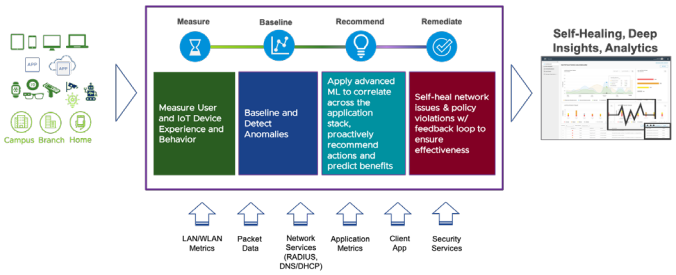
VMware Edge Network Intelligence

VMware Edge Network Intelligence overview

VMware Edge Network Intelligence™ (formerly Nyansa Voyance) is an artificial intelligence for IT Operations (AIOps) solution focused on the enterprise edge, ensuring end user and IoT client performance, security, and self-healing through LAN/WLAN, SD-WAN and secure access service edge (SASE). The solution employs machine learning 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 IoT devices, automatically establishes baselines, understands every single client interaction and monitors for deviations to provide actionable insights that operations teams can proactively remediate.



Product-specific questions

Q. What are the advantages of VMware Edge Network Intelligence?

A. The following key benefits set VMware Edge Network Intelligence apart:

- It focuses on performance of the edge device from the device perspective, unlike other solutions that are mainly focused on monitoring infrastructure components and can't learn from edge device behavior patterns.
- VMware Edge Network Intelligence is a vendor-agnostic solution tailored for the enterprise environment.
- Rich client experience for end-user and IoT devices with correlated and deep insights in a distributed enterprise reduces the demands for physical IT presence, and empowers remote workers/end-users to lessen IT dependency and resolve issues themselves.
- Proactive remediation addresses issues caused by WLAN, LAN, SD-WAN, network services, security services and applications.
- Assurance for over 3000 applications, with contextual performance indicators including the number of clients or sites affected.
- For business continuity and work from home use cases, VMware Edge Network Intelligence provides deep visibility and proactive insights into client performance. Remote workers also get visibility into issues they can troubleshoot.
- The solution performs device auto-discovery, automatic performance baselining, monitoring, fault detection and root cause analysis, providing actionable insights and analytics – all leading to greater operational simplicity.
- Customers can verify that changes worked, and get quantifiable data for ROI justification, by comparing performance before and after changes are made.
- Internal and industry benchmarking supports predictive recommendations and proactive remediation opportunities
- API support for seamless integration with enterprise tools increases agility for IT Ops and helps drive enterprise automation.

Q. Does the solution support work from home use cases?

A. VMware Edge Network Intelligence supports business continuity and work from home use cases. The Client App is an additional data-source that can be installed on end user devices to collect performance metrics such as Wi-Fi metrics from the client perspective, and run on-going synthetic tests to measure performance of Wi-Fi, Internet and VPN connections, and audio/video call quality. Client App will offer IT Ops teams visibility into client experience for employees working from home.

VMware Edge Network Intelligence also has Cloud API integrations with critical SaaS applications such as Zoom, which enables IT Ops teams to track the client experience of employees using cloud-based applications from home. This helps give them insight when users are having issues—for example, what is the underlying root cause, is it specific to a region or to a service provider?

Q. How is VMware Edge Network Intelligence licensed?

A. VMware Edge Network Intelligence has two license components. A software subscription license is sold per-node for a 1-year, 3-year or 5-year term, and includes a hardware component for the Analytics Edge/Crawler. If the Analytics Engine is deployed on-premises, then the hardware component for purchase also includes a Private Cloud Appliance. A node here refers to Switch and Access Points.

Q. What AI framework does VMware Edge Network Intelligence use? Does it use supervised and unsupervised learning?

A. To automatically learn baselines of client experience and behavior, the solution uses a variety of time-series based machine learning algorithms, including Bayesian techniques. This is augmented by a variety of other ML techniques including nearest-neighbor and unsupervised clustering algorithms to automatically isolate faults, identify root causes, make recommendations and offer predictions.

Q. What are the data sources for VMware Edge Network Intelligence?

A. One or more on-premises Analytics Edges (Crawlers) gather data from wireless LAN controllers. The Analytics Edge is deployed out of line and directly connected to the wired network using a SPAN or tap on a core or intermediate network switch. The Analytics Edge performs deep packet inspection on all traffic, identifies network applications and correlates traffic with user information. This information is analyzed and correlated locally. Only metadata trends and analytics are sent to the Cloud Analytics Engine for use by all levels of IT staff, from help desk to CIO. No packet data is ever stored. The polling interval varies depending on the data source.

When the Analytics function is used in conjunction with SD-WAN functionality on the VMware SD-WAN Edge, the collection is done inline.

Q. What applications does VMware Edge Network Intelligence analyze and provide assurance for?

A. The software can analyze more than 3000 applications. It is also possible to define custom applications. The software can identify nearly any application on the network and analyze on a per-user basis. This includes hundreds of popular SaaS applications including Facebook, Box, Google Mail, Microsoft 365, Stripe, Slack, Netflix, Skype for Business, Cisco UC, Zoom, and Wi-Fi calling apps, as well as custom applications specifically defined by the customer.

Q. Which voice/video applications does VMware Edge Network Intelligence support?

A. The software provides explicit application analytics for three industry leading UC applications: Cisco UCM, Skype for Business, and Zoom. For these UC applications, the software delivers detailed information such as call duration, historic service baselines, quality of experience (QoE) for individual clients, and systemic incident root cause analysis.

Q. Which wireless vendors does the software support?

A. We are vendor-agnostic and support Cisco, HP Aruba, Extreme, Mist, Cisco Meraki, and VMware SD-WAN Edge Wi-Fi today.

Q. How does the solution identify and classify IoT devices?

A. VMware Edge Network Intelligence is an agentless security platform for IoT and unmanaged critical devices that collects data passively, via the Analytics Edge (Crawler) sitting out-of-band in the customer's network. This vantage point enables the platform to monitor every single client transaction on the network to identify and classify IoT devices. The solution ensures deep insights into device connections by creating visibility that extends from the access layer (wired and wireless) all the way up the network stack. The platform employs a machine learning based, hierarchical device classification system that uses the detailed behavioral signature of each detected device to automatically inventory and classify IoT devices. Beyond automatic classification, customers are also given the flexibility to tag critical devices and assets for continuous analysis within the VMware Edge Network Intelligence IoT security lifecycle management framework. As a cloud-native solution, the collective insights and learnings about IoT device behavior and threat intelligence on one network is shared anonymously across all customers.

When the Analytics function is used in conjunction with SD-WAN functionality on the SD-WAN Edge, the collection is done inline.

Q. How many devices can the solution currently identify automatically and how long does it take after deployment?

A. The VMware Edge Network Intelligence platform currently analyzes end-to-end behavior of more than 30 million devices. The platform can be deployed in under 30 minutes and starts identifying devices immediately as it sees client activity on the network. It takes about 24 hours for the software to establish a baseline of what is 'normal' behavior and start tracking deviations.

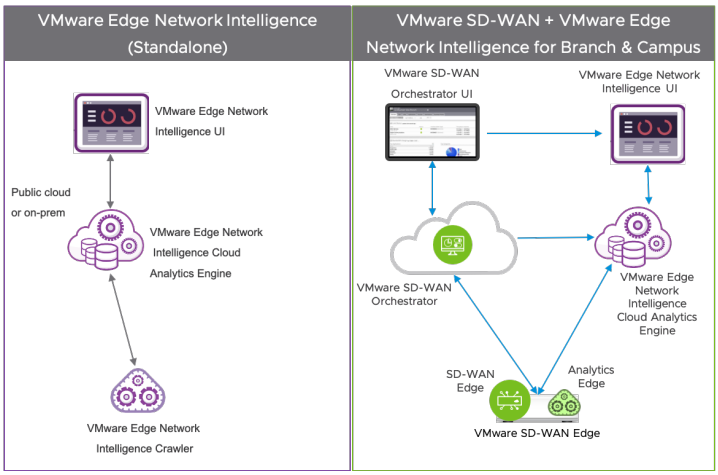
Q. How long is the data retained in VMware Edge Network Intelligence, and how much storage is needed?

A. The platform holds on to raw data for two weeks. Historical trends and baseline data from aggregated analysis is held for two years. There is no data stored in the Crawler/Analytics Edge. The Analytics Engine is hosted in the cloud, removing the need to size storage, CPU, memory, or manage the life cycle in general.

Q. How is VMware Edge Network Intelligence deployed?

A. VMware Edge Network Intelligence has two components. One component is the Crawler/Analytics Edge, which is deployed on-premises or using a Virtual Edge instance in the data center or public cloud. The second component is the Cloud Analytics Engine, which is hosted in the cloud. Some customers prefer to use Analytics Engine on-premises in the data center. This deployment option is also available.

The crawler component of the former Nyansa Voyance solution will be integrated into the VMware SD-WAN Edge, in all available hardware models and in the Virtual Edge form factor. The Crawler can be deployed in stand-alone mode or as an Analytics Edge function on the SD-WAN Edge device, for visibility that extends from SD-WAN to branch and campus.



For more information, visit *https://sdwan.vmware.com/products/edge-network-intelligence*.