AvidThink®

Sponsored by ACCEDIAN now part of CISCO | CISCO

Intent-Based Assurance

Ensuring end-to-end service quality at scale

RESEARCH BRIEF

Table of Contents

Research Briefs are independent content created by analysts working for AvidThink LLC. These reports are made possible through the sponsorship of our commercial supporters. Sponsors do not have any editorial control over the report content, and the views represented herein are solely those of AvidThink LLC. For more information about report sponsorships, please reach out to us at research@avidthink.com.

About AvidThink®

AvidThink is a research and analysis firm focused on providing cutting-edge insights into the latest in infrastructure technologies. Formerly SDxCentral's research group, AvidThink launched as an independent company in October 2018. AvidThink's coverage includes 5G infrastructure, private wireless, edge computing, SD-WAN, SASE, SSE, ZTNA, cloud and containers, SDN, NFV, and infrastructure security. Our clients range from Fortune 500 enterprises and hyperscalers to tier-1 communications service providers, fast-growing unicorns, and innovative startups. AvidThink's research has been quoted by the Wall Street Journal, Light Reading, Fierce Telecom, Fierce Wireless, Mobile World Live, and other major publications. Visit AvidThink at avidthink.com.

RESEARCH BRIEF

Intent-Based Assurance

Ensuring end-to-end service quality at scale

Introduction and Background

Global events in the past few years have highlighted the importance of connectivity. Communication service providers (CSPs) and infrastructure providers worldwide continue to invest in soon-to-be ubiquitous 5G wireless infrastructure, fiber build-out, subsea cable runs, and low-earth orbit (LEO) satellite launches — all in service of increasing the connectedness of people and devices.

Meanwhile, enterprise IT departments struggle to securely connect growing numbers of devices and people across multiple locations — employees, contractors, partners, customers, and visitors. The mandate to support work from home (WFH) and work from anywhere (WFA) has expanded the enterprise footprint from campuses and branch offices to field locations, public and private clouds, and home and mobile offices.

This exploding number of network elements and connections that require management and maintenance show no signs of abating (Cisco estimates near 30B networked devices by the end of 2023 [1]).

As a result, network managers and operators urgently need to improve manageability and increase scalability even as they try to rein in capital and operational expenditure. At the same time, enterprise and CSP network providers must meet quality-of-service (QoS) and quality-of-experience (QoE) expectations, making service assurance a critical capability that needs to be built in parallel with their networks. For CSPs in a competitive arena, the reliability of connections and quality of the end-user experience differentiate one provider from another.

While traditional network management and orchestration solutions have served network operators well, the upcoming scale of managed elements and new requirements will exceed the capabilities of legacy frameworks.

Intent-based frameworks have been touted as a solution to managing network complexity. However, network operators are at the beginning of this journey. Networking vendors are, likewise, early in the innovation cycle. This AvidThink research brief will examine intent-based networking, focusing on intent-based assurance — a less-covered topic. Our goal is to support and educate IT and networking leaders by providing an understanding of the intent-based approach to assuring user and application experience while meeting service-level objectives (SLOs) and service-level agreements (SLAs).

Why Intent and Why Now?

While traditional network management and orchestration solutions have served network operators well, the upcoming scale of managed elements and new requirements will exceed the capabilities of legacy frameworks. New demands are driven by several ongoing trends:

- **Internet of everything and business digitization** — We touched on this in the introduction. Businesses and consumers appreciate the value of increased digitization — better automation and productivity, improved experiences, deeper insights, and opportunities to optimize businesses. This digitization of everything drives increased data generation and consumption, and along with that, a need for connectivity to everything, everywhere, to carry that data where it can provide the most insight and value.

[1] Cisco Annual Internet Report 2018-2023

- **Increased sophistication of services** — Basic connectivity is no longer what customers purchase. The days of buying a simple fixed circuit from point A to B and waiting weeks or months for provisioning are over. Software-defined wide-area networks (SD-WAN), secure access service edge (SASE) and security service edge (SSE), private backbones with strict QoS SLAs, and 5G fixed wireless access (FWA) are among the new breed of services enterprises, and consumers are purchasing, with a more complex solution stack and many more elements to coordinate.
- **Increased customer expectations for end-to-end services** — As enterprises and consumers depend on consistent connectivity for running their businesses, and their lives, the expectations placed on networks staying healthy have increased. The performance of business-critical and life-essential SaaS apps, cloud-based storage, and streaming video is essential to end-users. As a result, timely issue reporting, automated fault detection, and fast remediation have become table stakes for connectivity offerings.
- **Network virtualization and disaggregation** — Ten years ago, spurred by the success of virtualization and disaggregation in the enterprise IT space, carriers embarked on an ambitious plan to virtualize their networks. This virtualization and disaggregation of monolithic single-vendor hardware appliances into software network functions running on commercial off-the-shelf hardware platforms (x86 or Arm) resulted in an expansion of the number of elements that require management and orchestration, many with non-standard interfaces.
- **Investor push for lower operational expenses and healthier profits** — Even as carriers continue to invest in 5G and fiber infrastructure, investors and the markets demand lower costs and increased profitability. Enterprises feel a similar squeeze with capital becoming more expensive in today's economic climate. Lower expenses provide companies with increased flexibility and long-term viability. As crucial as connectivity is, cost-efficient connectivity is even more critical.

With these trends, legacy human-driven network management no longer works. Even humans augmented with traditional network automation will struggle to manage the scaled-up real-time monitoring and configuration needed to address failures or optimize the network as conditions change.

Networking experts across the industry believe, and we concur, that an intent-based system is the best solution to addressing these issues. Intent-based systems are superior in managing, optimizing, and maintaining large-scale complex networks. For readers who need a primer in intent-based networking, we refer you to the Appendix at the end of this reseach brief.

Previously, the technology maturity to build autonomous intent-based solutions was not present. With recent rapid advances in AI/ML, data management, analytics, and software-defined architectures, the situation has changed.

The Era of Intent is Now

Intent-based frameworks began with the policy-driven network systems of the early 90s and took on new life at the beginning of the software-defined networking (SDN) movement in the early 2010s. Despite its long history, intent-based solutions have seen limited commercial deployments.

Previously, the technology maturity to build autonomous intent-based solutions was not present. And instrumentation and availability of network telemetry were challenging. However, the situation has changed with recent rapid advances in data management, analytics, software-defined architectures, and especially AI/ML.

In domains such as data center switching, enterprise WiFi, and enterprise WAN, we see AI/ML used to detect network anomalies and even auto-remediate common issues. AvidThink, and other networking experts in the industry, believe networking software vendors now have sufficient capability to build sophisticated and intelligent intent systems.

For example, with WiFi, enterprises can define service quality with prioritization. AI/ML systems can then use real-time telemetry to configure and fine-tune WiFi access points and controllers to maximize performance for select enterprise applications or devices serving critical functions.

Likewise, as described earlier, advanced SD-WAN controllers can translate the intent of connecting a set of branch locations with a minimum QoS into a set of configuration commands. These commands are applied to each site's network routers and customer premises equipment to achieve the desired goal.

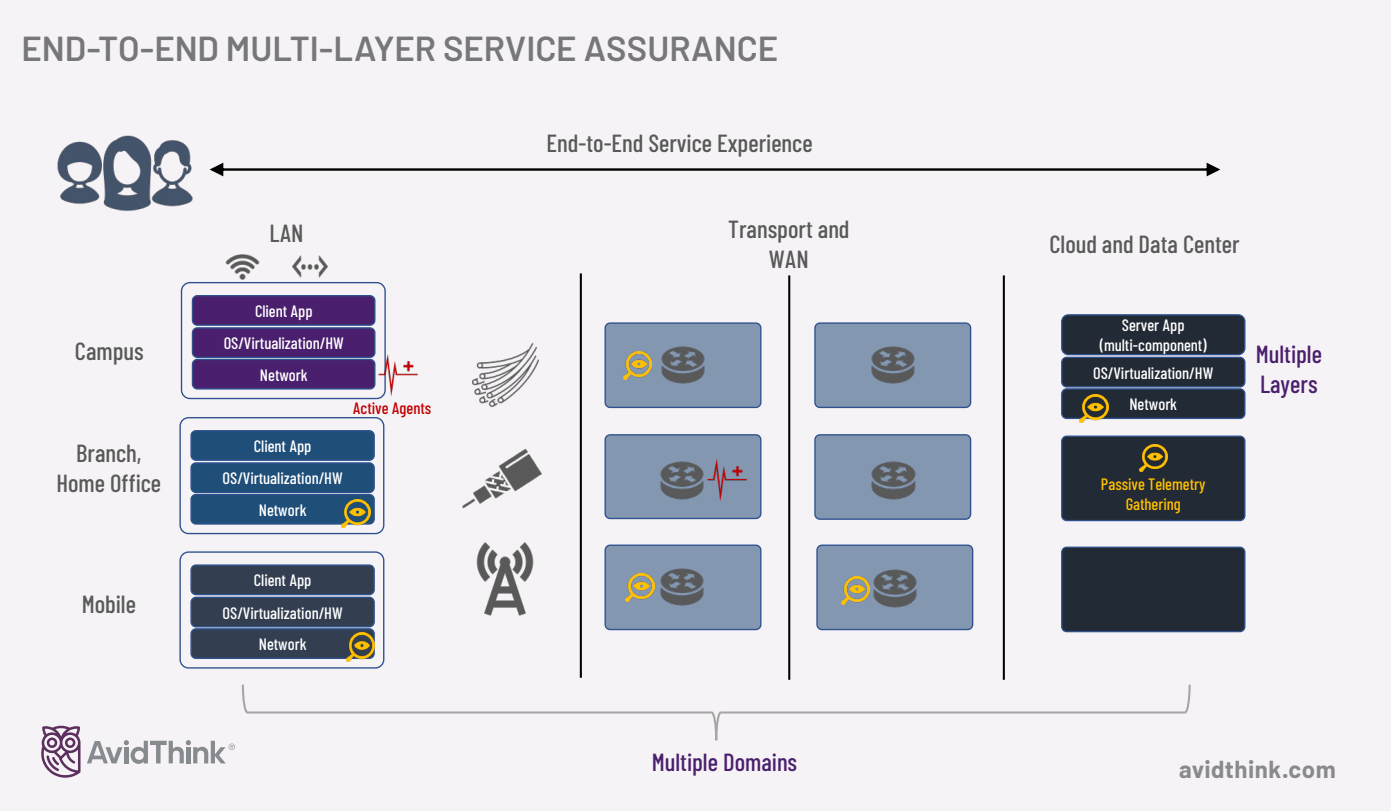
While many networking vendors focus on the provisioning and fulfillment functions associated with intent-based networking, there's less discussion around assurance. We'll address that shortly but first, let's visit the topic of assurance today.

State of Service Assurance

We touched on the evolution of service expectations earlier — enterprises and carrier customers no longer want to interact with infrastructure services in a piecemeal manner. Services must be provisioned and presented as end-to-end, spanning domains (local area, wired and wireless access, transport, and data center networks) and up and down the stack (network and application). Service assurance must also support end-to-end, multi-domain, and multi-layer (full stack) capability, accommodating physical, virtual, private, and public infrastructure.

Unfortunately, cross-domain visibility can be challenging to achieve because of organizational boundaries and the ability and willingness of carriers and cloud providers to share network and other telemetry data on a per-customer, network segment, tenant/instance basis.

Historically, service assurance has leaned on **passive** techniques involving placement of sensors and gathering of telemetry information from the various network and computing elements (routers, switches, virtual agents hosted at critical locations) and using analytics to pull together a picture of network health, correlating performance events to the underlying traffic streams. Due to restrictions on probe placement and access to telemetry data, many assurance systems have added **active** techniques involving injecting synthetic transactions that mimic real-world interactions and measuring the outcomes to determine performance.



Today's service assurance solutions use the combination of information from active and passive systems to determine the quality of a service end to end (from a network connection to an application connection). The result can be tracked against SLOs or SLAs or checked against historical trend data to ensure that unusual degradation in service has not occurred (even if it doesn't yet violate an SLO or SLA).

Challenges with Service Assurance

Even with advances in service assurance technology, enterprises and carriers must put in significant effort to assure an end-to-end service today, placing sensors in various network locations and on systems to provide telemetry and install agents that can perform active testing from different locations. While many network elements have transitioned from physical to virtual, requiring less physical placement of hardware sensors, there are still multiple challenges network operators face today:

- **Manual and static instrumentation** — Service assurance systems today require network engineers to activate telemetry on networking elements and decide where to place sensors and agents to capture the relevant data streams. Even with the virtualized and programmable network infrastructure of today's modern networks, the instrumentation is often a manual operation.
- **Supporting dynamic and scalable networks** — Related to the first point, if a network is reconfigured (as SDNs and virtualized networks are likely to be), the service assurance sensors and agents must be reconfigured and reinstalled. The service assurance system will also have to be reconfigured appropriately. And with autoscaling applications that instantiate new virtual machines or containers on additional servers or in new locations, the assurance sensors and agents must be inserted as the network dynamically scales to these new instances.
- **Translation of raw telemetry into KPIs and experience measures** — Even after telemetry from the network elements streams into the service assurance system, network engineers have to configure these data streams to map to key performance indicators (KPI) and relevant user experience metrics. Raw metrics like packet loss, jitter, delay, and round-trip times are meaningless without application context. End-to-end assurance is impossible without understanding the impact on user experience — this is yet another manual configuration task for the network engineer.
- **Disconnect between network automation and network assurance** — The success of intent-based systems requires tight coupling between an intent-based provisioning system built on top of network automation and the output of an assurance system. To the extent that the assurance system can provide the necessary context to support the remediation of any network issues, it closes the automation loop and enables an end-to-end intent-based network system.

Intent-Based Assurance

The past focus of intent-based networking discussions has been the provisioning and fulfillment capabilities. Leading network vendors describe how an intent-based system can help auto-configure multi-site WAN setups across branch locations and leaf-spine switches in a data center. Similarly, zero-touch provisioning (ZTP) using declarative configurations is in vogue in enterprise and carrier networks.

Yet we gloss over the assurance systems that monitor and keep the services running. These assurance systems can feed into a closed-loop system that auto-remediates or that intelligently knows when to alert network operators upon service degradation and violation of SLOs/SLAs for human assistance.

Whether playing a role as part of an intent-based system or integrated with an existing network automation system, an intent-based assurance solution can add immediate value to today's networks.

Whether playing a role as part of an intent-based system or integrated with an existing network automation system, an intent-based assurance solution can add immediate value to today's networks.

What is Intent-Based Assurance

When we defined intent-based networking, we showed how a top-level intent declaration is translated into a set of policies and rules that drive a provisioning/fulfillment system and govern an assurance system that monitors the services, providing ongoing verification and visibility into the quality of that service. The assurance system, as described, is intent-based. It is critical in detecting degradation and initiating remediation operations.

Key capabilities of this intent-based assurance system include:

- Taking a **service model definition** and figuring out the network elements that comprise the service model, the topology, and the required configuration to assure this service.
- Understanding **where to place** the appropriate sensors (to gather telemetry) and agents (for active assurance) and deploying them.
- **Mapping** of the **telemetry data** to session and application-aware KPIs that reflect the quality of service and experience.
- **Setting** appropriate **triggers** so that the system is alerted if KPIs violate or are at risk of violating (using predictive alerting) SLOs or SLAs.
- **Sending alerts** in real-time to an intent-based orchestration or SDN controller system to provide rapid remediation actions.

Benefits of an Intent-Based Approach to Assurance

At the highest level, the benefit of an intent-based assurance system is the avoidance of multiple manual steps in enabling monitoring and remediation for network services. This translates to the following benefits:

- **Faster time to deployment of assurance** — Without an intent-based system, it will take network engineers time to figure out where and how to configure sensors and agents and map telemetry data to KPIs.
- **Reduction in costs** — By reducing the amount of manual effort and potentially detecting SLO/SLA violations earlier and mitigating them (avoiding financial penalties), intent-based assurance can reduce the operational costs of maintaining network services.
- **Agility and greater scalability** — An intent-based assurance system that tracks dynamic network provisioning adds assurance as the network is built out, providing automatic scalability.
- **Increased intelligence in assurance** — An intent-based assurance system can understand the appropriate behavior of a service and, by leveraging AI/ML for predictive analytics, provide warnings of potential service degradation. Likewise, the system can learn to auto-remediate failing (or soon-to-fail) network services.

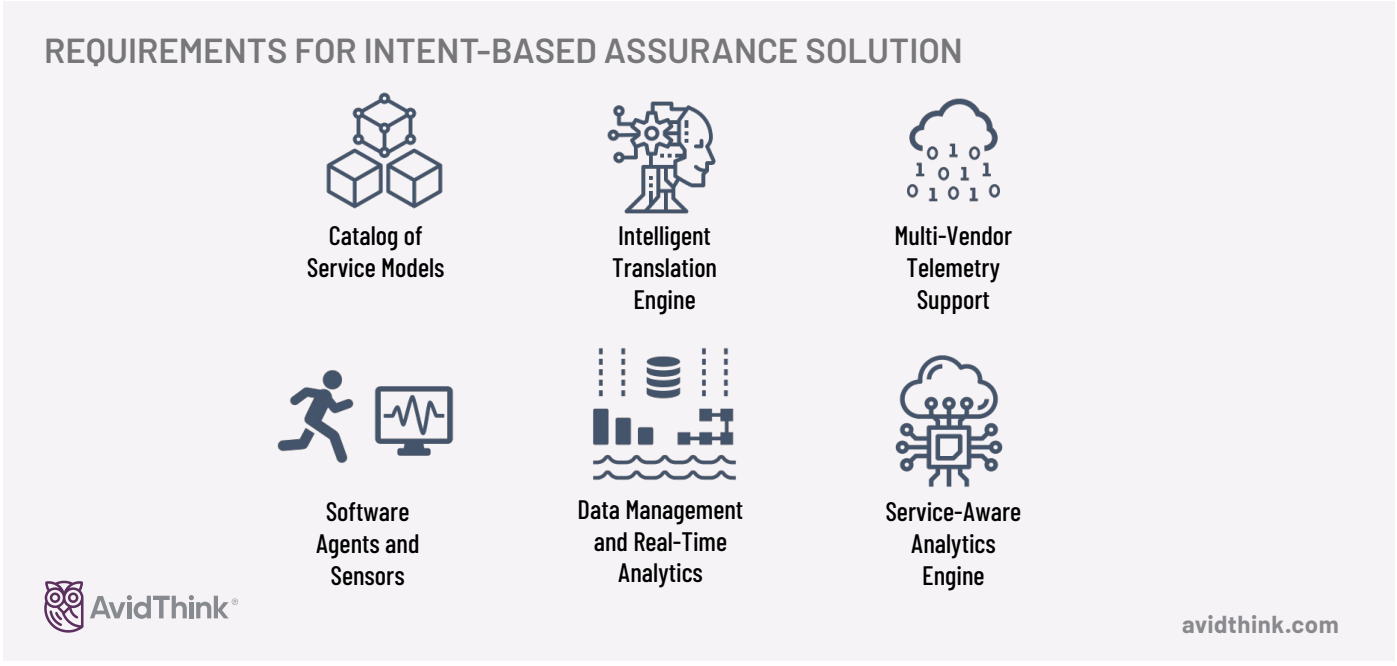
Even in a rudimentary intent-based network system, where automated provisioning and fulfillment are limited in scope (e.g., not all domains or services are yet supported), intent-based assurance can accelerate the configuration and deployment of service-level monitoring. Deploying this next-generation of assurance adds value by providing automated placement of probes and agents, configuring telemetry on routers (e.g., TWAMP/Y.1731), creating service-relevant KPIs, and automate monitoring of SLOs/SLAs. This frees up network engineers from time-consuming tasks and helps the organization take a big step forward towards an end-to-end intent-based network.

Requirements for Next-Gen Intent-Based Assurance

Intent-based assurance is evolving. Early commercial solutions show promise and have demonstrated significant value for the domains and services models that they support.

These commercial solutions typically include the following vital components necessary to support an intent-based system:

- **A growing catalog of service models** — As we explained earlier, the key to intent-based networking and intent-based assurance as a subset is the richness of the service model. The model captures the critical parameters of a network service, such as the endpoints, any constraints, optimization goals (e.g., costs, performance, resilience), target SLOs/SLAs, and a notion of the type of service (and the corresponding measure of the quality of experience).
- **Intelligent translation engine** — The intent-based assurance system needs to translate the service model into some capture of the network topology, the participating network elements, what agents and sensors to use, and where to place those elements. It also needs to figure out relevant active tests to run that are a close proxy of the service. Finally, it needs to prepare the telemetry store and analytics algorithms to be used, along with the KPI calculations and trigger rules for warnings.
- **Rich telemetry facilities supporting multi-vendor elements** — Many networks are multi-vendor and contain diverse elements. The intent-based assurance system will need to support a wide range of telemetry types and be able to configure the appropriate schema to consume relevant data streams from multiple network elements.
- **Software agents and sensors** — While it's not necessary that the provider of the intent-based assurance system supply their software agents and sensors, it's practical and ensures fast deployment and compatibility of data streams. Until standards form around intent-based assurance and standardized APIs for software agents, organizations will likely purchase full-stack assurance solutions from a single vendor for expediency and efficacy.
- **Scalable data management** — Intent-based systems have to consume a lot of telemetry and perform fast processing on the data set. Vendor-supplied data management and analytics pipeline are thus a key component, and the pipeline's performance will impact the speed of system response to network events.
- **Smart service-aware analytics engine** — Whether big data analytics or newer AI/ML models, translating telemetry into KPIs and then into service- and context-aware user experience ratings requires smart analytics capabilities.



Journey to Intent-Based Assurance

Today, much of the service assurance in enterprise and carrier networks are semi-automated, with the manual deployment of sensors and agents, the semi-manual configuration of telemetry streams on multi-vendor network devices, and manual mapping of telemetry to KPIs. While enterprises have some network automation systems rolled out, closed-loop network automation systems (not yet intent-based) are present in a few leading carriers and large enterprises.

Closing the Gap

To accelerate the journey to intent-based fully-autonomous networks, the push needs to come from multiple parties — first, the enterprises and carriers, who need to demand that their networking vendors and partners drive towards intent-based frameworks, which will scale better, be more cost-effective, and allow the organizations to provide better network services to employees and customers.

Likewise, networking equipment providers and independent software vendors must drive faster toward intent-based systems and invest more in AI/ML. The complexity and scale of today's networks can no longer be managed by humans alone, and customer expectations of service quality continue to rise. Intent-based networking is the strongest candidate to solve today's network management and automation challenges.

Strategies to Get Started

For enterprises and carriers looking to start their journey towards intent-based networking and service assurance, the **first step** is to **evaluate** their **existing networking and assurance vendors** to determine their plans and roadmap for such capabilities. **Benchmarking** preferred vendors against other vendors offering such capabilities would be a close **second step**. Even for communications service providers with extensive resources, intent-based systems can be complex and require specialized expertise, not to mention a deep understanding of autonomous systems and AI/ML. Networking vendors have the incentive to build specialized in-house capabilities. The vendors can gain higher leverage and a better investment return in developing intent-based systems than other parties. Our recommendation to carriers and enterprises is to find the right vendor partner instead of building in-house.

Nonetheless, commercial end-to-end intent-based solutions are not yet mature, and we recommend **trialing solutions in a small domain** as the **third step** in getting started. Once the service model is robust and the outcome matches the enterprise's needs, the service can be rolled out across more domains in a final step.

We urge prudence and suggest monitoring any autonomous remediation capability, especially those directed by AI/ML. Remediation decisions can occasionally (but rarely) generate unexpected and hard-to-explain decisions. Nevertheless, cautious vendors may have already put guardrails and governors in place to prevent runaway systems. For each new service model shipped by vendors, pilot deployments should be repeated, and system performance carefully re-assessed.

Closing Thoughts

Intent-based assurance is a critical component of intent-based networking systems. Comprehensive intent-based end-to-end networking systems spanning multiple domains and layers are still evolving.

However, intent-based assurance can add value even with today's automation solutions. Intent-based assurance solutions that provide the right combination of service models, intelligent translation engines, and powerful analytics engines enable organizations to cost-effectively manage their end-to-end network services and bring assurance to their customers.

AvidThink believes there is an urgent need for networking system providers and independent software vendors to invest in this technology to match the increasing complexity of today's networks and customer expectations of service quality. Enterprises and carriers should start evaluating now and take steps to pilot the technology in their networks.

As with all our reports, AvidThink appreciates and welcomes feedback from our readers. We can be reached at **research@avidthink.com** and would love to hear from you.

Accedian Skylight Intent-Based Assurance Solution Review

Introduction

Accedian is a performance analytics and end-user experience solution company, building products to help its customers assure digital infrastructure. Accedian was established in 2004 and is headquartered in Montreal, Canada. Customers include leading global communications service providers and enterprises worldwide.

Accedian's solutions are built on their Skylight performance assurance platform providing end-to-end network, application, and service performance visibility, spanning user and device edge to core networks and the cloud. As a comprehensive assurance solution, Skylight combines Accedian's software and hardware sensors with its orchestration and analytics layers to provide performance monitoring, visualization and insights via customizable dashboards and end-user portal views.

Intent-Based Assurance with Accedian Skylight

Accedian recently launched intent-based capabilities on the Skylight platform. As part of Accedian's go-to-market plan, it has **integrated Skylight's intent-based assurance with Cisco's Crosswork Network Automation platform**.

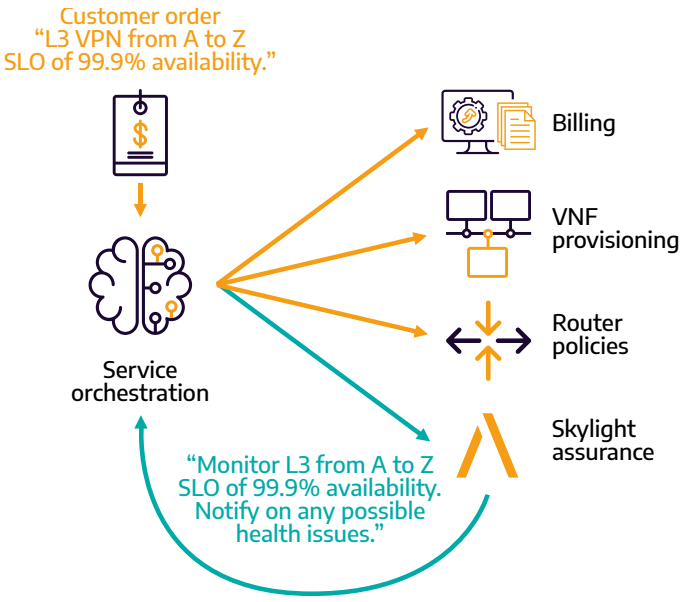
Accedian continues to leverage its performance sensors in its intent-based assurance suite. These sensors are available in VM and container form factors for software and in hardware as low-cost small-form-factor pluggable (SFP) sensors or modules with embedded FPGAs for strategic placement in networks where no native assurance capability is available or where additional functionality, accuracy, and precision is needed.

Likewise, Accedian's full suite of multi-layer, standards-based, on-demand or continuous tests are utilized in their intent-based offering to provide end-to-end and per-segment performance metrics.

Skylight's New Intent-Based Capabilities

To support intent-based assurance, Accedian has added three main sets of capabilities to Skylight:

- Given an input model that describes a service, Skylight can figure out how to instrument the network to provide assurance for the service and automate the placement, deployment, and configuration of instrumentation with sensors.



Source: Accedian

As part of this research brief, the sponsor, Accedian, has requested that AvidThink provide an independent review of its solution. AvidThink conducted this review using the information provided by the sponsor and AvidThink's market research on intent-based networking and assurance. AvidThink has not verified the sponsor solution's features and capabilities. Readers interested in the sponsor's solution should ascertain the veracity of vendor claims themselves. AvidThink cannot be held liable for any unexpected or incorrect operation and damages due to any inaccuracies listed here.

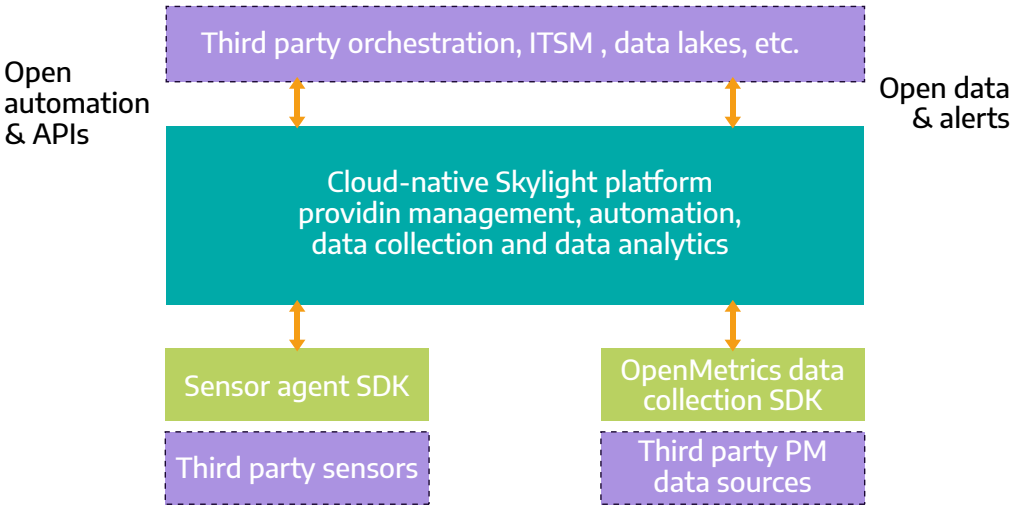
- Skylight can understand how a service should behave, create the KPI metrics relevant to maintaining appropriate QoS, track those metrics, detect when the service has an issue, and inform a companion orchestration system to trigger remedial action and optimization.
- Accedian has added APIs for provisioning intent-based assurance and has also built integration back into network automation controllers for streaming data and alerts.

With these additions, Skylight can provide the assurance input as part of an autonomous closed-loop system that adapts to potential service degradation or any potentially user-impacting trends or behavior and drives auto-remediation.

Skylight Platform Enhancements Details

Accedian's Skylight platform includes the following new and enhanced features:

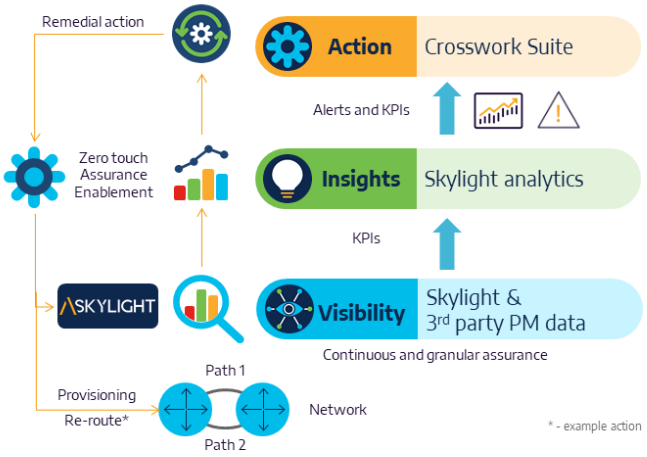
- **Provisioning:** REST, RESTConf/YANG API interfaces for provisioning intent-based assurance.
- **Service Modeling:** Skylight can take incoming models and build templates for service activation to support intent-based assurance. Using incoming input on the type of service, connection points, and target service level objective (SLO), Skylight can determine which sensors and reflectors to use, which sessions to provision in its orchestrator, and then pre-provision metadata in its analytics user interface that reflects the appropriate KPIs and alert triggers.
- **Events and Visibility:** MQTT/Kafka/RESTConf/gNMI APIs to send data and events from the platform to an external system.
- **Open-standards Monitoring:** Support for OpenMetrics, an open standard for data ingestion from Linux Foundation's Cloud Native Computing Foundation used by the popular Prometheus open-source monitoring system.
- **Analysis Engine Upgrade:** A streaming analytics and machine learning system to analyze, correlate, and find anomalies in the data.
- **User Interface Enhancements:** An updated user interface for internal customer troubleshooting and external end-user portals.
- **End-to-end Intelligence:** Skylight can use its intelligence to combine measurements from multiple sources to create end-to-end KPIs and service views when an end-to-end metric is unavailable via any other native method.



Source: Accedian

For integration with Cisco Cisco Crosswork Network Services Orchestrator (NSO), Accedian Skylight now supports:

- Accedian NSO Network Element Driver (NED) with support for RESTConf to interface with Skylight to automate provisioning from NSO, and also alerts back to NSO to drive closed loop automation use-cases.
- Cisco Crosswork Data Gateway (CDG) integration via gNMI interface to feed data into Cisco Crosswork Network Controller for additional visibility into CNC network and service health.



Source: Accedian and Cisco

Assessment of Skylight for Intent-Based Assurance

To understand how Accedian Skylight measures up as an intent-based assurance system, we'll examine it through the lens of high-level capabilities in the main research brief:

- **Service model decomposition**: Skylight can take a service model definition (in RESTConf/YANG) of supported services, figure out how to instrument the network elements with its sensors, create a list of sensors required, along with metadata configuration for analytics KPI and alerts.
- **Network instrumentation:** Skylight supports automation of network instrumentation and zero-touch provisioning to easily deploy Skylight into the network.
- **Mapping to application-aware KPIs:** IIn the service model decomposition step, Skylight generates the session configuration and metadata needed to appropriately monitor the sessions in its dashboard.
- **Detection and alerting:** Skylight can alert consumers using its assurance data stream (e.g., via Cisco NSO) based on fixed SLAs or on anomalies and predictive intelligence.

And when we look at the components-level view of Skylight as laid out in the brief, we observe:

- **Growing catalog of service models:** It's all about the models and their sophistication and richness. Skylight supports end-to-end topologies today with mesh, hub and spoke, and other more complex capabilities in the future.
- **Intelligent translation engine:** Skylight has the foundational capabilities to translate the service model into sensor configuration and placement, session context, and metadata for KPIs and alerting.
- **Rich telemetry facilities supporting multi-vendor elements:** Accedian's use of standards-based telemetry and support for different types of incoming data allows it to support multiple networking vendors. As an established player in the assurance space, most Accedian customers today successfully use their products in multi-vendor networks.
- **Software agents and sensors:** While Accedian can integrate third-party sensors and agents into its platform, it also provides its software and hardware sensors, reducing integration hassle and time to deployment.
- **Scalable data management and real-time data analytics:** Skylight is a proven system deployed at tier one service providers collecting and analyzing data from millions of objects.
- **Powerful analytics engine:** Accedian has a capable analytics engine today as part of Skylight that is deployed at customers for service failure, degradation detection, and anomaly detection in performance and security. We expect this will be an area of continued investment for Accedian to improve the richness of services it can support and predictive events that it can spot.

Review Wrap-Up

Accedian Skylight's enhanced platform shows what intent-based assurance systems can bring to customers — reduction in time to deployment for assurance, reduced manual intervention, and autonomous creation of service-aware KPIs and alerts.

Skylight's integration with the Cisco Crosswork Network Automation suite gives them a credible and expansive go-to-market motion. It brings value to Cisco customers using Crosswork by enhancing the intent-based capabilities of that platform.

In our networking industry, intent-based systems are in their early days. AvidThink expects rapid innovation in this space as models become more sophisticated and the catalog of supported services grows. Still, even at launch, Accedian Skylight already provides value for customers with a strong promise of what's to come.

Intent-Based Networking Primer

What is Intent-Based Networking?

Legacy network management involves issuing directives on a network device's command-line interface (CLI). Network engineers would repeat similar commands across multiple network elements, taking them from their current state to the desired state. This manual activity evolved into basic automation through scripting, which graduated into reusable libraries, then templates with run-time variable replacements, and eventually morphing into sophisticated network automation software.

However, much of traditional network automation software relies on an **imperative** framework: issuing sequential network device commands, sometimes with conditional branching, but a stepwise command-by-command approach nonetheless.

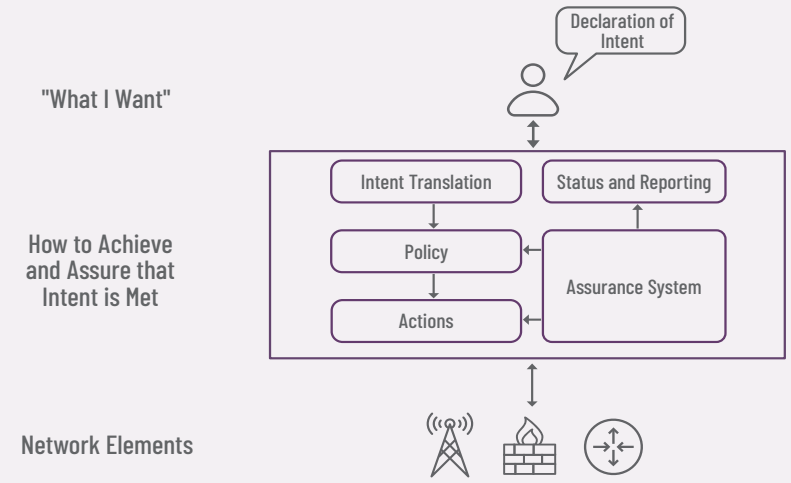
Intent-based networking approaches the network automation problem differently. Intent-based systems describe the "what" that should be achieved, not "how" that goal should be achieved.

The Self-Driving Network

Networking experts use autonomous self-driving vehicle examples to explain intent. Instead of giving a vehicle explicit step-by-step commands such as turning the steering wheel right or left, accelerating, or braking, an autonomous vehicle is only given its destination. The autonomous vehicle, equipped with artificial intelligence and machine learning (AI/ML), determines "how" to drive to that destination independently.

This method of defining the end state and letting the system work out how to get there is termed a **declarative** approach. While the directives into an intent-based network are simple — e.g., connect locations A, B, and C securely, with a minimum bandwidth of 1Gbps, optimizing for cost, and ensuring no connections exit the United States — the amount of technology and sophistication of AI/ML under the hood to implement this is significant.

Basic Intent-Based Networking Framework



Achieving Intent

The formalization of intent can take different forms. Networking and independent software vendors (ISVs) who claim to support intent-based solutions will have their specific intent solution architecture. Many intent frameworks tend to look like the diagram above.

The intent directive (expressed in human/business language) on top will be translated into a set of policies or rules that can be enacted on all the elements in a network. In parallel, an assurance subsystem monitors the network for policy violations and can trigger the system to remediate issues autonomously.

As the system operates, the intent can be changed and updated, resulting in a regeneration of the intent model and updated policies, including for assurance. AI/ML is typically employed in translating business directives to network rules and policies. Similarly, AI/ML can be leveraged as part of assurance to keep the system compliant with the intent.

Note that intent is network-agnostic and domain-agnostic. When engineered correctly, it can universally be applied across 5G wireless, wired fiber, data centers, and even satellite networks. Also, intent-driven systems are constrained by data models — they can't generate new actions or invent network capabilities not encoded in the model. We want to emphasize the importance of the data model because it dictates the sophistication of the intent framework.

Hopefully this provides you with enough context around intent-based networking to appreciate the importance of intent-based assurance as discussed in the main research brief.

AvidThink, LLC
1900 Camden Ave
San Jose, California 95124 USA
avidthink.com

Rev B