Enrich the Client Experience with VMware Edge Network Intelligence

An AIOps solution for a distributed and secure workplace

VMware Edge
Network Intelligence™

KEY HIGHLIGHTS

• An AIOps solution focused on the enterprise edge. Ensures end user and IoT client performance, security, and self-healing through wireless and wired LAN, SD-WAN and SASE.

• Customers have seen a 40 to 55% improvement in client device productivity by deploying this solution.

• Accelerates transformation of IT Operations to a proactive mode.

Organizations have seen an exponential increase in end user and IoT devices driven by productivity. Critical to the performance of these devices is their ability to access a plethora of SaaS applications, including real-time voice and video and a number of network services.

The modern network of today is delivered as a cloud-first service over a wireless-first infrastructure. Device heterogeneity and device mobility, combined with high transaction and data volume, have made the network far more dynamic and the operations significantly more complex at the edge. Legacy management solutions were designed to manage static networks used by a limited set of IT sanctioned clients and applications. These outdated solutions lack coherent and meaningful insights from a client context. If a client has issues with application performance, it is hard to pinpoint if the problem is systemic or isolated, a result of poor Wi-Fi performance, an impairment on WAN, a problem with network services, or an issue with the application. IT teams cannot rely on these antiquated tools to ensure modern day clients get the best performance from the network infrastructure, network and security services, and applications. IT teams, and the organizations they support, require advanced analytics and actionable intelligence made possible by an AIOps solution.

VMware Edge Network Intelligence: A comprehensive AIOps solution

VMware Edge Network Intelligence is a vendor agnostic AIOps solution focused on the enterprise edge that ensures end user and IoT client performance, security, and self-healing through wireless and wired LAN, SD-WAN and secure access service edge (SASE).
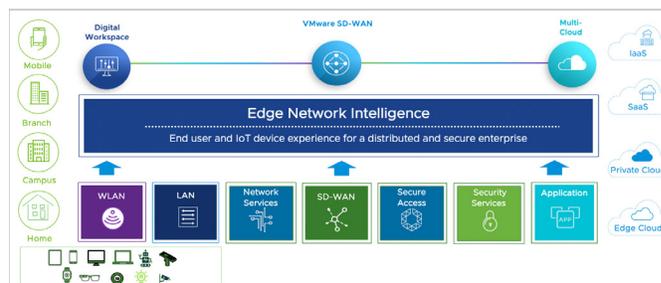

FIGURE 1: VMware Edge Network Intelligence overview

The solution employs machine learning (ML) algorithms and modern big data analytics to process high volumes of data from a wide range of network, device and application sources. In doing so, the solution auto-discovers end user and internet of things (IoT) devices, automatically establishes baselines, understands every single client interaction and monitors for deviations to provide actionable insights that operations teams can proactively remediate.

Solution benefits

Rich client experience

VMware Edge Network Intelligence significantly improves and quantifies the end user & IoT device experience at any location. With a distributed workforce, IT teams lack visibility into the client experience at every location. They need a solution that reduces the need for IT visits. VMware Edge Network Intelligence can pinpoint with clarity whether a perceived application problem is due to issues with the local Wi-Fi network, broadband network, WAN, network services or with the application. Customers using VMware Edge Network Intelligence have seen 40 to 55% improvement in client device productivity.

Proactive remediation

VMware Edge Network Intelligence uses ML techniques, including nearest neighbor and unsupervised clustering algorithms, to automatically isolate faults, identify root cause, make recommendations and predict benefits. Using internal and industry benchmarks, the solution provides opportunities for continuous improvements. Using VMware Edge Network Intelligence, customers have seen a 50% reduction in time to find and fix issues.

Application assurance

Enterprises use hundreds of SaaS applications. While a small percentage of these applications are sanctioned by IT, a large majority of productivity applications are not. Tracking these applications becomes untenable for IT teams. VMware Edge Network Intelligence provides assurance for over 3000 applications with contextual performance indicators like number of clients affected or number of sites impacted.

Operational simplicity

VMware Edge Network Intelligence currently detects and analyzes over 30 million devices. The wide variety and growth in the number of devices makes it impossible to manually identify, classify and analyze performance. The solution uses time-series based ML algorithms to auto-discover these devices and establish a baseline for monitoring.

vmware®

Use cases

Application assurance

VMware Edge Network Intelligence analyzes from over 3000 applications, tracking performance for fault detection and fault isolation. The solution uses a Bayesian ML approach to analyze time series data for each client. This helps IT teams determine the worst performing clients for an application, identify if the problem is systemic or isolated, and compare performance with other locations within the organization and with peers in the industry.
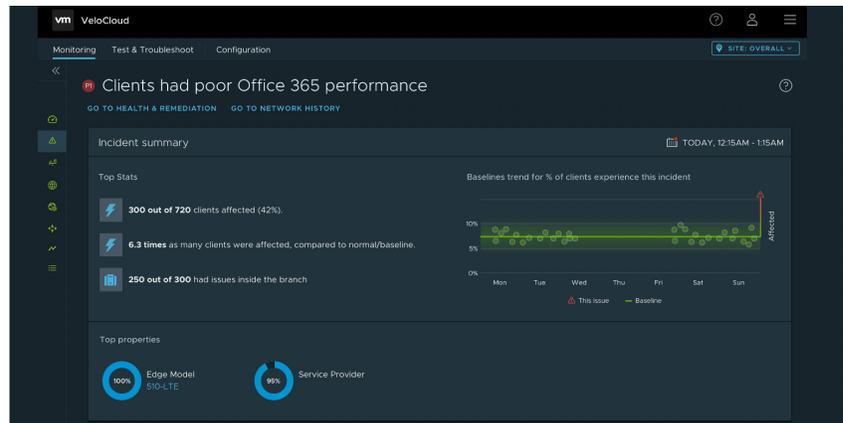

FIGURE 2: Application assurance with contextual performance indicators

Wireless and wired end client experience

VMware Edge Network Intelligence provides deep visibility into a client's wireless state, such as its location and associated access point (AP) radio, signal strength and layer 2 retransmissions, noise levels and co-channel interference observed. The solution surfaces issues like noise, roaming, coverage, radio frequency (RF) interference, capacity and channel planning and makes predictive recommendations. Customers have seen Wi-Fi client issues reduced by 50% and client experience improved by 35%.
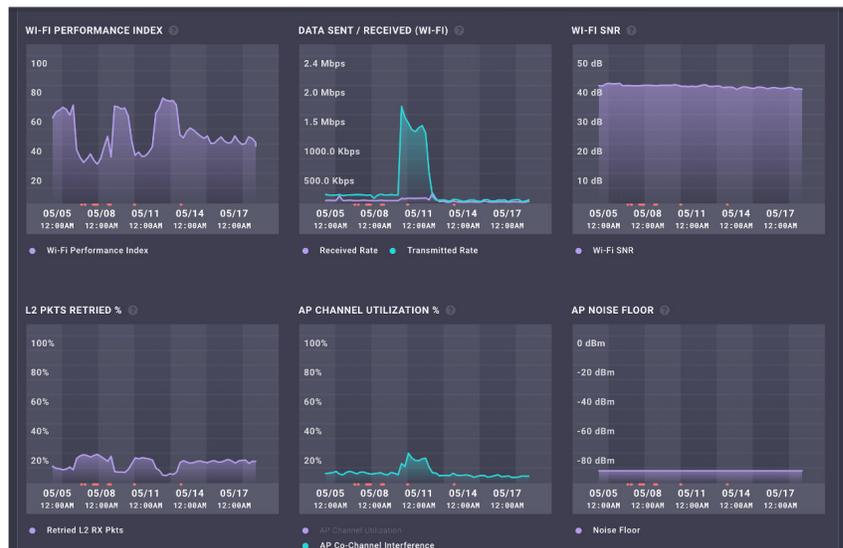

FIGURE 3: Wi-Fi performance tracking with real-time metrics

vmware®

Business continuity and work from home

The work/life boundary has merged with the onset of COVID-19 as more users work from home. To manage their remote workforce, IT teams need visibility into the client experience. VMware Edge Network Intelligence collects application data related to user experience directly from SaaS applications. An example can be data from a unified communications (UC) application that includes service provider, frame rate, bit rate, packet loss, and output resolution. The solution combines application data with data from a client application installed on the end user device. This helps IT understand the baseline performance of that application across the entire organization, to gain insights into worst performing clients, worst performing sites and service providers. The solution can isolate problems to identify the source of the issue: local network, broadband internet provider, VPN or the application. Remote workers are also empowered with visibility into issues they can troubleshoot on their own.
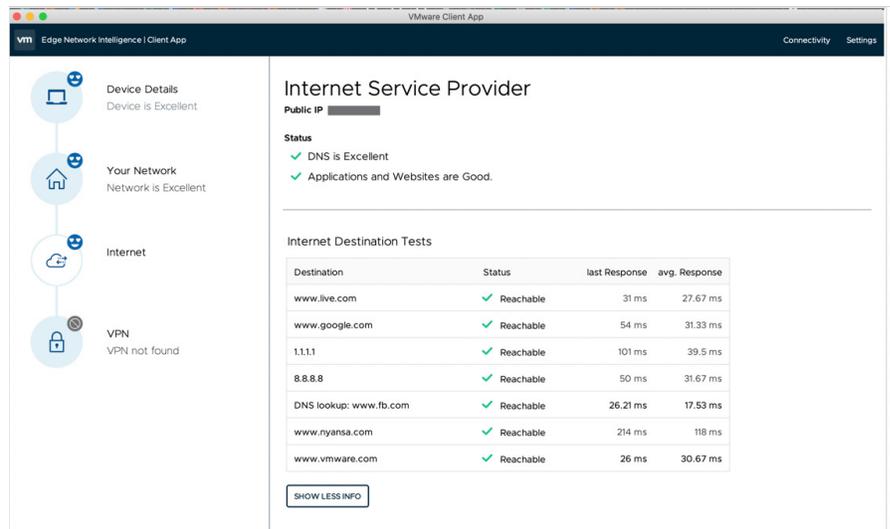

FIGURE 4: Client app for end user troubleshooting and IT visibility

Change verification and ROI

VMware Edge Network Intelligence offers change verification by comparing performance before and after a change to provide quantifiable data on whether a change has resolved an issue or whether a rollback is required, instead of waiting for users to open cases to find out. This helps justify the ROI.
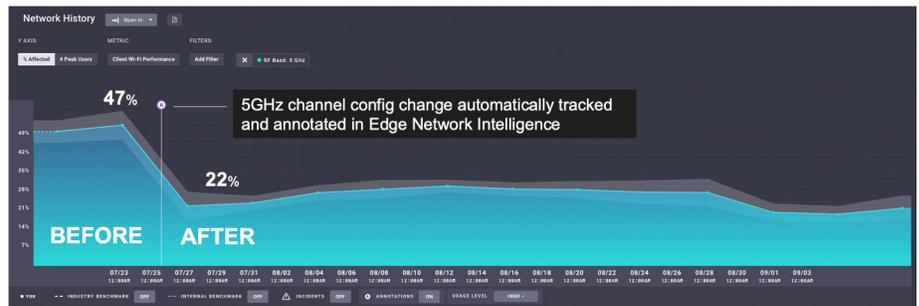

FIGURE 5: Change verification shows reduction in percentage of affected clients

Fault isolation and recommendations

A perceived application issue may point to a problem in a local Wi-Fi network, WAN, data center, cloud or the internet. Legacy management solutions offer fragmented visibility into each of these areas, making it difficult to isolate faults and identify root cause issues. VMware Edge Network Intelligence gets data from different vantage points for each application flow, which includes wireless controller, LAN switch, network services, VMware SD-WAN Edge, VMware SD-WAN Hub, VMware SD-WAN Gateway and application performance metrics. The solution can isolate the fault to the client LAN, WAN, data center LAN, cloud, the internet or the application. Using ML algorithms, such as clustering, VMware Edge Network Intelligence analyzes historical network data to determine where the problem occurs and makes recommendations and predictions to IT.
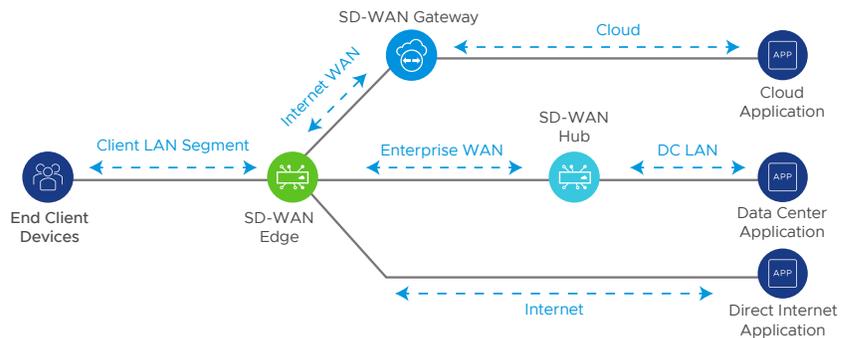
FIGURE 6: Fault isolation using bifurcated stats from multiple vantage points

IoT operational assurance

Understanding how IoT devices perform on the network is critical to their productivity, as these devices conduct tedious transactions on their SaaS applications. Organizations have challenges identifying these devices, classifying them, and managing their performance and security. VMware Edge Network Intelligence is an agentless solution that leverages an ML-based hierarchical device classification system and uses the detailed behavioral signature of each detected device to automatically inventory and classify them. The solution learns the normal baseline of a particular device by looking at similar IoT devices in a single environment and across multiple customer environments. VMware Edge Network Intelligence has over 30 million devices currently under observation and continuously updates the unique pattern for each family of devices, minimizing false anomalies. The solution measures risk profiles when these devices talk to a suspicious URL or an unauthorized IP address, or when they share network segment with non-critical or user devices. VMware Edge Network Intelligence incorporates over 300 billion global threat data points from a continously updated URL and IP threat intelligence database. The solution quantifies utilization, risk and performance of critical IoT devices.

From reactive to proactive

VMware Edge Network Intelligence offers deep visibility and actionable insights powered by AI and ML, across an application stack that extends from end user and IoT devices to cloud applications, spanning wireless and wired local networks, SD-WAN, network services and security services. This solution accelerates the transformation of IT Operations to a proactive mode with the power to predict outcomes and demonstrate success in implementing recommendations.

For more information on VMware Edge Network Intelligence please visit https://sdwan.vmware.com/products/edge-network-intelligence or contact your VMware representative.