VARS

Whitepaper

BREACH PROTECTION FOR HEALTHCARE

Powered by Cynet

Business Challenge

The healthcare industry has undergone a period of rapid digital transformation. Healthcare IT environments span a mixture of modern and legacy applications while often housing highly proprietary intellectual, medical and financial data. Data and systems are accessible by a variety of in-house and third party personnel both inside and outside of the network perimeter. The challenge of protecting a healthcare environment, while allowing the free flow of critical, time sensitive information, is extreme.

Unfortunately, the allure of highly valuable data assets and a broad attack surface make healthcare providers prime targets for cybercriminals. In October 2020 the FBI issued a warning of impending ransomware attacks on the healthcare sector with the intention of stealing data and disrupting healthcare services. Healthcare records are up to 50 times more valuable than credit card data on the black market while nation-state attacks on medical research data is skyrocketing.

Most smaller healthcare organizations face these risks with limited security budgets and smaller security teams. The speed at which some attacks occur, such as ransomware, require security teams to actively monitor their environments 24x7, which can be impossible for a small security team. Conversely, the dwell time associated with advanced persistent threats requires significant expertise to detect, another challenge for smaller security teams.

Top Security Challenges

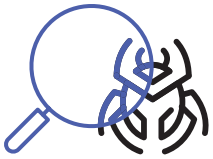
Broad access to legacy and modern applications and systems by internal and third party providers are difficult to protect

Small security teams with limited cybersecurity technology budgets and expertise

Reliance on traditional antivirus and anti-malware software provides limited protection against newer threats like ransomware and cryptolocking

Key Cyber Security Challenges

The breadth of systems, applications and data assets readily accessible by internal staff, third party providers and customers makes a healthcare company's environment quite challenging to protect. Most healthcare providers must additionally comply with stringent regulatory mandates so balancing easy access with strong controls adds to their burden.



Limited visibility across environment

With a vast amount of endpoints, shared systems and access points, many companies don't have a complete picture of the environment under protection. The old adage "you can't protect what you can't see" holds true. Visibility is a fundamental cybersecurity strategy to protect IT assets and information. But maintaining a complete asset inventory, especially endpoints which tend to be the primary target of cyberattacks, can be difficult in the heterogeneous, often shared, morphing healthcare environment. Ultimately, healthcare companies need full visibility into their environment, including files, hosts, users and networks.

Many healthcare companies rely on antivirus and anti-malware software, which only detects a fraction of advanced attacks. This type of software provides limited protection against newer attack techniques and is especially vulnerable to highly advanced targeted attacks. Importantly, most antivirus is ineffective against the advanced ransomware and advanced persistent threats faced by the healthcare industry.

To extend protection beyond antivirus solutions, companies incorporate additional tools such as endpoint detection and response (EDR) and network detection and response (NDR). EDR solutions were borne out of the premise that because all endpoint threats cannot be prevented with antivirus software, these threats still need to be detected after they successfully infect an endpoint. EDR solutions continuously monitor endpoints to detect malicious activity and system behaviors that are indicative of compromise.

NDR solutions extend protection to the network to provide additional visibility across the environment. If an attack somehow bypasses both an antivirus and an EDR solution, the ability to detect lateral movement and other network traffic indicators could uncover a threat actor that has successfully infiltrated the environment.

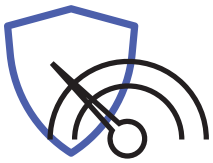
Siloed security controls

While each of these security controls described above extend needed visibility across the environment, they are not without their problems. First, EDR and NDR solutions are notorious for false positive alerts. Security analysts either chase down these false flags or tend to ignore all but the highest risk alerts. In the first instance considerable time is wasted, in the second instance ignoring alerts is far from good security practices and opens the company to compromise.

Key Cyber Security Challenges
Cont'd

Siloed security controls
cont'd

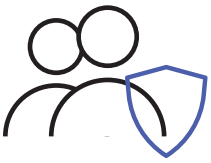
Siloed controls also mean more "panes of glass" for the security team to monitor and access when investigating potential threats. Because each security tool has a separate management console and presents information differently, it is challenging for security analysts to make sense of all the information being presented and then link activities together between the various security controls to see the big picture. This is why stealthy attacks are able to bypass environments with multiple layers of controls.



Small security teams with limited bandwidth

Putting siloed controls aside, which do create significant manual overhead, most security tools require a meaningful human investment to operate. When threats are discovered, security analysts must investigate to determine the root cause and then uncover the full scope of the attack across the environment.

Once the root cause and scope are determined, all threat components must be fully remediated. This often involves access to multiple systems and can be a painstaking, time consuming process.



Small security teams with limited cybersecurity skills

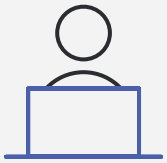
With the threat landscape rapidly evolving even the largest, well funded security teams are vulnerable to threats. Look at any review of breaches against large companies and it's quick apparent that even the best cybersecurity experts with leading-edge tools are challenged to protect their organizations. For smaller security teams with limited technology budgets and cybersecurity expertise, the risk of breach is compounded exponentially.

The Cynet-VARS Approach

Cynet was built for small cyber security teams with limited bandwidth, cybersecurity expertise and technology budgets. Cynet XDR provides a single, unified platform to automatically prevent, detect, investigate and fully remediate the broad range of attack vectors faced by healthcare companies. Visibility across endpoint, network and user activities, plus the power of deception provides the broadest and deepest protection against all threats.

Cynet XDR is the only solution that triggers an automated investigation following each endpoint, user, or network alert, fully disclosing its root cause and scope and applying all the required remediation activities to fully eliminate the threat. Cynet also provides a broad set of automated and highly customizable remediation actions to address threats according to your preferences. Moreover, Cynet provides an expert team of cybersecurity experts to augment and guide your team 24 hours a day, 7 days a week – included with the Cynet 360 platform.

Cynet Benefits for Healthcare



Easy to Deploy and Operate

The Cynet agent can be deployed to over 5,000 endpoints in less than an hour. While many solutions require months to deploy and become fully operational, Cynet is fully functional within 24 hours of deployment, providing all the insights and protections available in the platform. The Cynet console was built to be intuitive and effortless so smaller security teams do not need years of expertise to operate.

Full Visibility Out of the Box

Cynet XDR provides complete visibility and multiple points of telemetry leading to low false positives and early detection of stealthy threats. A single, unified Extended Detection and Response (XDR) platform that provides Next Generation Antivirus (NGAV), Endpoint Detection and Response (EDR), Network Detection and Response (NDR), User and Entity Behavior Analytics (UEBA) and Deception technology fully integrated and easily configurable with a single dashboard out of the box.

Cynet Benefits for Healthcare

Cont'd

Automated Protection

Cynet's Incident Engine automatically performs all required threat investigation and response actions, uncovering the root cause and full scope of high risk threats and taking appropriate actions to fully eradicate the threat across the environment. Cynet additionally provides an array of remediation playbooks that can be executed automatically in response to a detected threat for immediate response or can be triggered manually to provide more oversight and control. Cynet's autonomous response actions provide the comprehensive protection needed by smaller and overburdened security teams.

Include Managed Detection and Response Oversight

All Cynet clients are automatically protected by a comprehensive Managed Detection and Response (MDR) service, included with the Cynet platform at no extra cost. Small security teams at healthcare companies rely on Cynet's MDR team (CyOps) to proactively monitor their environment 24x7 to ensure nothing is overlooked. They can contact VARS at any time for guidance in configuring the Cynet platform, providing attack investigation expertise and guiding them on all necessary response actions. CyOps becomes an extension of the healthcare company security team, adding resources and world-class cybersecurity expertise.

Summary

Protecting healthcare environments from cyberattacks is beyond challenging, especially with a smaller, less experienced security team. With limited budgets, most small to mid-sized healthcare companies cannot obtain, integrate and operate the required security controls to protect the organization from advanced threats. Healthcare companies rely on Cynet's intuitive, comprehensive breach protection platform to solve their security challenges, knowing they always have a team of cybersecurity experts watching their backs.