OnWatch NP

*Powered by Nyansa**

FAQs

1. WHAT IS THE ONWATCH NP SOLUTION?

OnWatch NP (Network Performance) is a vendor-agnostic network performance solution to assist Healthcare Technology Managers (HTMs) and IT professionals to better manage all wired and wireless IoT devices on a hospital network to help ensure device uptime, visibility and transfer of data.

2. WHY IS IT NEEDED?

One of the biggest challenges IT and network staff faces in Healthcare is managing and monitoring the performance of an influx of wireless, network-attached devices such as cell phones, laptops, VoIP phones, networked TVs and medical devices such as labs, image management, workstations, retrospective data analysis, all of which depend on other parts of the network infrastructure to perform properly. OnWatch NP quickly and easily analyzes and tracks client devices and their behavior with the network in real-time and over time.

3. HOW IS IT DIFFERENT FROM OTHER SOLUTIONS?

Conventional network management and emerging IT analytic solutions typically provide raw data that IT staff must manually analyze and correlate into meaningful information to take action on. OnWatch NP differs significantly by aggregating a collection of capabilities:

- Full-stack analysis of wired and wireless data for every client network transaction real-time and historical
- Automatic root cause analysis and remediation “next steps”
- Automatic baselining of client incidents and network services
- Anonymized cross-company sharing and comparison of network key performance indicators and infrastructure metrics
- Vendor-agnostic big data analytic system, purpose built for enterprise environments

4. HOW DOES IT WORK?

OnWatch NP ingests data from across the network stack – from both wireless and wired sources – to monitor transactions on the network. The platform provides end-to-end visibility of how network clients and devices are behaving. Advanced analytics and AI/ML techniques process this data into actionable information and provide recommendations allowing customers to proactively optimize their IT infrastructure.

5. HOW IS IT DEPLOYED?

One or more small software extractors (known as a crawler) are deployed off a span, monitor, or tap port set up on one or more switches, pushing data to the crawler(s). The crawler gathers and inspects packet data from real user traffic, fusing it with wireless LAN metrics obtained from WLAN controllers. The crawlers securely transmit performance metric summaries of the data to OnWatch NP cloud-based analytics engine for analysis. Software crawlers are available as a VM software download (EXSI v. 5.5 or higher) or within a small physical appliance.

* Nyansa is a fast-growing innovator of advanced IT analytics software technology.

6. WHAT TYPE OF DATA DOES IT COLLECT AND INSPECT?

OnWatch NP analyzes packets it sees on the wire as well as wireless metrics collected from WLAN controllers. This includes a broad range of protocol, flow, network, WLAN, and device statistics as well as information such as client device type/vendor/ capabilities, OS version, DHCP issued IP addresses, DNS, DHCP, HTTP response times, packet loss, transmission error rates, Wi-Fi channel utilization, signal-to-noise ratios, application performance, WLAN controller configuration and much more.

7. HOW MUCH DATA IS SENT TO THE CLOUD?

For every 1Gbps of real user traffic that goes to the crawler, approximately 500kbps is sent securely to the cloud.

8. IS IT SECURE?

OnWatch NP provides hardened security across a number of dimensions including user, backend, and application security. No packets or payload are stored or leave the customer premise. Anonymization options for classifier metrics (e.g. IP hostnames, ports, etc.) are also available. Strong encryption of in-transit data from onsite crawlers to the OnWatch NP cloud analytics engine is achieved using SSL (TLS) communications. Backend secure access controls provide two-factor authentication and audit trails. Logical isolation of the OnWatch NP service within the AWS virtual price cloud delivers state-of-the art security supporting SOC1, attestation standards. Application-level security is achieved through third-party penetration and vulnerability testing with protection against SQL injections and cross-site scripting, weekly Nmap scans are also performed.

9. HOW MUCH HISTORICAL DATA IS STORED?

While there are is no real limit to how long historical analytics and data can be stored, OnWatch NP can provide up to 6 months for historical trending data at no charge and 15 days for real-time (by minute) client transaction data.

10. HOW LONG DOES IT TAKE TO DEPLOY?

The configuration and deployment of OnWatch NP typically takes approximately one hour and can be installed in less than 30 minutes depending on the environment.

11. WHAT WI-FI SYSTEMS ARE COMPATIBLE?

OnWatch NP currently integrates with Aruba™, Cisco®, and Ruckus™ wireless LAN controller systems.

12. WHO IS NYANSA?

Nyansa is a fast-growing innovator of advanced IT analytics software technology based in Palo Alto, California. Founded in September 2013 by technology professionals from MIT, Meraki, Aruba™ networks, and Google™, Nyansa is credited with developing the first cloud sourced network analytics system, called Voyance.

13. WHAT IS THE RELATIONSHIP BETWEEN GE & NYANSA?

- GE Healthcare and Nyansa have entered into a strategic alliance under which the companies are integrating the GE CARESCAPE™ Network, the trusted near-real-time patient monitoring network, with OnWatch NP AIOps, the leading AI-based platform for network and device performance management
- The arrangement establishes GE Healthcare as the sole distributor of the Nyansa AIOps platform in health care facilities primarily dedicated to patient care, providing customers integrated sales and support of the complete OnWatch NP solution
- GE Healthcare and Nyansa will collaborate on product and technology roadmap to bring to market new services during the course of the multi-year agreement

For more information about OnWatch NP and other GE Healthcare network solutions, please contact your GE Sales Representative or visit our website: *https://www.gehealthcare.com/en/products/patient-monitoring*

© 2019 General Electric Company – All rights reserved.

GE Healthcare reserves the right to make changes in specifications and features shown herein, or discontinue the product described at any time without notice or obligation. Contact your GE Healthcare representative for the most current information. GE, the GE Monogram, and CARESCAPE are trademarks of General Electric Company. GE Healthcare, a division of General Electric Company. All other third party trademarks are the property of their respective owners. GE Medical Systems, Inc., doing business as GE Healthcare.

September 2019
JB69105XXa