Five Health Care Trends That Necessitate Network Monitoring

Technology Investments Reduce Cost and Improve Patient Care

The health care industry is coming to terms with the 2018 inflection point that is caused by various factors like: new entrants into the market (e.g. Amazon), confusing legal and funding changes to the Affordable Care Act, persistent and targeted cybersecurity attacks, hospital consolidation, the consumerization of medicine, and many other changes. Fortunately, technology is poised to assist in many of the areas. At the heart of the solution is network visibility. Visibility has tentacles that stretch into almost every facet of the health care network including: security, compliance, performance, troubleshooting, quality of experience, and cost reductions.

In fact, these five key health care trends are creating the following network and data monitoring changes:

- The cybersecurity threat is gaining critical mass
- IT applications and network performance are now center stage
- Health care mergers and acquisitions are increasing network visibility blind spots
- Patient experience and consumerization has begun the ascent to center stage
- Compliance validation remains a fundamental requirement

At the heart of the solution is network visibility. Visibility has tentacles that stretch into almost every facet of the health care network including: security, compliance, performance, troubleshooting, quality of experience, and cost reductions.

Network visibility (monitoring) components and techniques can be used to overcome these challenges. Better visibility eliminates blind spots, decreases troubleshooting and monitoring costs, improves operational efficiency, and enhances compliance data.

What Is Network Visibility?

Before we address how network visibility can help health care IT networks, what is it? Network visibility is simply a focused component of network monitoring. IT teams are under ever-increasing pressure to improve various responsibilities, such as optimizing performance and security of IT networks and applications, monitoring security posture, and monitoring and enforcing compliance mandates. These initiatives require access to comprehensive network data. For security and monitoring solutions to perform optimally, they need full visibility into the network. The ramifications of limited visibility include extended threat analysis times, more false positives, inaccurate conclusions, and longer mean times to repair (MTTR). Simply put, more data results in better monitoring, which reduces your troubleshooting and forensic analysis costs, as well as the cost due to missed security threats.

When it comes to data monitoring, ensuring proper access to network data is the most critical thing you can do. After that, data filtering and the conversion of data into actionable information can take place. This is where a visibility architecture is important.

A visibility architecture is a design that provides access to network traffic, intelligently filters the requisite data, sends the groomed data to analysis tools, and then delivers information from the monitoring tools so that IT can make informed decisions about problem resolution and network performance. With the proper visibility architecture in place, you'll be able to see what is (and what is not) happening on your network.

A visibility architecture is a design that provides access to network traffic, intelligently filters the requisite data, sends the groomed data to analysis tools, and then delivers information from the monitoring tools so that IT can make informed decisions about problem resolution and network performance.

To accomplish these goals, two fundamental components are required:

- Installation of test access ports (taps) to access network data
- Installation of a network packet broker (NPB) to filter and distribute that data to purpose-built devices for analysis

Proper visibility starts with proper data access. The first and easiest task is to install taps. Taps are passive devices that are typically "set and forget" devices. Once deployed, you never have to touch them again. After a one-time disturbance to the network to install the taps, you benefit from always-on visibility, resulting in fewer change board approval meetings to gather troubleshooting, monitoring, and security data. This one step gets you better data to reduce your troubleshooting and forensic analysis costs.

Taps are an alternative to the use of switched port analyzer (SPAN) ports. Taps are superior to SPAN ports, primarily because SPAN ports do not provide a complete copy of all network data, and because taps are more versatile and can be deployed anywhere in the network without performance concerns. SPAN port configuration costs, including change board approvals, far outweigh the simplicity and cost of taps.

In addition to taps, you will want to add an NPB to optimize your filtering methodology. An NPB can provide several features that off-load compute intensive processing from security and monitoring tools. Powerful NPB features include: packet filtering, load balancing, packet deduplication, packet trimming, and multiprotocol label switching (MPLS) stripping.

By filtering data within the NPB, the monitoring tool is freed to perform the work that it was originally purchased to do, resulting in more useful work being done by the monitoring tool. Since the tools are now as efficient as possible, less devices may be required to accomplish the same goals. In addition, the right choice of an NPB optimizes filter programming costs by removing the manual command line interface (CLI) process used in SPAN ports and some NPB models.

By filtering data within the NPB, the monitoring tool is freed to perform the work that it is optimized to do. This results in more useful work being done by the monitoring tool. When all tools are operating as efficiently as possible, you may need fewer tools to accomplish the same goals.

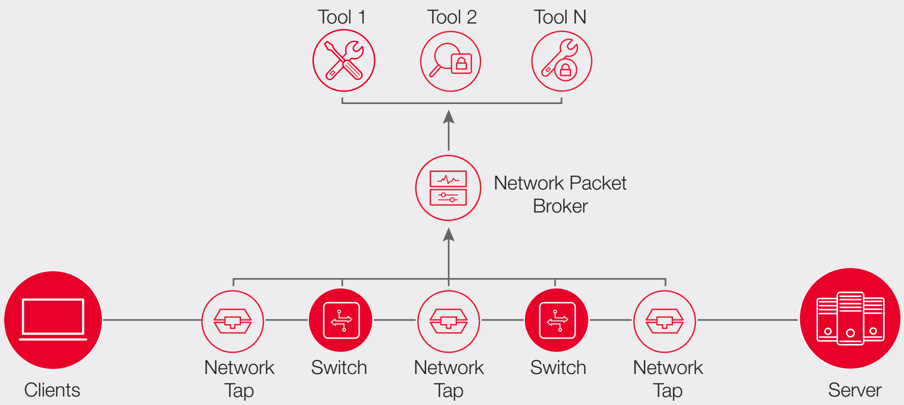

Figure 1. A network packet broker aggregates data from tap and SPAN ports.

Application intelligence is an enhanced feature of network packet brokers which allows them to deliver true signature-based application identification and packet filtering along with the correlation of metadata information like geolocation, user device type, and user browser type. This gives you much more explicit control over exactly what you want to monitor.

If your tools can not consume packet-level data, the packet broker can generate NetFlow metadata and additional detailed contextual information metadata that gives your security and monitoring tools a very optimized set of data to analyze.

This means is that your monitoring tools can now be much more intelligent, not just more efficient, and you have access to data and intelligence in a way not possible with other visibility solutions.

The following sections provide examples of how a network visibility architecture can be integrated into the IT network for several different types of financial industry organizations.

The cybersecurity threat is gaining critical mass for health care

Ransomware and distributed denial of service (DDOS) attacks are on the rise for health care organizations. In fact, health care is the second most targeted industry, after Finance, in annual cyberattacks.[1] In addition, the health care industry has more insider-related security incidences from internal sources than from external sources (i.e. from hackers). Therefore, it is essential that health care organizations secure their networks and devices. This includes medical devices (which the US government reports has recently seen a 525 percent increase in cybersecurity vulnerabilities)[2] as well as electronic health records (EHR), which are the primary repositories of patient personal health information (PHI) and personally identifiable information (PII).

From a network visibility and security perspective, there are some easy actions that can be implemented to alleviate several of these issues. The following diagram illustrates how these technology components can be inserted into a generic hospital network.

> Health care is the second most targeted industry, after Finance, in annual cyberattacks. In addition, the health care industry has more insider-related security incidences from internal sources than from external sources (i.e. from hackers).
>
> **2018 Verizon Data Breach Investigations Report**

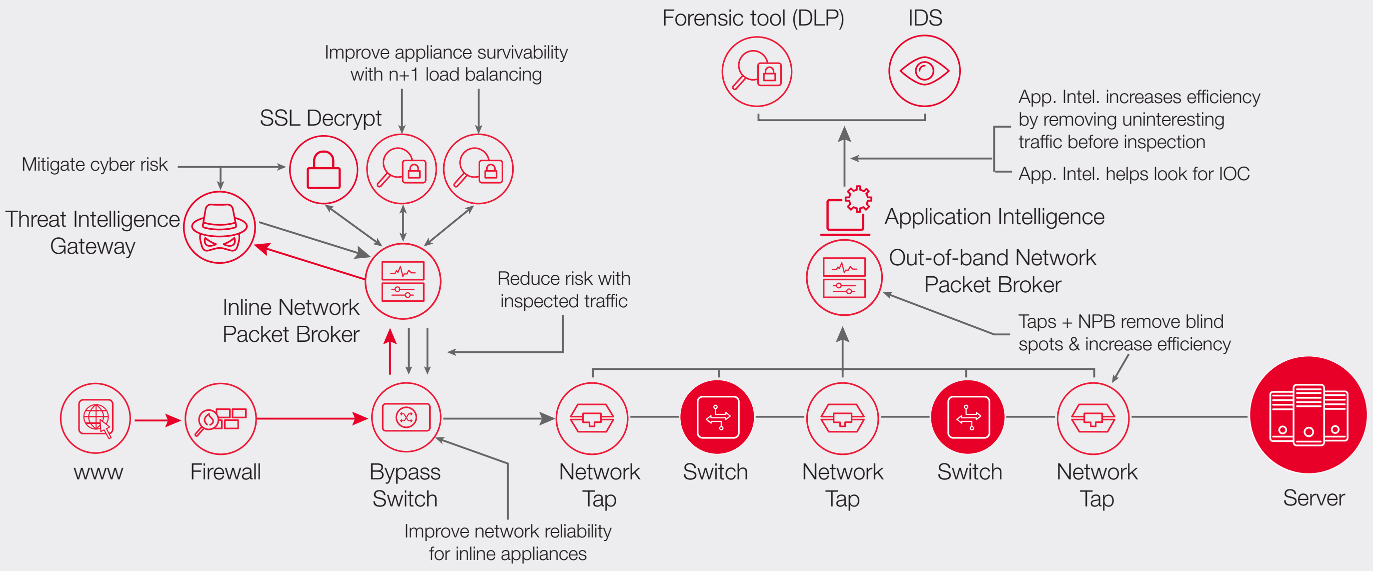
Forensic tool (DLP)
IDS
Improve appliance survivability with n+1 load balancing
SSL Decrypt
App. Intel. increases efficiency by removing uninteresting traffic before inspection
App. Intel. helps look for IOC
Mitigate cyber risk
Threat Intelligence Gateway
Application Intelligence
Out-of-band Network Packet Broker
Reduce risk with inspected traffic
Inline Network Packet Broker
Taps + NPB remove blind spots & increase efficiency
www
Firewall
Bypass Switch
Network Tap
Switch
Network Tap
Switch
Network Tap
Server
Improve network reliability for inline appliances

Figure 2. Example of network visibility and security solutions for hospitals.

[1] 2018 Verizon Data Breach Investigations Report, Verizon Inc. April 2018.

[2] Top Health Industry Issues of 2018: A Year of resilience amid uncertainty. PwC Health Research Institute. 2017.

As Figure 2 illustrates, there are specific security-related activities which you can integrate into your existing visibility and security architectures that will yield the following benefits:

- **Remove on-premises blind spots** – Install physical taps and packet brokers to get better access to security data. This is especially important to thwart malware and ransomware attacks as visibility into packet data increases network security.
- **Mitigate cyber risk** – Threat intelligence gateways, inline security tools, and integrated secure socket layer (SSL)/transport layer security (TLS) decryption solutions should be added. Threat intelligence gateways pre-filter unwanted traffic to reduce the workload for monitoring tools by up to 30%, helping reduce security event false positives. In addition, inline security tools provide the ability to stop threats in real-time while SSL decryption allows IT to expose malware hidden by SSL encryption.
- **Strengthen threat investigations** – NPBs can filter data for security tools, like an intrusion detection system (IDS) or data loss prevention (DLP) appliance, which lowers cost and improves efficiency. Application intelligence can also be used to filter data based upon application to better isolate data and enhance tool performance and make the security devices up to 35% more efficient.
- **Improve network reliability** – Inline external bypass switches should be added in front of inline security appliances to eliminate single points of failure within the network.

Digital health care in particular is "creating challenges for governments, health systems, and insurers, which must collect, analyze, and store more and more data."

Deloitte 2018 Global Health Care Outlook report

IT applications and network performance move to center stage

IT organizations are constantly trying to optimize operations and troubleshooting activities and for good reason. Once established, end users' perception of "slowness" can be hard to get rid of. According to research that Enterprise Management Associates (EMA) performed in late 2016, 41% of organizations surveyed spend more than 50% of their time responding to network and application performance problems.[3] Digital health care in particular is "creating challenges for governments, health systems, and insurers, which must collect, analyze, and store more and more data."[4]

This is obviously a large source of time and energy. It can also be an unwanted high-profile activity. Let's look at one example for the medical industry. Networked applications, such as electronic health records (EHR), are vital for hospitals to provide outstanding service to their patients and physicians. These applications enable 24x7 application transaction monitoring, packet storage, and network analysis, while providing integrated software add-ons for dependency mapping, SNMP reporting, database monitoring, and pre-deployment application testing.

[3] EMA survey performed for Keysight, A Keysight company. October 2016.

[4] 2018 Global health care outlook = The evolution of smart health care, Deloitte. January 2018.

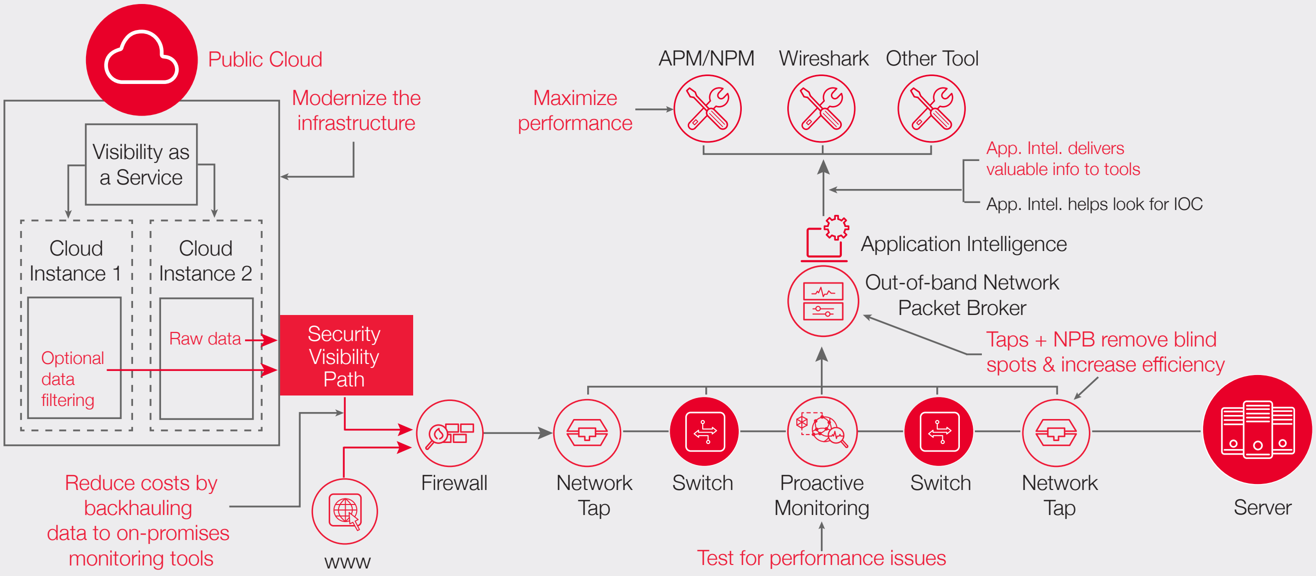
Public Cloud
Modernize the infrastructure
Visibility as a Service
Cloud Instance 1
Cloud Instance 2
Optional data filtering
Raw data
Security Visibility Path
Reduce costs by backhauling data to on-promises monitoring tools
WWW
Firewall
Maximize performance
APM/NPM
Wireshark
Other Tool
App. Intel. delivers valuable info to tools
App. Intel. helps look for IOC
Application Intelligence
Out-of-band Network Packet Broker
Taps + NPB remove blind spots & increase efficiency
Network Tap
Switch
Proactive Monitoring
Switch
Network Tap
Server
Test for performance issues

Figure 3. Example of health care performance monitoring.

As Figure 3 illustrates, there are specific performance-related benefits derived from integrating visibility with your network and security architectures which includes the ability to:

- **Increase monitoring efficiency** – NPBs can be deployed to remove duplicate traffic and filter the remaining traffic so that monitoring tools only receive relevant traffic. Deployment of packet brokers can improve monitoring device efficiency 30%. This reduces both analysis cost and CAPEX, and reduces the amount of monitoring tools needed.
- **Maximize OOB network performance –** Out-of-band (OOB) performance tools can be added to better understand network performance issues. This is easily accomplished by deploying an NPB which then connects to a network performance monitoring appliance. Application intelligence can also be used to filter data based upon application to better isolate data and enhance tool performance.
- **Maximize network performance** – Add proactive monitoring capabilities to your network to actively test on-demand for performance issues in on-premises and cloud networks.
- **Improve troubleshooting responsiveness** – Once taps and a packet broker are installed, IT has immediate access to monitoring and troubleshooting. This all but eliminates Change Board approvals to and can reduce MTTR by up to 80%.
- **Modernize the infrastructure** – Cloud instances are great for spinning up business critical applications, but there is often limited visibility into cloud data and functionality. IT managers should add a cloud visibility solution to overcome this issue.
- **High Availability and n+1 survivability** – The features can be added to improve monitoring tool availability and to provide cost reduction techniques while maximing monitoring performance.

Cloud instances are great for spinning up business critical applications, but there is often limited visibility into cloud data and functionality. IT managers should add a cloud visibility solution to overcome this issue.

Health care mergers and acquisitions are increasing network visibility blind spots

Over the past several years there have been a lot of mergers and acquisitions (M&As) of health care companies. The second quarter alone of 2018 saw 255 deals announced, making it the 15th consecutive quarter of 200 or more M&A announcements in the health care industry.[5] These M&As are driving hospital consolidation to reduce costs and improve efficiencies. Unfortunatley, they are also increasing network management and troubleshooting blind spots. As the companies merge, the IT systems are two separate, and disparate, islands. To achieve the promised efficiencies, IT needs to share troubleshooting and performance information between the two networks. As long as the two systems continue to be islands, there will be blindspots and decreased efficiency.

From a network visibility and security perspective, there are some easy actions that can be implemented to address these issues. The following diagram illustrates how these technology components can be inserted into a generic hospital network.

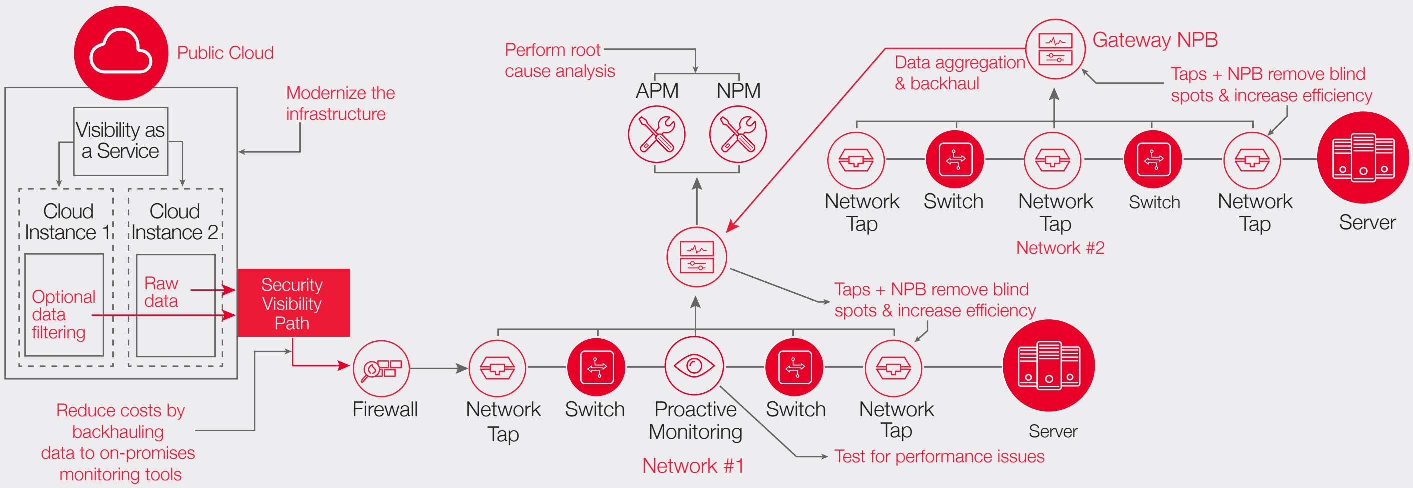

Figure 4. Example of network visibility and security solutions for M&As.

As Figure 4 illustrates, M&As pose specific challenges for health care networks. Here are some of the specific benefits from integrating visibility into your network architecture:

- **Remove on-premises blind spots** – First, once the primary network is determined (probably the acquiring company), taps can be added to the secondary network at key points to gain specific information to collect performance information. Then a packet broker can be added at the gateway between the two networks. Relevant taps can be connected to the NPB which then aggregates the data and passes it through one port back to the network operations center (NOC), where data can then be sent to dedicated or communal monitoring tools.

[5] PwC Deals - US Health Services Deals Insights Q2 2018.

- **Test for performance issues** – As the integration of the two systems progresses, proactive monitoring can be used to understand how well (or not) data flows between the two networks and how network performance changes as the two networks are integrated and software updates are introduced.
- **Perform root cause analysis** – Once the taps and NPB is in place, monitoring data can be captured and passed on to purpose-built tools like application performance monitoring (APM) and network performance monitoring (NPM) for analysis as to why applications (like EHR) and/or the network is running slow.
- **Reduce costs** – Another consideration is to implement a hybrid cloud/on-premises approach where you backhaul monitoring data from the cloud to on-premises NPBs to get a consolidated view and lower costs by reusing existing physical security and monitoring tools. A cloud visibility solution is central to capturing the cloud data and exporting it back to on-premises monitoring tools. This can save thousands of dollars on security and monitoring applicance costs.

Once the primary network is determined (probably the acquiring company), taps can be added to the secondary network at key points to gain specific information to collect performance information. Then a packet broker can be added at the gateway between the two networks.

Patient Experience and Consumerization of Medicine Has Begun the Ascent to Center Stage

While patient experience is not a core activity yet, it is definitely increasing in importance. According to a PwC study, “Forty-nine percent of provider executives said revamping the patient experience is one of their organization’s top three priorities over the next five years. Many already have or are building the role of chief patient experience officer.”[6] One intent is for health care organizations to differentiate themselves by investing heavily in this function. Speed of access to data within EHR is critical to this perception along with new services. For instance, nearly three quarters of Americans think it’s important that their provider uses modern tools like web portals, live chat/ instant message or two-way video.[7] Eighty percent of insurers also intend to invest money to improve the member experience.[5]

The following diagram illustrates how network visibility technology components can be inserted into a generic health care network to address the unique challenges of patient experience monitoring.

> “Forty-nine percent of provider executives said revamping the patient experience is one of their organization’s top three priorities over the next five years. Many already have or are building the role of chief patient experience officer.”
>
> **PwC Health Research Institute**

[6] Top Health Industry Issues of 2018: A Year of resilience amid uncertainty. PwC Health Research Institute 2017.

[7] 2017 Connected Patient Report, Salesforce Research. June 2017.

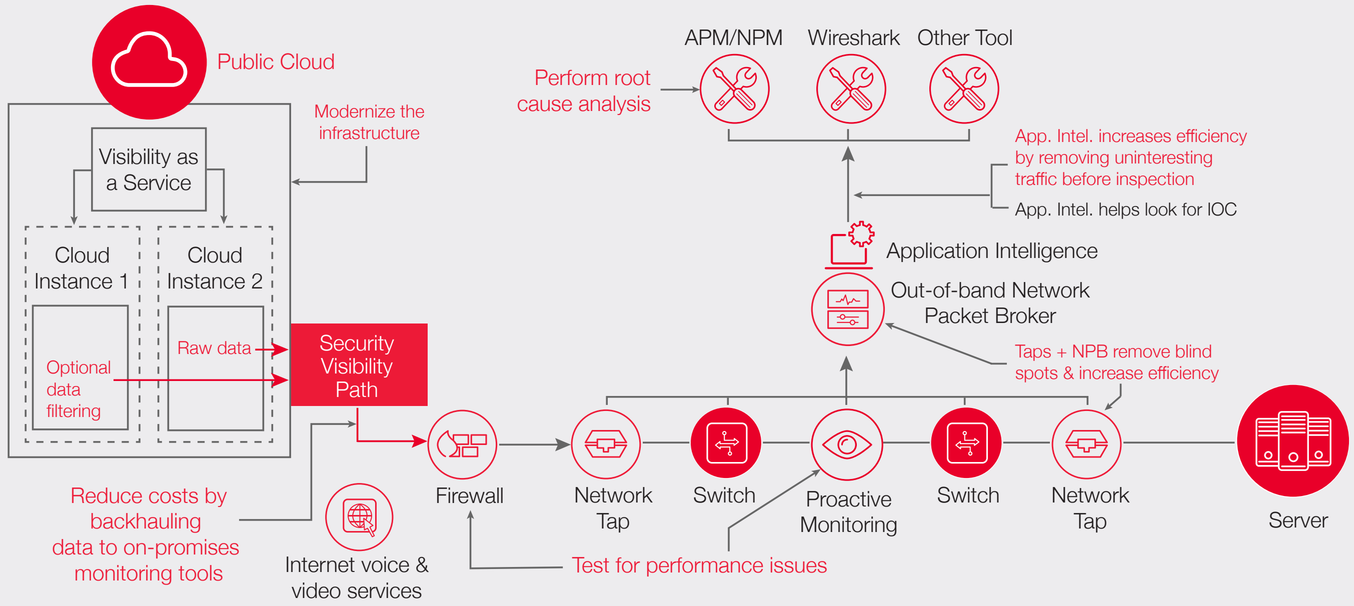
Public Cloud
Visibility as a Service
Cloud Instance 1
Cloud Instance 2
Optional data filtering
Raw data
Modernize the infrastructure
Security Visibility Path
Reduce costs by backhauling data to on-promises monitoring tools
Internet voice & video services
Firewall
Network Tap
Switch
Proactive Monitoring
Switch
Network Tap
Server
Test for performance issues
Perform root cause analysis
APM/NPM
Wireshark
Other Tool
App. Intel. increases efficiency by removing uninteresting traffic before inspection
App. Intel. helps look for IOC
Application Intelligence
Out-of-band Network Packet Broker
Taps + NPB remove blind spots & increase efficiency

Figure 5. Example of network visibility solution for patient experience monitoring.

As Figure 5 illustrates, these are some of the specific benefits from integrating visibility with your network and security architectures:

- **Test for performance issues** – As real-time voice and video services are deployed as part of remote telehealth deployments, IT teams will need the appropriate proative monitoring tools to troubleshoot and maintain an acceptable quality of experience (QOE) for data flows between the core server and remote users. This involves prompt verification and remediation activities to provide reliable high speed data access.
- **Maximize network and application performance with integrated application intelligence** – Application performance issues on the network can often be easily identified by deploying an NPB equipped with application intelligence. Application intelligence allows IT personnel to observe all of the applications running on the network, geolocation of users, and the amount of bandwidth being consumed per application and gepgraphy. This is essential to determining what apps are running on the network, who is abusing network bandwidth (e.g. is there a lot of bandwidth consumption for Netflix watching), and potential throttling of usage for network hogs.
- **Validate cloud deployments** – As health care entities modernize the infrastructure and deliver other innovative solutions, cloud technology will be increasingly relied upon. However, while cloud instances are great for spinning up business critical applications, there is often limited visibility into cloud data and functionality. IT managers can add a cloud visibility solution to capture key pieces of packet data required for troubleshooting, performance, and compliance activities.
- **Perform root cause analysis** – Once the taps and NPB is in place, monitoring data can be captured and passed on to purpose-built tools like APM and NPM for analysis as to why applications (like EHR) and/or the network is running slow.

Compliance validation remains a fundamental requirement

According to the SAI 2018 Health care Compliance Benchmark Report, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) is currently the most important compliance concern for health care organizations. In fact, it holds the top two positions—HIPAA security which is the primary concern and HIPAA privacy which is the second most common concern. Another concern that has emerged is compliance to the European General Data Protection Regulations (GDPR) law, which imposes stiff fines for the loss of consumer and patient PII.

According to KPMG research, "Compliance monitoring and testing is a key compliance activity that can be automated, helping organizations achieve greater risk coverage and consistency."[8] One way to mitigate risk is to invest in technology. This includes investment around automation capabilities and the collection of good monitoring and compliance data. Investment in these two areas will help you significantly if there is an audit from the Office of Inspector General (OIG) or Department of Justice (DOJ).

> According to KPMG research, "Compliance monitoring and testing is a key compliance activity that can be automated, helping organizations achieve greater risk coverage and consistency." One way to mitigate risk is to invest in technology.

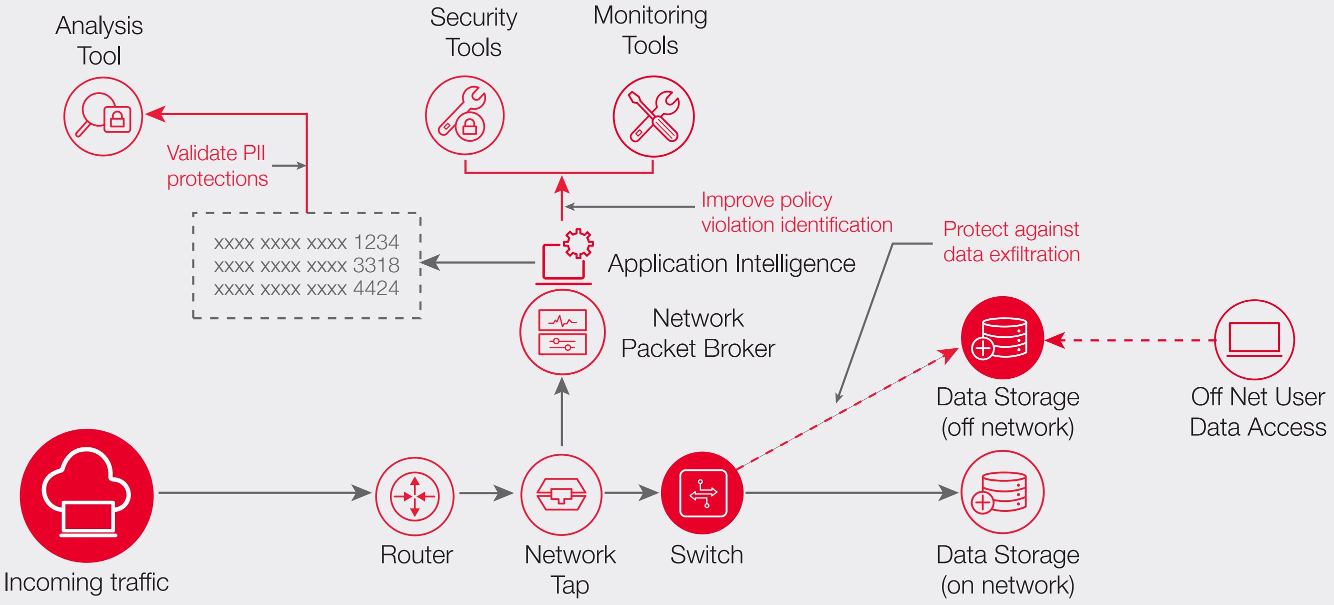

Figure 6. Example of network visibility solution for compliance monitoring.

[8] Keeping up with shifting compliance goalposts in 2018, KPMG. November 2017.

As Figure 6 illustrates, there are specific performance-related benefits derived from integrating visibility with your network and security architectures. Here are some specific suggestions:

- **Protect against sensitive data exfiltration** – Application data can provide many benefits in this area including monitoring application usage, data masking, data searching, and even data validation. For instance, application monitoring lets you know that employees may be using services like Drop Box to transfer company files and bypass your security policies. Once an employee is no longer employed by the company, they could still have access to those files, since IT cannot restrict the privileges to off-network storage devices.
- **Improve IT policy violation identification** – Application intelligence can help here as well. One example is where employees may be using other, non-company standard, email services (like web-based mail services) to access and download files. This use case usually involves accessing media that does not go through anti-virus/malware inspection and can therefore pose a security threat to the corporate network, especially regarding file downloads.
- **Validate PII data protections** – Sensitive data needs to be masked and/or encrypted to reduce breach risk and cost. Application intelligence within a packet broker and regular expression Regex can be used to search for PII, like 16 digits credit card numbers or 9 digit social security numbers. It is quite common to find home grown applications from the past, or even current apps, that have this data stored in clear text, which violates PCI and HIPAA rules.
- **Enhance virtual data compliance activities** – For virtual data centers (VDC), a virtual tap can be added to get access to east-west data and then export key virtual data to your physical tools for a consolidated view of your network. For public cloud instances, a cloud visibility solution can be inserted to capture compliance key data within the cloud or backhaul it to a physical data center for a analysis and a consolidated view.

Application monitoring lets you know that employees may be using services like Dropbox to transfer company files and bypass your security policies. Once an employee is no longer employed by the company, they could still have access to those files, since IT cannot restrict the privileges to off-network storage devices.

Conclusion

The health care industry is experiencing a wave of digital disruption based upon increased security threats and new technology. To stay competitive, these companies will have to innovate. They can address the changing landscape by deploying new and adjusting existing technologies. One such area ripe for improvement is network visibility and monitoring technology.

Organizations can maximize the usable data they gather through the following:

- Deploy taps and NPBs to collect the proper monitoring data and to refine that data so that it can be processed into information as fast as possible
- Deploy threat intelligence gateways to immediately eliminate traffic from known bad sites
- Deploy inline bypass switches to increase network reliability
- Deploy inline NPBs, decryption and security tools to respond to cyber threats and minimize both risk and cost
- Use application intelligence to filter data for security and monitoring tools more efficiently
- Use application intelligence to proactively look for indicators of compromise
- Deploy NPBs to reduce costs by using load balancing, deduplication
- Capture cloud data and backhaul it to on-premises equipment and tools to reduce cost and improve compliance

Keysight network visibility solutions are a powerful way to optimize your network monitoring architecture and strengthen your network security. For more information on network monitoring solutions, visit https://www.keysight.com/us/en/cmp/2020/network-visibility-network-test.html.

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