OnWatch NP

Powered by Nyansa

Frequently Asked Questions (FAQs)

1. WHAT IS ONWATCH NP?

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 DOES IT COLLECT INFORMATION?

OnWatch NP uses an on-premise VM (or appliance), called a crawler, which collects performance, and meta data from the network. The virtual crawler may be configured on GE Healthcare provided hardware or an ESXi server provided by the customer. OnWatch NP collects Wi-Fi metrics from the wireless LAN controllers via SNMP and vendor APIs and examines network traffic by performing deep packet inspection on the traffic received off the SPAN port. The extracted performance metrics are sent to the cloud for analysis and correlation. **No ePHI or user data is sent to the cloud.**

4. DOES ONWATCH NP PROCESS OR STORE PII OR EPHI?

OnWatch NP does not process or store personally identifiable information (PII). OnWatch NP will process and store hostname, MAC address, and username associated with client devices. The product does not store packets or payload information and this data never leaves the customer premise. Anonymization options for classifier metrics (e.g. IP hostnames, ports) are also available. Strong encryption of an in-transit data from the on-premise crawler to the cloud analytics is achieved using SSL (TSL) communications.

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.

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. The extracted performance metrics are sent to the cloud for analysis and correlation. **No packet or payload information is sent to the cloud.**

7. HOW MUCH DATA IS SENT TO THE CLOUD?

For every 1 Gbps of real user traffic that goes to the crawler, approximately 500 kbps 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 DO YOU PROTECT DATA IN TRANSIT?

We use standard TLS to encrypt all data in transit. Data-to-AWS is terminated on the AWS ELB which only has port 443 open. UI traffic is terminated on the nginx servers , which only have port 80 (redirect to 443) and 443 open . The following protocols are used to transmit encrypted data:

- Crawler to Cloud: TLS 1.2
- Web App: TLS 1.2

10. CAN YOU DESCRIBE YOUR ENCRYPTION KEY MANAGEMENT PROCESS?

Crawler to Cloud uses public key for encryption. The private key stored in AWS Elastic Load Balancer is used to terminate the TLS traffic. The private key cannot be retrieved. The UI TLS traffic is terminated on the nginx server, which contains the private key.

11. 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.

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 Healthcare 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*

November 2019
JB69105XXb