Nova Active

Critical QoS and QoE insight

Table of contents

Networks have changed, customers haven't

Today's networks are becoming more difficult to operate effectively. Operations teams are squeezed between increasing complexity, new technologies, shrinking budgets and the pressure to deliver new and differentiated services, faster.

But the customer still expects a flawless quality of experience (QoE) and will punish carriers who don't deliver. It's never been easier to switch networks and customer loyalty is short lived.

The average customer churn rate for mobile operators is 25% per year. Customer acquisition is the second largest expense, behind the network itself.[1]

To address this challenge, service providers are digitally transforming themselves to embrace automation, machine learning and artificial intelligence to support their operations' needs.

Highly scalable QoS and QoE visibility is essential for delivering a flawless customer experience—but it needs to be more than just key performance indicators.

The key to making performance data actionable is putting it in context with network, service and business drivers.

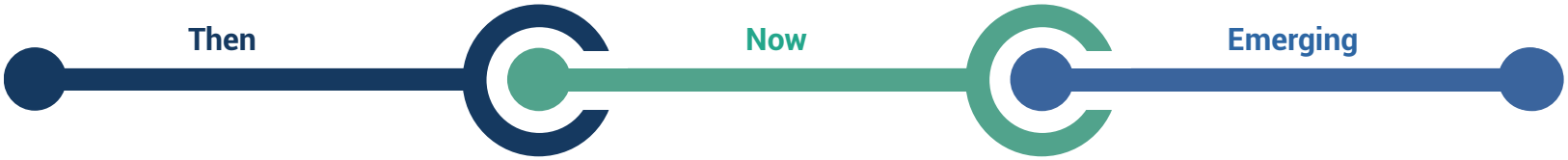
What's required is the ability to instantly detect, diagnose and resolve issues impacting data, voice, IoT and streaming video service QoE.

1. Quotient Consulting and Ipsos 2019

Active assurance is changing

The scope of active assurance is changing to address the emerging needs of virtual or cloud-based networks and 5G services. A changing service mix, more stringent latency requirements, dynamic network and service topologies, and hard to detect service degradations are some of the key drivers behind this change.

What's emerging is an ecosystem of solutions focused on visibility into the customer's QoE—delivering the right actionable insight (results) rather than alarms and KPIs



L2/3 End-to-end transport

L2/3 End-to-end transport

L4/7 Application

L2/3 End-to-end transport

L4/7 Application

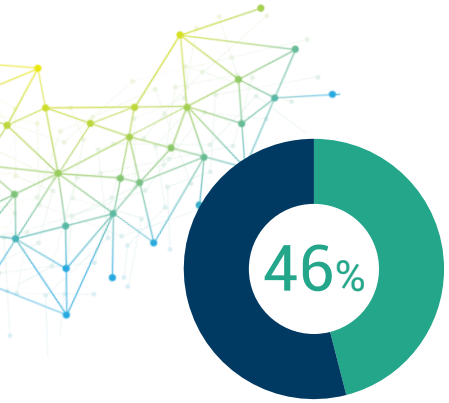
ML for scalable detection

AI for predictive/ prescriptive assurance

Multi-domain correlation for context

The new normal

Virtualization + Massive scale + Increasing complexity + Tighter specs



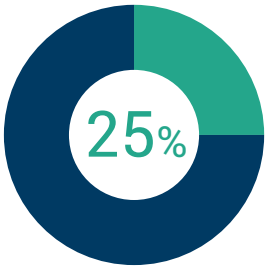
Virtual/cloud networks are challenging SP operations. Over the last 3 years, outages have risen 46%, on average. An estimated 65% come from virtualized domains.[2]

Emerging services will challenge the SP ability to scale.

- **LLC** will require 1 ms round trip
- **UR** services will need >5-9s availability
- **eMBB** will require 1 Gbit/s or greater

Over the next 5 years traffic volume will grow by 700%, driven by OTT video.[3]

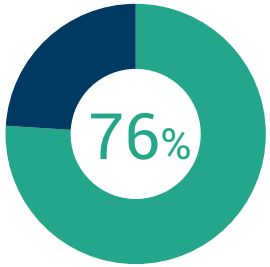
IoT devices will surpass humans on the network (25B) and M2M traffic will double.



On average, 25% of the customer base will churn, per year. Poor QoE is cited as the primary reason for leaving. Studies show that it will be at least 60 months before most would consider returning.[4]

2. Heavy Reading global study of 75 mobile operators, 2019-08
3. TMF 2018, "The foundation of intelligent automation"
4. Analysys Mason global churn rates table, 2019-09; Ovum 2019

Virtual networks means more blind spots



Encrypted OTT / streaming video

As the dominant source of network traffic, ensuring QoE for video services is critical.[5] However, encryption makes this traffic invisible to monitoring above layer 4.

60× more fiber links

On average, there will be:

- 10 small cells per macro cell
- 3x the number of macro cells
- More "X2" interface connectivity

All of this leads to as least 60x more fiber to monitor.

Virtualized & cloud infrastructure

Highly dynamic network & service topologies make relating service issues to infrastructure difficult —and there's no guarantee the topologies will remain stable during troubleshooting.

Dynamic, slice-based services

1000+ network slices per SP with rapid turn-up and tear-down of slices and a vast diversity of SLA requirements per slice. 100% visibility for orchestrated end-to-end assurance is critical to success.

Distributed core & network functions

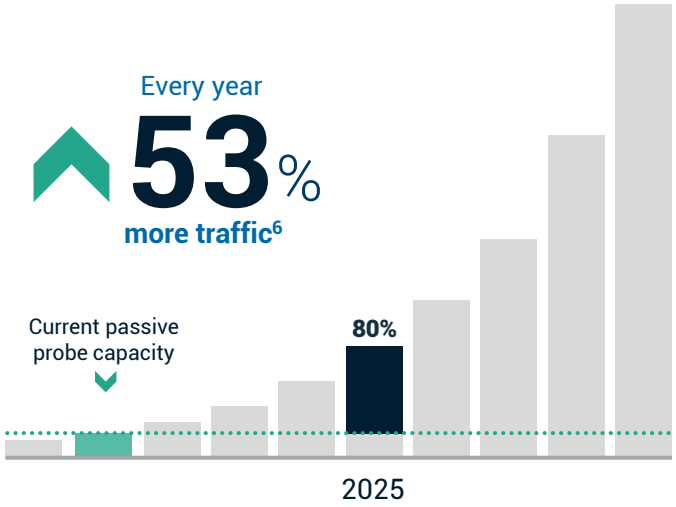
Orchestratable network functions + MEC allow service functionality to be distributed where needed. This flexibility makes service topologies challenging to correlate with service issues.

5. Sandvine, 2019-03

Passive running out of capacity, active ideally suited to fill the gap

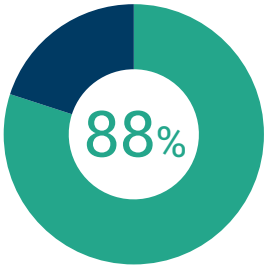
Passive probing is running out of capacity and continued expansion is not affordable, both from a cost of probing and cost of data storage perspective.

According to one Tier 1 US SP, this means 80% of user plane traffic will be invisible by 2025. Scaling up is not practical.



Active assurance is ideally suited to fill this ever-widening gap.

- Highly scalable solution that directly measures QoS and QoE without a dependency on big data analytics
- Real-time measurements for immediate visibility
- Installed in the service chain and follows the service path, even during topology changes



Number of MNOs planning to deploy new active assurance solutions within 24 months[7]

Where?[8]

64% MEC & edge sites

56% Streaming video

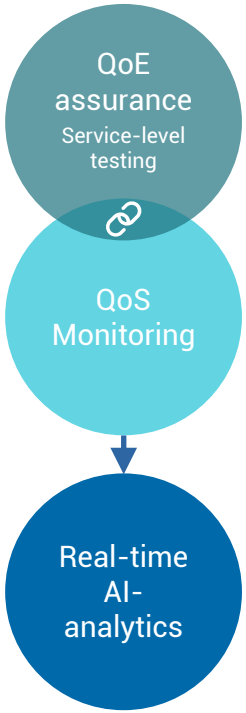
54% URLLC SLAs

52% Cloud / NFVI

6. TMF 2018, "The foundation of intelligent automation"
7,8. Ovum global survey of 150 mobile network operators, 2019

Attributes of effective active assurance

Active monitoring must not only measure network performance, but also how it affects the customer experience. This requires granular testing that can generate high-capacity metric streams. AI-driven analytics provides the real-time analytics to sift through these data feeds to extract critical insights that enable effective action.



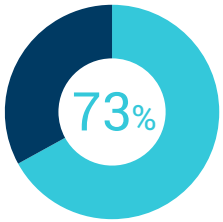
Directly measure the quality of experience (QoE) of data, voice, video, IoT and web services'

Dynamically monitor hybrid networks' quality of service (QoS) end-to-end using industry-standard methods.

Overcome big data barriers with AI-analytics to extract critical insight from granular monitoring metrics.

Correlate service level QoE testing with QoS monitoring to proactively assure the user experience.

Automatically identify issues hiding in massive volumes of monitoring data and rapidly diagnose their root cause.



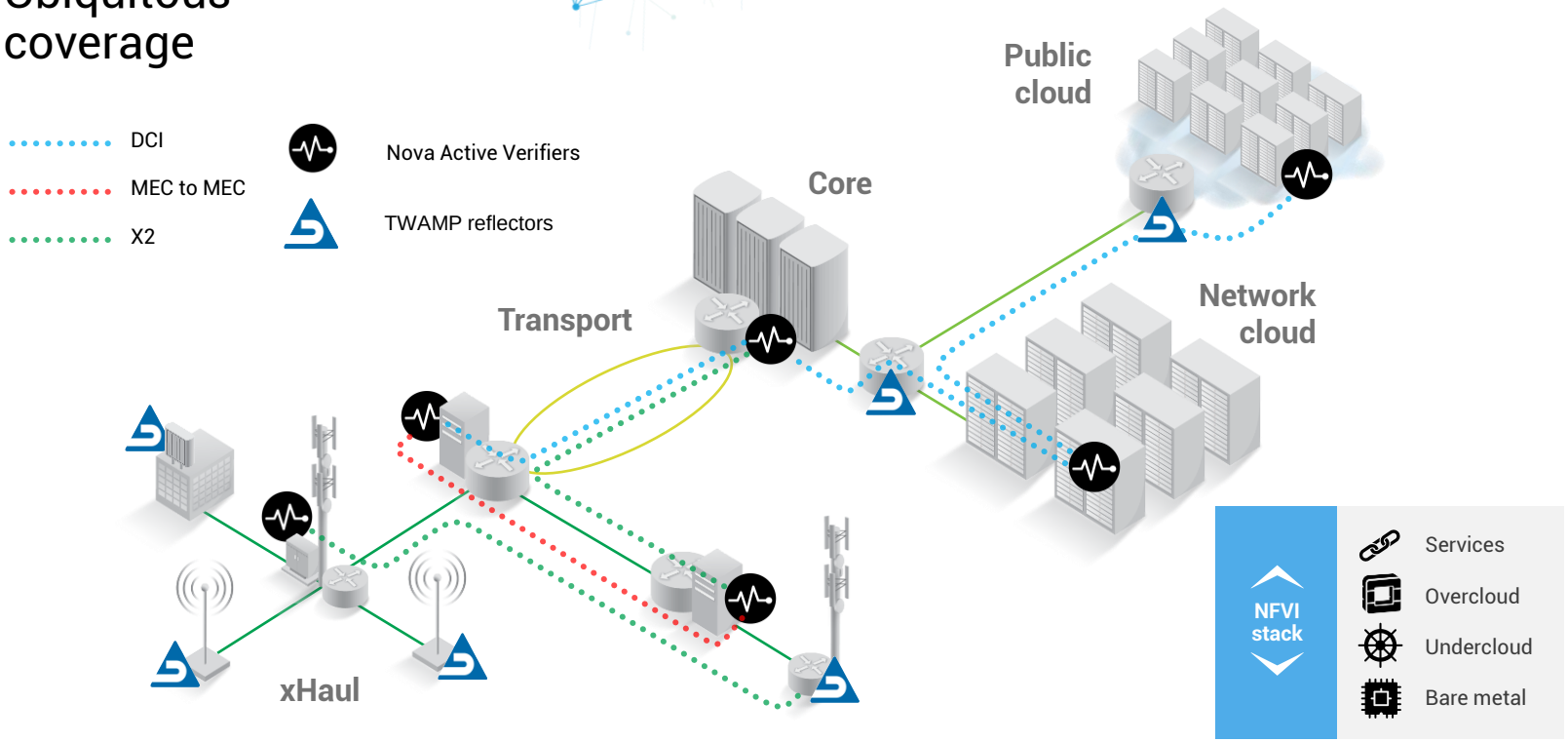
… of CSPs say correlated active QoS and QoE monitoring is essential to assure hybrid network and service performance[9]

A complete understanding of network and service health and how to resolve impairments means operations and support teams can make the most effective decisions as quickly as possible.

NOVA Active + NOVA SensAI = Critical insight — active monitoring data comes alive with SensAI's dynamic AI-analytics

9. Ovum global CSP survey, 2019-08

Ubiquitous coverage



Visibility in the virtual network and in the NFVI

Having full visibility in the virtual network is only half the problem. The virtual network still needs a physical network to run on—the NFVI. Unless you can detect and correlate issues in the NFVI with issues in the virtual network, you're missing half the story.

Monitoring the NFVI

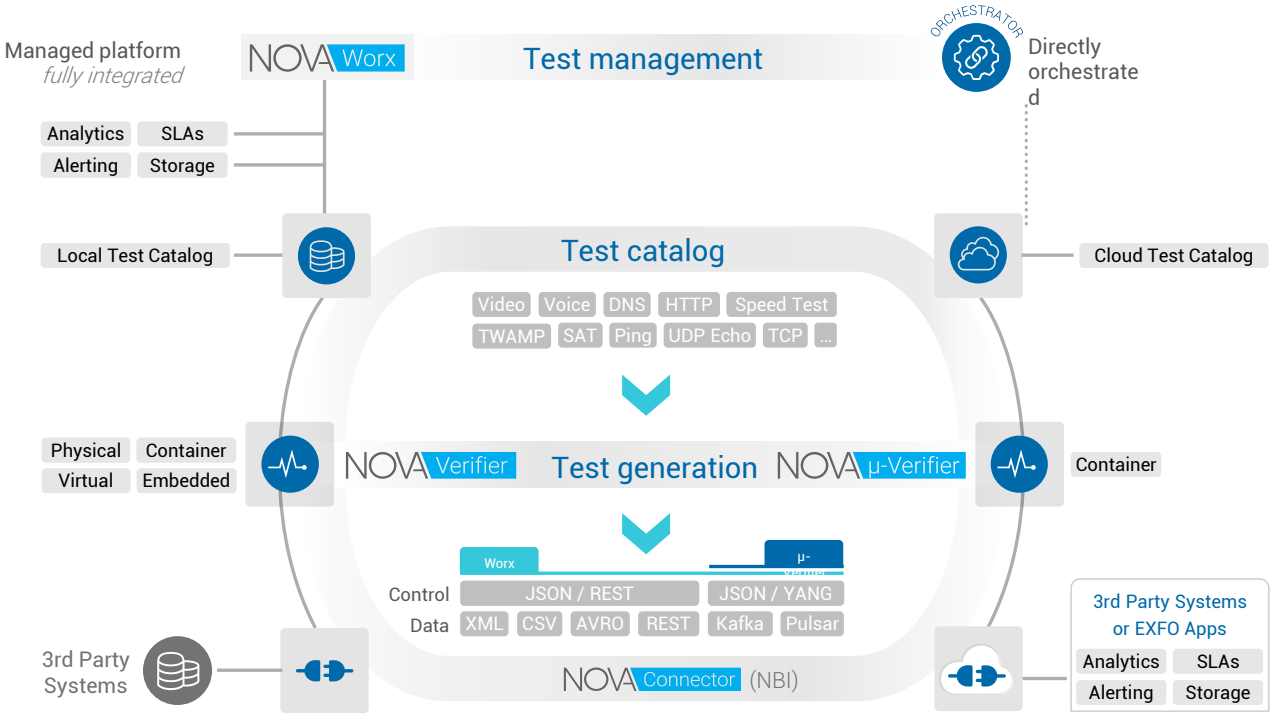
Deploying active monitoring in the NFVI provides insight into its performance and health—from the services (virtual network) layer all the way down to the bare metal.

Being able to correlate this with QoE/QoS issues in the virtual network truly provides full visibility and insight.

NOVA Active Solution components

The Nova Active test and monitoring platform is comprised of integrated components for platform and test management, test generation and system integration.

Active tests can be generated from Nova Verifier probes available in physical, virtual, container and embedded formats, or via Nova µ-Verifiers that are directly managed by orchestrators.



Nova Active's test catalog includes more than 100 network QoS and user QoE tests, with **more than 33% measuring quality of experience.**

Nova Verifiers and the tests they run are based on common software code, making them **fully interoperable regardless of how they are deployed.**

Active testing and monitoring capabilities

NOVA Active test suite

Nova Active covers all layers from service to network and throughout the underlying cloud infrastructure. QoE and QoS test capabilities can be deployed from head-end to customer device, cloud to edge to establish a clear picture of how each domain contributes to service impairments.

100+ tests
1/3rd for QoE

- One-way performance active test
- Abbreviated one-way performance active test
- TWAMP sender test
- TWAMP reflector test
- Continuous two-way active measurement protocol
- Ping active test
- Continuous ping
- Traceroute active test

- Ethernet Y1731 SOAM-PM continuous/periodic active test
- Ethernet loopback test
- Ethernet link trace test

- EtherSAM (ITU-T Y1564) turn-up test

QoE – Layer 4/7

- Media active
- SIP active
- File transfer
- Web
- UDP application
- Infrastructure assurance

QoS – Layer 2/3

- IP network
- Ethernet
- Turn-up

- Advanced VoIP—RTP network active test
- IPTV multicast active test

- Advanced VoIP—SIP Network active test
- Advanced VoIP—SIP assured services test
- Advanced VoIP—SIP service active test

- FTP performance active test
- FTP multi-file performance active test
- FTP multi-connection active test
- FTP availability active test

- HTTP active test
- HTTPS active test
- HTTP multi-connection active test

- DNS active test
- DIAMETER & RADIUS active test
- DHCP active test
- NTP active test
- LDAP service active test
- PPPoE active test
- iPerf performance test (iPerf 2/3)

- UDP bandwidth active test
- UDP echo active test

Augmented active assurance

NOVA Active

QoS & QoE aware monitoring

More than Layer 2/3 transport. Nova Active tests VoLTE, VoIP, OTT video, web protocols and more. Available in both physical & virtual form factors to monitor everything from the undercloud to Layer 7.

Built for closed-loop, automated solutions

Standards-based APIs for ease of integration, 5 sec reporting along with high-capacity streaming for results ingest make this solution ideal for large scale network and service monitoring.

Proven large scale solution

Deployed at several Tier-1 SP, this solution is capable of monitoring from edge to core to cloud – Layers 2 through 7. And since most networks will be hybrid for some time, the solutions are deployable in PNF, VNF, or CNF.

Programmable

Flexible enough to be dynamically scalable up or down to suit the level of monitoring required. Under the control of a test orchestrator, even the sampling rate can be adjusted, dynamically.

+

NOVA SensAI *EXTENSIONS*

Real-time ML QoE analytics

NOVA Context

Multi-domain topology modeling

Taking active assurance to the next level

Nova SensAI extensions bring active monitoring data to life. ML-based analytics overcome big data delays to reveal actionable insight on the fly. Detect, predict and resolve customer-impacting events, and assure SLAs.

Nova Context provides a federated view of service and network topology and inventory. Immediately identify dependencies and pinpoint fault location within virtualized networks to save hours of troubleshooting time.

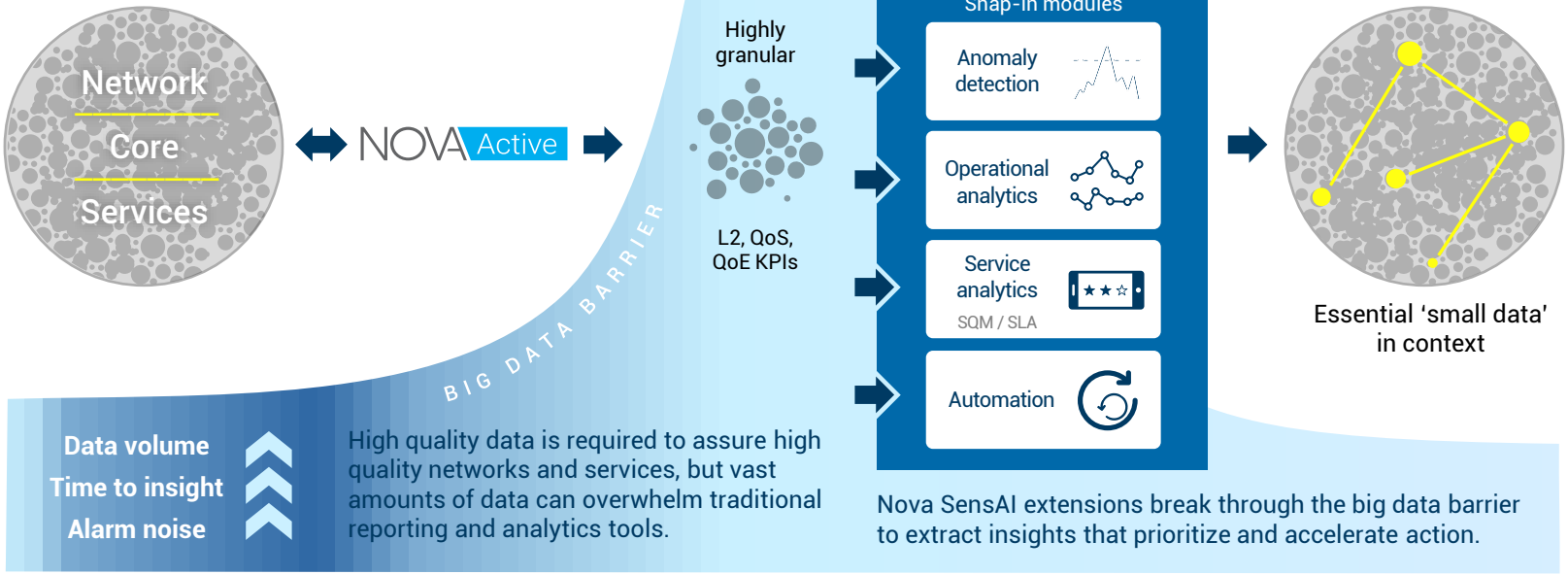
NOVA SensAI EXTENSIONS for actionable insight

Nova SensAI is a modular, AI-powered platform for automated problem detection and diagnostics, analytics and reporting.

Nova SensAI extensions are **preconfigured modules** that simply integrate into Nova Active deployments to **extract actionable insight from highly-granular, precise monitoring metrics in real-time.**

Modules can be added incrementally to address network operations, service quality and automation use cases.

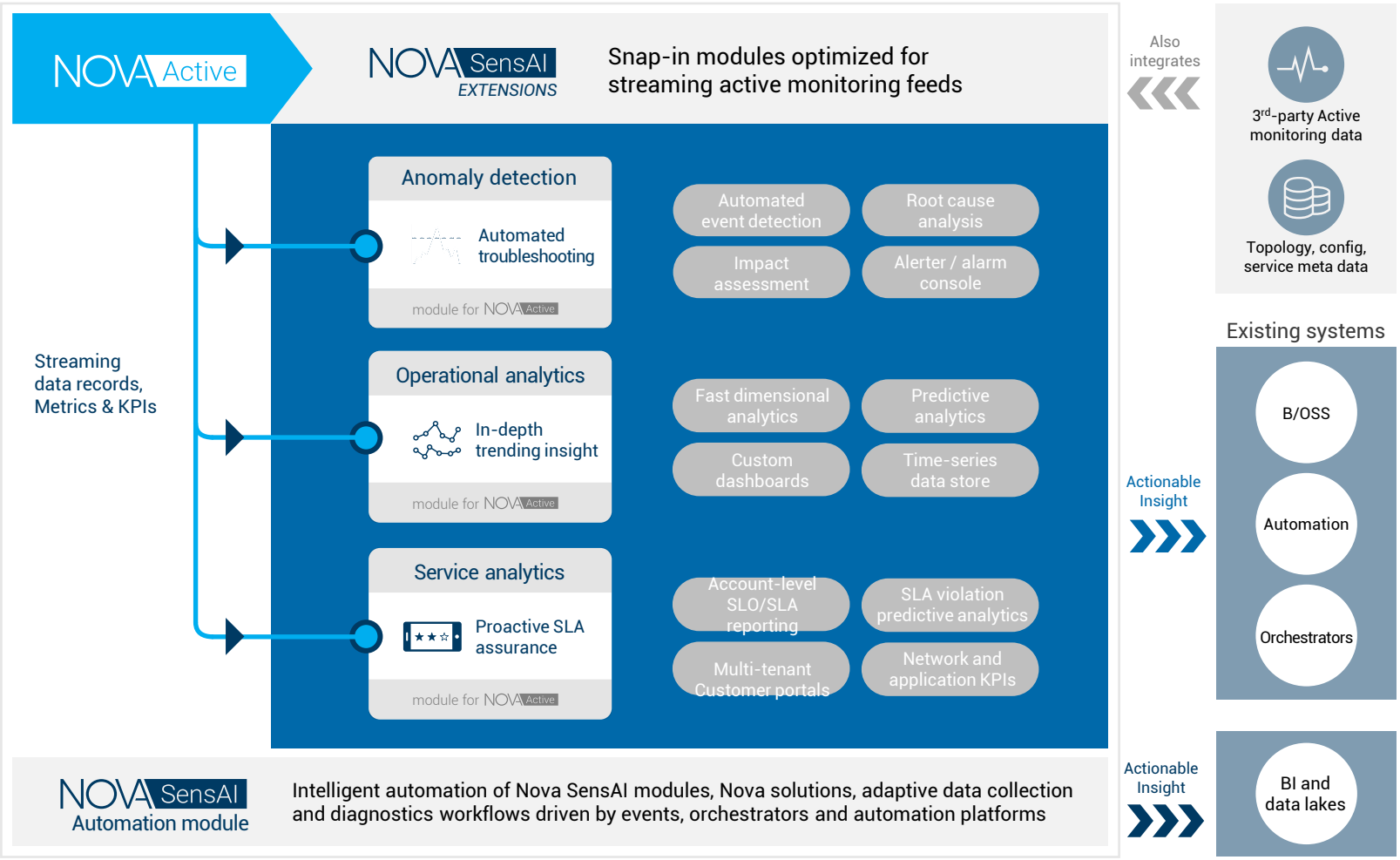
Open interfaces allow streaming insight to be delivered to existing fault management, visualization and SLA reporting and big data platforms.



NOVA SensAI EXTENSIONS for actionable insight

Nova SensAI extensions are cloud-native microservices that scale efficiently in high-capacity, dynamic networks.

Learn more →



Summary

Active assurance done right — benefits

Deploy faster

The key to faster deployments is automation—and automation needs visibility.

Active assurance provides complete visibility into end-to-end network and service performance. Orchestrating active testing into the lifecycle of a service or network slice provides the feedback needed for closed-loop operation.

The upshot for the SP is faster time-to-revenue, assured SLA-grade network slices and a more optimized DevOps environment.

Resolve faster

In operations, time is the enemy. Significant time is spent manually collecting and correlating network and service information needed to identify the root cause of issues.

Active assurance, combined with real-time anomaly detection and cross-domain topology visibility can cut this time to minutes from hours.

Instantly detecting customer impacting issues along with correlating & isolating faults in minutes will ultimately lead to more satisfied customers and lower churn.

Enable automation

In the end, your automation solutions are only as good as the data feeding them. Slow data, poor or incomplete data will all lead to poor automation.

Do it right, and the goals of reducing OPEX, and increasing QoE, AMPU, and NPS are well within reach.

The scale and complexity of virtual and 5G networks demands automation and closed-loop solutions. EXFO's augmented active assurance solutions deliver the actionable insight required for success.

Glossary

AI	artificial intelligence
AMPU	average margin per user
API	application programming interface
CNF	containerized network function
CSP	communications service providers
eMBB	enhanced mobile broadband communications
IoT	Internet of Things
LLC	low latency communications
LTE	long term evolution (4G)
M2M	machine to machine
MEC	mobile edge compute
ML	machine learning
mMTC	massive machine type communications
NFV	network function virtualization
NFVI	network function virtualization infrastructure
NPS	net promoter score
OTT	over the top
PNF	physical network function
QoE	quality of experience
QoS	quality of service
SLA	service level agreement
SP	service provider
UR	ultra reliable
VNF	virtualized network function
VoIP	Voice over IP
VoLTE	Voice or LTE

EXFO corporate headquarters

400 Godin Avenue, Quebec City (Quebec) G1M 2K2 CANADA
T +1 418 683-0211

Toll-free (USA and Canada)
1 800 663-3936

info@EXFO.com
EXFO.com