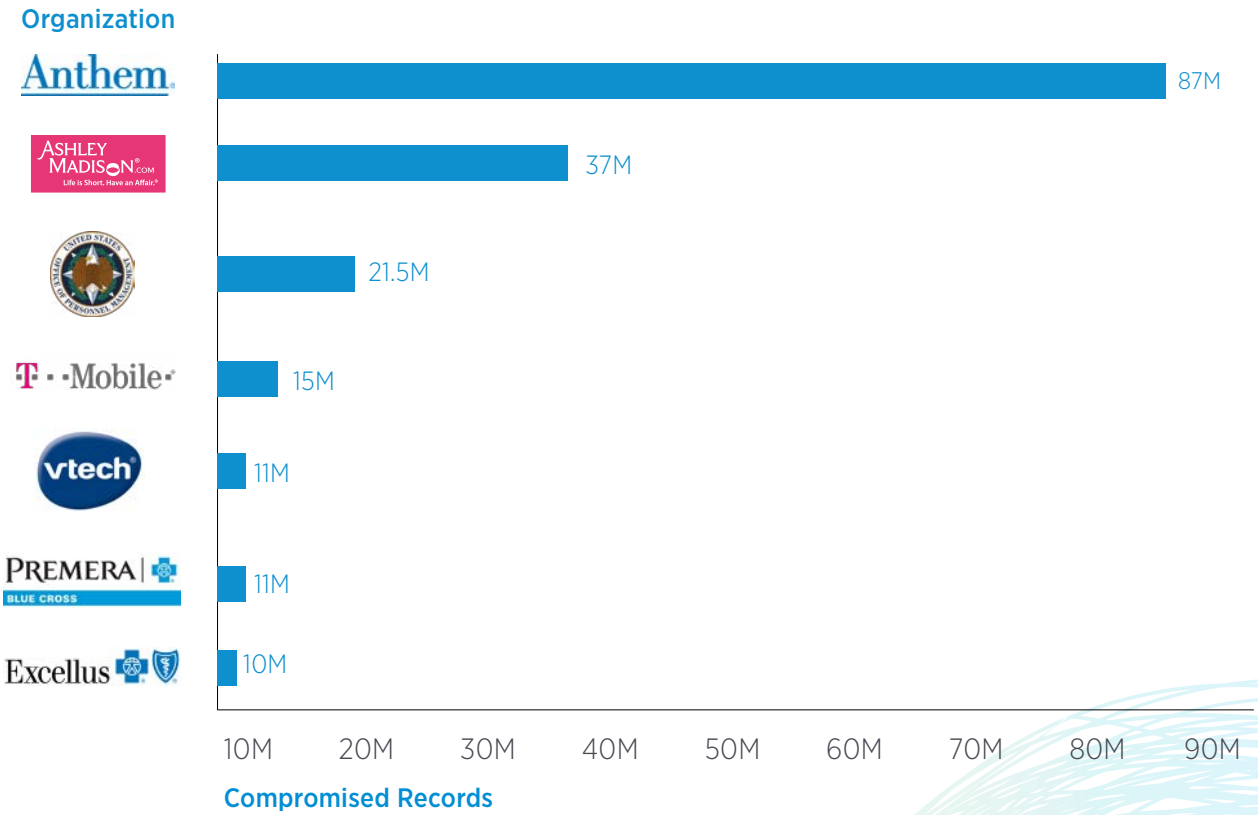
New Malware Threats Demand Action from Healthcare Sector

Whitepaper

SentinelOne

Introduction: Defending Data During the Healthcare Shift in Health Information Access and Storage

The average cost of a breached credit card, sold on the darknet, is hovering around the two dollar mark. Meanwhile, the potential price of a stolen health record now exceeds $350. Health records are serious business for cyber criminals, and the butchers' bill of breached organizations reflects this interest. According to IBM, healthcare now tops the list of most targeted industries,[1] and in a Health IT News article on the top seven data breaches of 2015, the top three attacks took place against healthcare organizations, with Anthem topping the list with 87M breached records.[2]



Payers and providers need to walk a tightrope. On the one hand, they must protect sensitive information from hackers. On the other, they must keep their information accessible for compliance reasons and patient access. When it comes to protecting the endpoints and servers of IT infrastructures, signature-based antivirus technologies no longer offer the level of security that healthcare organizations require. That's because it's trivial to modify malicious software so that it appears different from what traditional antivirus is programmed to recognize. Discerning malicious activity from benign activity also presents a particularly complex challenge for technologies reliant upon signatures and rules

This white paper examines challenges for healthcare organizations and presents how the key to effective endpoint and server protection lies in the ability to dynamically analyze behavior in order to recognize malicious software by its actions, not its appearance. Intelligent response at machine speed is required to prevent, contain and mitigate potential threats. Success in this mission results in a major benefit for providers and payers: the ability to keep IT systems operational so medical and non-medical personnel can stay focused on patient care.

The Security Challenges Faced by Healthcare Providers and Payers

For healthcare organizations, IT security is now more than just protecting patient records from being stolen: cyberattacks can also lock up records and make them unusable. Consider the case of Presbyterian Hollywood Medical Center in Los Angeles, which was held hostage by hackers in February of 2016. For more than a week, cyber criminals shut down the hospital's internal computer system for a ransom of 9,000 bitcoin (almost $3.7 million). The cyberattack forced the facility to revert to paper registrations and medical records. They also had to re-route 911 patients to other area hospitals.[3]

As of 2016, documented ransomware attacks have begun to match more traditional breaches in terms of frequency and damage.

Because hospitals appear to be the most high-profile ransomware targets, providers and payers must establish sufficient security measures. But the endeavor also presents many challenges:

- Defending against advanced cyber threats—known and unknown—such as malware and ransomware
- Preventing the loss of ePHI (electronic private health information) without impacting system performance
- Freeing up valuable IT resources from time-consuming, error-prone mitigation practices
- Ensuring the continuous and secure operation of critical medical IT systems
- Enabling rapid threat detection and mitigation on compromised endpoints and servers
- Performing automated responses to quarantine malicious software
- Terminating malware processes to proactively prevent data breaches
- Monitoring all endpoints, desktops, servers and mobile platforms that store or access HIPAA-sensitive electronic records and ePHI.

At the same time, providers and payers must contend with policy and HIPAA compliance issues, such as the necessity of a streamlined reporting process that frees up administrative personnel. Other issues include the ability to transfer data without suffering from "lost laptop" data breaches, securing data via encryption while leaving it accessible to physicians, and complying with the dictates of sometimes contradictory compliance regimes such as PCI-DSS.

The Weakest (and Costliest) Links: Why a New Approach Is Needed

When addressing IT security and compliance challenges, key areas of focus for healthcare providers should be their endpoints and servers—which are often the weakest links within security defense solutions. Though the cause is not confirmed, Ars Technica reported that Hollywood Presbyterian Hospital's attack originated from a phishing attack with a malicious attachment.[4] The website later reported a variant of crypto-ransomware targeted unpatched servers in late March, infecting the Medstar Health networks.[5] Medstar was forced to take many of their hospital systems offline to clean up the attack.

Endpoints and servers are also the costliest components to manage when considering the multiple burdens that increase the total cost of ownership:

- **Network**—Malware spreads, either automatically or under direction of a bad actor. Whatever infects one endpoint will inevitably go after the rest.
- **Vulnerabilities**—Both servers and endpoints contain software that must constantly be patched to the latest version in order to remain secure. This is a time consuming process, however, and is often neglected. According to the 2015 Verizon Data Breach Incident Response report, the vast majority of exploits due to vulnerability persisted for over a year after a patch was released.
- **Visibility**—without automated and immediate visibility into attacks that can potentially threaten endpoints, servers and the network, IT must spend an inordinate amount of time searching for attacks.
- **Response**—IT can also spend a lot of time prioritizing which threat to respond to first; in addition to wasting their time on false positives and relatively harmless threats, this also increases the chances they will fail to respond to a major attack.

Many healthcare organizations have frustrating experiences with their existing endpoint and server security solutions as they fail to stop the attacks. After getting hit by major attacks, they also spend an inordinate amount of time on clean-up. In the case of a severe ransomware attack—and especially in cases where the attacker refuses to unlock a victim's files even after a ransom is paid—the lost cleaning up infection and restoring documents can be immense.

Providers and payers also discover that costs increase with each endpoint and server security element they add—each layer promising to protect, identify and respond. The potential arsenal includes antivirus, anti-malware, forensics, advanced threat protection, host-based IPS, desktop firewall, and data loss prevention. Not only are these technologies expensive from a cost perspective, they are also resource and bandwidth intensive—causing frequent blue screens and introducing negative impacts against business performance.

Compounding this bandwidth problem is the fact that each separate security solution may require herculean efforts to work effectively in tandem. A proper Security Operations Center (SOC) must have the ability to see all relevant security data in a single pane of glass. If interoperability problems prevent this, then security professionals are forced to divide their attention—which will inevitably lead to error.

Top Three Attack Vectors Targeting the Healthcare Industry (according to a recent Ponemon study)[6]

1. Ransomware is on the rampage, holding business systems and data for ransom, perhaps even threatening to destroy them if the terms are not met

2. Malware, such as Zeus (Trojan) attacks, continue to be re-packed and altered time and time again to infect financial institutions

3. Denial of Service is often being used as a diversion tactic while attackers extract information from the organizations network and systems

Tips to Protect Endpoints

To address the short-comings of human intervention, healthcare organizations need to augment their antivirus solutions with endpoint detection and response. Doing so reduces the amount of time to discovery and mitigation.

When evaluating potential solutions for your organization, look for one that provides these key capabilities:

1. Monitors all endpoints, desktops and mobile platforms that store or access HIPAA-sensitive records and protected health information.
2. Detects advanced and unknown threats that evade traditional antivirus and legacy security products.
3. Automatically mitigates risks posed by compromised endpoints that may be connected to the network.
4. Enables rapid compliance reporting through comprehensive data collection and reporting on the status, threat activity and remediation actions across all endpoints.
5. Leverages intelligent automation to contain and mitigate threats, including proactively disconnecting hosts from the network to prevent malware from infecting other hosts or to kill and quarantine threats.
6. Conserves CPU resources so endpoints can function as they are supposed to.

Tips to Protect Servers

In addition to endpoints, also consider the protection your servers require. These assets host all of your most valuable healthcare assets—personally identifiable patient information.

Cloud, on-premises, and hybrid servers each present their own security challenges. Co consider a strategy for protecting each type. While servers running on the Microsoft Windows operating system have long been susceptible targets, the Linux OS is starting to emerge as another threat vector for cyber criminals.

As you consider which endpoint detection and response solution to deploy for your servers, be aware that many security solutions utilize precious system resources. Signature-based antivirus can push CPU utilization to beyond 50%, especially when updating or running scans Each time you apply patches and configuration changes, they can degrade server security levels.

When evaluating potential solutions for your organization, look for one that provides these key capabilities:

1. Requires extremely conservative CPU utilization (under 2%) so business can operate as it should.
2. Monitors all server platforms that store HIPAA-sensitive records and protected health information.
3. Detects advanced and unknown threats that evade traditional antivirus and legacy security products to buy time when a zero-day exploit is discovered.
4. Automatically mitigates risks posed by compromised servers that may be present within the datacenter.
5. Enables rapid compliance reporting through comprehensive data collection and reporting on the status, threat activity and remediation actions across all endpoints.
6. Leverages intelligent automation to contain and mitigate threats, including proactively disconnecting hosts from the network to prevent malware from infecting other hosts or to kill and quarantine threats.

Key Regulatory Tips to Achieve and Maintain Compliance

Tip 1

HIPAA Security Rule: The Health Insurance Portability and Accountability Act (HIPAA) requires Covered Entities to take strong measures to protect the privacy and security of health information. At the endpoint, this translates to ensuring the host is protected from malware.

Tip 2

HIPAA Security Rule Administrative Safeguards: §164.308(a)(5)(ii)(B) specifically requires Covered Entities and Business Associates to implement and maintain procedures to protect, detect and report on malicious software throughout their environment. These safeguards require maintaining up-to-date systems and leveraging leading cloud reputation services. If malicious files are detected, alerts generated on the endpoints must include the capability to alert administrators, not only by e-mail but also by text message. Reports should be generated and stored on an encrypted file system on the management server. Generated logs should be sent to a security information and event management (SIEM) system for further investigation.7

Tip 3

The Health Information Technology for Economic and Clinical Health (HITECH) Act: This regulation promotes the adoption and meaningful Use of health information technology. The act also addresses the privacy and security concerns associated with the electronic transmission of health information, in part, through several provisions that strengthen the civil and criminal enforcement of HIPAA rules. Specifically, Core Set Rule 15 requires organizations “ensure adequate privacy and security protections for personal health information” to “protect electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities” where a failure to do so “due to willful neglect is a violation for which the Secretary is required to impose a penalty.” Systems that host, manage, and access protected health information must be protected at all times with an enforceable and auditable endpoint security policy.

Tip 4

PCI DSS - The Payment Card Industry Data Security Standard (PCI DSS) protects cardholder data wherever it resides to ensure that merchants (including payers and providers executing transactions) and service providers maintain the highest information security standard. PCI DSS is a set of comprehensive requirements for enhancing payment account data security. The standard was developed to help facilitate the broad adoption of consistent data security measures on a global basis. PCI DSS Requirement 5 requires the protection of all systems against malware. To maintain PCI DSS compliance, healthcare organizations need to deploy security measures that achieve the following objejectives:

- Install antivirus software on all systems commonly affected by malicious software.
- Confirm antivirus programs detect, remove and protect against all known types of malicious software.
- Keep all antivirus mechanisms current, perform periodic scans, and retain all audit logs.
- Ensure antivirus mechanisms are actively running and cannot be disabled or altered—unless specifically authorized by management on a case-by-case basis and for a limited time period.

SentinelOne for HealthCare

To help healthcare organizations take on the security challenges, SentinelOne's Endpoint Protection Platform and Critical Server Protection Platform monitor all endpoints, desktops, servers and mobile platforms that store or access HIPAA-sensitive electronic records and protected health information. The platforms also detect threats that evade traditional antivirus and legacy security products while automatically mitigating risks posed by compromised endpoints within healthcare IT datacenters. In addition, SentinelOne enables rapid compliance reporting through comprehensive data collection and reporting on the status, threat activity and remediation actions across endpoints.

Key Benefits of SentinelOne for Healthcare Organizations

- Prevents loss of electronic Protected Health Information without impacting performance
- Ensures continuous secure operation of critical medical IT systems
- Enables rapid threat detection and mitigation on compromised endpoints
- Performs automated response to quarantine malicious software
- Kills malware processes to prevent data breaches

SentinelOne for HIPAA and PCI: Tevora, a compliance assessor, tested SentinelOne and found its platforms meet HIPAA 164.308(a)(5)(ii)(B) and PCI DSS 3.1 requirements 5.1, 5.1.1, 5.2, & 5.3. For specifics on their findings, see Enterprise Protection Platform for PCI DSS & HIPAA Compliance.

Unified Threat Prevention, Detection and Response Keep the Focus on Patient Care

Now more than ever, deploying a unified threat prevention, detection and response solution is critical for healthcare organizations as they transform how they store, access and protect health records while defending against malicious threats. As payers and providers adapt to electronic patient record requirements—while enabling the portability of information through electronic data storage and communication—they can take on this challenge by deploying sophisticated machine learning and intelligent automation, such as SentinelOne, which defeats advanced malware, ransomware, exploits and other cyberattacks.

By taking this approach, healthcare organizations can ensure data is protected from breaches while also making sure data continues to be easily accessible for compliance reporting. Success in this mission also results in a major benefit for providers and payers: the ability to keep IT systems operational so medical and non-medical personnel can stay focused on patient care.

For more information on SentinelOne, visit www.sentinelone.com. To schedule a demo tailored for your organization, visit www.sentinelone.com/contact.

Citations

1. "Healthcare Was Most Attacked Industry in 2015: IBM," by SecurityWeek News, April 25, 2016: http://wwwsecurityweek.com/healthcare-was-most-attacked-industry-2015-ibm
2. "7 largest data breaches of 2015," by Jessica Davis, Healthcare IT News, 11 December 2015: http://wwwhealthcareitnews.com/news/7-largest-data-breaches-2015
3. "The hospital held hostage by hackers," by Anita Balakrishnan, CNBC, 16 February 2016: http://www.cnbc.com/2016/02/16/the-hospital-held-hostage-by-hackers.html
4. "Hospital pays $17k for ransomware crypto key," by Sean Gallagher, Ars Technica, 18 February 2016: http://arstechnica.com/security/2016/02/hospital-pays-17k-for-ransomware-crypto-key/
5. Ponemon Study
6. "Maryland hospital: Ransomware success wasn't IT department's fault," by by Sean Gallagher - Apr 7, 2016: http://arstechnica.com/security/2016/04/maryland-hospital-group-denies-ignored-warnings-allowed-ransomware-attack/
7. SentinelOne HIPAA PCI Whitepaper_22 APR 2016.pdf

SentinelOne

With intelligent automation becoming an obvious replacement for signature-based detection, SentinelOne offers a comprehensive solution for servers and endpoints. Full-context behavioral threat analysis that leverages machine learning captures and neutralizes both known and unknown threats, while providing a forensics package that allows administrators to visualize attack paths and remediate vulnerabilities. The solution is also extremely lightweight.

AV-TEST, a leading independent anti-virus research institute, has awarded SentinelOne Endpoint Protection Platform (EPP) the Approved Corporate Endpoint Protection certification for both Windows and OS X, which validates its effectiveness for detecting advanced malware and blocking known threats. SentinelOne EPP is the only next generation endpoint protection vendor to obtain this certification on both platforms.

SentinelOne EPP has also been validated against HIPAA and PCI-DSS by a third-party compliance assessor. This validation now enables healthcare organizations to replace their existing corporate antivirus suites with SentinelOne EPP and still meet HIPAA and PCI-DSS compliance requirements.

In addition, SentinelOne is the only vendor to offer financial insurance against ransomware attacks with the Ransomware Cyber Guarantee. SentinelOne EPP customers are eligible for up to $1M of coverage (up to $1000 per endpoint) in the event a ransomware attack occurs.

With SentinelOne, Healthcare IT teams finally have a viable path forward that allows them to stay ahead in the arms race against bad actors. Instead of spending limited time, money, and manpower remediating breaches that are already in progress, security practitioners can now usefully devote their time to reinforcing the solid foundation that SentinelOne provides.

For more information about SentinelOne, please visit www.sentinelone.com.