HEALTHCARE BRIEF

Security in Healthcare

Effective response ensures effective security

Key Points:

- The healthcare industry is a multi-trillion dollar industry that is the subject of twice the number of cyberattacks as other industries
- The known obstacles of device management, patient information, resource constraints and regulatory concerns hamstring teams seeking to secure healthcare provider and payer networks
- The unknown obstacles posed by the integration of unknown networks via M&A further challenge these teams
- Quick detection and rapid response/investigation is key to secure these networks
- **Solution: Gigamon Insight** Gigamon Insight is a cloud NDR solution that is purpose-built to address this need

Challenges

Your industry is large, and you're a target. Consider the following data points:

10 trillion USD
Healthcare Industry expenditures, 2017-22[1]

1.4 million USD
Estimated recovery cost, per cyberattack[2]

2x the amount
Number of cyberattacks Healthcare undergoes as other industries[3]

Besides the financial implications there are the standard 'reputation and recovery' issues that organizations must undergo after the attack is re-mediated. And that does not count the potential loss of PII data that may never be recoverable, and which then exists out there somewhere in the world.

The immediate reaction to these facts: if this is such a large problem, what's being done about this? The reality: organizations are doing many things, spending billions in healthcare security. With this amount of spending taking place, why are organizations still dealing with larger and larger numbers of Cybercrime? Answer: they need to effectively empower Incident Response

The Obstacles

In speaking to Healthcare Security teams, a number of themes regarding known obstacles are prevalent:

- Security Teams are constrained
- Teams often must react to threats with a patchwork of technologies or methodologies
- Regulatory concerns

Constrained Teams

The first item is known to healthcare security professionals working with healthcare providers. Medical devices are unique entities; they are certified to perform certain tasks using predictable deployments of operating systems and applications. As such, they cannot by patched or upgraded, and cannot run third party applications that could cause unpredictable behavior. When devoid of the tools used to commonly

secure endpoints, healthcare security professionals often feel that they have to 'go back to the drawing board', and use antiquated tools designed for unsupported applications (the use of Internet Explorer and Windows XP is widespread, for instance). For healthcare payers, security concerns center around PII or more generally, patient data. Since healthcare is twice as likely to be targeted by attackers, end-to-end security, i.e., knowing where data is located and how it is being secured, is paramount, on top of all of the needed security tools, processes and teams to handle incoming threats. However, teams are hamstrung for a variety of reasons: budget, the simple 'control over their own network' (outsourcing) and lack of qualified personnel (a problem prevalent across all verticals) are most often cited as the top areas of concern.

Patchwork of technologies or methodologies

The second item listed above is the logical response to the obstacle: you still have a mission to complete, so you do what it takes to perform the security mission, even if it takes 3 or four team members inefficiently 'checking their work' and covering, as best they can, the problems they're seeing in the environment. When you consider outsourcing of some of the core network functions and network architectures that have organically grown over years (and in healthcare, in some cases, decades) teams are even more pressed to react as best they can, with little opportunity to pro-actively fix root problems within their networks.

Regulatory Concerns

The third item: regulatory concerns. In addition to HIPAA, patient financial information is also subject to GLBA compliance, and overall financial transactions, to SOX,
among others.

Unknown obstacles

So, the known obstacles are already quite challenging. What about the unknown ones? In this era of ever-changing organizations, Mergers and Acquisitions (M&A) are notorious for exposing the greatest concerns regarding the unknown. The concerns:

- Who is potentially buying our organization? Who are we buying or merging with?
- What does their network look like? Remote sites? We have our network and processes setup a certain way, what are we taking on? The concerns are real.

Effective Response

The combination of challenging organizational environments, lack of resources, regulatory concerns and unknown challenges (in addition to the incredibly large bullseye created by the amount of money at stake) provides the 'perfect storm' of issues that are ripe for attacker exploitation and reward. As such, healthcare security professionals have long ago adopted the stance of security-through-agility (detect, respond, investigate/protect) as the preferred methodology for security in this vertical. Yet, even after taking this stance, most organizations still are confronted with how to best provide effective response. Why? Often, teams wrestle with the very solutions they have chosen to deploy, as many solutions do not provide a holistic view into information that is attack-related. Thus, teams spend huge amounts of times sifting through 'first level alerts' (alerts related to only a small aspect of an attack), or large log data files (often collected for more than just security concerns) or finally, looking through vast quantities of data (wherein well-constructed queries into the recordings of network traffic can take hours or in some cases, days, before relevant information is attained, not very efficient).

Healthcare Security Teams: The Needs and Solutions

Teams need visibility into all traffic across the network, but concurrently, they cannot expose PII data:

Visibility is a tricky thing; most organizations believe that visibility is achieved by collecting data from a network, simply be done via deployed network devices, and find to their dismay that large tracts of their network are literally unknown and uninspected, providing perfect hiding spots for malicious activity. Often, teams respond by 'recording everything' and then have the concern over securing the recorded data, due to privacy concerns. One problem is thus replaced with another.

Solution: Collect Metadata. Investigators, hunters and responders need to answer 3 questions:

- **Who** was in the network?
- **What** did they affect or compromise?
- **How** did they do it so I can prevent it in the future?

Enriched metadata provides all of this information without having to record every transaction, making datasets smaller, indexing and searches faster and teams more agile.

Teams need unobtrusive (read: no installed applications) forensics tools that provide more than just a first level detection:

Detections and their corresponding alerts are also a tricky thing: teams are often taught that a security device should be alerting...a silent device isn't doing its job. Vendors respond by alerting about everything...and teams are then stuck having to make sense of the alerts. True forensics tools should both detect and ingest detections and alerts from other systems, and provide an analysis of the information, correlating detections related to the same threat, and providing teams with context to the threat (what the threat is, what it does, what to expect next, how to re-mediate). Teams can more rapidly respond to a detection on an unpatched system, for instance, if they already have all needed relevant information about the threat, and the means to do something about it.

Solution: Deploy a Network Detection and Response (NDR) technology. Network Detection and Response technologies use a combination of unobtrusive sensors and analytics engines (driven by threat intelligence), to collect relevant data and provide context behind a string of alerts, providing teams with relevant data quickly.

Teams need quick to deploy and adapt, scalable technologies that can provide near instantaneous access to specific data, used for rapid response:

M&As, 'organic' widely-separated networks, large data throughputs...all of these challenges need technologies that can be rapidly deployed, scaled and adapted, that also can track threats over longer periods of time (needed for today's sophisticated threats) without breaking the bank on the storage, indexing and querying of vast quantities of data).

Solution: Deploy a Cloud NDR Solution. For solutions that record Metadata, PII concerns are lessened (see Figure 1, Metadata Use for Investigation and Response). The use of a cloud-deployed architecture provides coverage and scalability for even the most disparate networks, while deployment, ease of use and adaptability are kept to a maximum.

An Effective Solution

The security industry has recognized the overall needs listed above, and has addressed the need in manner of sorts: many solutions collect network metadata for visibility and rapid retrieval. There are also solutions that provide intelligence, and others yet that provide flexible deployment architectures. However, many security solutions are purpose-built to provide emphasis in specific areas of security (network analysis, forensics, data capture, etc.) but none emphasize architecting solutions that specifically address all of these concerns from the point of view of the consumers: the Investigator, Responder and Threat Hunter. As such, solutions are incomplete from an investigative-platform point of view. Their inadequacies are left to be addressed and absorbed via processes and teams that can ill-afford to take on yet another responsibility. An effective solution addresses all of these concerns in one platform, as seen in Figure 1 and Table 1.

Figure 1: Gigamon Insight metadata collection for incident response

Example:
A user posts a photo online.

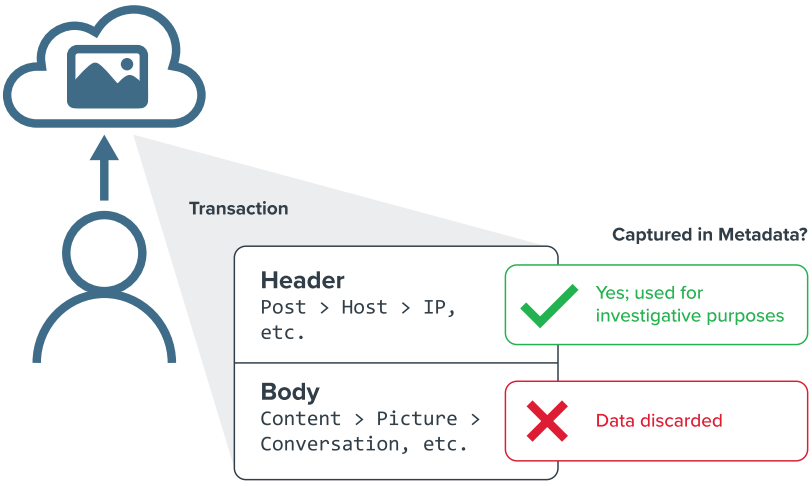

Table 1: Security needs and the Gigamon Insight solution

Item	Reason	How Gigamon Insight Solves
Visibility and Metadata	Only full visibility into a network can provide the data and context behind the data needed by teams for rapid detection and response	The Insight solution utilizes a series of lightweight (read: non-management intensive) sensors that continuously record all data. Metadata is extracted and enriched, providing indexing for rapid queries and lower storage needs
Network analysis; no agents	Healthcare appliances have strict requirements in terms of testing and certification; they cannot arbitrarily support additional applications apart from what was present when certified	The Insight solution analyzes the network (no agents required) thus allowing for easy deployment in networks containing a variety of operating systems, devices and applications. Insight also uses forensics provided by Gigamon's Advanced Threat Research (ATR), which provides proper context behind alerts, enabling rapid response and investigation.
Cloud deployment	Distributed networks and lack of team resources require solutions that can rapidly integrate and deploy without requiring additional management by overburdened teams	The Insight sensor is cloud-deployed and managed by Gigamon. Deployment is quick, scalability large and integration (as well as adoption) is fast.

Conclusion

Security in healthcare continues to be a huge challenge. Though the issues are varied, solutions that target specific healthcare concerns (data privacy, rapid response, ingrained analysis/less alerts, M&A and both device and network challenges), like the Gigamon Insight solution, should be high on healthcare security team's radar, as rapid response, beyond being just a security concern, is also a human one.

References

1. Allen, Stephanie. "2019 Global Health Care Sector Outlook." Deloitte Global Public Health & Social Services. January 09, 2019. Accessed June 12, 2019. https://www2.deloitte.com/global/en/pages/life-sciences-and-healthcare/articles/global-health-care-sector-outlook.html.

2. Davis, Jessica. "Healthcare Cyberattacks Cost $1.4 Million on Average in Recovery." HealthITSecurity. January 22, 2019. Accessed June 12, 2019. https://healthitsecurity.com/news/healthcare-cyberattacks-cost-1.4-million-on-average-in-recovery.

3. Adefala, Ladi. "Healthcare Experiences Twice the Number of Cyber Attacks As Other Industries." CSO Online. March 06, 2018. Accessed June 12, 2019. https://www.csoonline.com/article/3260191/healthcare-experiences-twice-the-number-of-cyber-attacks-as-other-industries.html.

4. Kasumov, Aziza. "Cyberattacks on Health-Care Providers Are Up in Recent Months." Bloomberg.com. July 17, 2018. Accessed June 12, 2019. https://www.bloomberg.com/news/articles/2018-07-17/cyberattacks-on-health-care-providers-are-up-in-recent-months.

Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | www.gigamon.com