



Ensuring Healthcare Networks for the Perfect Storm





With COVID-19 affecting healthcare worldwide, hospitals depend on reliable network connectivity. The increased use of telemedicine by patients unable to visit their doctor only adds to the congestion. In short, this is no time for traffic bottlenecks or outages.

ITOps and HTM professionals in the healthcare industry share responsibility for monitoring network performance, so they can quickly react to any issues or problems. It's a task becoming more difficult as an influx of new devices helps to manage increasing caseloads. Network visibility becomes critical in this environment.

This eBook analyzes the current “perfect storm” affecting the healthcare industry. We analyze a few scenarios hampering the operational efficiency of hospitals in the wake of COVID-19. An innovative new network monitoring product created by the partnership between Nyansa, now part of VMware and GE Healthcare ultimately provides the means to quiet this storm.



Urgency for Patient Care is Increasing Risks

In healthcare, clinical networks aren't optional. Instead, they are the DNA of clinical workflow, a critical part of providing effective treatments for patients. The current environment adds a sense of urgency for patient care, but numerous networking risks abound, including:

- A large influx of medical devices
- An increase in network usage causing traffic bottlenecks
- Obsolete networking technology
- Cybersecurity issues
- Compliance and liability considerations

Hospitals triaging and treating COVID-19 patients may require additional patient monitors, ventilators, infusion pumps—essentially an array of wired and wireless devices. At the same time, doctors increasingly leverage telemedicine to treat other patients remotely. The challenges in achieving these disparate goals are real. Merely throwing more networking equipment at the problem isn't enough. Everything must be connected and working in sync.

Because of this new urgency, healthcare organizations may find it more difficult to follow their existing policies and procedures devised to mitigate risks. Ultimately those responsible for managing networks in healthcare need to be prepared for the unpredictable, with the shared goal of delivering high quality patient care.



Typical Network Challenges in Healthcare

Hospitals and medical offices face multiple challenges with their network infrastructure, such as:

- Adequate access control for network closets
- Damage to wiring due to construction or pests
- Poor communication between internal teams
- Power and infrastructure outages amplifying a lack of network redundancy

Understanding these issues helps in their management. However, it's critical for IT and HTM personnel to put the right processes and procedures in place to ensure those challenges don't adversely impact hospital operations. More importantly, what happens if and when we miss something? To help answer this question, let's analyze a scenario on redundancy in healthcare networking.

Frost & Sullivan, "Best Practices for Managing Patient Monitoring Networks across the IT & Biomedical Depts."





Common Challenges with Medical Devices

Hospital personnel and IT departments face multiple challenges when networking medical devices. The more common problems include:

- Lack of visibility regarding device communications
- Wired or wireless connectivity issues
- Locating devices for upgrades and maintenance
- Problems with gateways, proxies, and firewalls
- Poor communication and alignment between IT and HTM teams

The differences between IT and operational technology (OT) lie at the heart of these medical device challenges. Whereas IT is the standard computer technology used to connect and share information among computing devices and networks, OT describes computerized systems where sharing information isn't their primary purpose.

As medical devices are typically OT, the challenges highlighted above generally come into play. Maybe a device's communication isn't traceable using an IT monitoring tool? Perhaps it connects to the network using a non-standard protocol? Maintenance, updates or, even locating certain devices can be difficult.

Finally, who "owns" the device? At times, either the hospital IT team or the clinical engineering team claim ownership. Communication between those teams may be a problem in this situation.

Hospitals are increasingly focused on three specific goals for their clinical networks: increased redundancy, better visibility, and vulnerability identification.





Increased Redundancy

Proactive healthcare organizations are planning for network infrastructure failures by adding in redundancy. Rather than allow single points of failure, there is a primary system, for instance a switch or a router, with a redundant backup. In the case that there is an issue with traffic flow through the primary component, the backup will kick-in seamlessly—preventing poor client experience.

Redundancy is a very important concept for preventing large scale network issues, but just like a tree falling in the woods, if the primary system fails, is anyone made aware that it is down? If traffic continues to flow normally and users are not reporting issues, this outage may be overlooked, leaving the network at greater risk of a complete crash.





Better Visibility

As hospitals have been ramping up to treat larger numbers of patients, they have been forced to drastically increase their capacity, adding numerous devices to their clinical networks. These systems may be sourced from various places—old legacy devices, newly purchased refurbished equipment, new capital equipment. Network infrastructure may have to be adapted to accommodate the sudden influx of new connections and additional traffic.

In this landscape, with the rapid deployment of new and additional systems, users may experience some technical issues. Problems with compatibility, limited bandwidth, and interference are bound to occur. It can be very time consuming and complicated to pinpoint the root cause of these troubles as they are often intermittent. If the issue arises in a certain device group or at a certain time, it is often difficult to fully grasp the occurrences, as busy clinicians are focused on their patients, not logging tickets related to the performance of their networks or devices.

This scenario reveals the importance of consistent network visibility for any healthcare organization. Expansion projects may introduce new variables into the existing environment due to lack of insights into the network performance before and after a project. Having an accurate baseline of your existing network's performance and an understanding of the typical device behavior is key.





Vulnerability Identification

Proactive vulnerability assessments are an important component to cybersecurity planning in the healthcare environment. There are some existing and publicly available tools to assist IT and HTM departments to perform this function: MDS2 documents, service manuals, manufacturer portals and notifications.

So, imagine that your hospital has taken all the right proactive steps to understand and mitigate the risks and vulnerabilities on your network. However, one morning you arrive into work to find out there is a sudden influx of complaints for poor performance. Every resource on the network is running slowly and some resources are not accessible at all.

Could this be a failure of some common network resources? Is your network experiencing bandwidth or wireless interference issues? Could there be something more sinister, perhaps a denial of service attack happening?

Triaging a problem like this is difficult without visibility into the hospital's network infrastructure and the typical behavior of the devices and systems on it. Understanding "the normal" when it comes to network and device traffic is key.



The Perfect Storm

The infamous “Perfect Storm” of book and movie fame formed when a standard nor’easter merged with Hurricane Grace. Forecasters at The National Weather Service didn’t think this combination was possible. As such, their predictions were faulty. They weren’t sufficiently prepared for the oncoming storm, and lives were lost.

In the wake of COVID-19, the healthcare world faces a similar perfect storm. This environment has created a set of extreme conditions where multiple failures, if experienced simultaneously, could lead to catastrophe.

This situation requires hospitals and medical offices to always be aware of the operational state of their network infrastructure. Alerts of any problems must be immediately reported to the responsible IT and HTM personnel. Ultimately, healthcare organizations need the right solution for monitoring both their clinical and enterprise networks.





Introducing OnWatch NP Powered by Nyansa

When considering a large enterprise integration with multiple networks and geographically dispersed sites, pinpointing and solving network problems becomes more complex. Ultimately, there needs to be a single source of truth, taking into account networks and devices hosted in many different locations.

GE Healthcare and Nyansa partnered on an innovative network performance monitoring solution for hospitals and other healthcare organizations. OnWatch NP is tailored specifically for monitoring clinical device networks and enterprise networks, all with one platform.





Artificial Intelligence in Healthcare

So how can OnWatch NP help healthcare organizations solve their network visibility issue? Two words reveal the way: artificial intelligence. Growth in the AI healthcare market is predicted to reach \$6.6 billion by 2021—a compound annual growth rate (CAGR) of 40 percent.² That massive number shows how AI and machine learning are no longer the future of healthcare; they are the present.

AI and machine learning are already making a huge impact automating various healthcare IT processes. Even more importantly, they help improve the end to end clinical experience. Nyansa works alongside a number of innovative healthcare providers; helping them manage the perfect storm discussed earlier. The ultimate goal is actually using the data available in their network to improve patient care, instead of drowning in a sea of data.

This real-world application of AI also brings a practical return on investment (ROI). As such, AI and machine learning are projected to create around \$150 billion in annual savings in the US healthcare economy by 2026.³ Many organizations in the healthcare ecosystem are already on their way to realizing this. There's no doubt AI is going to have a profound effect on all the components of the healthcare value chain. Examples include digital therapeutics using predictive analytics, clinical AI-based applications, and many more.

2. <https://www.healthcareitnews.com/news/investment-ai-growing-health-systems-look-future>

3. <https://www.accenture.com/us-en/insights/artificial-intelligence-index>



AIOps Transforms IT Operations

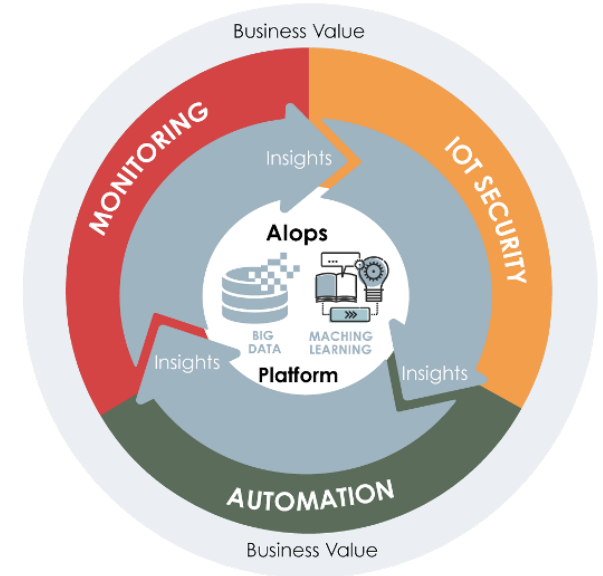
Let's look more closely at how AI is transforming IT operations, creating a new term known as artificial intelligence operations (AIOps). An AIOps platform utilizes Big Data, machine learning, and other advanced analytics to parse all enterprise network data for enhancing IT operations with proactive dynamic and contextual insights.

It's a technology innovation especially relevant to healthcare, largely because the impact of any downtime could be catastrophic, ultimately affecting patient care. How does AIOps help in this scenario? Look at device inventory. Disparate ownership of a large influx of connected clinical devices can lead to the creation of silos. Biomedical teams, imaging teams, facilities teams, and finally the networking team all own portions of a diverse technical infrastructure, including a mix of OT and IT devices.

Because of this dispersed ownership, no single source of truth exists on what devices are on the network, let alone information on their current performance. The first step in this identification process uses existing enterprise network data to discover and classify these devices automatically. An AIOps platform analyzes every single device interaction on the network, performing deep packet inspection and protocol dissection. This data feeds a hierarchical identification engine automatically fingerprinting these devices.

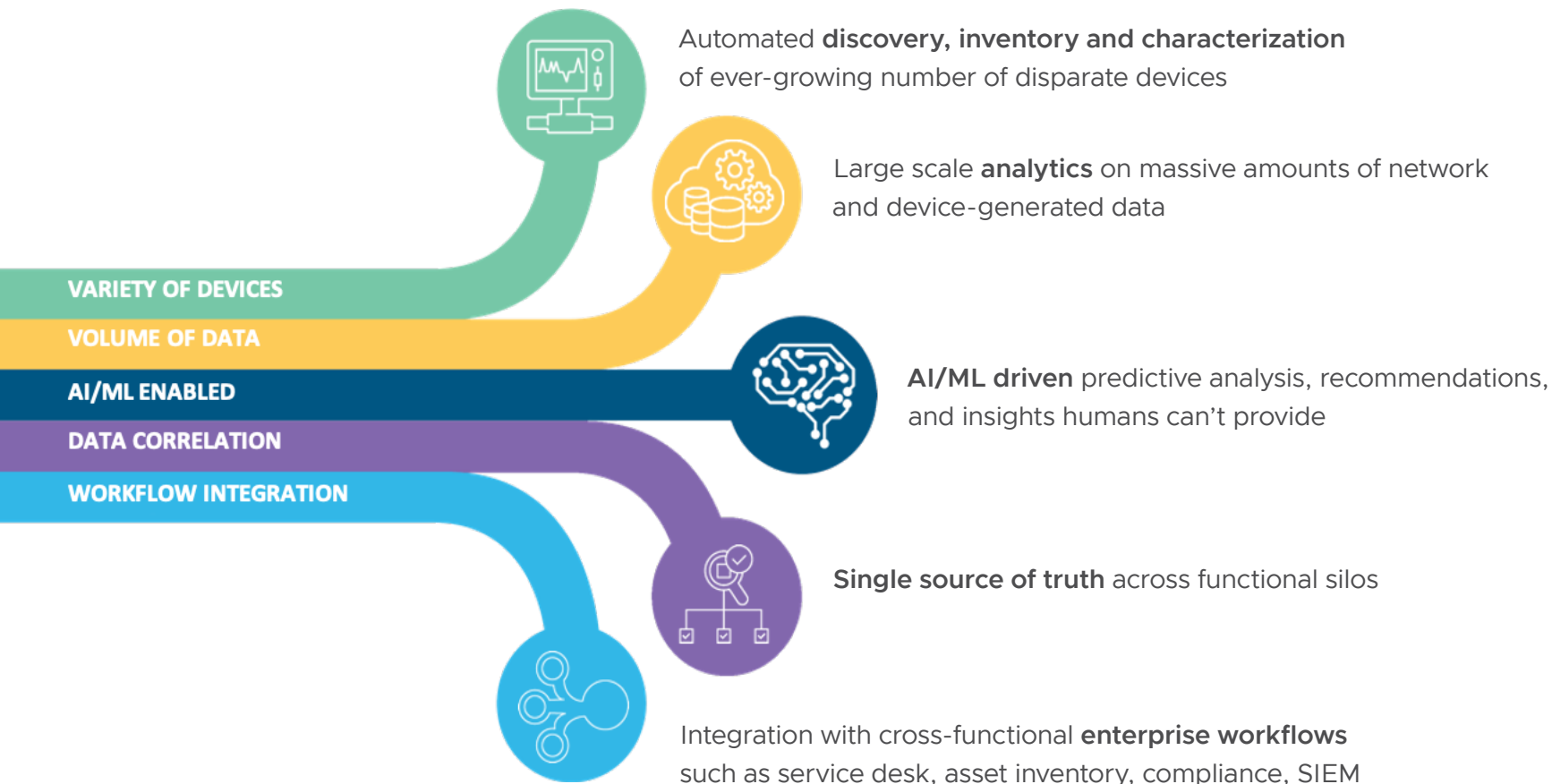
After identifying the device inventory, the platform communicates with existing inventory management systems like a computerized maintenance management system (CMMS) or a configuration management database (CMDB). The goal is to remove any blind spots while providing real-time visibility into the status of the device. This approach replaces the manual inventory tracking process, improving efficiency with enhanced network monitoring.

The AIOps platform leverages this single source of data to create performance and behavior baselines for each device. It then alerts network personnel to any degradation in performance, or any strange behavior indicating a potential security risk.





AIOps Enables Success





The Importance of Baselining in Hospital Networking Analysis

Baselining is an important part of a healthcare network analysis. Every hospital network is different and understanding what is normal for any individual network is critical. Baselines help identify performance issues as well as potential security risks.

A few examples illustrate this concept. Consider an infusion pump figuring out how to connect to a wireless network, a glucometer unable to authenticate using RADIUS, or even temperature sensors that are, for some unknown reason, communicating with Domain Name System (DNS) servers in Asia and Europe. The latter case is likely to increase the security risk on the network and warrant immediate investigation.

Leveraging all of this data allows ITOps and SecOps teams to be proactive in remediating these issues as quickly as possible. As a result, issues get fixed before becoming systemic; causing an impact on the end-user experience, which in the case of a hospital, would be clinicians and patients.

An AIOps platform goes beyond just flagging these deviations. More importantly, it uses massive amounts of data to correlate insights from a variety of disparate sources. Ultimately, it provides a detailed root cause analysis and remediations to tech professionals, enabling them to address and fix any issue quickly.





AI Fosters the Future of Seamless Integration and Self-Healing Networks

The future of AI and computer networking is one where these platforms become intelligent enough to allow networks to actually heal themselves. Architecting and building AIOps platforms so they seamlessly work with existing enterprise systems helps to achieve this goal.

In a similar fashion, these platforms also need to include an open application programming interface (API), allowing them to easily integrate with platforms such as ticketing systems, like ServiceNow, asset inventory, data lakes, and more. This seamless integration lets healthcare organizations continue using any established workflows without a new platform disrupting those critical operations.





Maximizing IoT Value in Healthcare

AIOps and mobility help improve the patient experience while saving money. Here are a few key benefits of using this platform.

Patient Experience



- Workstations on wheels, mobile imaging units, biotelemetry devices, and more
- Real-time
- Mobile
- Individualized
- Remote care

Lower Cost of Care



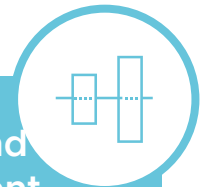
- Measure ROI on technology investment
- Improve asset utilization
- Administrative accuracy (ADT)

Operational Efficiency



- Status at-a-glance
- Prevent incidents
- Faster incident resolution
- Efficient preventative maintenance
- AI/ML-powered

Biomed and IT Alignment



- Single source of truth
- Asset inventory and status
- Device onboarding
- Technical resource allocation



Automating Manual Processes in Medical Device Management

Switching from a largely manual process to using an intelligent, automated system provides significant benefits to medical device management. An automated approach monitors devices remotely, helps troubleshoot problems in real-time, and streamlines preventative maintenance. Now valuable personnel in healthcare organizations are using their time more efficiently for more important tasks.

Once again, consider the importance of a single source of truth in healthcare technology, for both networking and medical devices. Having a central platform as a single source of truth, both from the HTM as well as an IT administrator's perspective, improves technical process efficiency. It also helps better align these different departments, improving the collaboration between the separate teams.

In the end, an AIOps platform delivers a shared set of reliable and actionable data on network and device health as well as performance and troubleshooting information. This helps IT and HTM teams' function both independently and collectively. Any healthcare organization is now able to focus on providing exemplary patient care in a more cost-effective manner.



OnWatch Network Performance

OnWatch NP provides AI-powered performance analytics for clinical networks and devices and includes the following features.





How OnWatch NP Makes the Promise of AIOps a Reality for Hospitals

AIOps helps technical organizations overcome challenges to their network infrastructure from mobile and diverse IoT devices. Powered by the partnership between Nyansa and GE Healthcare, OnWatch NP is an AIOps platform providing significant benefits to hospitals and other healthcare organizations.

GE Healthcare's OnWatch NP, powered by Nyansa, is a cloud-based, vendor agnostic solution tailored for healthcare networks. It combines a deep understanding and knowledge of healthcare networks with advanced analytics technology like AI and machine learning, providing a comprehensive view of the network infrastructure in real-time.

This approach allows IT and HTM personnel to focus on making critical decisions and other operational changes, instead of wasting time with inefficient manual activities. The platform leverages data from a wide range of sources to power its machine learning algorithms. It's actually listening to every activity on the network in an unobtrusive fashion.

OnWatch NP analyzes data from wired and wireless infrastructure, network services like RADIUS, or Dynamic Host Configuration Protocol (DHCP) and DNS servers. It dives into packet data as it flows back and forth, helping determine the current state of network and application performance. The platform seamlessly handles a variety of healthcare specific protocols, like Digital Imaging and Communications in Medicine (DICOM) or Health Level Seven (HL7). This functionality helps OnWatch NP deliver actionable insights while providing the visibility needed to manage the complex healthcare networks of today.





A Closer Look at OnWatch NP's Features and Functionality

GE Healthcare OnWatch NP, powered by Nyansa, provides dedicated dashboards and workflows designed for different roles in healthcare IT. Specific platform workflows support a variety of healthcare functions, including biomedical teams, facilities teams, network engineers, network operations, security operations, and the customer service desk.

These different teams use the platform with different expectations and skill sets. It's vital for OnWatch NP to offer separate workflows and dashboards catering to each of these diverse resources. Of course, the data underneath is valuable, but if the platform can't present it to these teams in a meaningful way, then the data is of no use.

The screens presented to a network engineer need to be very different from what a service desk support person sees. Similarly, what a biomedical person managing infusion pumps expects the platform to provide is very different from a network administrator managing the wireless network. OnWatch NP recognizes these differences and presents the right workflows and screens for each role.





Intelligent Alerts Ensure Healthcare Network Security

Another important piece of information is network segmentation. Every hospital network has segmentation policies that must be followed, but how to verify their adherence? What if a Tesla smart car or an Alexa device is trying to connect to a health care network? Rest assured, OnWatch NP is monitoring the network on a 24/7 basis.

Intelligent and actionable alerts let OnWatch NP users quickly react to any critical issues. These alerts are prioritized based on context and impact. This is an important feature as otherwise multiple alerts just become noise, which can lead to them simply being ignored.

The priority of each alert is set dynamically, based on the deviation from the network or device baseline. Alerts are reported using a variety of platforms, including email, SMS, or a ticketing system. The goal is ensuring users won't ignore the alerts generated by the platform.





Analyzing Critical Healthcare Network Performance Benchmarks

The cloud-based OnWatch NP platform lets our customers benchmark the performance and behavior of their connected devices. They can analyze internal performance and compare their findings to industry peers. This analysis provides an objective view of how their network measures up within the healthcare industry.

These external comparisons are very powerful. The baselines for any healthcare organization might appear acceptable in a vacuum but comparing those results to a similar-sized hospital network with a similar infrastructure offers better insights. It helps answer a critical question: is there room for improvement? Not surprisingly, this is one of the most popular features on the OnWatch NP platform.



End to End Healthcare Network Infrastructure Insight

Ultimately, the partnership between GE Healthcare and Nyansa, now part of VMware, makes the promise of AIOps a reality for the healthcare industry. OnWatch NP helps hospitals improve their network performance, manage disparate medical devices, and even save money. It provides the critical end-to-end network insight that leads to better patient care.

This critical networking platform innovation arrives at a time when the medical world truly needs a lift. This new dawn in hospital operations is transformational. If interested in learning more about the positive impact OnWatch NP makes for any healthcare organization, connect with us as soon as possible for a personal demo.

For more information see, www.velocloud.com.

www.gehealthcare.com/services/clinical-network-solutions/onwatch-np

Join us online:



vmware®

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com Copyright © 2020 VMware, Inc. All rights reserved.
This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>.
VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. Item No: sdwan-884-ensuring-healthcare-networks-eb-0520 5/19