Malwarebytes

INDUSTRY SOLUTION BRIEF

Malwarebytes for healthcare

Protecting patient information from cyberattacks

THREATS HEALTHCARE FACES

Malware

- Malware spreads across networked endpoints, and is the top concern of hospital IT security staff.

Ransomware

- Redirects to malicious websites containing ransomware, which encrypts hospital and patient data and holds it for ransom.

Botnet attacks

- Malware compromises and hijacks a group of Internet-connected devices to mob a targeted system for malicious purposes.

Employee negligence

- Employees fall victim to social engineering, including email phishing, social media attacks, and tech support scams—giving attackers access to sensitive data, passwords, or other confidential information.

Attacks on mobile

- Increases in attacks on improperly secured mobile devices leave healthcare networks and data vulnerable.

Exploits

- Exploits find vulnerabilities in outdated software and deliver malware.

State of healthcare

Modern healthcare offers levels of care and treatment that might have seemed like science fiction a generation ago. But the degree to which healthcare settings have embraced information technology to power and deliver those advances comes at a price. That same technology is creating vulnerability to data breaches and cybercrime. Hospital and medical research networks link not only sensitive records of patients' personal and medical affairs, but also the hospitals' diagnostic and treatment equipment, financial and health insurance information, and even intellectual property from medical trials. Such assets are a treasure trove for cybercriminals, whose increasing malware and ransomware attacks threaten their targets' obligation to protect data privacy and maintain service availability. In fact, the number of healthcare attacks has increased 125% over the past five years at an average cost of $2.2 million per data breach[1].

Challenges healthcare faces

Multiple users, multiple devices

Doctors, nurses, clinicians, technicians, and an extended staff in constant rotation all depend on the same vulnerable network. Often, it is a legacy IT system powered by an outdated operating system such as Windows XP, which is ill-equipped to effectively fend off cyberattacks. In addition, the Internet-connected clinical information system can surrender access to healthcare information through the connected devices' IP addresses. Those devices can include anything from exam room computers to imaging equipment, sensitive diagnostic devices, drug delivery machines, medical data input tablets, and blood-oxygen or insulin monitoring machines. Often, such dedicated hardware doesn't have security built in, which leaves the rest of the network open to attack. Such an event transpired at Banner Health, which operates 29 hospitals in Arizona, when hackers accessed millions of records after breaching the card processing systems across the hospitals' many food-and-beverage outlets[2].

Another challenge is the increased use of personal devices by medical professionals while on the job. A recent report indicates that 88 percent of healthcare organizations permitted medical staff to use their own tablets and phones to do their jobs, including for clinical communication purposes[3]. More than half of the organizations admitted that they were not certain of the devices' security, as they did not have visibility to ensure their security status.

Also, hospitals often share access to patient records with doctors' offices, insurance companies, and other related organizations. Some of these employees can be temporary, or visiting from partner organizations, which further complicates proper security.

Regulatory compliance

The tidal wave of malware and ransomware attacks the healthcare industry faces also points to increased regulatory oversight from federal and state authorities. It's a driving factor toward spending more budget, effort, and time to not only avoid breaches, but also the fallout from not protecting patient privacy. One such new oversight action recently came down from the Healthcare Insurance Portability and Accountability Act (HIPAA) to address ransomware attacks[4]. Noncompliance comes at a cost, as another case in 2016 made clear when the U.S. Department of Health and Human Services' Office for Civil Rights (OCR) announced that the Advocate Health Care Network has agreed to pay a $5.55 million settlement for multiple HIPAA violations related to a massive breach that occurred in 2013[5]. The reasons for the settlement came down to negligence and lack of risk monitoring.

Budget constraints

Cybersecurity budgets tend to be the stepchild of healthcare organizations' financial planning. While financial services firms generally allot 30 percent of their budgets to information technology, a typical hospital spends only about two to three percent on IT. Even with the rise in healthcare cyberattacks, many organizations have either decreased their cybersecurity budgets or kept them the same[6]. Another research report estimates healthcare spending on cybersecurity will reach about $10 billion by 2020, which is only about 10 percent of what the critical infrastructure industry expects to spend on securing itself against cyberattacks[7].

External threats

The security measures taken by the healthcare industry often focus on unsophisticated adversaries—individuals such as script kiddies or small groups that seek medical records in a shotgun approach. But several other categories of adversaries are at work, which are more ambitious in their motivations and sophisticated in their methods[8].

For instance, political groups or hacktivists target a specific victim's records for political reasons. Organized crime groups do the same, sometimes even with intent to harm a particular patient. Terrorists and their organizations are focused on harming both specific and indiscriminate patients, while nation states embrace all targets—threatening both patient well-being and patient records.

There is a black market in patient records, where identity thieves are willing to pay high prices for credit card data, email addresses, social security numbers, employment information, and medical history records. Insurance fraud also cheats insurers for nonexistent services, or to create fake IDs, purchase prescription meds, or file false insurance claims.

---

1 http://www.ponemon.org/blog/sixth-annual-benchmark-study-on-privacy-security-of-healthcare-data
2 http://www.cio.com/article/3118800/ehr/will-forensics-thwart-data-thieves-lurking-in-hospital-ehr-corridors.html
3 http://www.information-age.com/why-healthcare-industry-badly-needs-cyber-security-health-check-123460052/
4 http://www.hhs.gov/blog/2016/07/11/your-money-or-your-phi.html#.V4QHbf32lWA.twitter
5 http://thevarguy.com/secure-cloud-data-storage-news-and-information/healthcare-industry-can-t-seem-cure-cyber-attack-plag
6 http://www.cio.com/article/3118800/ehr/will-forensics-thwart-data-thieves-lurking-in-hospital-ehr-corridors.html
7 http://www.information-age.com/why-healthcare-industry-badly-needs-cyber-security-health-check-123460052
8 https://www.securityevaluators.com/hospitalhack/securing_hospitals.pdf

How Malwarebytes can help

Malwarebytes Endpoint Protection—Centrally protects hospital endpoints against known and unknown attacks, including ransomware. Provides multi-vector protection managed through cloud-based platform.

Malwarebytes Incident Response—Rapid detection and complete removal of advanced threats from Windows and Mac endpoints using cloud-based console. A perfect solution for large healthcare organizations and hospital networks supporting endpoints across multiple facilities.

Malwarebytes 3.0 (Windows)
Malwarebytes Anti-Malware (Mac, Android) Automatically and instantly stops malware threats on Windows computers and laptops. Removes malware and adware from Mac computers. Protects Android smartphones, tablets, and Google Chromebooks from malware, infected applications, and unauthorized surveillance.

What healthcare organizations say

> Malwarebytes is proactive protection. We see it block malware and ransomware every day. It works perfectly for us.
>
> —Juan Forero, Lead Info Security Engineer, AvMed

> Malware was in our environment and that was a huge source of concern when it comes to maintaining HIPAA and PCI DSS compliance. Now we're sure that malware doesn't even get in to start with.
>
> —Paul Feilmeier, IT Infrastructure Manager, Faith Regional Health Services

> Some companies rely primarily on their traditional antivirus solution. I'm the opposite—Malwarebytes is my go-to solution and my traditional antivirus is the backup.
>
> —Eric Leaf, Systems Engineer & Helpdesk Supervisor, CellNetix

Healthcare providers trust Malwarebytes

Cancer Treatment Centers of America
BROWARD HEALTH
Allscripts
FAITH REGIONAL HEALTH SERVICES
CELLNETIX PATHOLOGY & LABORATORIES
AvMed
TriHealth
International Medical Corps

malwarebytes.com/healthcare corporate-sales@malwarebytes.com 1.800.520.2796

Malwarebytes is the next-gen cybersecurity company that millions worldwide trust. Malwarebytes proactively protects people and businesses against dangerous threats such as malware, ransomware, and exploits that escape detection by traditional antivirus solutions. The company's flagship product combines advanced heuristic threat detection with signature-less technologies to detect and stop a cyberattack before damage occurs. More than 10,000 businesses worldwide use, trust, and recommend Malwarebytes. Founded in 2008, the company is headquartered in California, with offices in Europe and Asia, and a global team of threat researchers and security experts.