WHITE PAPER

A more affordable way to enhance your healthcare security

PRESENTED BY: HUNTRESS

PUBLISHED BY: FIERCE Healthcare

DECEMBER 2023

PRESENTED BY: HUNTRESS

PUBLISHED BY: FIERCE Healthcare

CONTENTS:

Choosing the Right Partner 4

The Huntress Difference 5

Managed EDR 6

MDR for Microsoft 365 7

Security Awareness Training 8

More Reasons To Choose Huntress 9

The Time To Act Is Now 9

How big of an impact can cyberattacks have on the healthcare sector? The truth is, it can be quite staggering. In fact, recent ransomware attacks on Thanksgiving Day interrupted dozens of facilities operated by Ardent Health Services, including emergency care and telehealth appointments. These continued attacks can be debilitating for anyone, but especially for healthcare organizations like yours.

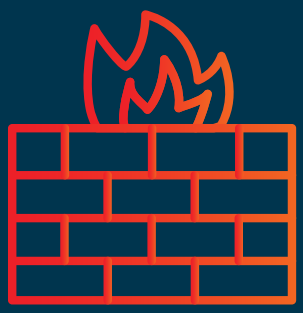
That's because small to medium-sized businesses (SMBs) across the healthcare sector are now facing tighter budgets and major resource challenges. So, how can you protect yourself and build an effective cybersecurity strategy? The best way is to seek outside help.

However, most outsourced cybersecurity solutions on the market aren't designed for operations like yours. They're built for larger enterprises with complexities and price tags that are way out of reach for SMBs.

There are more affordable managed security options that can bring resource-strapped healthcare organizations the services of a fully managed, purpose-built cybersecurity solution backed by a human-led 24/7 Security Operations Center (SOC). This approach is intentionally designed to:

- "Serve the 99%." It's tailored to the needs of SMBs like you rather than the 1% of organizations with big budgets and large security staff.
- Eliminate the burden of hiring and retaining internal security staff. When healthcare organizations like yours rely on Huntress, our cyber experts will manage the majority of your security tasks and offer 24/7 protection.

As a broadening array of criminals launch pervasive attacks on healthcare organizations, you can no longer afford to "fight fires" all day in an attempt to thwart numerous attacks. Instead, you're better off shifting gears to a more proactive approach, relying on a partner to leverage managed endpoint detection and response (EDR) and other security solutions.



As a broadening array of criminals launch pervasive attacks on healthcare organizations, you can no longer afford to "fight fires" all day in an attempt to thwart numerous attacks.

Choosing the Right Partner

It's essential to choose a partner that's tuned into the threat landscape, knows how hackers operate, can track the latest trends in cyberattacks, and use those insights to empower the community with intelligence, helping healthcare organizations like yours fight back.

Huntress' *SMB Threat Report*–based on third quarter 2023 statistics from its client base–shows a continuing change in the nature of threats against SMBs that require a shift in security strategies, especially in healthcare.

Threat actors have largely moved away from malware-focused tactics, the report states. In most incidents, threat actors focus on non-malware mechanisms and abuse of legitimate tools and system commands. Notably, 56% of recorded incidents in this time frame were, in essence, "malware free" across multiple types of intrusions.

Other findings include:

- 65% of incidents involved threat actors exploiting remote monitoring and management (RMM) software as an avenue of intrusion, taking advantage of the broader attack service created by the explosion in remote access to clinical systems and the reliance on cloud computing.
- 64% of incidents involved malicious forwarding or other malicious inbox tools. These email attacks are designed for identity theft that opens the door to systems access.
- 29% of incidents featured LOLBins (living-off-the-land binaries) or similar abuse as a tool for intrusion. LOLBins refers to using trusted, pre-installed systems to spread malware, with attackers attempting to "blend in" to avoid detection.

The cybersecurity landscape for SMBs calls for a profound reassessment of defense strategies. The dominance of non-malware tactics, coupled with the exploitation of RMM software and identities, necessitates a nuanced approach to threat detection and response and expanding your security purview beyond conventional perimeters.

For smaller healthcare organizations that lack a robust cybersecurity strategy, launching a nuanced approach will be much easier if they rely on an experienced partner who specializes in the SMB space.

The Huntress threat report also points out that visibility remains a key to defense in all sectors, especially healthcare. Particularly given trends in adversary operations, relying more on abusing legitimate applications than distributing custom code and tools, the ability of organizations to identify and differentiate "malicious" from "normal" and "benign" is vital to enable meaningful, useful defense.

Another significant trend is that more organized threat actors are offering "ransomware as a service," opening the door for more criminals to easily wage attacks. With these nefarious organizations popping up, almost anyone can leverage their cyberattack capabilities. This means relatively unskilled criminals are now waging attacks across the board in healthcare, with little concern for human life.

That's why ramping up your cybersecurity is so essential. For SMBs in healthcare, partnering with an experienced, SMB-focused cybersecurity organization like Huntress allows you to enhance your security faster than if you rely only on limited internal resources.

The Huntress Difference

Huntress offers an affordable, yet comprehensive approach to security. We detect threats early, take a behavioral-based approach, simplify security for your IT team, and back you with our dedicated cyber experts.

Our three-pronged approach to security is tailored to address the current threats that you might face. Easily implemented at hospitals, clinics, nursing homes, pharmacies, and other healthcare organizations, our approaches include:

- **Managed EDR.** Huntress Managed EDR combines technology custom-built for your needs with industry-leading expertise through a 24/7 SOC and a dedicated support team. Managed EDR helps minimize the "alert fatigue" that's prevalent with other tools. It comes at an affordable price with no surprise add-ons or extra tiers, and it's deployable throughout your network in literally just minutes.
- **MDR for Microsoft 365.** This solution continuously monitors indicators and behaviors of business email compromise (BEC) attacks, such as users logging in from suspicious locations or a malicious email forwarding rule. Our SOC reviews any detections, instantly isolates any compromised users, and supplies you with a guided remediation plan for further necessary actions.

For smaller healthcare organizations that lack a robust cybersecurity strategy, launching a nuanced approach will be much easier if they rely on an experienced partner like Huntress.

- **Security Awareness Training.** Huntress SAT provides managed security awareness training that you'll love but hackers will hate. Our in-house security experts create and manage story-based episodes, phishing simulations, and reports to enable your employees to become more cyber-savvy. Your teams can gain the expertise they need to fight against social engineering, and you get the expertise of Huntress' SOC to fully manage your security awareness program.

You can leverage these three offerings separately or as a group, with each component complementing the others.

If you have onsite servers and systems, you may choose to focus initially on implementing Managed EDR to protect your endpoints. But if your organization has an online environment that relies heavily on cloud computing and remote access to systems, then adopting MDR for Microsoft 365 to help protect identities may be your top priority.

A rise in BEC and an increase in remote access to systems, including remote surgeries, is leading more healthcare organizations to look for solutions like MDR for Microsoft 365.

Managed EDR

What separates the Huntress offering from other EDRs is how we react to intruders' behaviors. Our SOC can directly tune into the alerts to spot threats quickly. Then, we can isolate the threat and provide simple remediation steps so you don't need to resort to your own investigation or attempt to remediate things on your own.

Simply put, we look at processes carefully. If we see a process isn't running in normal parameters, we know that's a very early indicator of a compromise. In short, identifying compromises earlier is key to preventing potentially life-threatening attacks in healthcare.

Relying on a partner for managed EDR can help you avoid the "alert fatigue" so common with other security systems that often generate alerts to staff for many perceived threats, no matter how significant.

That's why Huntress reviews all suspicious activities, and we only send you an alert when a serious threat is verified or action is required. This helps eliminate the clutter and false positives found in other platforms that can create a huge burden for SMBs in healthcare.

In most cases, we'll offer a step-by-step walkthrough of how you can remediate the threat or even a one-click auto-remediation. You can trust that when Huntress shares an alert with you, it's for a threat validated by human experts.

The Huntress Managed EDR solution also includes a “canary in a coal mine” function for early detection of ransomware, which now poses a formidable threat in the healthcare sector. The “canary” is one of the first things that gets “popped” should a ransomware attack happen. It’s an early indicator that ransomware may be affecting a system. At that point, our SOC receives an alert, and a SOC analyst will take action while the ransomware is initially triggering.

To sum up, our four-step EDR approach includes:

Detect: Huntress finds attackers who abuse legitimate applications, bypass other security tools, or are in the process of deploying payloads, such as malware and ransomware.

Analyze: Our threat hunters and security analysts review suspicious activities and send easy-to-understand incident reports that explain the scope and severity of a threat.

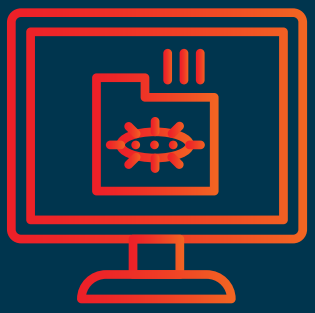
Respond: We isolate endpoints, remediate threats, and kick attackers to the curb with one-click approval for automated actions and clear instructions for manual tasks.

Report: With detailed summaries and brandable reports, you can accurately measure (and articulate) the value you’re getting.

MDR for Microsoft 365

Hackers can use a single stolen credential or compromised email account to launch a crippling cyberattack against modern, cloud-based infrastructure. Identifying user behaviors and detecting malicious activity early, like unauthorized access or email manipulation, enables rapid response to a nascent intrusion even before serious damage may occur.

Huntress MDR for Microsoft 365 enables your healthcare organization to detect and respond to early signs of a cyberattack, such as BEC, to shut down hackers quickly. It



Hackers can use a single stolen credential or compromised email account to launch a crippling cyberattack against modern, cloud-based infrastructure.

secures your Microsoft 365 users, applications, and environments by leveraging the 24/7 SOC. Our SOC experts interpret threat detections and deliver incident reports with actionable remediations for recovery.

A Huntress staff member will review every detection for you, filtering out the noise and only escalating customized reports when malicious activity is suspected.

MDR for Microsoft 365 protects you around the clock, with no gaps or lags in coverage during the peak seasons, off hours, or holidays. It integrates with your Microsoft Cloud environment, collecting user, tenant, and application data which is enriched using organic and external threat feeds to supply information like geolocation and IP reputation. Our SOC utilizes this context-added data to provide the most accurate and precise incident reports and the best remediation options to neutralize threat actors quickly.

Security Awareness Training

Cyberattacks can impede access to critical electronic health records, delay ordering of medications, block online education for the chronically ill, and even derail scheduling. In addition to these major clinical impacts, attacks can expose personally identifiable information (PII) such as credit card numbers and other financial data.

Given all those risks, and the rise in remote system access, the need for increased cybersecurity is paramount. Simply implementing the right security solutions, however, isn't enough. Training staff on how to avoid mistakes that can open the door to cyberattacks is equally important.

Huntress Security Awareness Training offers animated, story-based lessons that show relatable examples of real-life cyber threats you're likely to encounter. Topics include guarding against phishing attacks, complying with HIPAA, and gaining awareness of emerging attack methods.

"Most of the training in HIPAA is very dry with a 'check the box' kind of mentality," says Jared Couillard, CISSP, a senior director, IT, and security officer at Cohere Health. "I was looking for something different and was introduced to Security Awareness Training from Huntress. I loved this new idea for how to present this information."

Huntress can also manage "phishing simulations" with messages sent by our SOC to test your organization. These simulated phishing attempts help pinpoint your employees who may be vulnerable to erroneously clicking on phishing emails, allowing them to get targeted, actionable training.

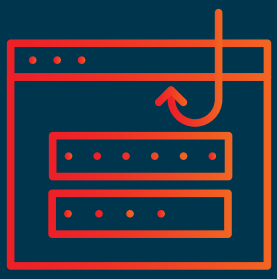
More Reasons To Choose Huntress

Our founders come from the National Security Agency (NSA), where time and time again, they saw SMBs being pummeled by cyberattacks. To help those businesses fight back, they established Huntress.

Huntress was built to serve SMBs, filling their essential cyber skills gap while being conscious of their limited budget and resources. We offer 24/7 protection without placing strain on your staff or your budget. And we're a trusted, top-rated partner that already protects over 100,000 SMB customers and more than 2.3 million endpoints while maintaining a customer satisfaction rating of over 98%.

The Time To Act Is Now

Security in healthcare can be a matter of life and death. If you cannot access patients' electronic health records as a result of an attack, you could inadvertently make inappropriate treatment decisions. In addition, attackers can block remote access to



Huntress can also manage "phishing simulations" with messages sent by our SOC to test your organization. These simulated phishing attempts help pinpoint your employees who may be vulnerable to erroneously clicking on phishing emails, allowing them to get targeted, actionable training.

systems that physicians and others have come to rely on. That's why an effective data security strategy is so essential for your healthcare organization.

The threat landscape today remains a difficult one for the majority of organizations that lack the resources and expertise residing in enterprise network environments. This is especially true in the healthcare sector, where many organizations have tight budgets and lack staff members with cybersecurity expertise.

Whether for monetization purposes through ransomware or BEC, or potentially even state-directed espionage activities, SMBs remain at risk from a variety of entities. Of greater concern, these adversaries are taking advantage of "holes" in visibility and awareness to subvert or avoid many legacy security controls. Whereas once a small organization could likely get by with a combination of a good anti-malware solution and spam filtering, the current threat landscape renders these simplistic—if historically reasonably effective—efforts no longer satisfactory.

In addition to learning about adversary tendencies and operations, healthcare network administrators and others must also understand how these adversaries increasingly take advantage of the very nature of modern networks and distributed environments.

The path forward entails a dual-pronged approach—enhancing visibility into events while simultaneously reducing the available attack surface. This adaptive approach is indispensable in co-evolving with threat actors in today's ever-changing cybersecurity landscape.

In the end, a solid security strategy doesn't have to be difficult, costly, or resource-intensive. When you rely on Huntress, you gain more than effective, affordable security, but an experienced partner who has your back 24/7.

If you'd like to discover how Huntress can help secure your healthcare organization, start your free trial today.

Hackers are constantly evolving to better attack small and mid-size businesses – Huntress is how SMBs and managed service providers stay ahead with managed cybersecurity solutions for endpoints, email, and identity.