Cisco AI Network Analytics Overview

About Cisco AI Network Analytics

Cisco AI Network Analytics is an application within Cisco DNA Center that leverages the power of machine learning and machine reasoning to provide accurate insights that are specific to your network deployment, which allows you to quickly troubleshoot issues. The following figure and the information that follows describes the Cisco AI Network Analytics architecture:

*Figure 1: Cisco AI Network Analytics Architecture*
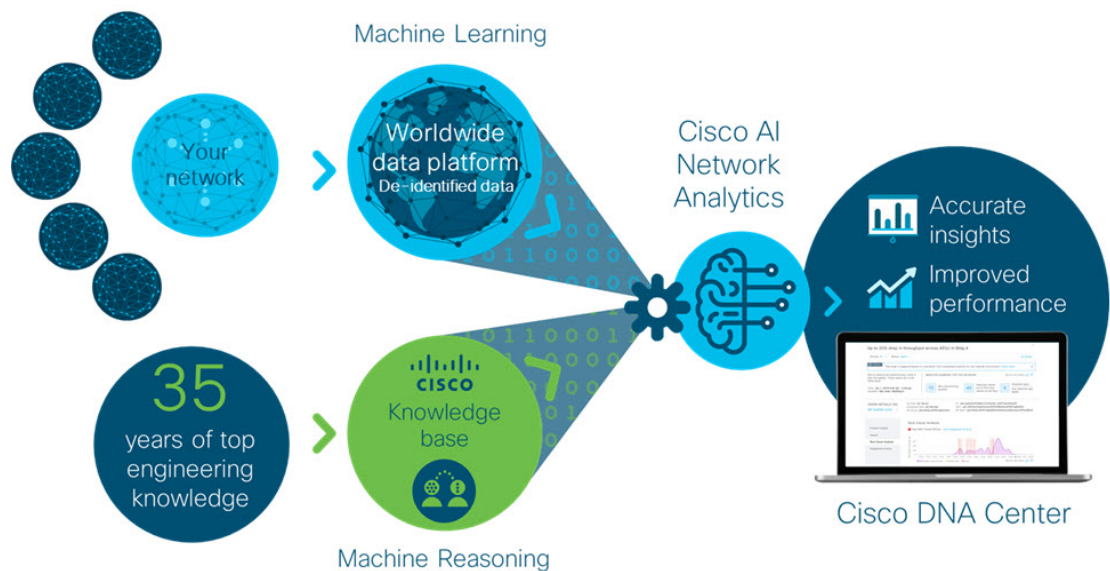
Cisco AI Network Analytics consists of the following:

- A worldwide cloud-based data platform where machine learning models are built and analyzed for your specific network environment.

- A machine reasoning inference engine that automates human expertise and captures the workflows in a knowledge base repository.

Machine Learning

Cisco AI Network Analytics leverages advanced machine learning techniques and an advanced cloud learning platform with deidentified network event data to identify critical issues in your network. Cisco AI Network Analytics provides a rich set of information so that you can quickly troubleshoot issues, know their root causes, identify trends and insights, and obtain relevant comparative perspectives. Cisco AI Network Analytics provides this value using a simple, intuitive, and powerful user interface within Cisco DNA Center that is fully integrated with Cisco DNA Assurance.

Figure 2: Cisco AI Network Analytics Features
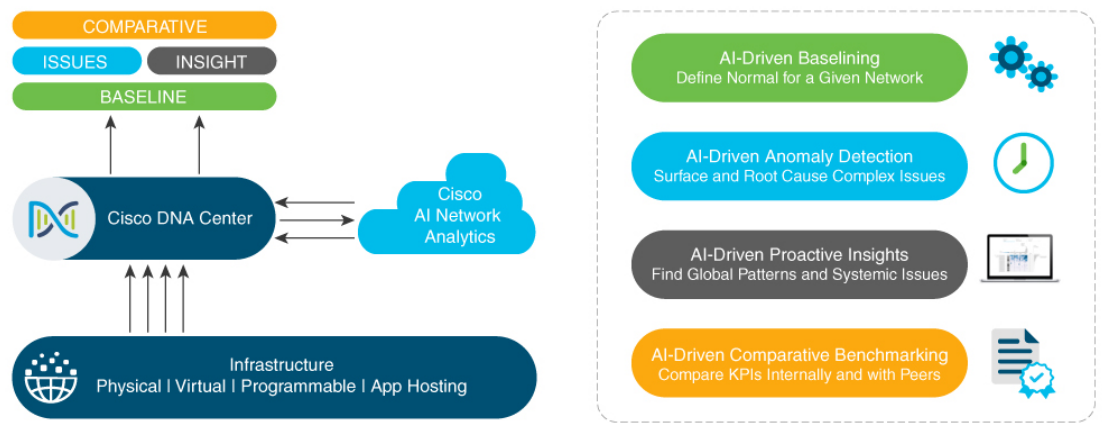
Cisco AI Network Analytics provides the following:

- **Cloud-Based Infrastructure**: Network events information is deidentified in Cisco DNA Center and sent through a secure encrypted channel to the Cisco AI Network Analytics cloud-based infrastructure. The Cisco AI Network Analytics cloud runs the machine learning model with such deidentified network event data and brings the issues and overall insights back to Cisco DNA Center.

- **Intelligent Issue Detection and Analysis**, which includes:

  - **AI-Driven Baselining**: Baselining is a method used to analyze network dynamics to extract behavioral patterns that help define what is the *normal* (baseline) behavior for that specific network. The actual network performance is then compared with that baseline.

    Cisco AI Network Analytics uses the most advanced machine learning techniques to define the baseline that is relevant to your specific network and sites with the current conditions. With this information, Cisco AI Network Analytics is able to define what is normal for each network and site at a specific moment, and identify the most important issues.

  - **AI-Driven Anomaly Detection**: Detect anomalies to determine their root causes and ease troubleshooting.

    Cisco AI Network Analytics can detect the following types of AI-driven issues:

- **Connection Issues** (onboarding issues): Excessive Time, Excessive Failures, Excessive DHCP Time, Excessive DHCP Failures, Excessive AAA Time, Excessive AAA Failures, Excessive Association Time, and Excessive Association Failures.

- **Application Experience Issues**: Total Radio Throughput, Media Application Throughput, Cloud Application Throughput, Collab Application Throughput, and Social Application Throughput.

- **Trends and Insights**, which includes:

  - **Trend Deviations**: Determine global patterns (trends) and deviations to provide system-generated insights.

  - **AP Performance Advisories**: Detect APs that have a consistently poor client experience, and provide a root cause and suggested actions.

- **Comparative Benchmarking**, which includes:

  - **AI-Driven AP Comparisons in Network Heatmaps**: Compare all of the APs in your network for a given month in a heatmap to spot trends and gain insights.

  - **AI-Driven Peer Comparisons**: Determine how your network is performing in comparison to your peer networks for a selected Key Performance Indicator (KPI).

  - **AI-Driven Network Comparisons**: Determine how a network (such as sites, buildings, AP models, client types) is performing compared to another network for a selected KPI.

Machine Reasoning

The Machine Reasoning Engine (MRE) is a network automation engine that uses artificial intelligence (AI) to automate complex network operation workflows. It encapsulates human knowledge and expertise into a fully automated inference engine to help you perform complex root cause analysis, detect issues and vulnerabilities, and either manually or automatically perform corrective actions. MRE is powered by a cloud-hosted knowledge base, built by Cisco networking experts.

Cisco AI Network Analytics Benefits

Cisco AI Network Analytics provides the following benefits:

- **More Visibility**: Each network is unique, with the network environment always changing. Cisco AI Network Analytics continuously collects the relevant data from the local networks, correlates the data against the aggregate de-identified data set, and then leverages sophisticated machine learning models to create baselines that are relevant to specific networks and sites. These baselines learn and adapt as the network environments change and as the devices, users, and applications evolve.

- **Greater Insight**: Cisco AI Network Analytics uses machine learning to correlate the immense amount of data that is coming from the network against the individualized network baselines, to uncover the issues that can have the greatest impact on the network. This improves issue relevancy. Cisco AI Network Analytics discovers trends and patterns in the network behavior, so that IT can identify issues before they become a problem.

- **Guided Action**: Cisco AI Network Analytics uses machine learning algorithms and automated workflows to perform logical troubleshooting steps, which enable an engineer to execute and resolve an issue. This helps IT detect issues and vulnerabilities, analyze the root causes, and quickly execute corrective actions.

Cisco AI Network Analytics Licensing and Deployment

Cisco AI Network Analytics is part of the Cisco DNA Advantage software license for Cisco DNA Center and is provided as an additional component that seamlessly blends in with the Assurance user interface. Cisco AI Network Analytics provides advanced machine learning-generated insights to issues, along with the visualization tools required for analyzing, troubleshooting, and reacting to the issues raised by the machine learning engines.

Deploying Cisco AI Network Analytics requires a working instance of Cisco DNA Center (which runs in an appliance form factor) as well as HTTPS connectivity to the Cisco AI Network Analytics cloud. HTTPS connectivity is also supported through a proxy server. If you use the proxy server for HTTPS connectivity, the settings are inherited from the Cisco DNA Center global settings. Network event data is deidentified before it is sent to the cloud. Results and insights are returned by the Cisco AI Network Analytics cloud services, and are displayed after decryption, directly into the Assurance user interface. For more information, see "Addendum 1 Cisco AI Network Analytics" in the Cisco DNA Center Privacy Data Sheet.

Cisco AI Network Analytics requires connectivity to the cloud infrastructure for storage and analysis. If you have less than 500 wireless APs, you can expect data usage of only 150-200 MB per day due to efficient encoding and optimization schemes. Data usage is proportional to network deployment size in terms of APs and wireless clients; therefore, larger deployments with 1800 APs have a data usage of 500-700 MB per day.

Supported Cisco AI Network Analytics Features on the Cisco Catalyst 9800 Series Wireless Controller

The following table lists the Cisco AI Network Analytics features that are supported on the Cisco Catalyst 9800 Series Wireless Controller and the minimum software version.

Cisco DNA Center Release	Supported Features	Minimum Cisco IOS-XE Software Version
2.3.3	- **Identification of Connection Issues**: Cisco AI Network Analytics can identify onboarding issues, such as excessive time, excessive failures, excessive association time, excessive association failures, excessive authentication time, excessive authentication failures, excessive DHCP time, excessive DHCP failures, and throughput issues. - **Identification of Trends and Insights**	16.12.1s