IDC ANALYZE THE FUTURE

IDC TECHNOLOGY SPOTLIGHT

Brought to You by VMware, Powered by IDC

This IDC Technology Spotlight is a playbook on why dynamic end-to-end service assurance (network core to the edge to the customer location) is business essential and customer critical in today's environment of evolving network technology, changing business models, and expanding partner ecosystems.

New Technology, Increased Expectations: Automated Service Assurance Has Become a Competitive Differentiator for Telecoms

August 2019

Written by: Karl Whitelock, Research Vice President, Communications Service Provider Operations & Monetization

Introduction

Delivering superior customer experience is a key driver for competing in the cloud economy. Automation is pivotal to business success and the operationalization of emerging 5G network technology. Meeting the needs of new technology requires different approaches to basic problems that now stem from increased levels of complexity associated with the joint management of new and existing network infrastructure. Automated assurance becomes a business imperative in bridging the gap between the two worlds and in managing 5G networks at scale.

The promises of 5G and the Internet of Things (IoT) are extensive, with the potential for communications service providers (SPs) to offer not only differentiated levels of network connectivity but also end-to-end (E2E) solutions to specific industry sectors and customer groups. Communications SPs would do well to increase business and service agility to reduce operational costs as network traffic scales. They would additionally benefit from embracing operations automation at every opportunity as a means of reducing human intervention.

AT A GLANCE

KEY TAKEAWAYS

- 5G/IoT evolution demands real-time monitoring and analysis to meet QoS requirements. Accomplishing this objective means service assurance must be part of the provisioning and activation process rather than an after-the-fact action as in the past.
- Service monitoring and automated trouble resolution must include the network core, edge, and SD-WAN connecting to the customer location. Using a single system to meet both service provider and enterprise needs in this environment, with the same data, is fast becoming a critical business and customer experience success factor.
- Automated assurance can reduce the cost of operations, in some cases as much as 90% over manual methods. E2E assurance is important now but will become critical to the expected customer experiences that 5G can deliver.

Service Complexity and Automated Operations

Mass deployment of 5G is in the early stages while the number of new use case opportunities continues to grow. Services are provisioned in this new environment through a hybrid layout of physical network functions (PNFs), virtual network functions (VNFs), and cloud-native network functions (CNFs). End-to-end service orchestration dynamically associates degrees of network definition (latency, bandwidth capacity, throughput rate, and packet loss) with customer needs based on predefined rules for some cases and learned insight for others.

Manual methods and semi-automated processes using existing operations and monetization systems can no longer address the divergently variable connectivity and service-level requirements that different network configurations from different industries now need. For example, service monitoring, revenue accountability, and business management requirements for healthcare solutions are radically different from those requirements in the mining industry. In a similar vein, industrial manufacturing, agriculture, and pharmaceuticals each have their own, different demands, which are requirements as well.

Dynamic E2E Service Assurance

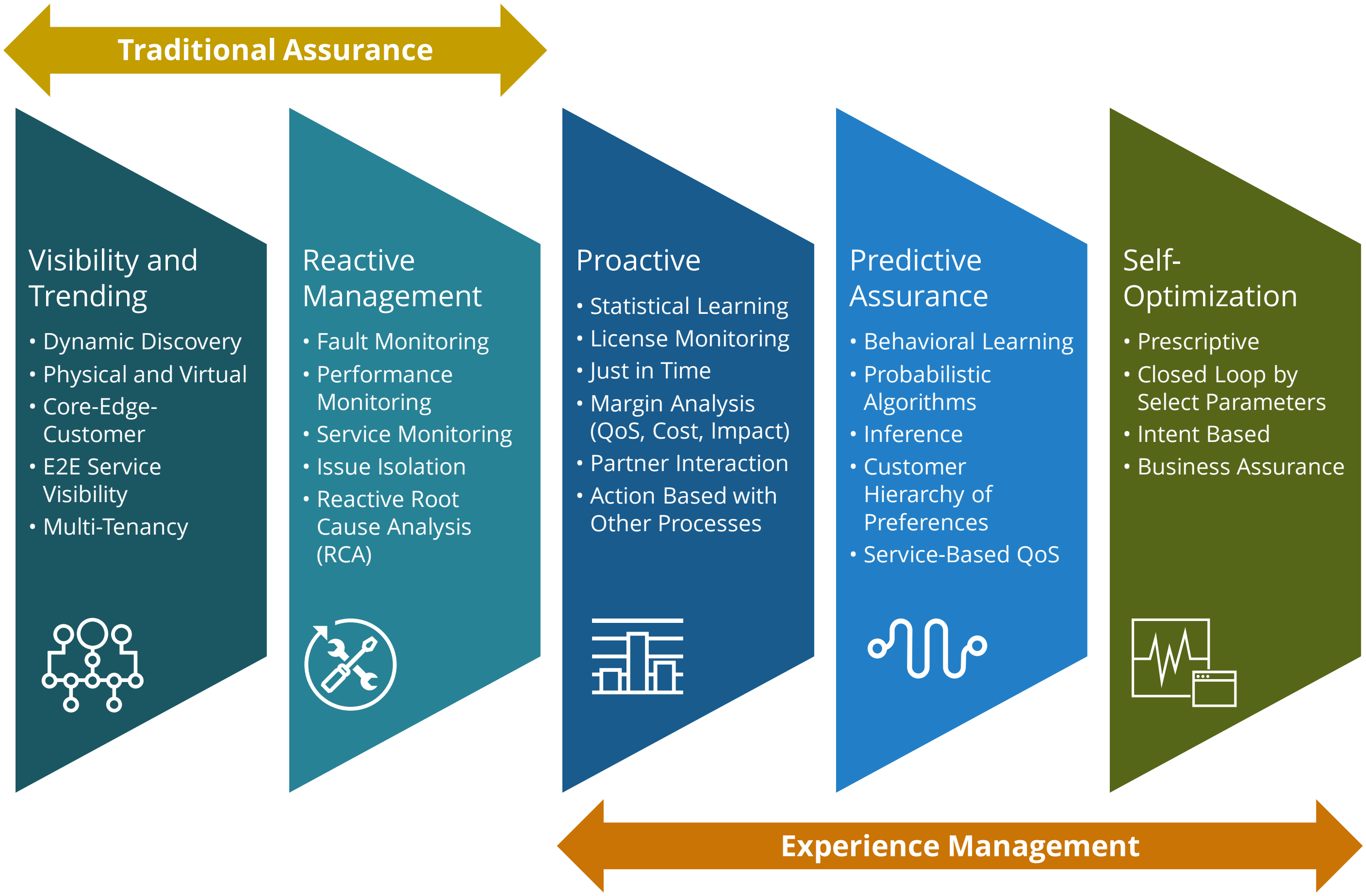
With 5G's promise of individualized network configurations and quality-differentiated services, the fulfillment, assurance, and billing (FAB) processes must collaborate with a 24 x 7 degree of availability to maintain acceptable customer experience levels. This means these processes must be integrated, automated, and monitored for service-level conformance so that the end-to-end customer experience meets or exceeds quality-of-service (QoS) specifications and provides customer transparency with all workflows including billing.

The service assurance processes contribute to E2E service performance and the overall customer experience. They include:

- Real-time E2E service-level monitoring based on parameters such as latency, packet loss, throughput speed, and data volume in addition to the more traditional parameters tied to network fault management, performance monitoring, trouble analysis, and problem resolution (This expanded role for service assurance significantly advances how service-level agreement [SLA] conditions need to be defined, negotiated with the customer, and monitored for compliance.)
- Real-time monitoring of network and partner interactions for SLA conformance (This means collectively addressing the increased complexity from services defined by hybrid physical and logical network components and/or services containing partner contributions. Real-time service-level monitoring also means managing service behavior within tiered levels of QoS tied to a variable pricing structure.)
- Real-time monitoring using provisional parameters (This is needed as hard-coded business rules are applicable for some situations but inadequate for others. Eventually, learned conditional changes to service definition, coverage area, or network behavior become the best option for all E2E service-level conditions.)
- Coordinated E2E management of the network core, edge, and a customer's SD-WAN connections to provide real-time insight for both the communications SP and end-user customer using the same data
- Real-time knowledge of E2E service behavior combined with the ability to make automatic changes as network conditions or customer usage definitions dictate or as a part of the problem resolution function
- The ability to satisfy new requirements as the network and edge clouds grow with virtualized and cloud-native network functions (This may require coordinated service-level assurance involving two or more 5G radio bands [e.g., mmWave + enhanced broadband] that address a set of customer service conditions. Also needed is continuous validation of network function software licenses for usage compliance and authentication.)
- The identification and resolution, sometimes proactively, of problems before they affect customers (This is often required due to the massive increase in network nodes [physical or virtual] tied to connected devices beyond just smartphones, as well as overall service complexity [multiple network configuration options].)

Automated service assurance solutions are essential for maintaining QoS conformance as the definition of "customer" expands from humans making a voice call to machines collecting and transmitting information to the cloud. As Figure 1 illustrates, service assurance solutions should do more to improve the customer experience. This eventually includes proactive, predictive, and optimizing steps, which increase in importance as customer service demands grow more complicated.

FIGURE 1: ***Service Assurance Evolution***



Traditional Assurance

Visibility and Trending
- Dynamic Discovery
- Physical and Virtual
- Core-Edge-Customer
- E2E Service Visibility
- Multi-Tenancy

Reactive Management
- Fault Monitoring
- Performance Monitoring
- Service Monitoring
- Issue Isolation
- Reactive Root Cause Analysis (RCA)

Proactive
- Statistical Learning
- License Monitoring
- Just in Time
- Margin Analysis (QoS, Cost, Impact)
- Partner Interaction
- Action Based with Other Processes

Predictive Assurance
- Behavioral Learning
- Probabilistic Algorithms
- Inference
- Customer Hierarchy of Preferences
- Service-Based QoS

Self-Optimization
- Prescriptive
- Closed Loop by Select Parameters
- Intent Based
- Business Assurance

Experience Management

Source: IDC and VMware, 2019

Throughput capacity, latency requirements, and delivery speeds are variable from one customer to the next when 5G connectivity is involved. According to expectations, this service mix can dynamically change (within minutes at most, seconds or even faster ideally) on regular intervals according to trigger conditions often unique to each customer.

Why Dynamic Service Assurance Is Strategically Important

Within an evolved 5G network, many use cases depend on latency configuration levels, bandwidth rate, and throughput volume centered on varying customer needs. Several types of service offerings will likely include a multipoint parameter definition for the network, such as the following:

An advanced, real-time service assurance solution enables E2E customer-level management to become a *business differentiator* for organizations that master how connectivity, in combination with other solution capabilities, meets customer needs and business expectations.

- During parts of the day, a customer may want an ultra-low-latency connection with a specific bandwidth level to address various download and upload workflows. Other customers will want similar, but differing levels of these same network parameters for a variety of business usage scenarios. Each combination of network capabilities (network slice) must be monitored and managed to SLA-defined performance specifications that may be unique from one customer to the next.
- Business conditions will fluctuate over time, requiring a different set of network parameters, perhaps for when latency expectations are less severe but are still significantly different than "normal." At this point, alternative bandwidth levels and throughput volumes, potentially all different by customer, need to be put into effect. Service assurance parameters will change to other customer-defined SLA definitions established at the time of initial service configuration.
- Downtime, based on non-linear requirements such as business management needs, maintenance windows, or production quotas/limits, figures into any customer's connectivity needs. Network usage "stop" times could be planned, while others will be based on dynamic conditions. Customers will expect the option for network revectoring according to measured usage conditions.
- A standard connection involving "normal latency," bandwidth, and throughput volume will likely be needed for office operations such as email or reporting tasks. This connectivity need would be addressed by a possible second network slice if 24 x 7 availability is needed. It may be provided across the initial network link on a best effort basis if there is no disruption to previously defined QoS levels. Dynamic service assurance monitoring would be the driving force.
- For each condition-defined network configuration, customers expect to pay an agreed-upon price for the service according to a contract specification (SLA) that is compared with measured service-level performance. For each new network configuration, according to new usage parameters, the service rate will be different — higher or lower than the first depending on service definitions and monitoring compliance to those definitions. The rate would then change again for the next network configuration if needed. In addition, communications SPs will likely charge for accommodating each network configuration change.

Many services will involve multiple network slices, each with variably different configuration options, further adding to the complexity of a joined service assurance and charging function.

Sophisticated customers will ask for a self-care portal to make do-it-yourself configuration decisions and changes, which will need to include a "what if" calculator to satisfy customer expectations. Such an approach has the added benefit of keeping operational costs in check compared with manual operations, along with increasing loyalty from a satisfying customer experience. Real-time service monitoring would contribute to how service-level recommendations could be offered to the customer whenever possible.

Benefits

Complexity continues to grow from the ongoing rollout of 5G LTE technology and use cases that take advantage of the potential this new wave of network capability offers. Existing systems and processes fall considerably short in meeting business expectations that come from such a radical technology refresh and strategy change. Within the service assurance domain, updating from presently installed systems and current business processes with an E2E automated assurance solution provides significant business benefit, summarized around three key areas:

- **Enabling real-time service monitoring and problem resolution.** Traditional service assurance solutions play an essential role in the identification and resolution of network problems almost always after they are noticed by the customer. These systems rarely have knowledge of service-level configuration details, often lack the ability to correlate fault and performance conditions across physical and virtual network components, and depend on a significant level of human intervention for problem resolution. Automated service assurance solutions, geared to support 5G technology, must possess advanced problem-solving capabilities to detect network issues and initiate trouble resolution procedures in many cases without human involvement. While not possible for all conditions, automated service monitoring systems should provide a much-improved means for recognizing service-affecting issues before they become customer-affecting problems.
- **Providing an impactful customer experience.** Partially automated processes and systems that address some business requirements not only fall short of expectations but also set the stage for a disappointing customer experience. An advanced, real-time service assurance solution enables E2E customer-level management to become a *business differentiator* for organizations that master how connectivity, in combination with other solution capabilities, meets customer needs and business expectations. Within a 5G network architecture, QoS-defined services via network slices will be commonplace. In this environment, predictive assurance and self-optimization move from the realm of a nice-to-have luxury to a necessity as complexity requires solution-level attention not possible by direct human interaction.
- **Taming service-level complexity.** The degrees of complexity placed on any of the key FAB processes only increase as networks grow and customer needs evolve. Services delivered through hybrid physical and logical networks, combined with the management challenge of dynamic service configuration and real-time assurance, point to automation as the only option for delivering a quality customer experience and in dynamically satisfying both service requirements and customer needs.

> Within a 5G network architecture, predictive assurance and self-optimization move from the realm of a nice-to-have luxury to a necessity as complexity requires solution-level attention not possible by direct human interaction.

VMware Smart Assurance

VMware Smart Assurance is a real-time automated service assurance solution designed to holistically monitor and manage — integrated fault and assurance management — networks at the service, virtual, physical, and transport layers. It is designed to eliminate the need for a communications SP to use multiple tools in addressing the E2E service assurance needs of multi-technology services and, in the process, reduce complexity and cost. While many service assurance solutions are available on the market today, few of them are designed to monitor the network from the core to the edge and now across the SD-WAN connection to the end-customer location, in addition to the various layers of network infrastructure that define today's hybrid networks.

The Smart Assurance solution provides an automated approach to operations for minimizing service impact and expense. The system is designed to prevent network incidents by proactively detecting abnormal patterns. However, when incidents cannot be prevented, Smart Assurance uses an automated approach to address root cause analysis. It does this by correlating all active, inactive, and unknown alarm statuses with the network topology to rapidly focus on the problem. This is accomplished using a multi-dimensional deterministic model-based engine that correlates events and alarms with auto-generated computer signatures to isolate true problems from just symptoms. The model is not based on traditional alarm management rules; rather, it follows an auto-discovery process that maps all layers of the digital network. Smart Assurance can trigger closed-loop actions and problem resolution via API integration with orchestration tools and operations management systems. Smart Assurance can also prioritize issues based on correlation of service and tenant impact.

VMware has several telecom and large enterprise customers that use Smart Assurance as part of their daily operations. One telecom customer successfully reduced the number of network alarms per day from 250,000 to 110 authentic alarms by leveraging Smart Assurance's automation. More typically, the company stated that Smart Assurance reduces the number of network alarms by up to 95% compared with non-automated systems. Another telecom customer noted that with automated root cause analysis, 99.7% of its alarms are identified in real time, thereby reducing time to repair and preventing service disruption, which in turn can ensure SLA commitments.

With multi-tenant support, VMware Smart Assurance enables communications SPs to gain comprehensive insight across network environments, which helps prioritize VIP customers and tenants based on characteristics determined by the communications SP, such as management details from an SLA contract. The Smart Assurance solution integrates with VMware's portfolio of NFV solutions providing real-time root cause analysis of issues across virtualized and legacy environments. Smart Assurance also supports multi-vendor SD-WAN enterprise services monitoring, including VMware SD-WAN by VeloCloud and Cisco ACI software-defined networking.

The race to deliver high-quality network services continues. 5G now enables communications SPs to provide personalized network connectivity, coupled with partner-provided capabilities, to business and high-value customers. Central to the success of these new service options is the ability to monitor all parts of the service across all network links. This is no small task. IDC believes that VMware's Smart Assurance solution is one of just a few commercial products that are strongly positioned to meet the needs of multi-vendor, multi-technology networks not just across the network core and edge but also across an enterprise's SD-WAN to the end-user location. The dynamic nature of 5G also suggests that only solutions with automated assurance capabilities need to apply.

Industry Challenges

Innovative solutions such as VMware Smart Assurance face challenges from communications SP–embedded processes and systems, organizational structure, and multiple generations of network technology. However, automated solutions also give communications SPs a chance to restructure their organizations over time to provide uniformity across their different networks. The following sections highlight these challenges.

Embedded Processes and Systems

When new technologies were introduced in the past, most communications SPs built new greenfield IT stacks and created new standalone business teams to work with customers and deal with any subsequent management issues that involved these technologies. This time around is different. Hybrid network technology will remain fully operational as 5G nodes are deployed. This is especially true with 4G LTE evolution to 5G.

The FAB systems need to be updated along with the business processes they support. Central to the service assurance challenge will be integration of embedded systems with the VMware Smart Assurance solution to handle issues with already deployed network technology. VMware claims to support over 4,000 physical and virtual devices today, but providing support for new devices —as well as for very old technology that may not be amenable to today's API and software development standards — will always be a challenge. Perhaps harder for communications SPs will be managing the interaction with existing processes and trouble reporting procedures when new technology issues occur that still involve some portion of their legacy network. Smart Assurance helps mitigate these risks by integrating with existing tools to expedite initial deployment. VMware states that operators have often replaced legacy tools with Smart Assurance once it's up and running, interfacing directly with network devices to reduce opex and to achieve real-time monitoring.

Organizational Structure

The VMware Smart Assurance solution is deployed as an on-premises solution today. However, as the trend in the industry and with customers collectively continues moving to an off-premises (cloud) model as a means for reducing the cost of hardware and to better address solution elasticity needs, the Smart Assurance solution will be made available through a public cloud option in early 2020. Many network management teams globally are not familiar with the operational impacts a cloud service model can deliver as well as the reduction in technician support that comes when a communications SP moves from semi-automated processes and systems to the level of automation that the Smart Assurance solution can provide. Overcoming these challenges in the months ahead will need to remain a key operational focus.

Layers of Legacy Network Technology

Communications SPs globally understand that legacy technology has limited use in many of today's new business opportunities. However, existing services with their entourage of network hardware and management systems will endure if customer demand dictates. Even though the VMware Smart Assurance solution is engineered to work with legacy systems and a vast number of mature network nodes, some of those nodes are so unique that service monitoring will be difficult. In addition, some devices are incapable of supporting a standard interface. Connecting with an installed system, rather than the network node, may be a good alternative for maintaining full visibility into an end-to-end network.

Holistic service assurance solutions such as Smart Assurance can buy communications SPs the time needed to unify operations across a plethora of legacy tools, other operations support systems, and network nodes. This is critical as communications SPs continue to establish an efficient means to manage both old and new networks together.

Conclusion

Digital transformation has been underway for a few years now. Some network operators have made substantial progress in supporting digital business strategies, while others are still analyzing the best way to address their transformation objectives. However, it's clear that as network services are becoming more customer specific, the degree of flexibility required from the network to address various business conditions is rapidly evolving.

Change with current business processes and systems is a must as growth continues in the number of new requirements tied to 5G and the degree of business challenge coming from industry-specific IoT opportunities. Flawless network connectivity is a differentiating factor in competitive markets, especially when network operators and their enterprise customers can see how the connection meets or exceeds expectations, not just with reliability but with other factors such as throughput rate, latency, and flexibility in dynamically shifting connectivity parameters according to changing customer needs. Communications SPs would do well to leverage the automation found in next-generation service assurance solutions to manage today's increasingly complex, multi-technology networks in order to achieve a competitive edge both now and in the future.

About the Analyst

Karl Whitelock, *Vice President, Communications Service Provider Operations & Monetization*

Karl Whitelock is Research Vice President of IDC's Communications Service Provider Operations & Monetization industry practice. He provides strategic insight and global perspectives concerning the operations and monetization functions such as rating and charging, policy management, partner management, subscriber data management, customer service assurance, and network operations.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Corporate USA

5 Speen Street
Framingham, MA 01701, USA

T 508.872.8200

F 508.935.4015

Twitter @IDC

idc-insights-community.com

www.idc.com

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.