VIEW POINT

# INTELLIGENT NETWORK ASSURANCE FOR A CLOUD-READY WORLD

Infosys®
Navigate your next

## Introduction

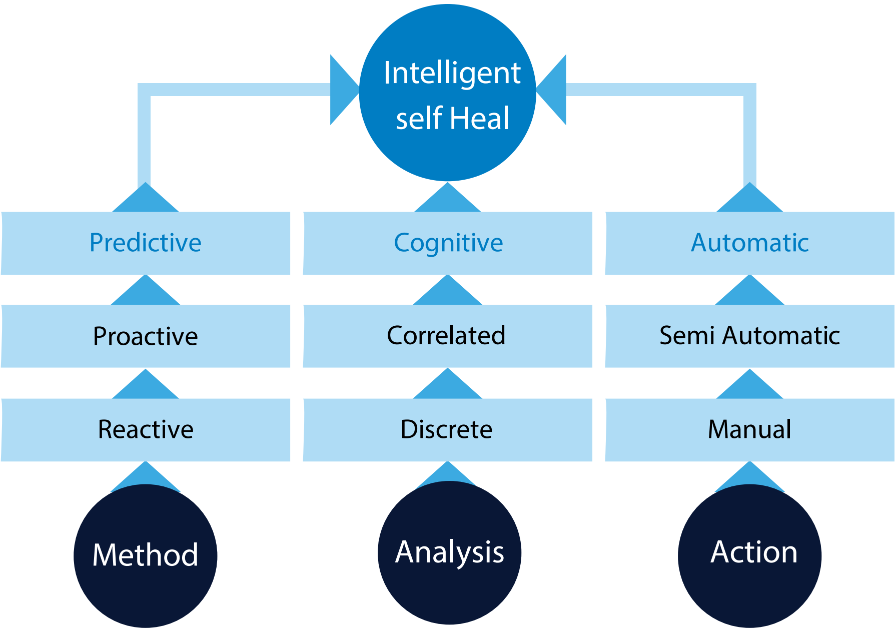
As the network world moves towards more cloud-native and software-defined infrastructure, the need for a predictive and self-healing way of network assurance is becoming increasingly evident. As per a Gartner study, the average network downtime cost per minute is USD 5,600 which makes it approximately USD 300,000 - 400,000 for an hour. For industries that depend on the network for production, such outages can be catastrophic if the troubleshooting and restoration take a longer time. Hence, it is essential to move away from the current reactive way of network assurance to a more proactive, data driven and automated method.

## Where is the current gap?

As per our experience, approximately 30% of network faults like connectivity down and system downtime are repeated, implying a similar problem has occurred earlier. Also, another set of problems typically build over time, giving enough early indicators in network telemetry data. To identify these and reach insightful conclusions, you need analytical and correlation capability in the assurance systems, which most systems do not possess currently. Secondly, most of the corrective actions for network faults are performed manually and reactively. These add to the Mean Time To Repair/ Recover (MTTR) and operational cost. Adding to the woes, often you need highly skilled people to debug and troubleshoot the problems and recover after the outage.

## The solution path

The solution involves progressively moving the assurance method from reactive to proactive to predictive, analysis from event-based to analytical to cognitive, and operations from manual to semi-automatic to automatic. This means that instead of waiting for the fault to occur and then resolving it, the assurance must anticipate what will happen and take proactive action towards resolution quickly.



## So, how will a future intelligent network system look?

In the future, with software-defined, 5G and edge enabled networks, the services and use cases will be highly resilient and latency sensitive.  A few seconds of outage could itself cause a significant service impact. Imagine the network flapping while a connected vehicle is in motion or an immersive media stream is in transit. The network assurance systems of the future should look at the historical data and machine learning the fault patterns and signatures as much as possible. This intelligence should then be used to correlate the real-time data and predict a possible network fault.

Further, if the data suggests a fault, a proactive self-heal action could be triggered if it's a known problem. If it's a new problem, the system could learn the new pattern and proactively alert for planned maintenance. This way, the artificial intelligence (AI) of the system keeps growing. It's obvious then that the future assurance systems will be distributed, cloud-native and more towards edge for faster closed loop.

## How will this work in the real world?

To explain better, let's take the example of a critical business application on edge connected through 5G and assume that one of the interconnecting network links had started flapping. With intelligent network assurance in place, the system interprets from the leading network fault indicators that a potential problem pattern is in the making. It then compares this with any already "machine learned" pattern and automatically identifies the root cause based on this real-time comparison. The system then looks for the possible configured self-heal action. In the above case, it could be redirecting the traffic through a healthy link. So, even before the link failure happened and the application suffered, the system had taken proactive corrective action using its AI.

## Conclusion

Through this point of view, we presented the impact of a network outage in a modern-day enterprise and how it can cause business and service degradation. It's clear why we need an intelligent system to handle network assurance proactively, especially with the advent of 5G and edge. Our recommendation to any enterprise considering network digital transformation is to include data driven closed loop assurance in their blueprint.

Infosys' cloud-ready Intelligent Network Assurance solution can help.

Infosys Smart Network Assurance, part of Infosys Cobalt, is a carrier grade AI/ML driven closed loop assurance solution. It powers enterprises and telecom service providers to move towards a more predictive and automated Live Enterprise. It is the only solution with a comprehensive set of features covering the key areas of monitoring, diagnostics and self-heal compared to any similar market product. Designed as fully cloud-native and modular, it is easily deployable. Its standard southbound and northbound interfaces allow seamless network and systems integration. We believe Infosys Smart Network Assurance will transform the way network assurance is viewed and significantly contribute to building highly resilient modern-day cloud-native networks.

Infosys Smart Network Assurance solution was awarded NASSCOM Next Gen Product of the Year at NASSCOM Engineering R&D Showcase 2021

External Document © 2021 Infosys Limited

## About the Author

**Sreekanth Sasidharan - AVP**, Senior Principal Technology Architect, Infosys Ltd

Sreekanth Sasidharan is an AVP and Senior Principal Technology Architect at Infosys Ltd and is a global leader in next-generation network architecture and consulting. He is the Technology Practice Lead for Next Generation Network Engineering (SDN, 5G, Edge, Network Automation and Open Networks) architecture and consultancy. He is also responsible for partnerships with industry bodies and organizations to define standards and co-create innovative solutions to support network transformations. He champions open source and open network adoption, and has helped rollout carrier grade open source solutions for supporting next generation networks for multiple operators.

For more information, contact askus@infosys.com

Infosys®
Navigate your next

© 2021 Infosys Limited, Bengaluru, India. All Rights Reserved. Infosys believes the information in this document is accurate as of its publication date; such information is subject to change without notice. Infosys acknowledges the proprietary rights of other companies to the trademarks, product names and such other intellectual property rights mentioned in this document. Except as expressly permitted, neither this documentation nor any part of it may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, printing, photocopying, recording or otherwise, without the prior permission of Infosys Limited and/ or any named intellectual property rights holders under this document.