WHITE PAPER

How To Mitigate Five IT Problems Affecting The Healthcare Industry

New hardware and software technology changes can be used for both constructive and destructive purposes. Unfortunately for healthcare, new technologies have created new security risks.

IT Challenges for Healthcare

The healthcare industry has been suffering from five major IT challenges over the last several years including:

- How to minimize security breaches, reduce cyber theft, and increase patient privacy
- Eliminating network blind spots due to hospital mergers and acquisitions
- Transformation of the business to align with the Consumerization of Medicine
- How to leverage technology to provide a competitive advantage
- How specifically to use technology to improve overall network performance

New hardware and software technology changes can be used for both constructive and destructive purposes. Unfortunately for healthcare, new technologies have created new security risks. Specifically, security breaches resulting in the theft of personally identifiable information (PII) are growing. A prime example is the 2015 Anthem/Blue Cross security breach that resulted in the theft of PII for 78.8 million people.[1] It was one of the biggest data breaches of the 21st century, and it had significant financial and brand impacts for Anthem. Other companies have been impacted by security breaches as well. In January 2018, for

1 https://en.wikipedia.org/wiki/Anthem_medical_data_breach

KEYSIGHT TECHNOLOGIES

example, 53,000 patient records were breached in a phishing hack on Onco360 and CareMed Speciality Pharmacy. That same month, 280,00 Medicaid patient records were breached in a hack on the Oklahoma State Heath Sciences network.[2] And these attacks are just the tip of what has become a very large industry-wide problem.

Most ransomware victims had to shut down their computer networks, directly impacting patients, so they could begin remediation of the malware attack.

In addition, hospitals and clinics are specifically under attack by ransomware, like the January 2018 attack on the Hancock Health hospital[3] and the May 2017 WannaCry attack that hit the United Kingdom's National Health Service.[4] There have been other ransomware attacks on hospitals in 2018 as well. Most ransomware victims had to shut down their computer networks, directly impacting patients, so they could begin remediation of the malware attack.

But the problems for healthcare IT aren't just centered on security. Company mergers and acquisitions (M&A's) between different hospitals and clinics cause network integration issues as well. According to a 2017 year-end report from Kaufman, Hall & Associates, LLC, a total of 115 hospital and health system M&A transactions were recorded in 2017.[5] That number represented an almost 13% increase from 2016 and was the highest number of recorded transactions in recent history. More M&A's were pending for the rest of the year. These resulting M&A's typically translate to the creation of "blind spots" within IT networks because disparate corporate data networks trying to communicate with each other do not transmit data correctly. Blind spots are areas where IT does not have complete visibility into what is happening on the network or how applications are behaving. Mergers between IT systems for any organization, especially healthcare systems, can take time. The problem is that patients and doctors don't have time to wait. Electronic medical records (EMR) need to be available at all times, for all patients.

Consumerization and the need to be more competitive are also key drivers for the healthcare industry. Cloud networks, Internet of things (IoT), bring your own device (BYOD), telemedicine, and other new technologies are driving change into the healthcare system. How individual IT organizations can take advantage of these technology changes will decide the success of those companies. This includes visibility into potential network and application problems as a result of the new technology and the ability to improve the performance of healthcare networks.

Network visibility and testing solutions are available to help overcome these challenges, regardless of whether the healthcare institution is a hospital, clinic, health insurance company, or any other institution. The secret is to eliminate network blind spots, perform key network assessments, and harness technology to replace outdated,

2 http://www.healthcareitnews.com/projects/biggest-healthcare-data-breaches-2018-so-far
3 http://www.zdnet.com/article/us-hospital-pays-55000-to-ransomware-operators/
4 https://www.scmagazineuk.com/ransomware-attack-forces-us-healthcare-provider-turn-away-patients/article/1661355
5 https://www.kaufmanhall.com/sites/default/files/2017-in-Review_The-Year-that-Shook-Healthcare.pdf

manual processes. In this whitepaper, we will explore how a visibility architecture and your network validation solutions can be integrated with your network and security architectures to maximize network defenses and performance.

Minimizing Security Threats & Protecting Patient Privacy

New threats continue to emerge. Hackers are now embedding new malware threats into secure socket layer (SSL) encrypted traffic. W-Fi usage for IoT devices (like automated pain dispensers and vital statistic monitoring) is also posing a new threat as this gives hackers a new attack vector.

To combat these threats, healthcare organizations need to understand that they ARE being targeted and maximize their security defenses.

To combat these threats, healthcare organizations need to understand that they ARE being targeted and maximize their security defenses. So what is the answer? One course of action is to improve the deployment of inline security tools (intrusion prevention system (IPS), firewalls, threat prevention systems, SSL decryption/encryption techniques, etc.) to prevent breaches. A second course of action is to maximize the deployment of out-of-band security tools like data loss prevention (DLP), security information and event managements (SIEMs), and intrusion detection systems (IDS) to analyze suspect packet data and log data to determine if a breach has occurred and how. A third course of action is to upgrade the resiliency of your defenses with high availability and load balancing between tools to create maximum uptime. A fourth course of action is to deliberately test network security defenses, in the lab and before therollout of upgrades, to validate the technology updates.

Healthcare IT organizations can improve their security solutions by deploying bypass switches and inline network packet brokers (NPBs) with heartbeat technology. These two components improve network availability and enable new capabilities like High Availability (maximum resilience against failure), load balancing across tools (very useful if your IPS does not support clustering and exchange state information), and the serial chaining of data across multiple tools (firewall, IPS, etc.) to deliver improved analysis of suspect data.

NPBs are also needed to segregate, load balance, and regenerate the aggregated traffic before the data is sent to out-of-band tools like IDS', DLPs, SIEMs, and SSL decryption tools. SSL decryption technology can be very useful in this portion of the network by giving you full visibility into the network traffic before capturing, indexing and storing it for DLP processing.

Threat prevention systems with automated updates for known bad IP addresses can help protect against various security threats (malware, ransomware, DDOS, etc.) by preventing inbound and outbound communications to and from those bad IP addresses. The automated updates help keep systems as up to date as possible as bad actors change IP addresses to launch new threats. The alternative is to use firewalls with access

lists but the updates to those access lists are usually a manual process, which can have significant delays between updates. This translates to more vulnerability and risk.

Another often overlooked solution is to thoroughly test your security architecture before you rollout new updates. This is often seen as difficult to do but in reality it can be quite simple. All a security architect needs to do is to create a lab environment that mimics the security architecture. Next, a test solution (like the Keysight BreakingPoint product) is installed into the lab. The test solution can then run automated test scripts with a combination of application load and malicious traffic to see how the solution performs against various threats (malware, DDOS, etc.) and configuration errors before general roll out. The last thing you want is self-inflicted injuries from network and security architecture changes. According to the Verizon DBIR, up to 25% of security breaches are caused by internal actors.[6]

For high security environments, application intelligence can be used to create a “safe zone”. In this safe zone, the number and types of applications are limited. Signatures can be created for the approved applications. Once this is done, application intelligence can be used to constantly monitor that environment to make sure that there are no unauthorized applications, which would probably be security threats, running in those environments. An example would be a research lab that has maybe five different applications running in the protected environment. If any other application traffic is discovered, it can be quickly analyzed to determine location and source.

Application intelligence can also be used to identify applications running on the general network that should not be there. This could be important if web-based applications are being used that circumvent the general anti-virus, anti-malware inspections of the normal email system. These uninspected emails could be carrying links to malware like ransomware. Application Intelligence can also be used to see if private web-based email is being used that circumvents your stated email security policies.

6 Verizon, 2017 Data Breach Investigation Report.

SOLUTION OPTIONS

- Improve inline security deployments with bypass switches and packet brokers
- Improve data analysis policies to analyze suspect data better
- Implement High Availability and load balancing for security tools
- Deploy threat prevention systems for better IP address screening
- Test security solutions before roll out to validate configurations
- Use Application Intelligence to create a safe zone against malicious programs
- Use Application Intelligence to validate security policy adherence

Eliminating Network Bling Spots During Mergers and Acquisitions

The solution to blind spots is better monitoring strategies. Taps can be placed anywhere in the network that data access is needed, whether the network is physical, virtual or cloud-based.

As mentioned earlier, the consolidation of hospital and other healthcare institutions can cause network blind spots. This is because as the hospital IT networks are integrated, those two networks typically coexist for a time, possible a long time, as essentially separate networks with a gateway between them. This gateway can become a chokepoint. There may also be a difference in network architectures (leaf and spine vs. hub or cloud networks), different network monitoring strategies, and so forth.

In addition, the use of the same applications doesn't automatically mean instant interoperability. For example, while both networks might be using Oracle, the configuration setup could be different enough that some fields are unsupported in both systems, causing data loss when communicating between systems. This can happen across many applications, not just Oracle.

An increased use of cloud networks could also cause a loss of network visibility. It is common for an enterprise to have up to 6 cloud networks.[7] During a merger and acquisition, this could be 12 or more cloud networks. At this point, security becomes another risk, especially for EMR systems (like EPICs, Cerners, McKesson, and other HL–7 v3 applications), health information exchanges, and HIPAA compliance between networks.

As hospital institutions are consolidated, the need for monitoring the whole hospital IT network will increase, driving the need for additional hardware, tools, system management changes, and special integrations.

The solution to blind spots is better monitoring strategies. Taps can be placed anywhere in the network that data access is needed, whether the network is physical, virtual or cloud-based. This data can be especially necessary if centralized data centers and IT Operations groups are created by the merged hospital entities. IT needs the proper data to address application and performance problems on the network as well as creating

7 https://www.rightscale.com/lp/state-of-the-cloud?campaign=701700000015euX

visibility into what is causing performance problems and where the problem is located. In addition to taps, network packet brokers are necessary to filter out extraneous data being fed to the different monitoring tools.

SOLUTION OPTIONS

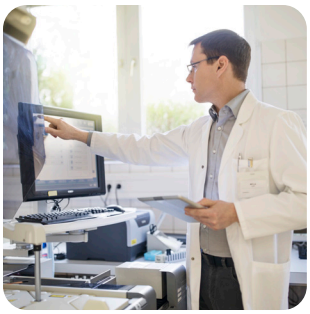
- Taps can be placed anywhere for network access and application monitoring
- Virtual taps create access points for virtual monitoring data
- Network packet brokers enable monitoring data filtration and dispersal to tools

Transforming the Business to Align with Consumerization

A big area of interest for healthcare institutions is the consumerization trend where a lot of information is now being collected and made available to mobile and web-based devices. For instance, hospitals are now embracing BYOD for healthcare professionals and even support the use of patient accessible Wi-Fi. However, as the role of Wi-Fi networks expand within healthcare facilities, one of the drawbacks of consumerization is the uncontrolled consumption of bandwidth. Not all consumption is equal, or linear.

For instance, recent years have seen an explosion of IoT-based medical devices. One example is the use of infusion pumps, called “smart pumps,” that can disburse medication without a nurse being present. Electronic patient monitors are another example. These devices do more than just output data periodically to the nurses’ station. Infusion pumps need to download drug libraries and WLAN-based telemetry transmitters send alarms and waveform data to a central station. Mission-critical medical devices and applications need to be able to transmit critical alarms.

There are other bandwidth hogs as well: VoIP-based medical communication systems (like Vocera badges), data downloads onto healthcare institution laptops and notepads, and guest access by patients (both data and video watching). IT needs enough bandwidth and prioritization of data types to guarantee real-time medical transactions are passed through the network without delays. Therefore, IT needs to be able to understand who is using the bandwidth and who is abusing it. For instance are Vocera Wi-Fi badges consuming the bandwidth for Voice over IP (VoIP) activities or are patients watching lots of Netflix?



Consumerization is also driving other forms of IP-based communication, like web-based billing, point-of sale (POS), and mobile payments. Consumers like the multitude of payment options that fit their varied needs. Web-based appointment scheduling is another new app that allows both patients and staff more convenience in scheduling appointments.

Telemedicine is another technology driver. Geographically remote consumers like the convenience and access benefits of telemedicine. Busy consumers like it too as they can get 24-hour, instant access to physicians (like Teladoc and Doctor on Demand) at a low cost without having to travel to an office. This can be a great option for the flu or rashes. From an IT perspective, both front end and back end technologies need to be in place to enable these services.

To be viewed as “cutting edge”, many hospitals are trying to adopt newer technology like: public Wi-Fi, IoT for medical equipment like electronic pain dispensers and patient vital statistics monitors, and telemedicine. However, this is predicated upon the network functioning correctly. To validate this, routine testing needs to be performed on the Wi-Fi system and the wired network.

Wireless networks can have a multitude of impairments due to: frequency planning issues, building obstructions, lead-lined walls in radiology rooms, tilelined bathrooms, the proliferation of BYOD devices from staff and patients, radio performance (as not all radios are created equal), and roaming issues between access points. Because of the traffic intensiveness for wireless LAN connections, IT should perform testing of the wireless LAN network consisting of: frequency interference, traffic generation for load, automated test cases, and performance analysis by quantifying application performance and user perspective.

Once the network is tested for proper operations, an NPB with application intelligence can assist with determining what applications are running on the network and who’s abusing network bandwidth (e.g. is there a lot of Netflix watching). Other technology can then be used to throttle back usage for network hogs so that telemedicine and IoT devices have enough bandwidth.

Thanks to IoT, there are literally thousands of devices in a hospital. To make it easier for IT to understand what is happening on the network, it is common to separate different device types (infusion devices, patient monitoring, VoIP) based on a VLAN and ESSID. As part of the network and application monitoring strategy (to ensure quality of experience and service validation), these data types can be segmented using an NPB (based upon the VLAN information) and the requisite data can be forwarded to the appropriate monitoring tools.

SOLUTION OPTIONS

- Perform continuous wireless LAN testing to optimize the Wi-Fi network
- Use Application Intelligence to determine bandwidth location by application type
- Use an NPB to perform VLAN filtering to segment monitoring data as needed

Using Technology to Gain a Competitive Advantage

While competitive advantages are often fleeting, the IT network is a critical focal point for healthcare institutions to capitalize upon. Not only does it enable data transfers, but communications is a second area of importance. According to CRICO Strategies research, healthcare miscommunications cost 2,000 lives and $1.7 billion in malpractice costs over a four year period. During that same timeshare, an estimated 30% of all claims involved a communications failure.[8] The key to improving this issue is the integration of your network and visibility architectures.

Two ingredients are critical to maintaining a competitive advantage—using technology to reduce downtime and control costs and deploying new technology to improve productivity. Downtime is critical. According to a study from Information Technology Intelligence Consulting, an average hour of downtime can cost a business over $100,000.[9] Controlling costs is also important as precious capital can be redeployed to support other business objectives to create a competitive advantage due to new features, products, etc.

New technology like electronic medical records have consistently proven that electronic versions of records help drive down costs and make it simpler for patients to obtain better treatment. In some countries (such as the United States, Denmark, New Zealand), EMR technology is now mandated by policy. The access to EMR data is also changing, with more access coming from mobile wireless-enabled tablets and smart phones.

Other useful technology includes using bar code medication administration (BCMA) and smart infusion pumps (mentioned earlier) that decrease errors at the point of care. The use of middleware to capture alarms from wirelessenabled medical devices, and providing this information to the clinician, improves patient safety.

Asset tracking is another source of productivity improvements. High cost mobile and connected medical devices need to be efficiently tracked. Knowing where infusion pumps and similar mobile devices are located can have a huge impact on the bottom line.

8 https://www.prnewswire.com/news-releases/failures-in-communication-contribute-to-medical-malpractice-300212716.html

9 https://itic-corp.com/blog/2016/08/cost-of-hourly-downtime-soars-81-of-enterprises-say-it-exceeds-300k-on-average/

As mentioned earlier, Wi-Fi networks are becoming a crucial asset for healthcare institutions. In addition to consumerization benefits, there can be internal process improvements and cost savings, like using Vocera badges to improve the timeliness and quality of communications as well as using Wi-Fi enable asset location badges. However, just as was mentioned earlier, you will need to validate that your Wi-Fi solution has enough bandwidth and is capable of handling sensitive and critical voice communications.

Using an NPB to optimize your monitoring strategy can drive tremendous reductions for mean time to repair. First, the NPB can be used to filter and feed only traffic of interest to monitoring, security, and probe tools. The NPB also aggregates data from multiple taps and SPANs which allows you to centralize your tools and increase tool efficiency. Maybe most importantly, an NPB can reduce, if not eliminate, the need for many Change Board approvals. This eliminates a lot of delay because the NPB is already installed into the network—so there is no network disruption and no need for Change Board approval. This is a key component to increasing speed of resolution and reducing MTTR by up to 80%.[10]

According to Zeus Kerravala, Principal Analyst at ZK Research asserts that, "Problem identification is IT's biggest challenge." He explains that 85% of mean time to repair (MTTR) is the time taken to identify there is in fact, an issue. This is where deploying the right types monitoring tools and solutions will help.

An NPB can also be used for load balancing data across multiple tools. This prevents tool overloads and provides a very acceptable level of survivability. Load balancing also has the benefit of reducing costs for unnecessary tool purchases as the load can be spread evenly across multiple tools.

Data retention is one of the main challenges within forensic security projects. This is due to the relatively high cost incurred by the customer to allocate a huge storage capacity for the captured network traffic. NPBs can further be used to filter out unimportant traffic before sending it to the forensic probes like DLPs for processing and storage. This filtering capability can deliver a tremendous reduction in the solution's overall storage cost.

Data masking and Regex searches can also help with Big Data analytics. For instance, EMRs can contain details of diseases and treatment that is not provided in medical codes. Researchers are now aggregating data from multiple EMR databases to get more detailed information to create better treatments. However, patient privacy must be adhered to, which is where data masking can be used to obscure personally identifiable patient details.

10 https://www.keysight.com/resources/childrens-health-care-system-improves-visibility-and-solves-application-performance

SOLUTION OPTIONS

- Validate Wi-Fi networks support new technologies like VoIP and location badges
- Use an NPB to reduce troubleshooting time as well as downtime
- An NPB can be used for monitoring tool load balancing to reduce costs
- Improve data analysis policies to reduce the cost of analyzing suspect data
- Data masking can be used to protects sensitive information

Using Technology to Improve Network Performance

To enable new technology benefits, the IT network has to be working at peak performance. Undetected issues result in internal and external customer complaints. And unfortunately for IT, the MTTR clock starts ticking whether they know there is an issue or not. The hardest part of the process is determining what the issue is. According to Zeus Kerravala, Principal Analyst at ZK Research, “Problem identification is IT’s biggest challenge.” He explains that 85% of mean time to repair (MTTR) is the time taken to identify there is in fact, an issue.[11] This is where deploying the right types monitoring tools and solutions will help.

The first place that IT engineers often start is by implementing APM and NPM tools. While these tools are definitely an important part of the equation, simply deploying these tools will probably not give you adequate results. An Keysight application performance monitoring survey from 2016 proves the point. It shows that 79% of survey respondents report not getting expected results from their APM tools. The IT organizations reported that their monitoring efforts were complex, inefficient, and costly.

This is where implementing a full visibility architecture comes into play. The first consideration is to use taps to capture data at key points within your network. This allows you to feed the performance monitoring solutions with the correct data to minimize analysis delays. The second step is to aggregate data flows using an NPB. This simplifies the flow of data to the tools and removes port contention issues. The NPB can also implement data deduplication to clean up data that is being delivered to APM and NPM tools. This makes the APM and NPM solutions faster by removing extraneous information.

At this point, this is where deploying the right performance monitoring tools help solve performance problems. NPM solutions can be used to document the quality of service (QoS) on the network and isolate where problems exist. APM solutions can be used to identify the quality of experience (QoE) for users and capture data that can be used to observe and diagnose application slowness. The APM solution can also be used to analyze user behaviors.

Proactive performance monitoring solutions are the final piece of the puzzle. Instead of waiting for APM and NPM tools or users to tell you that there is a problem, the proactive solution allows you to generate synthetic traffic and send it across the network whenever you want.

11 https://www.keysight.com/resources/childrens-health-care-system-improves-visibility-and-solves-application-performance

Proactive performance monitoring solutions are the final piece of the puzzle. Instead of waiting for APM and NPM tools or users to tell you that there is a problem, the proactive solution allows you to generate synthetic traffic and send it across the network whenever you want. This allows you to capture mean opinion score (for voice), network delay, jitter, packet loss, and packet loss bursts. The results are displayed in a real-time dashboard. Now you know what is really happening at that point in time and lets you start to troubleshoot network problems (if there are any) faster—whether you are using physical, virtual, or cloud networks.

SOLUTION OPTIONS

- Use taps to capture the right data from the right places
- Use an NPB to optimize the flow of information to APM tools to make them faster
- Implement APM and NPM solutions to identify performance problems
- Actively test your network delay to understand network performance
- Actively test your Wi-Fi network to understand its performance

Summary

Healthcare industry IT departments have significant challenges to face when trying to protect and update their networks. At the same time, there are solutions available to mitigate these challenges. These solutions involve eliminating network blind spots, performing key network assessments, and harnessing technology to replace outdated, manual processes.

Here are some specific recommendations:

- Deploy physical taps, virtual taps and bypass switches to get better access to data
- Deploy network packet brokers at the entrance to the network to optimize the flow of data between security analysis tools
- Deploy network packet brokers elsewhere in your IT network to make the flow of monitoring data to your monitoring and security tools more efficient
- Deploy Application Intelligence capabilities within your network to augment APM and NPM tools
- Perform security assessments against new security architecture changes before rollout to the production network
- Deploy virtual tap agents within your cloud network to capture monitoring data for analysis
- Conduct proactive network performance monitoring to get objective performance data
- Conduct wired and wireless network assessments to validate network designs
- Deploy threat intelligence gateways to block traffic to and from known bad IP addresses

For more information on how to eliminate problems in your healthcare network, refer to these Keysight solutions:

- Keysight taps and bypass switches (e.g. Flex Tap, iBypass 40)
- Keysight network packet brokers (e.g. Vision One)
- BreakingPoint
- CloudLens Private
- Hawkeye
- IxLoad
- IxVeriWave
- ThreatARMOR

Learn more at: www.keysight.com

For more information on Keysight Technologies' products, applications or services, please contact your local Keysight office. The complete list is available at: www.keysight.com/find/contactus

KEYSIGHT TECHNOLOGIES