FEDERAL NEWS NETWORK ciena.

Safer, smarter and closer to the edge: 3 network trends for 2021

This content is provided by Ciena.

Running an agency network has never been a simple task, but 2020 proved that the need for a safe, reliable, and scalable network has never been greater. Between unprecedented traffic generated from the massive shift to telework and concerns from the SolarWinds breach, networks that relied on traditional network security measures and infrastructure were left stressed and vulnerable. Agencies are now forced to address these new developments with three major emerging trends: security, intelligence, and edge computing.

Safer networks

“When people talk about making the network safer, there are a number of different pieces that go into it,” said Steve Alexander, Senior Vice President and Chief Technology Officer for Ciena. “The network should be resistant to attack, it should be resilient, and if there is a failure, it should self-heal. It should be highly available, trusted, and allow you to have ‘confidence’ in it, meaning that the information flowing on it is correct, and you are confirmed to be connected to the entity you expect to be.”

Software-Defined Networking (SDN) is mission critical—especially with 400G speeds coming to edge devices in the very near future. Agencies have a need for their networks to be flexible and fast, yet secure. With increased amounts of data, ever-evolving cyber threats, and a greater variety of endpoints, agencies must enable their networks to protect themselves. Transforming the network into a sensor is one way to create a safer network. Achieving this requires establishing a baseline for what is normal on the network and then gaining an understanding of the telemetry, flows, configurations, inventory, services, and the users themselves. It is a big data problem, but one for which there is a solution—which leads to the second major trend of smarter networks.

Smarter networks

When dealing with datasets of this scale, automation becomes necessary with “a really disciplined and deliberate approach,” said George Holland, Vice President and General Manager of Ciena Government Solutions. Holland continues, “If you are trying to support the warfighter, or you are trying to support analysts, or law enforcement, if you want to give officers more capability, you want to make sure that they not only get the needed functionality, the advanced analytics—and everything else that goes with it, but that it is protected as well.”

While tempting, agencies should not jump straight into automation without careful planning and a firm grasp of the fundamentals—like confidence in the network infrastructure—or it will simply be a rush to failure.

“We spend a lot of time making sure that operators absolutely understand their inventory and configuration state, basically knowing the absence or presence of every physical and virtual device, what they are connected to, and what the traffic flows across those devices look like,” Alexander said. “Because if you don’t, and then you start to automate, you are just going to fail faster. Our belief is automation must start with an accurate knowledge of what the network inventory is. You can’t automate what you can’t see.”

There are three main processes that organizations usually consider for automation when establishing a telecommunications service: planning, process, and trouble-to-resolve. The planning function is anticipating need. It has a big data aspect to it; knowing what the customer base is doing creates the ability to figure out their needs. Second is the process between taking an order and delivering a service. The goal of automation here is always to shorten time to delivery. The third and final process is trouble-to-resolve; how quickly an organization can identify an issue and fix it.

“We really try to figure out what the customer wants to do as they move forward. Where is their mission going to take them? Where are their other operations going to take them? Then figure out if you’re going to get there, how can we use virtualization and automation to build a safer, closer, smarter network.” said Holland.

Moving closer to the edge

5G may be the biggest change in networking in the next decade. It is the intelligent edge—where mobile devices live—and is expected to facilitate a proliferation of smart devices by an order of magnitude, leading to billions of devices connected to the networks across the world. It is the beginning of a real foundation for the Internet of Things (IoT).

Steve Alexander refers to ‘mean-time-to-cloud’, the time required to get to the cloud for the desired end-user experience. “That means the construction or modernization of an awful lot of the Central Office (CO) infrastructure that is out there. We are either building new data centers, or we are converting what were old COs into data centers that can handle this edge computing requirement. I’m not sure everybody fully appreciates how much of that has to happen to really get the 5G experience that people want”, Alexander said.

The network is going to get faster and will have to become smarter to deal with the scale and diversity of demands to come. The enhanced 5G network will allow agencies—especially employees operating in the field—to take advantage of next-gen technologies like augmented reality and facial recognition. This combination of technologies requires a massive amount of computing and storage at the edge with low latencies.

“We really see a revolution in the whole interactive nature of future networks: AR/VR headsets for education, health care, first responders, warfighters,” Alexander said. “That will all be impacted by our ability to produce connections out to the edge that are high capacity and low latency.”

With the right balance of services, technology, and industry expertise; a safer, smarter, and closer-to-the- edge network of tomorrow is available today.

Get started
www.ciena.com/government