VMware Edge Network Intelligence
Raising the Bar for AIOps in the Distributed Enterprise
The enterprise edge is not what it used to be. Not that long ago, “work” was something that happened in a corporate office or branch. Today, people could be working from anywhere, especially in the wake of COVID-19. Millions of new home-based workers still need office-quality connectivity—but now, over access networks that enterprises don’t control.

It’s not just people that enterprises have to worry about, either. Millions of new Internet of Things (IoT) devices now connect to enterprise edge networks, transacting vast amounts of data for mission-critical applications. The upshot: maintaining network visibility has never been more important, even as edge networks become exponentially more complex. Enter “AIOps”—the application of artificial intelligence (AI) to network operations, to better understand and react to a more diverse, dynamic edge.

VMware Edge Network Intelligence™ provides a vendor-agnostic AIOps solution to optimize the performance of end-user and IoT clients. At the same time, it strengthens security and enables self-healing across wireless and wired local-area networks (LANs), software-defined wide-area networks (SD-WAN), and secure access service edge (SASE) solutions.

VMware Edge Network Intelligence is designed for today’s distributed enterprise edge, where a client device could be connecting from home, an office building, a manufacturing floor, or a hospital bed. It can give you the advanced analytics and actionable intelligence you need to operate your network more proactively, while improving client device performance by up to 55%.

Ready to learn more? Keep reading.
The Enterprise Edge Is Getting More Complex

To meet the needs of today's distributed, cloud-first businesses, enterprises are rapidly adding more users, devices, and application intelligence out at the edge. As they do, the enterprise edge has become enormously complex and hard to manage.

As IT grapples with this complex web of devices, applications, and clouds, they face new operational challenges along multiple vectors.

Growing Diversity and Volume of Connected Devices, Applications, and Data

The growth in edge complexity started with the “bring-your-own-device” trend, and the need to onboard and secure employee-owned devices outside enterprise control. Next, enterprises began adding millions of new IoT devices into the mix.

Not that long ago, “connected devices” mostly meant things like printers and Wi-Fi access points. Today, IoT applications can use a wide range of devices, from bedside monitors in hospitals, to barcode scanners at ports and warehouses, to retail point-of-sale systems, sensors, robots, industrial equipment, and much more.
Dynamic Transformation of Applications and Clients on the Move

Many of these new devices are mobile, which means they could be connecting from practically anywhere. They’re also designed to be cloud- and wireless-first. They still may need to access resources in the corporate data center or over traditional enterprise LAN/WAN connections. Yet more and more of their activity involves accessing applications in the cloud and over wireless networks.

Need to Analyze More Data to Ensure Device Performance and Security

All these heterogeneous devices, applications, and clouds make understanding client performance and security—much less optimizing it—a lot harder. A diverse mix of infrastructure segments and services can now be involved in every single device transaction.

As a device connects with the wireless network, accesses network services like DNS and DHCP, and then traverses the WAN to reach applications in the cloud or on the Internet, any number of issues could arise that impact performance. IT needs clear visibility into the client device experience as it traverses all these vantage points.
Out-of-Date Tools Cannot Meet this Need

It’s not that enterprises don’t have tools to measure client performance. It’s just that those tools were designed for an earlier time, when IT only had to worry about static networks used by a limited set of IT-approved clients and applications. Most of these tools are also domain- or vendor-specific point solutions that focus on one narrow segment of the environment.

This model may have worked in the past. Today, the sheer density of devices at the edge, the hundreds of applications they may be accessing, and the huge volume of data and transactions they generate render these legacy solutions ineffective. IT teams seeking to detect issues and identify root causes are left to make sense of a mountain of disparate logs and alarms on their own.

It’s Time for a Smarter Approach

All these challenges point to a pressing need for a new kind of monitoring—one that uses AIOps to contend with the edge networks businesses have today, rather than a decade ago. IT needs the ability to manage the edge more proactively, identifying complex problems before they affect users. Ideally, this new approach should lay the foundation for tomorrow’s self-healing networks, where the network can detect and fix issues autonomously, without needing any human intervention at all.
VMware Edge Network Intelligence

VMware Edge Network Intelligence is a vendor-agnostic AIOps solution designed for today's dynamic cloud- and wireless-first edge networks. It uses machine learning (ML) and big data analytics to ensure that end-user and IoT devices at the edge of the distributed enterprise can access applications in the cloud with consistent performance and strong security.

To do this, VMware Edge Network Intelligence collects data from a wide range of sources across your extended environment, including:

- **The wireless and wired LAN**, the first point of access for edge devices getting on the network
- **Network services** like DHCP and DNS
- **SD-WAN**, including the ability to natively integrate with VMware SD-WAN™ gateways and hubs
- **Applications**, via prebuilt integrations with Zoom, Citrix, Cisco Unified Communications Manager, and other critical enterprise applications

In the future, VMware Edge Network Intelligence will also collect data from the diverse security services (cloud-based firewalls, secure web gateways, zero trust remote access frameworks, and more) that are part of the VMware SASE Platform™.
Gain Deep Visibility into the Client Experience

VMware Edge Network Intelligence uses ML algorithms and big data analytics to correlate massive volumes of dispersed data into meaningful insights. It provides deep visibility into a client device’s experience with each application, whether connecting from a manufacturing floor, a branch office, or home office. The solution then surfaces actionable intelligence to enterprise IT.

Is a client issue caused by poor Wi-Fi performance? An impaired WAN? An issue with specific network services or the application? If you’re using antiquated tools, you’ll have to figure that out yourself. VMware Edge Network Intelligence gives IT teams the visibility to quickly isolate and resolve client issues, instead of spending hours (or days, or weeks) on root cause analysis. In this way, the solution also brings you a big step closer to the long-term vision of a self-healing network.
Comprehensive Cross-Data Correlation and Analysis

In this figure, you can see a more detailed view of how VMware Edge Network Intelligence correlates data from across the distributed enterprise to provide actionable insights.

On the left is the distributed edge, where a long and growing list of client devices connect, mostly over wireless networks. These devices access network services and traverse the SD-WAN to connect to applications, many of which now live in the cloud—or, more accurately, in multiple clouds.
Measuring End-User and IoT Device Experience and Behavior

VMware Edge Network Intelligence tracks every single client interaction. To do this, it consumes data from multiple sources, including from wireless data packets and data about network services. The solution also features an optional client application that can be installed on end-user devices like phones and laptops, providing an additional data source to measure the performance that mobile users experience.

In the future, VMware Edge Network Intelligence will also collect data from the various security services within the VMware SASE Platform. In fact, this kind of deep insight into the client experience fits squarely within the broader edge transformation businesses are undergoing as they use SASE to “cloudify” security and remote access services at the edge.

Establishing a Baseline and Detecting Anomalies

VMware Edge Network Intelligence measures every single client transaction to establish a baseline of normal behavior for each application on each client. The solution then monitors clients on an ongoing basis to detect any deviation from that baseline. If it detects a deviation (once again, by correlating information from diverse segments and services across the application stack), the platform notifies IT teams.
Proactive Recommendations
With the root cause of an issue identified, VMware Edge Network Intelligence can provide proactive remediations to mitigate the issue. IT teams no longer have to spend hours or days manually sifting through mountains of data to make sense of all the alarms and logs, just to arrive at a root cause. Instead, they know the root cause as soon as they receive the alert, and they can focus on solving the problem.

That’s a huge benefit in itself, but the advantages of these insights extend beyond incident resolution. Because VMware Edge Network Intelligence baselines performance, it can help you understand how the user experience is trending over time for critical applications. Did the changes we just made improve the quality of Zoom calls from home offices? You get quantifiable data to measure the return on your infrastructure investments and the ability to track the effects of those changes in real time.

Building the Foundation for a Self-Healing Network
VMware Edge Network Intelligence can deliver major performance and operational improvements with any SD-WAN solution. If you’re using it with VMware SD-WAN, however, you gain an even deeper level of insight and integration, which can provide the foundation for self-healing networks.

In the future, you’ll be able to feed VMware Edge Network Intelligence insights directly back to the VMware SD-WAN control plane. In this way, your SD-WAN can not only make smarter traffic-handling decisions, it can enable a feedback loop that measures the positive and negative effects of those decisions to continually optimize itself.
Address All Aspects of the Evolving Edge with a Single Solution

Let’s take a closer look at the data sources that VMware Edge Network Intelligence uses to measure performance across branch and campus networks, SD-WANs, and home offices.
Extending Branch Connectivity into the Home
VMware Edge Network Intelligence began as a means to bring advanced analytics and deep visibility into the client experience on branch and campus networks. The solution still does that today, but the reality is, the “workplace” has changed dramatically in recent years, especially as millions shifted to home offices and kitchen tables in the wake of COVID-19.

No matter where people are working, IT teams are still responsible for ensuring that they can work productively. Remote and home-based users still need a consistent, well-performing experience when accessing enterprise applications. But can we really expect IT to troubleshoot issues across thousands or tens of thousands of unique home networks outside their control? To address this urgent problem, VMware Edge Network Intelligence brings new information sources to the table to help extend IT’s visibility from branch to home users.
Deeper Integration with Enterprise Applications and User Devices

One of the ways VMware is extending visibility into home networks is via sophisticated integration with the Zoom API to measure home users’ experience on Zoom videoconferences. We also offer an optional client application that can be installed on end-user laptops and mobile devices. These extra data sources give enterprise IT the visibility they need to ensure business continuity in the event of major disruptions and better support users working from home.
Self-Service User-Facing Tools
With the solution’s optional Client App, end-users can gain visibility into their connectivity. Users can quickly identify and self-service issues within their control. For example, if work-from-home users are having connectivity issues, they can immediately see if the problem is with their broadband service provider, so they know who to call.

SD-WAN Integration
VMware Edge Network Intelligence can benefit any network or SD-WAN, regardless of vendor. When paired with VMware SD-WAN, however, it provides even deeper visibility.

By tightly integrating with VMware SD-WAN, VMware Edge Network Intelligence can collect data from diverse vantage points across your SD-WAN topology, including edge devices, SD-WAN gateway locations, and the SD-WAN hub in the data center. These additional data points augment the AIOps solution’s data set, allowing it to further refine and enrich insights into the client experience. For example, it can identify fault segments, whether in the branch, in the WAN, or towards the application.
Extend SD-WAN Visibility into the Branch and Campus

When VMware acquired Nyansa, this offered a unique opportunity to integrate Nyansa’s intelligent edge capabilities more closely with the industry-leading SD-WAN solution. One early result of this integration is that VMware Edge Network Intelligence can now use the VMware SD-WAN Edge to collect client transaction data, re-process it, and send that data to its analytics engine.

VMware SD-WAN already provides reliable, secure, and efficient access whenever client traffic traverses the SD-WAN solution. And, as the figure below shows, the VMware SD-WAN topology now extends to more places than ever—across branches, campuses, home offices, all the way to applications in the cloud. This means that VMware Edge Network Intelligence can now collect data from across this broader environment.

By combining VMware SD-WAN with VMware Edge Network Intelligence, you can extend your visibility beyond the SD-WAN edge and across the distributed enterprise.
VMware Edge Network Intelligence Deployment Options

How should VMware Edge Network Intelligence integrate into your environment? You have two deployment options:

- **SD-WAN integration**: As shown on the left side of the figure, if you use VMware SD-WAN, you can tightly integrate the solution with your SD-WAN. In this model, you use the VMware SD-WAN Edge appliance to perform data collection and analysis.

- **Standalone solution**: If you use another vendor’s SD-WAN, you can deploy VMware Edge Network Intelligence as a standalone solution, as illustrated on the right. In this model, you’ll use the VMware Edge Network Intelligence Crawler to collect data from your environment.

* Will be available with VMware SD-WAN R4.1

** On-Prem Analytics Engine is called Private Cloud Appliance
Inside the Standalone Solution Deployment

In the standalone deployment mode, you’ll deploy the VMware Edge Network Intelligence Crawler in your campus and branch locations. The Crawler application collects data from the wireless LAN, the WAN, network service transactions, and more.

The Crawler pre-processes this information and then sends on metadata to the VMware Edge Network Intelligence Analytics Engine. This analytics engine runs ML algorithms and performs the analysis to generate insights, which it then shares in the user interface. Typically, this analytics engine is hosted by VMware in the public cloud. However, if you prefer an on-premises deployment, you can deploy the analytics engine as a private cloud appliance.
Integrating with VMware SD-WAN

Today, more and more organizations are choosing to integrate VMware Edge Network Intelligence directly with VMware SD-WAN to gain deeper visibility, not just into the SD-WAN, but also extending into branch and campus locations.

In this model, the data collection capability is integrated into the VMware SD-WAN Edge solution, so a Crawler deployment may not be required. Deployed in branch and campus locations, as well as home offices, the VMware SD-WAN Edge solution unlocks additional capabilities and deeper visibility into client performance.

As part of the initial implementation, the VMware SD-WAN Edge communicates with the VMware SD-WAN Orchestrator in the cloud, and then uses zero-touch provisioning to implement VMware Edge Network Intelligence capabilities. Once the Edge solution is activated, it collects data inline, pre-processes it, and sends it as metadata to the analytics platform.
In following sections, we’ll examine some of the most important use cases in which your IT teams can benefit from VMware Edge Network Intelligence.

Across each of them, you’ll find the solution delivers two critical advantages:

- **Extending visibility:** Whether you use an SD-WAN from VMware or another vendor, VMware Edge Network Intelligence extends your visibility deeper into the branch and campus, all the way to the client device, to give you a clearer picture of the end-user experience.

- **Gaining deep insights through advanced analytics:** The advanced analytics engine at the heart of the VMware Edge Network Intelligence solution uses state-of-the-art AI and ML techniques to examine data from across your network and application stack. When integrated with VMware SD-WAN, that also includes measuring your SD-WAN hubs, VMware SD-WAN Edge appliances, and soon, diverse security services operating within the VMware SASE Platform.

Let’s take a closer look at how you can apply these capabilities to meet the most important challenges your IT teams face every day.
Application Assurance

Fundamentally, IT’s most important job is to make sure that users can access the applications and resources they need to do their jobs—reliably, with consistent performance and security. Edge Network Intelligence makes this task much easier. It identifies hundreds of individual applications, closely examines their packet data, and associates each application’s data with the many disparate data sources across your environment that could affect the user experience. In this way, IT gains a holistic understanding of application performance for every end-user and IoT device.

As noted, VMware Edge Network Intelligence starts this process by establishing a baseline for each application’s performance for each end user. Using this baseline for normal, expected behavior, the solution identifies any performance degradation as a deviation. The analytics engine quickly identifies any such anomalies, and then collects and correlates data from across your environment to determine why that deviation occurred. It presents these insights to your IT operations team in a simple, easy-to-consume way, so they can immediately take action to resolve the problem.
Optimizing Wireless and Wired End-Client Experience

As enterprise networks have evolved, wireless connectivity has become the dominant access method. This shift from wired to wireless access gives users much more flexibility, but also expands the list of problems that can arise to degrade the end-client experience. This is particularly true for home-based users, who may be relying on consumer-grade wireless LAN products outside IT control, which may not be configured optimally.

Whether connecting over wired or wireless access, there are many points where errors can occur, including:

- Attempting to acquire an IP address to DHCP
- Trying to resolve a hostname using DNS
- Attempting to authenticate using RADIUS
- Traversing the WAN to access business applications

VMware Edge Network Intelligence gives IT operations teams holistic visibility into steps in this process. It pulls data from across the network stack, correlates it, and ties it back to the individual end-client experience. IT gains a powerful tool to identify systemic issues that might be affecting the end-client experience, while help desk teams can now more easily troubleshoot problems when individual users need support.
Enabling Business Continuity and Work-from-Home Users

In 2020, every enterprise got a crash course on the importance of business continuity. When major disruptions happen, and IT teams suddenly find themselves supporting hundreds or thousands of users working from home, VMware Edge Network Intelligence can provide powerful capabilities to make this transition as seamless as possible. Now, IT has deep visibility into the client experience for these users and can help ensure they can work productively over home networks.

Change Verification and Return on Investments

The client experience baselines that VMware Edge Network Intelligence establishes can apply to more than just detecting anomalies. As noted, you can also use them to track historical performance trends from across your environment—Wi-Fi infrastructure, DNS, DHCP, and more—for each and every application you use. As a result, you gain a powerful, data-driven mechanism to evaluate changes to your network.

Whether you’re changing your infrastructure provider, updating business policy, altering a configuration in your wireless or firewall policy, or making any other change, you can clearly see the impact it has on end-client performance. And, you can do this on an ongoing basis for every new network investment you make. The ability to measure the effects of these changes in a granular, data-driven way can provide clear answers about whether the time and resources you’re investing are delivering the results you expect.
Isolating Faults and Getting Proactive Recommendations

As your network grows more dynamic and distributed, troubleshooting issues and identifying their root causes becomes far more complex. This is especially true when you adopt SD-WAN—adding a logical network overlay to your physical WAN infrastructure. Here, the combination of VMware Edge Network Intelligence with VMware SD-WAN can provide powerful new capabilities. Through this tight integration, VMware Edge Network Intelligence can collect data from across your SD-WAN: VMware SD-WAN Edges in the branch, hubs, gateways, and soon, SASE security and remote access services.

As clients access applications over various WAN links, whether hosted in the data center or the cloud, IT operations teams get deep insight into the client experience. If the solution detects any degradation in performance, it can examine data from every vantage point to understand which segment of the network is the source of the issue. Feeding that data into its analytics engine, the solution quickly identifies the root cause of the fault and provides actionable intelligence to IT in the form of proactive recommendations to correct the problem.
Building a Foundation for Self-Healing Networks

The close integration between VMware Edge Network Intelligence and VMware SD-WAN also provides a path towards the self-healing network. Today, the solution uses the SD-WAN data it collects to make recommendations to IT operations teams. In the future, it will be the VMware SD-WAN control plane itself making use of this data to take corrective actions autonomously. As it does, the system will once again feed data back to the analytics engine to measure the effects of those changes against the historical baseline, to determine whether the action taken is having the desired effect. If so, it can automatically apply that change globally across the network. If not, it can continue examining alternate means of alleviating the problem and begin the process again—all without human intervention.

Optimizing IoT Operational Assurance

In today’s distributed enterprise, the devices accessing business applications aren’t necessarily end-user clients. Increasingly, they are IoT devices, especially in vertical industries such as healthcare, manufacturing, and retail. For many enterprises, assuring consistent performance of these devices, as well as monitoring their behavior for potential security risks, is a business-critical priority.

VMware Edge Network Intelligence provides powerful tools to help both IT operations and security teams meet these objectives. The solution’s analytics engine establishes not only performance baselines for different categories of IoT devices, but behavioral baselines as well. If, for example, a hospital infusion pump suddenly attempts to communicate with an overseas DNS server it has never contacted before, VMware Edge Network Intelligence immediately flags that behavior and alerts the appropriate team.
Providing Targeted Insights to Vertical Markets

Around the globe, leading organizations in every industry are using VMware Edge Network Intelligence to optimize operations and assure consistent performance and security for end users and IoT devices. Often, that includes powerful, targeted use cases to address the unique challenges that businesses in those industries face every day.

Retail, Distribution and Manufacturing Use Cases

• Connect warehouses, distribution, stores and devices
• End-to-end visibility of clients, devices and robots
• Digitally transform the supply chain and measure ROI
• Drive digital transformation and customer engagement

General Enterprise Use Cases

• Full stack network analytics from client to application
• Eliminate blind spots, faster root cause analysis
• Improve productivity and operational efficiency
• Drive digital transformation and IoT initiatives
Healthcare Use Cases

- Inventory every IoT and medical device on the network
- Behavioral analytics and baselining
- Alerts for policy violations and behavior outliers
- Protect patient data and ensure regulatory compliance

Education Use Cases

- Satisfy diverse student and staff requirements
- Single source of truth for campus network health
- Seamless integration with IT service desk solutions
- Measure ROI of infrastructure CAPEX
Start Your AIOps Transformation

As your business and users become more distributed, your IT operations inevitably grow more and more complex. Now, you can harness the power of AI to make things simpler. With VMware Edge Network Intelligence, your IT operations teams can ensure consistent performance and security for every device, accessing every application, across your distributed environment.

Are you ready to give your operations teams the deep insights and holistic visibility they need to keep your business running productively? Contact your VMware account representative or visit: sdwan.vmware.com/products/edge-network-intelligence.