Extreme Networks Wireless Infrastructure and Nyansa Voyance Drive Operational Simplicity

An AIOps solution for proactive operations

velocloud™
Now part of VMware

Extreme networks

With their digital transformation underway, the majority of enterprises have moved to wireless-first networks. Most IoT devices, laptops, phones and tablets can't be wired. In "smart" factories today, robots and RFID tagged machine tools need always-on network access and superior performance. Loss of connectivity can lead to production losses. In the healthcare industry, medical devices like infusion pumps, bed monitors and mobile workstations depend on perpetual wireless network connectivity. Connectivity issues can be life-threatening. The number of devices that access the Wi-Fi network have increased exponentially, and the data traversing the wireless infrastructure has grown astronomically. In this dynamic environment, IT admins require meaningful insight into the network behavior from a client context. They want a complete view across the full stack—from access to applications—to understand where, when and why a client device may be having issues. This cohesive view must include all of the factors that impact performance, including device behavior, network performance, application performance, WAN performance and the impact from other concurrent clients.

Legacy operations tools lack depth, visibility and foresight. They require human capital to detect issues. IT teams are forced to adopt a reactive posture, troubleshooting issues from the past using the present-day infrastructure. The challenge is that the infrastructure has either changed over time or the problem is intermittent and unpredictable, and as a result cannot be reproduced. This leaves a pervasive blind spot in the infrastructure and a growing list of unknowns weighing on the shoulders of IT admins. The rudimentary nature of monitoring tools prompts operation teams to search through logs, packet capture and screen scrape CLI output to extract meaningful data and correlate it for root cause analysis.

In this new era of digital transformation, IT teams can no longer depend on legacy tools to manage their dynamic and agile wireless LAN (WLAN) infrastructure. They need a solution that can simplify the complex ecosystem of applications, clients and infrastructure to help understand the client experience during normal and impaired conditions. When a problem escapes the realm of human understanding, it is time for technology to intervene. The Nyansa Voyance solution, powered by artificial intelligence/machine learning (AI/ML) and big data analytics, reduces the complexity of managing this digital transformation. Nyansa Voyansa integrates with Extreme Networks, Inc. Smart OmniEdge solutions WiNG version 7.2.1, offering customers full stack visibility into their infrastructure with actionable insights to remediate performance issues.

vmware®

Extreme OmniEdge (WiNG) and Nyansa Voyance

Nyansa Voyance gathers rich Wi-Fi metrics from ExtremeMobility controllers and access points (APs). It also gathers information from IP infrastructure elements like network services rendered by RADIUS, Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) servers and clients, authentication servers, unified communication (UC) systems, cloud-based and custom applications and WAN flows. The data gathered is curated, analyzed and corelated to provide full-stack network visibility and analytics.

The advantage of big data analytics and AI/ML helps Voyance handle the velocity of incoming data, ensure the accuracy of analysis and the speed of results generated. With this integration, Extreme Network customers can quickly quantify user Wi-Fi performance and network behavior, automatically identifying best or worst performing APs, clients and locations. The results offer remediation steps to fix problematic Wi-Fi network behavior impacting user experience.

When a device actively communicates over the infrastructure and suffers from performance issues, finding the root cause is like searching for a needle in a haystack. This complexity is significantly reduced by Voyance's ability to track each client transaction. In a single session, a client gets associated with a WLAN, authenticated to access the infrastructure, assigned an IP address to establish end point reachability, and obtains a URL to reach a destination. In doing so, it traverses a WAN infrastructure to reach a data center or application in the cloud. Each aspect of this interaction touches Extreme Network's WLAN infrastructure, network services, WAN networks and cloud applications.

Each such transaction, for thousands of client devices, are analyzed in real time by the Voyance Analytics Engine hosted in the cloud or on-premises as shown in Figure 1. The Voyance Crawler synthesizes the information into metadata from a client context, compresses, encrypts and sends it to the analytics engine. With this approach, IT admins no longer need to manually trace each transaction sequence to understand the client state.

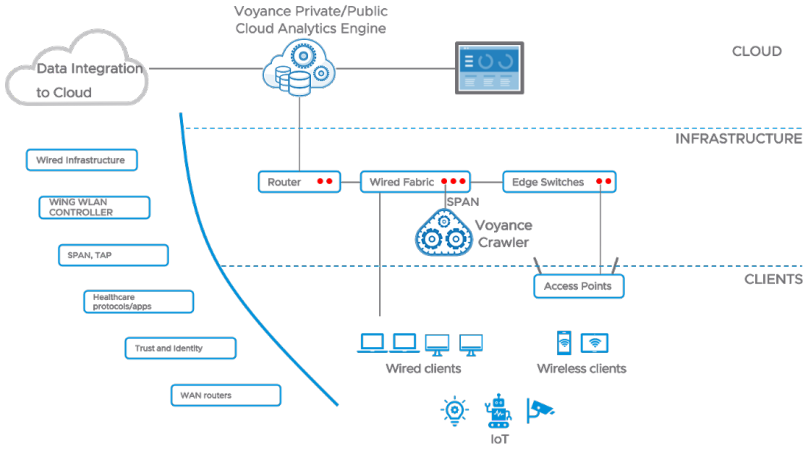

FIGURE 1: Extreme OmniEdge and Nyansa Voyance Integration

Simplified Wi-Fi operations

Integration of Extreme Network's Smart OmniEdge with Nyance Voyance transforms IT operations from reactive to a proactive. The combined solution reduces the challenges of maintaining and troubleshooting wireless connectivity, stability, and performance. The solution monitors the Wi-Fi infrastructure 24x7 for issues like noise, roaming, coverage, RF interference, capacity and channel planning. This reduces the need for constant attention from IT admins.

Detailed, real-time metrics are collected from Extreme Networks wireless infrastructure elements including the wireless LAN controller, individual AP and optionally, any client devices running the Voyance client. These metrics give extraordinary insight into both the infrastructure as well as a client's wireless state, including location and associated AP radio, signal strength and layer 2 retransmissions, noise levels and co-channel interference observed. An example of WI-Fi performance from a client context is shown in Figure 2.

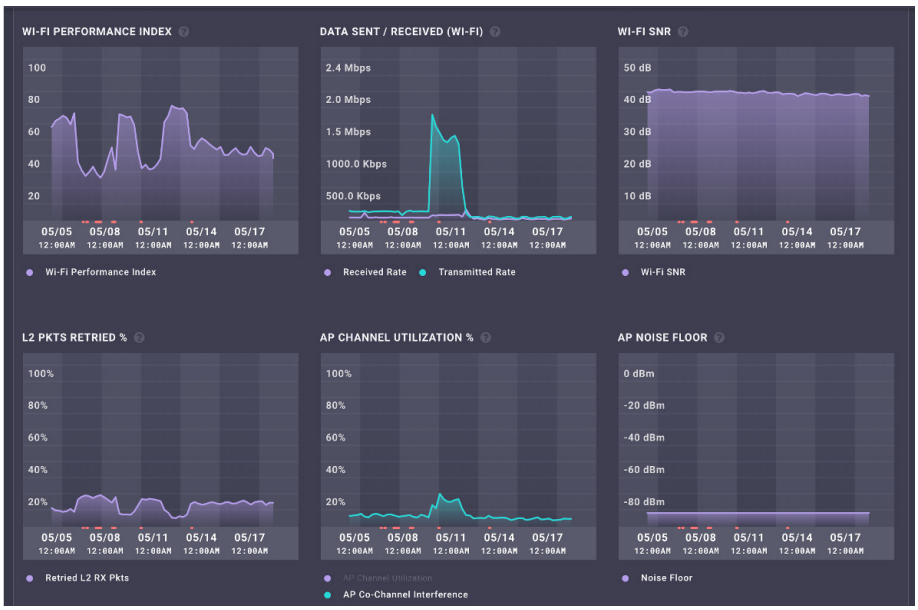

FIGURE 2: Extreme Networks Smart OmniEdge Wi-Fi performance from a client context

Apart from Extreme Networks wireless infrastructure, metrics are collected from other sources to provide detailed protocol interactions of network services like RADIUS, DHCP, Address Resolution Protocol (ARP), DNS and cloud applications. These metrics, collected for each client device and every infrastructure element, are combined to compute a client's wireless experience at any point in time. The data is curated and summarized in terms of "client hours" of poor connectivity performance for each client.

Analysis is also done to correlate different attributes and perform root cause analysis. For example, when a client has a poor application experience, Voyance determines whether problems emerged at the same time from Wi-Fi, the WAN or any other network service. In Figure 3 below, eleven clients had poor application performance as they deviated from the baseline. Correlation determines the root cause for each client even though they exhibit common symptoms as seen in Figure 3. The full stack visibility pinpoints issues in areas that extend beyond the WLAN infrastructure.

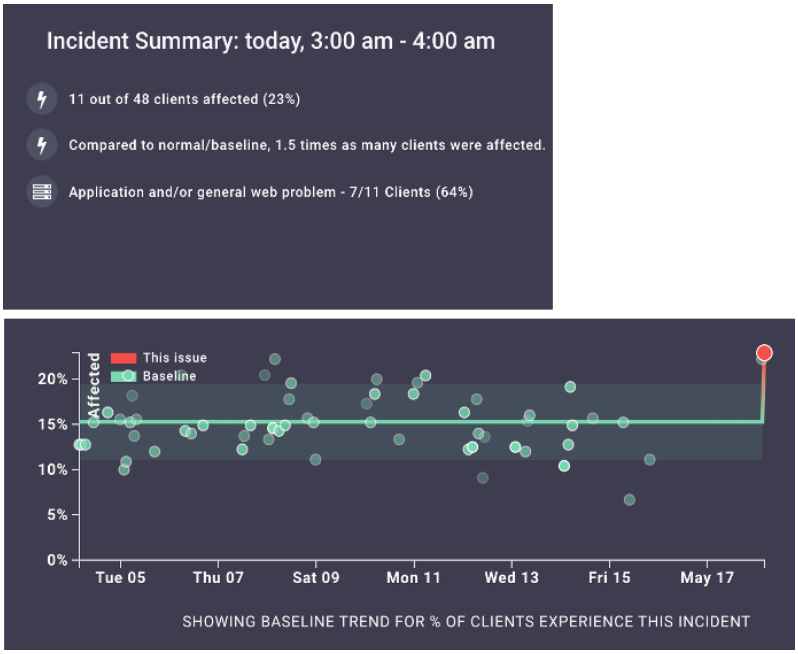

FIGURE 3: Eleven clients with application performance issues

FIGURE 4: Common symptoms among 11 clients with different root cause

Self-learning to auto-detect issues

The platform employs AI/ML techniques, such as clustering and regression, on all input data sources to automatically determine baseline performance, detect hidden trends, and identify anomalous behavior. Inherent to AI/ML is self-learning, where an IT admin does not have set thresholds for performance based on experience. Because the solution constantly gathers information on every client network transaction, it is able to baseline application and service behavior over time to understand what's "normal" and what is not. When activity deviates from this norm, the system is able to automatically recognize, rank and provide the who, what, when, where and why details that can otherwise take hours, days or months to figure out using legacy tools. When deviations occur from the baseline, incidents are generated.

Voyance maintains Wi-Fi analysis results with the data gathered from Extreme Mobility Controllers and APs. This helps IT admins go back in time to analyze their infrastructure without the burden of reproducing the state using logs, CLI screen-scraping and archived configuration retrieval. With annotations, it is possible to find out the before and after effect of making changes, as shown in Figure 5. For example, you can determine whether adding an AP made a difference to the baseline performance.

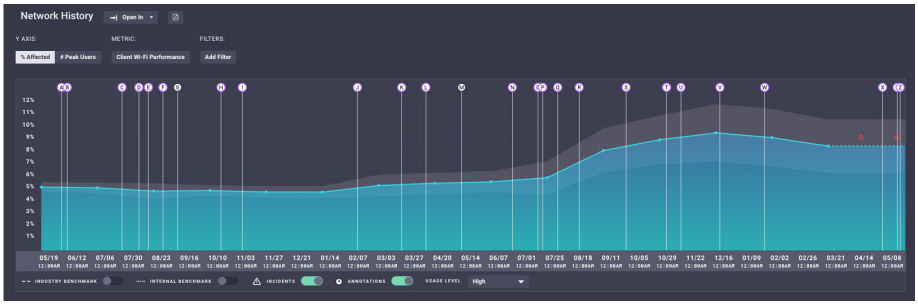

FIGURE 5: Historical trends help understand impact of changes for Wi-Fi infrastructure

Cloud sourcing a baseline from millions of devices across hundreds of production deployments, managed by Voyance, helps IT admins compare how their infrastructure is performing against similar enterprises in the industry. For example, a hospital can compare the Wi-Fi performance of a specific location to peer hospitals of similar size and geography, as shown in Figure 6. This information helps hospitals determine if they need to tweak the performance or add more APs. This knowledge empowers hospitals with tangible proof points to make informed decisions.

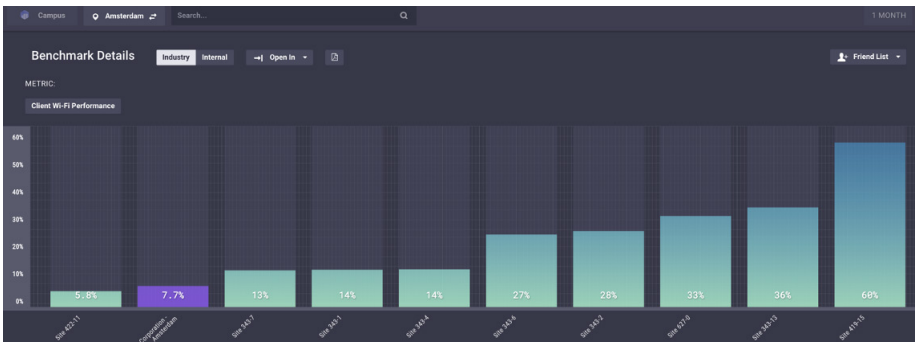

FIGURE 6: Comparison of Wi-Fi performance in Amsterdam with peers in the industry

Productivity gains for operations teams

Many IT organizations use the number of trouble tickets created and the duration the tickets stay open to measure their SLAs. In a reactive mode, Tier 1 operations teams waste valuable time chasing incomplete information from an open trouble ticket before they can route the issue to the right escalation team. The integrated solution from Nyansa Voyance and Extreme WLAN infrastructure provides a service desk dashboard with the right information ahead of time to help IT organizations take action proactively—even before a trouble ticket is raised by a user. In the scenario where a trouble ticket gets raised, the powerful search engine provides quick access and complete visibility to the client, network or application. This helps improve SLAs, reduce the number of tickets created and raises productivity for the organization.

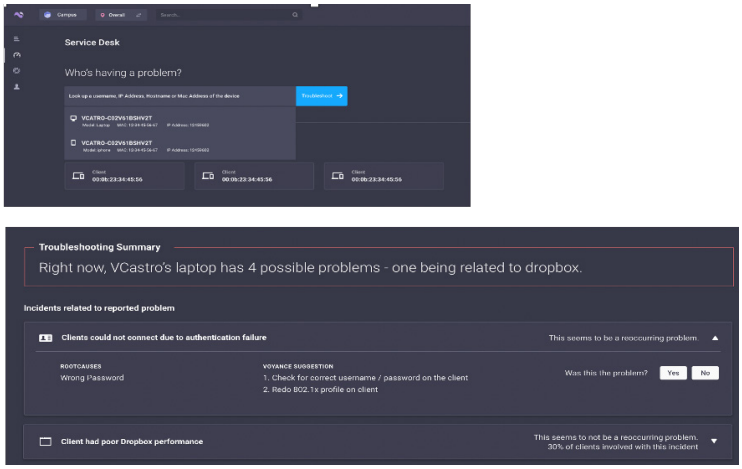

FIGURE 7: Powerful search engine helps identify issues for fast resolution

Performance assurance

Nyansa Voyance integrated with Extreme Networks Smart OmniEdge solutions WiNG version 7.2.1 provides end-to-end network visibility, actionable insights and predictive analytics to offer assured performance. The solution is designed to scrutinize every client network transaction, Wi-Fi performance, network service health, application response times and WAN link utilization to determine the root cause of any client performance problems.

Because this is a cloud-based SaaS solution, installation and deployment is quick and painless. The solution does not require any change to the Extreme Networks WLAN infrastructure, nor does it need any software agents or client software. The combined solution reduces the time period from Installation to results.

Extreme Networks customers can use Voyance as a single source of truth for their network teams to quantify the end user experience across the entire network, justify infrastructure changes, and accurately develop capacity plans using existing data running across their Extreme Networks WLAN networks. The solution is designed to scrutinize every client network transaction, Wi-Fi performance, network service health, application response times and WAN link utilization to determine the root cause of any client performance problems.

How to get started

Check out the Nyansa Voyance Demo at: *www.nyansa.com/demo/*

More information on Extreme Networks: *www.extremenetworks.com*