insidetelecom®

The Autonomous Future of Today’s CSP

By Harley Stowell 5/5/2021

Secure networks have become the heart of our daily lives.

They support teams working from home, mobility, how our children learn at school, how we shop and how we connect with our loved ones. They are also the fabric by which our enterprises do business.

As vital as they are, it comes as no surprise that these networks aren’t just growing, they’re exploding. This growth is being driven by 5G, IoT, IIoT, and trends like software-as-a-service, cloudification, and smart everything. Just check out these figures:

- IDC predicts that there will be close to 56B connected devices worldwide by 2025 and 75 percent of these will be connected to an IoT platform.
- Juniper Research projects that the number of IIoT connections will grow 107 percent, increasing from 17.7 billion in 2020 to 36.8 billion in 2025.
- Statistica reports that the number of Smart Homes in the market worldwide is expected to be 482.8 million in 2025.

The connected economy assumes secure networking (i.e.: SASE) at hyper scale. This in turn creates a requirement for service-level automation because you cannot scale services with point solutions and tools.

This growth is exciting for communications service providers (CSP) but it does unearth critical questions.

The big ones that come to mind for me are, how will we operate all of these endpoints and the network between them? How will we keep them secure? How will we make them reliable enough to literally bet our businesses and lives on them and how will we do this cost effectively at hyper scale?

At this point I’ll provide some background to help explain these concerns.

Today it takes between 5 and 9 man-hours just to deploy a basic secure SD-WAN endpoint. What this number includes are all the benefits of present-day network automation, and the penalty of swivel-chair, cross-domain manual convergence of the endpoint, transport and security domains and policy.

Now for what it doesn't include. For starters it doesn't cover ongoing service assurance, auto remediation, security updates, maintenance, restoration and upgrade or optimization operations. It also doesn't account for service enablement.

In today's SaaS and cloud-based world, where businesses are looking to leverage digital transformation, speed, and performance enhancements, and where services are being introduced regularly, we become more and more exposed to provider network reliability and security vulnerabilities if we continue to rely on manual processes.

The bottom line is this, you can't build a smart city on top of a dumb pipe delivering manually mediated end-user value added services.

One option for CSPs is a move to Autonomous Service Operations. Autonomous Service Operations address the fact that there are not enough trained personnel to meet scale requirements, that manual processes are too slow and too expensive, and that the cost and frequency of human errors will much too high.

The critical feature of Autonomous Service Operations is that it is, well, autonomous. Finishing in a very close second, however, is the fact that it operates the entire service, end-to-end, and not just some of the elements.

Let's use secure networks as an example of why this is so valuable. Secure networks have endpoints, underlay elements (the provider's physical network), overlay elements (the provider's virtual network components) and frequently cloud-based elements. They also have security applications and controllers, SD-WAN applications and controllers, and orchestrators at every level and technology domain in the network.

Are you still with me? Now each domain (network, security, application, cloud) has its own individual automation/orchestration tools, which are converged and mediated manually. The good news is that there is plenty of automation in the domains.

The bad news is that the knowledge of the customer, the end-to-end service and the goals (SLA) of the services reside only in humans, and only temporarily while they manually execute cross-domain alignment and orchestration to create the service end-to-end or wade through alarms and tickets to diagnose a failure.

I've already touched on the limitations that occur around deployment time and these issues grow when it adds on assurance, healing, maintenance and other 'day two' operations. For these, this end-to-end service knowledge has to be recreated in order to give the engineer the context for the data which they require to make decisions and act. Oh, did I mentioned that the end-to-end service context is never stored? This means that the process must be repeated with every outage, every maintenance and every optimization. What happens when there are hundreds of thousands if not millions of instances of converged services in operation?

Autonomous Service Operations can solve these problems AT SCALE by operating at the service level where it encapsulates and retains end-to-end context for each service instance and then works cross-domain to drive the individual domain orchestrators and controllers to meet the goals of the service.

This can all be done at deployment time and continuously for day two operations like assurance, healing, and maintenance. Unlike the manual scenario I mentioned above, in this instance the service context is preserved.

It does not care that the elements, which make up the service are distributed across underlay, overlay and cloud implementations. It also does not care if a third party is providing them or that some elements have controllers, some have orchestrators and some are applications.

In the end, Autonomous Service Operations are essentially an expert AI system that encapsulates the knowledge of the human experts and then applies it at scale and at computer speeds to provide distributed management and control to meet the customer SLAs.

For CSPs this means a dramatic reduction in the time it takes to deploy a secure network service, faster ticket resolution, and acceleration in detection and repair to the point that issues become invisible to customers.

The ability to rapidly bring mass scale service products to market at new standards of profitability and performance through automation is exactly what CSPs need to bring out the full potential of the secure networks.

This is especially vital now in new emerging markets driven by edge computing, 5G and access services to hyper scale cloud providers.

About the Author

Harley is a serial entrepreneur dedicated to creating transformative digital technology solutions that set new standards for economic and human productivity.
Currently, Harley is the Founder and CEO of Sea Street Technology, which provides an AI autonomous operations platform that enables large service providers and top tier enterprises to progressively transform their product lines and businesses to fully autonomous, closed-loop digital services and operations.

Prior to Sea Street, Harley founded LineSider Technologies, where as CEO, he led it to become a leading provider of cloud infrastructure management and network virtualization software. LineSider was later acquired by Cisco Systems.