources they're impersonating.



BEC

[Business email compromise](#) is just as it sounds—an email account has been compromised. BEC attacks are more targeted than your average phishing email.

These attacks are designed to look like they come from someone whom you trust, like your bank or your CEO. However, the account itself is either spoofed or under the control of an adversary impersonating the account owner. The messages will ask you to perform tasks like initiating a wire transfer on their behalf, or trick you into providing your own email login credentials. From there, the domino effect continues, as threat actors can take control of your account and email your contacts, misleading them into performing fraudulent tasks or infecting their systems with malware.

According to the [2024 Cyber Threat Report](#), our internal threat analysis reveals that nearly 35% of Microsoft 365 threats in healthcare involve malicious inbox rules. Malicious inbox rules allow cybercriminals to take control of your messages. They can intercept, delete, or redirect communications and even initiate unauthorized financial transactions—all without you even knowing.



Vishing

Though most social engineering is executed by digital means, a simple phone call can be as effective. If you've ever been contacted about your car's extended warranty, then you've encountered "vishing" (voice + phishing). In larger healthcare settings, where you may not know all of your coworkers, these calls can come from someone pretending to be from another department in need of your personal info such as your login credentials. The U.S Department of Health and Human Services (HHS) is warning healthcare orgs that hackers are directly [targeting IT help desks](#). Calling with local area codes, the hackers pretend to be employees from the finance department. Claiming their work-issued smartphones are broken, they request a new device under their control be enrolled. If successful, these tactics can allow attackers to gain administrative privileges, redirect bank transactions, and access sensitive patient data.

And with the rise of AI-generated voice-replication tools, someone may call you sounding just like a trusted colleague or a high-level executive, and you'd be none the wiser. So if you ever receive an unexpected call requesting personal credentials, regardless of who you think is on the other end of the line, remember, mum's the word.



Three-Letter Solutions, One Objective:

How MFA, MDR, and SAT Can Outwit Social Engineering



Threat actors want one thing—money. So much so that they'll invest considerable time and resources to research you and your specific role. This means the emails, texts, and calls you receive can appear far more legitimate and trustworthy, making it easier to deceive you and your colleagues.

The rise of social engineering highlights the need for a ["defense in depth"](#) approach, a holistic strategy creating barriers of protection to mitigate potential breaches. Multi-factor authentication (MFA) and a security awareness training (SAT) program can ensure your people are alert and serve as your first line of defense. And should any threats slip through, you can bolster your defenses with managed detection and response (MDR).

MFA

[MFA](#) adds a layer of security to your standard login processes. For instance, if you've ever tried to get into your banking app, but first had to input a code sent to a separate device, then you're already familiar with MFA.

In a healthcare setting, enabling MFA helps reduce the risk of phishing and BEC attacks. If a cybercriminal obtains your password, they may attempt to use it to gain unauthorized access to your other accounts. After all, many people tend to reuse the same usernames and passwords across accounts. However, with MFA, even if the attacker has your credentials, they'd still need an additional factor, such as a temporary code sent to your personal phone, to successfully authenticate and access the account. This additional layer of security makes it much more difficult for attackers to gain unauthorized access and helps protect against fraudulent activities.

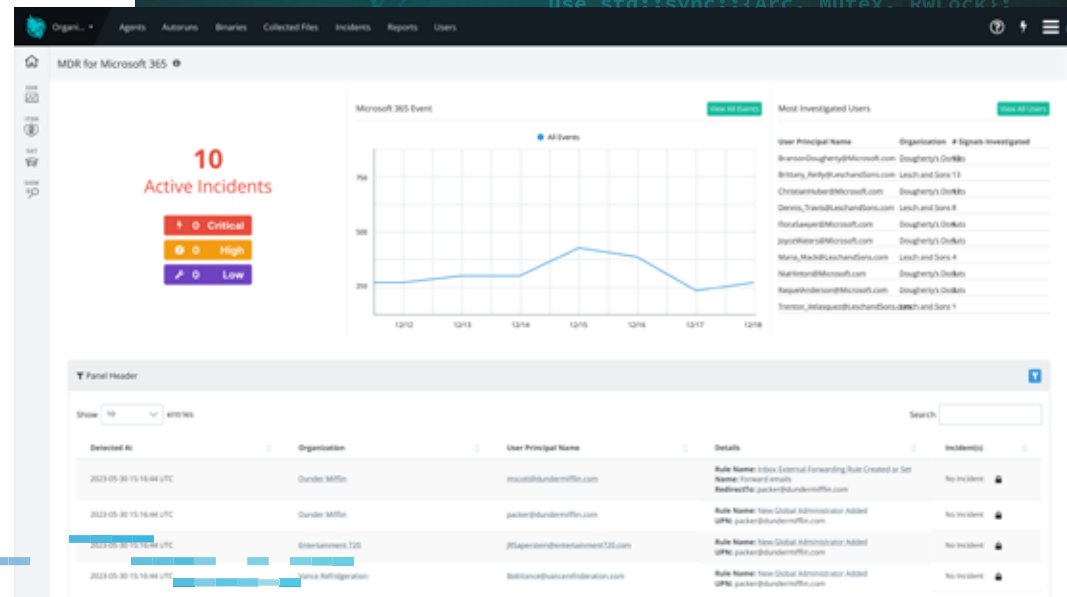
Because healthcare organizations handle so much sensitive patient data, MFA helps protect it by reducing the risk of unauthorized access. Of course, MFA alone can't be your only line of defense.



MDR

To defend your healthcare organization from social engineering tactics such as BEC and phishing, you must be able to protect individual identities. An MDR solution can collect and analyze information from logs, events, networks, endpoints, and user behaviors. Coupled with a team of cybersecurity analysts who can validate incidents, MDR solutions can escalate critical events and provide you with an action plan to remediate threats quickly.

Microsoft 365 delivers a suite of features and services that help medical professionals better communicate and collaborate, making it a popular tool across healthcare organizations. As a result, it's also a popular target for cybercriminals. [Huntress MDR for Microsoft 365](#) secures your Microsoft 365 users, applications, and environment by leveraging our 24/7 [Huntress Security Operations Center \(SOC\)](#). Our SOC experts meticulously monitor and promptly respond to real-time security threats, including anomalous login activities, email tampering, unauthorized forwarding, and attempts at privilege escalation. In short, Huntress MDR for Microsoft 365 can effectively thwart account takeovers.



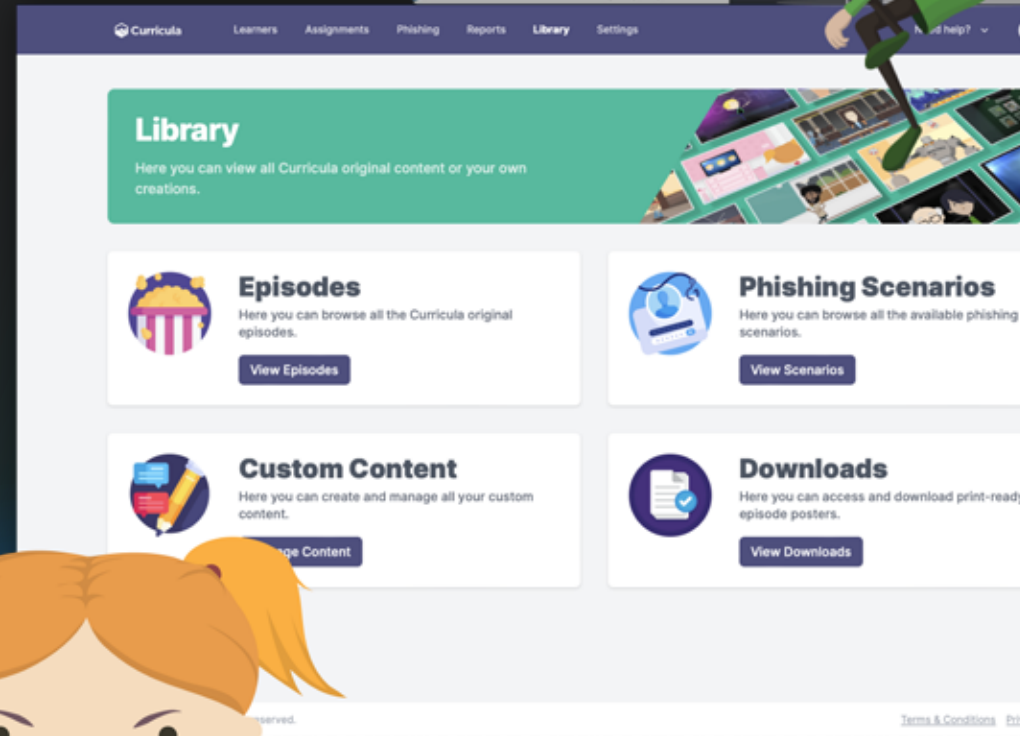
SAT

It can't be overstated, your people are your first line of defense. While sophisticated cyberattacks target systems, phishing and BEC go straight for human vulnerabilities. That's why it's so important that all individuals across your organization can identify potential threats. This is where a SAT program comes in handy.

SAT programs educate individuals across your organization on how to recognize and respond to potential cybersecurity risks. A [good SAT program](#) delivers regular lessons, tests, and phishing simulations, all designed to help your people better identify and defend against social engineering risks.

Every tactic taught in a SAT program must become second nature to the learner. To enhance knowledge retention, [Huntress designed a SAT solution](#) that fuses vibrant animations, memorable episodes, and science-based learning principles. A core component of Huntress SAT is the phishing simulations, which are created, curated, and deployed by our own experts.

Our Phishing Defense Coaching feature supports your users who may have fallen victim to phishing simulations. Instead of having the user repeat training (or admonishing them as failures), a Huntress cybersecurity analyst walks them through key elements in the email that were overlooked, such as fake links or unusual interfaces. This method helps individuals across healthcare organizations better understand why they're being targeted and enables them to prevent real attacks moving forward.



Real-World Incident

An Email-Based Attack UnCOVERS Larger Crimes

When a Midwest-based managed service provider (MSP) rolled out Huntress MDR for Microsoft 365, Huntress' SOC quickly uncovered a sinister plot unfolding for a client. Suspicious inbox rules had been created in the CEO's email account, redirecting senders to various bank domains.

The MSP sprang into action, alerting the unsuspecting CEO of the covert activities. Huntress automatically dismantled the shady inbox rules and reinstated MFA, shutting down the cybercriminal's access to the CEO's account. But the story didn't end there.

Reflecting on how his electronic mail had been impacted, the CEO realized he hadn't received physical mail in weeks. A call to his bank revealed a blackhearted scheme: multiple attempts were made to add new users to his account, which would've allowed the attackers to make wire transfers on a whim.

The hackers had siphoned valuable data from the CEO's email and tried to use it to their advantage. But Huntress MDR for Microsoft 365 detected the most subtle behavioral anomalies and averted a financial catastrophe for the client.

To learn more about how the digital and physical worlds became intertwined, read the case study [here](#).

Fighting the Plague of Ransomware

Threat: Ransomware

By now, we all have pandemic fatigue. But before we put our guards down, there's another contagion spreading: ransomware. It moves with ferocity, especially across healthcare, and if it can't be stopped in its earliest stages, it can have lethal consequences.

The stats alone tell a tragic story:

\$10.9M

average [cost of a healthcare data breach](#) in 2023

133M

[health records stolen](#), exposed, or impermissibly disclosed in 2023

20% - 35%

increase in [in-hospital mortality](#) for patients admitted to a hospital undergoing a ransomware attack

These numbers are just the beginning of the story. As healthcare providers increasingly rely on digital data to improve patient care, they're faced with a double-edged sword. While it's easier to access and share vital information, this very convenience leaves the systems storing that data wide open to cyberattacks.

[Ransomware](#) is like a viral pathogen, and social engineering, such as [phishing](#), is a vector for its transmission. Attacks can often go undetected until it's too late. Some estimates say [healthcare data breaches can go over 230 days](#) before they're even uncovered. Yet once ransomware propagates, it does so quickly, encrypting thousands of files within minutes.

Hackers particularly [love exploiting weaknesses in healthcare IT systems](#) to access an organization's protected health information (PHI), and then they hold it hostage until a ransom is paid. Upon receiving payment, the hackers—assuming they keep their word—will provide a decryption key to release your data.

According to [The HIPAA Journal](#), in 2021, even when healthcare organizations paid the ransom, less than 65% of their data was restored. Worse yet, only 2% of organizations that paid were able to restore all of their data.

Additionally, ransomware-as-a-service (RaaS) has helped proliferate cyberattacks on healthcare organizations big and small. Shady operators create RaaS tools and distribute them to affiliates, who, in turn, offer the operator a cut of the profits. This means anyone with a few technical skills and even fewer scruples can execute ransomware attacks.

And if you don't pay? That's no problem, at least for the hackers. PHI is quite lucrative on the black market. In fact, the U.S. Department of Health and Human Services (HHS) reports health records can fetch [up to \\$1,000](#) a pop.

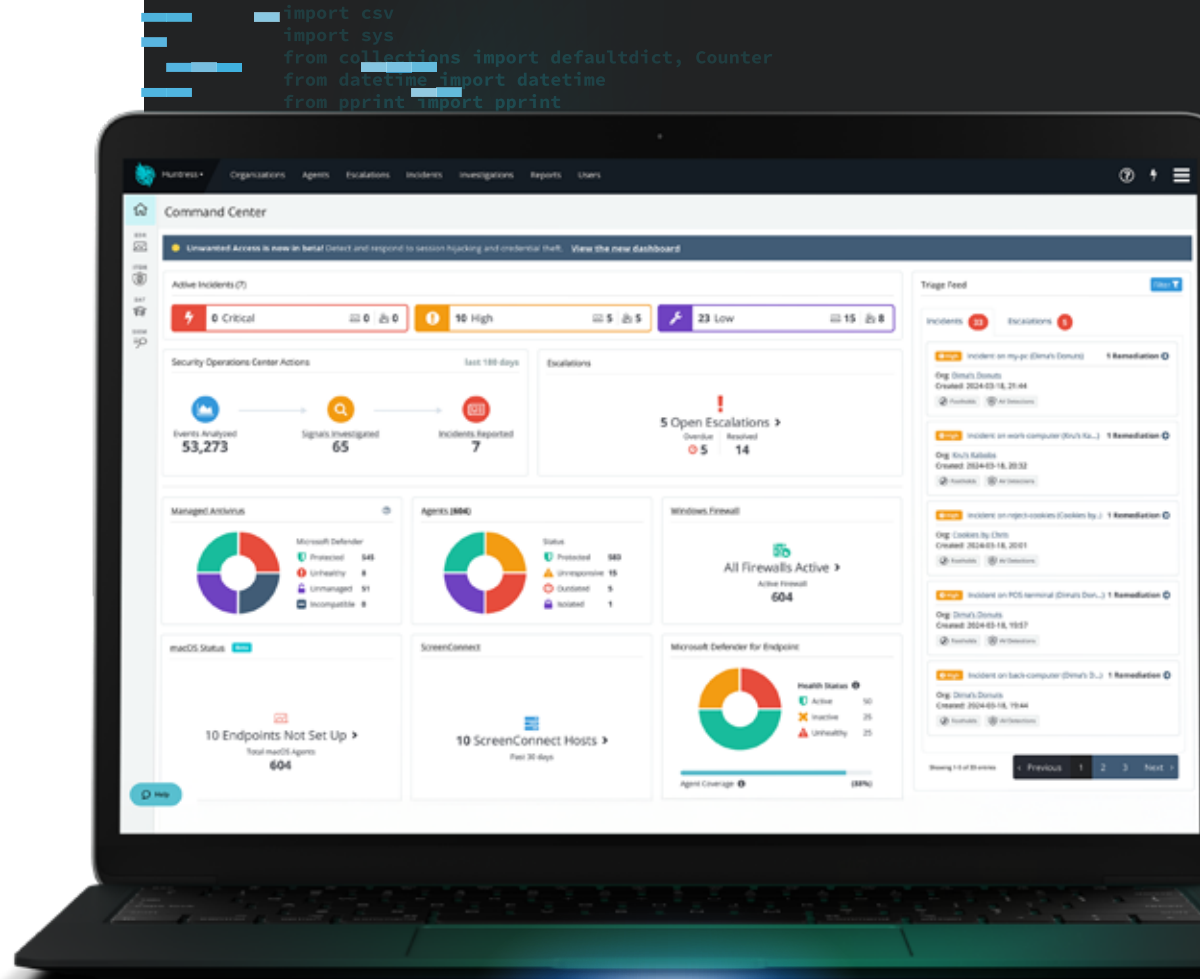


Leveraging Managed EDR Solutions to Protect Against Ransomware

Healthcare organizations have to become impenetrable fortresses against cybercriminals. While you can't always prevent hackers from approaching your gates, you can stop them from breaching your walls. This is where we recommend a defense-in-depth strategy, a holistic approach that strengthens your fortifications by layering tools like intrusion prevention, data encryption, and threat detection. Just like plates of armor, this approach builds strong barriers that can fend off cyberattacks, even if one layer is breached.

Managed endpoint detection and response (EDR) reinforces this strategy by identifying and responding to threats targeting endpoints like desktops, servers, and other connected devices. Using automated technologies and expert human analysts, a managed EDR takes charge of your healthcare organization's critical cybersecurity needs, including:

- Monitoring and gathering endpoint data
- Identifying and investigating potential threats
- Prioritizing alerts for action
- Providing easy remediation steps, including one-click solutions



With a managed EDR, you're not just defending your organization—you're partnering with a proactive ally that can help you enhance your security posture to mitigate the risk of ransomware attacks and better protect patient data.

Real-World Incident

An Ounce of Prevention Is Worth a Pound of Cure

In the early morning hours of December 11, 2023, a managed service provider (MSP) specializing in cybersecurity for medical practices, received an urgent alert from [Huntress' Security Operations Center \(SOC\)](#)—ransomware had been detected on a client server.

Fortunately, the MSP had deployed [Huntress Managed EDR](#) for the client, which enabled our SOC to take immediate action. By the time the MSP's team noticed the alert an hour later, the SOC had already isolated the server, preventing the ransomware from spreading further.

Following our guidance, the MSP promptly implemented the necessary remediation measures. Thanks to the proactive approach enabled by Huntress, the impacted client was up and running again by the following day. Without our prompt threat detection and the MSP's timely intervention, the consequences could've been much more severe.

But for those who aren't prepared, fortunes aren't as bright. At the height of COVID, a physician's office in the southwest was hit by ransomware. Only after realizing they'd been attacked did they scramble to deploy Huntress. By then, however, it was too little, too late. The damage was done. Personal information, financial records, and patient data had been stolen and posted for sale online. And, not surprisingly, it all sold.


When it comes to cybersecurity, procrastination is an invitation to disaster. Like a disease, the longer you postpone treatment, the worse your condition becomes, leaving fewer cures available to you. Though HIPAA might penalize medical practices for cybersecurity negligence, and while fines can run into seven figures, the threat of compliance pales in comparison to the fallout of a ransomware attack.

These incidents emphasize the [value of proactive security measures, especially in a healthcare setting](#). Threat actors love to exploit vulnerabilities, often lingering in healthcare IT systems for weeks before striking. Our knack for early detection enables preemptive action that can thwart ransomware attacks before they materialize into things far worse—damaged credibility, eroded patient trust, and significant financial losses.



Interconnected Devices Inject Risk Into Patient Safety

Threat: Attacks Against Interconnected Medical Devices



There's a huge shift taking place, where digital safety is affecting physical security. Healthcare providers must now look beyond traditional patient care and get a better glimpse into digital security, as this is absolutely essential for protecting patients in a world where cyber threats can have real-life consequences.

The Physical and Digital Realms are Now Interwoven

Digital health and security are becoming more intertwined with the physical world, creating complex risks that providers must manage to better protect their patients.

For example, a cyberattack on Change Healthcare [disrupted indispensable healthcare](#) services, including the accessing of patient records, scheduling appointments, and operating billing systems. The fallout was immediate, with patients encountering delays in receiving crucial care, diagnoses, and treatments. This disruption also led to missed appointments and prescriptions, further emphasizing the link between digital security and physical well-being.

[Research conducted at the University of Minnesota School of Public Health](#) exposed the grim reality of ransomware attacks on healthcare. Not only did these attacks disrupt crucial services, but they also had a measurable impact on patient mortality. The study estimated that ransomware attacks resulted in the deaths of between 42 and 67 patients over a five-year period, offering a harsh reminder of the human cost of digital vulnerabilities.

Interconnected Devices Are a Double-Edged Sword

The increasing integration of digital technologies like wearable heart monitors, smart inhalers, and connected imaging devices—collectively known as the Internet of Medical Things (IoMT)—is revolutionizing patient care. By 2026, healthcare providers are expected to [deploy over seven million IoMT devices](#), doubling the amount from 2021. Simply put, IoMT devices expand targets for cybercriminals due to their interconnectedness and specialized operating systems and software.

IoMT devices are quite vulnerable, with many lacking proper security protocols or running outdated software. For instance, [39% of nurse call systems \(NCS\)](#)—a vital component of patient care—harbor critical severity unpatched Common Vulnerabilities and Exposures (CVEs). Infusion pumps and medication dispensing systems exhibit similar security lapses. In addition, 19% of connected medical devices are running unsupported OS versions.



New Threats Demand New Approaches

The U.S. Department of Health and Human Services (HHS) recognizes the risks of interconnected devices, and so they're taking action. In fact, HHS acknowledges that over 53% of connected healthcare devices possess critical vulnerabilities. And while they've provided guidance, securing these devices is proving to be more challenging than traditional network devices.

Unfortunately, traditional security measures are falling short, leading to the adoption of more advanced approaches like Continuous Threat Exposure Management (CTEM). CTEM approaches such as Cyber Asset Attack Surface Management (CAASM), breach and attack simulation (BAS), penetration testing, vulnerability scanners, and other tools have been rising quickly. However, these tools can be complex and demand resources that often exceed the capabilities of small- and medium-sized healthcare providers.

That's why healthcare providers need a layered security strategy, one which integrates both proactive measures to harden interconnected devices along with continuous monitoring, detection, and response mechanisms to protect networks and patient safety when cybercriminals break through. Let's demonstrate why we need this comprehensive approach by looking at a possible real-world scenario.



Scenario

Breaching a Nurse Call System

Imagine a cybercriminal breaches your healthcare facility's network-connected NCS, a critical communication tool for patient care. Despite its importance, the NCS operates on outdated firmware and lacks strong encryption, making it an easy target. The hacker takes advantage of this vulnerability to gain unauthorized access, and the initial breach goes undetected by traditional security measures.

The true threat emerges when the cybercriminal, after having established a foothold through the NCS, begins to probe further, exploiting workstations and servers within your network. It's at this point—when the attacker moves off the NCS onto more conventional IT assets—that the layering of [managed endpoint detection and response \(EDR\)](#) capabilities come into play.

Through this scenario, it's clear that even when direct endpoint compatibility isn't present—as with certain IoMT or specialized systems like the NCS—managed EDR solutions play a crucial role in identifying and mitigating cyber threats once they attempt to spread to compatible parts of the network. This layered approach to security ensures that healthcare facilities can maintain robust defenses against sophisticated cyber threats, protecting both their digital infrastructure and the patients they serve.

How Managed EDR Stops the Attacker Before Patient Safety Is Compromised

Detecting Suspicious Activity

Managed EDR solutions keep a constant eye on your network's endpoints, identifying anything suspicious like unusual outbound connections or unrecognized scripts running on a workstation. If something seems off, it'll trigger an alert.

Digging into the Incident

Experts from the managed EDR solution's security operations center (SOC) will dive deeper into the incident. They can trace the attack back to its origin from the compromised NCS, mapping out the attacker's pathway and identifying all affected systems. Through careful examination of the compromised endpoints, they can gather intel on the malware and the attacker's tactics, techniques, and procedures.

Isolating Affected Endpoints

To halt the attacker's movements, a managed EDR solution can immediately isolate infected workstations and servers. This stops the spread and cuts off the attacker's access to other parts of the network.

Remediating and Recovering the System

Armed with insights from the investigation, the SOC facilitates remediation actions. This includes purging the malware from compromised endpoints, patching vulnerabilities, and restoring affected systems to their pre-attack state.

Getting Stronger After the Incident

Once the dust settles, the managed EDR solution delivers targeted recommendations to beef up the network's defenses. This might involve segmenting the network to restrict access between the NCS and more sensitive areas of the IT environment; enhancing monitoring on endpoints for indicators of compromise related to this attack pattern; and tightening security protocols for other devices within the healthcare facility.

Staying Vigilant

SOC experts enhance monitoring policies, especially for endpoints with access to communication with IoMT devices like the NCS. This way, they can ensure early detection of similar threats and protect patients down the line.

Accidental or Intentional Data Loss Can Be Debilitating for Healthcare

**Threat: Loss or Theft of Equipment and Data /
Insider Accidental or Malicious Data Loss**

For medical professionals, data saves lives. For hackers, data drives profits. When one has the data, however, the other does not. This ongoing battle for access keeps healthcare providers on their toes. Cybercriminals are relentlessly trying to grab everything from your patients' protected health information (PHI) to your email credentials to your organization's financial records. And while the explosion of [endpoints](#) across the industry has made it easier for you to access the data you need, it's also made it easier for hackers to do the same.

This proliferation of digital endpoints across healthcare—from electronic health records (EHR) to telehealth services to mobile health apps—has undeniably led to greater efficiencies and improvements in remote and in-person care. But these advancements have also expanded attack surfaces, giving threat actors more opportunities to access and exploit your devices.

Data Loss Due to Accidental Equipment Loss or Theft

Healthcare organizations and their staff must maintain awareness of all devices. Whether due to negligence or deliberate theft, the loss of mobile phones, tablets, laptops, USB drives, and other [interconnected devices](#) can have disastrous outcomes. A missing device doesn't just mean lost hardware—it means sensitive data has potentially fallen into the wrong hands.

Scenario

Hot Data and Cold Coffee

Imagine a doctor sitting in a coffee shop, casually stirring her morning espresso, reviewing patient charts on her laptop. After a few sips, she receives an urgent call, telling her she needs to get to the hospital right away. She grabs her coat and rushes out of the cafe, but in her haste, she doesn't just leave her drink behind but also her laptop. When she realizes her mistake an hour later, she hurries back to the shop, only to find cold coffee and no computer.

The choice the doctor makes next is critical. Ignoring the loss leaves sensitive data exposed to anyone with malicious intent. But if she reports the lost laptop, IT can disable the device and prevent unauthorized data access. This is important because even if the doctor somehow gets her laptop back, its data could've already been compromised. For instance, an attacker may have:

- Pulled the hard drive and uploaded medical records, client information, hospital billing, and other sensitive data
- Uploaded a backdoor Trojan onto the laptop and returned it to the doctor's office in the hopes that it'll be reconnected, exposing the rest of the hospital network to its backdoor access
- Installed a keylogger or [man-in-the-middle software](#) to track keystrokes or capture communication between the laptop and any apps or sites used

Put simply, threat actors want data because it's currency. It can be [extorted for a heavy ransom](#), sold online to the highest bidder, or exploited for identity theft. Though stemming from an honest mistake, the repercussions for the doctor and her practice can extend beyond financial burdens, including:

- She and other healthcare professionals struggling to deliver safe, appropriate patient care
- Increased inefficiencies in operations, which [could spike mortality rates](#)
- Patients receiving the wrong treatments or meds because of data errors



Scenario

One Good Nurse. One Crooked Nurse. Two Bad Outcomes.

Suppose you're a dedicated nurse, always putting your patients first, but you're a bit distracted one morning. It happens to the best of us. You mistakenly tap the wrong keys and misspell a patient's email address. The name looks right at a glance, but the email goes to the wrong recipient. As a result of a seemingly small error, you disseminate personal data to a complete stranger. This was an honest mistake, and you didn't commit the act with any intention of causing harm. This is an example of an accidental insider threat, and though it can be chalked up to simple human oversight, the consequences can still be serious. If the recipient acts with malicious intent, they might:

- Gather as much information from the PHI or personal identifiable information (PII) and conduct a [vishing](#) attempt on the actual patient—claiming to be the hospital or the insurance company—in the hopes of exploiting the data for personal gain
- Attempt to blackmail the intended patient by threatening to release personal records unless they pay up

But insider threats aren't always accidental. Malicious insiders with legitimate access to your systems may intentionally steal data for a fast profit. Imagine a disgruntled nurse—he's feeling overworked, underpaid, and unappreciated—stealing copies of patients' medical records, making copies of them, and selling them online, where each record can fetch [up to \\$1000](#) a pop. Insider threats are especially nefarious because they're premeditated by people you might know and trust, and you may not realize their intent to cause harm and compromise patient safety.

Whether the data loss is accidental or intentional, the outcome can be equally disastrous. Both types of loss highlight the need for robust security measures, employee training, and strict access controls to protect sensitive information in healthcare settings.



How to Protect Against Data Loss and Theft

Being vigilant is always the best step when securing sensitive data. Of course, mistakes can happen. And worse yet, no matter how aware we might be, those with malicious intent may always sneak by and get away with theft.



Report lost or stolen devices

Tell your IT department or supervisor ASAP if something's gone missing.



Keep track of your assets

Maintain a detailed inventory of your organization's devices to ensure accountability.



Encrypt sensitive data

Keep your data safe when sending it to other devices. And if someone finds your device, encryption locks them out.



Report suspicious activity immediately

Trust your gut. If something feels suspicious, it probably is. Report your concerns to HR, IT, or senior leadership.



Wipe data clean

Set up strict protocols for erasing data from devices at the end of their service.



Screen your vendors

Verify third-party vendors are who they claim to be and limit their access based on their specific roles and responsibilities.



Implement security awareness training

Regularly train staff to spot potential threats like social engineering and business email compromise (BEC).



Monitor equipment closely

Keep a close eye on who accesses patient info, server rooms, and EHR systems. Cut off access immediately when someone no longer needs it.

Make Security Awareness Second Nature for Your Organization

In any high-stress environment, people will make mistakes. But keeping security top of mind can mitigate risks. That's why a robust security awareness training (SAT) program is essential. It can better help everyone across your organization identify potential threats and understand the serious consequences of data loss. By keeping your people vigilant and proactive, your healthcare organization can protect sensitive data and maintain the trust of your patients.

[Huntress Managed Security Awareness Training](#) is a unique solution that fuses vibrant animations with science-based learning principles to help improve your organization's security posture. Through story-driven episodes focused on data protection, [Huntress Managed SAT helps drive meaningful behavioral changes](#) for you and your colleagues.



Notable episodes include:



HIPAA

Summarizes administrative, technical, and physical safeguards to ensure you remain HIPAA-compliant



Removable Media

Uncovers risks associated with removable media like USBs



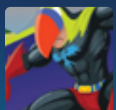
Locking Devices

Reveals the consequences of unlocked devices



Physical Security

Helps you recognize hacker tactics and highlights your role in protecting secure areas



Confidential Info

Demonstrates the importance of need-to-know access behaviors



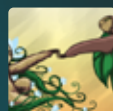
Clean Desk

Reveals techniques to secure your devices from information theft



Insider Threat

Analyzes types of insider threats and their consequences



Storing Passwords

Demonstrates best practices for storing passwords and keeping them out of the hands of bad actors

Real cybersecurity practitioners from the [Huntress Security Operations Center \(SOC\)](#) design each episode, fashioning them around the latest hacker tactics they observe in the wild. So as new threats face the healthcare industry, Huntress Managed SAT will adapt to them, keeping you and your staff one step ahead.

Your Prescription for Cybersecurity Success

Social engineering, ransomware, interconnected device attacks, and equipment theft aren't just passing trends—they're now persistent threats to healthcare. Whether you're running a bustling city hospital or a small rural clinic, system disruptions and lost data can be a real nightmare. We understand the stakes, so we put together this eBook for you.

We're here to help you outsmart the threat actors targeting your organization. Our mission isn't just about developing top-tier cybersecurity solutions, it's about empowering you with the knowledge to tackle the challenges posed by cybercriminals. Whether it's securing your connected devices or stopping data breaches in their tracks, Huntress stands alongside you, helping you keep your operations running smoothly, so you can focus on outstanding patient care.

Visit the Healthcare Cybersecurity Success Kit

To gain more strategies for defending your organization, check out our Healthcare Cybersecurity Success Kit.

[Learn More](#)

Demo Huntress for Yourself

When you're ready for a dedicated partner who's got your back, start your free trial with Huntress today.

[Learn More](#)

[X](#) [in](#) [▶](#) [f](#)