BTR

BROADBAND TECHNOLOGY REPORT®

ON TOPIC

Expanding Business Services

SPONSORED BY

ALIANZA™

ENDEAVOR BUSINESS MEDIA

The state of SMB cloud communications 2021

BY HANNA MILLER

While the telecom industry is ever-evolving, COVID-19 changed everything over the last 18 months. But what impacts did the pandemic really have? To find out, Alianza hired Independence Research, a broadband industry analysis firm, to gain insight into the state of the cloud communications market among small and medium businesses (SMBs).

In early 2021, Independence Research conducted a survey of over 500 SMB telecom decision makers in the United States at companies employing between 5 and 999 personnel. The respondents, who were professionals with direct control or knowledge of telecommunications spending strategies, were asked about the biggest market trends, their buying plans — including communications and collaboration requirements, priorities, and preferences — and the criteria they used for evaluating service providers and communications platforms. The results were notable.

This feature will review some of the key findings of that research with the goal of helping service providers identify potential customer requirements and market opportunities.

Top-line takeaways

Before we get into the survey result details, let's look at some of the highlights:

Key takeaways:

- The COVID pandemic has accelerated the adoption of cloud collaboration services.
- SMBs still view voice services as fundamental to doing business.
- SMBs prefer to obtain voice and collaboration services from a single trusted provider.
- Broadband providers are well positioned to win and retain cloud communications customers.

Noteworthy statistics:

- 70% of SMBs increased the use of existing collaboration solutions during the pandemic.
- 41% of SMBs said they introduced new collaboration tools during the pandemic.
- Fewer than half — only 48% — of SMBs believe their existing communications tools are adequate for work-from-home (WFH).
- 49% of SMBs would prefer to add collaboration services to their voice service — as opposed

Notable Statistics

Noteworthy statistics from the survey include:

87%

of SMBs would prefer purchase phone and cloud communications from their broadband provider, if the VoIP features met company requirements.

to adding voice to their collaboration solution (34%) or keeping voice and collaboration separate (17%).

- 91% of SMBs consider voice and/or advanced communication services essential to their success.
- 87% of SMBs would prefer to purchase phone and cloud communications from their broadband provider — if the VoIP features met company requirements.

What's behind these findings? SMBs have been embracing digital transformation and transitioning communications and collaboration services to the cloud for quite some time, but last year's COVID stay-at-home mandates caused many SMBs to accelerate their plans.

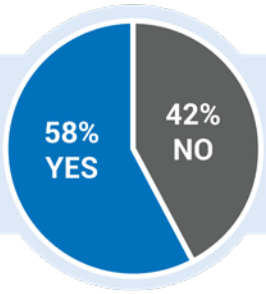
Looking ahead, many of the changes brought on by the pandemic will have lasting implications for service providers, such as the need to support increased numbers of SMBs that

COMMUNICATIONS IMPORTANT TO BUSINESS

How would you describe how phone and communications relate to your business?

SWITCHING PROVIDERS

Has your company switched or seriously considered switching voice providers in the past few years?



continue to rely on work-from-home or hybrid work models. For these SMBs, voice services will continue to play a vital role for both internal conversations and customer interactions. And, with 83% of SMBs preferring a single trusted provider for both voice and collaboration services, a growing number of opportunities exist for enterprising ISPs, MSOs, and telcos.

Let's take a look at these opportunities.

Abundant voice opportunities

Despite the headlines on cord cutting, mobile-only communications, and consumer preferences for texting, voice services are still considered essential for how businesses operate and succeed. While unified communications (UC) solutions are growing in popularity for internal communications, traditional voice is still seen by SMBs as fundamental – especially for customer interactions. This is highlighted by over half of the survey respondents (59%) saying that voice services are essential for their business and almost one-third (33%) indicating that advance voice features are critical for success.

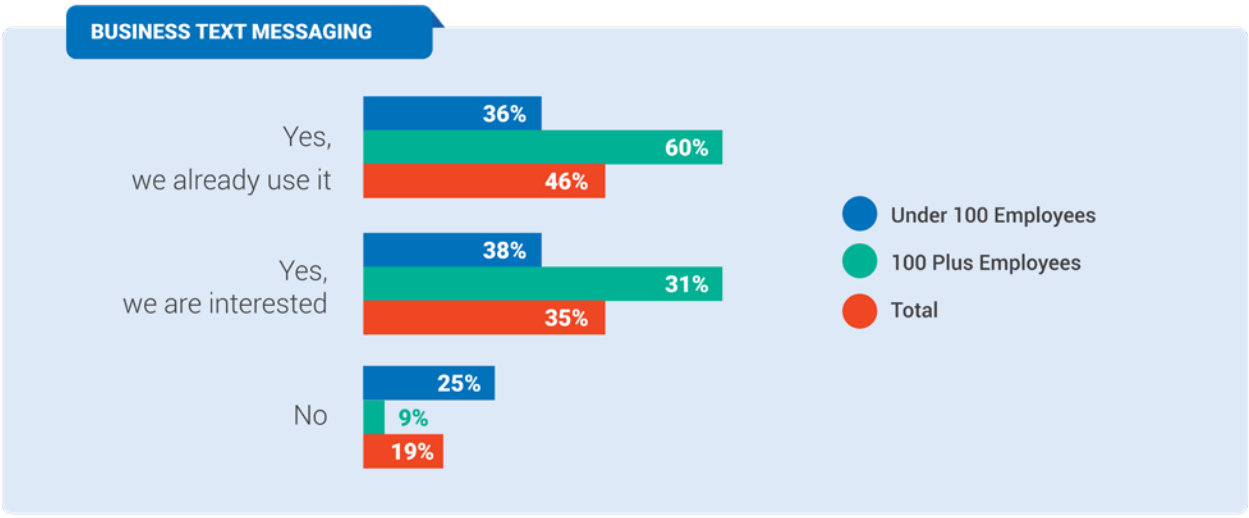
It's not surprising that the majority of SMBs (59%) get their voice services from a traditional telecom provider or cable broadband operator, as fewer than 20% of SMBs said they use an over-the-top (OTT) provider for voice services. Additionally, nearly 60% of survey respondents said they have switched or seriously considered switching voice providers in the past several years. Given these findings, service providers still have plenty of opportunities to retain existing customers, secure new voice customers, and win back old ones.

So, what are SMBs looking for in their voice provider? Their top criteria for selecting a voice provider are ease-of-use, speed and efficiency of deployment, and brand reputation. Surprisingly, SMBs don't place as much emphasis on a service provider's local presence. However, if all other criteria are equal, a local presence can certainly be a differentiator for a provider, given its advantages for setup and support.

Offer a choice in endpoints

Today's SMB workers have a variety of occupations and use cases that would benefit from being able to access their business communications services from anywhere – at home, in the office, on the road – using any device. The need for service providers to offer a softphone is emphasized by the fact that 63% of survey respondents said their employees *require* a softphone, and one-quarter of those indicated it's the only phone their employees need.

However, contrary to popular belief, good old desk phones aren't going away anytime soon. Of the survey respondents, 74% said their



employees require a desk phone, and over one-third said their employees require *only* a desk phone.

Business text messaging is a powerful communications channel

Business text messaging (BTM) services enable organizations to add new SMS and MMS communications channels using their existing phone numbers. With features like automated keyword responses, scheduled responses, contact management, and marketing campaigns, SMBs can leverage their phone number for multiple types of inbound and outbound communications. Most SMBs surveyed view BTM as a valuable communications channel, with 82% saying they use or are interested in using BTM services.

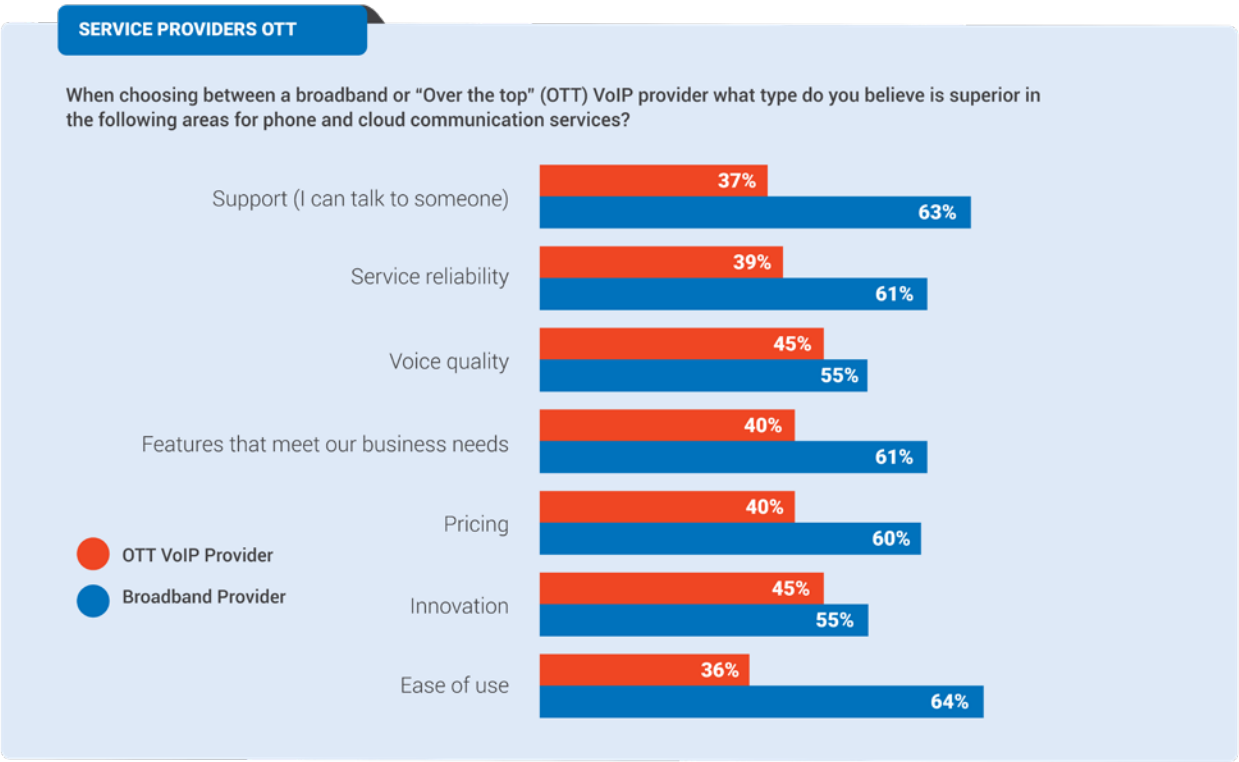
SMBs view BTM as an avenue for streamlining customer service, improving sales and marketing campaigns, and efficiently responding to prospect inquiries. Service providers can better serve their SMB customers by adding a BTM service as a standalone offering or bundled with their voice and UC services.

Be a single source for voice and collaboration

The vast majority of survey respondents (87%) said they'd prefer to add phone and cloud collaboration services to their existing voice services rather than purchasing each service from different providers. The larger the business, the more likely they were to prefer a single-provider solution.

- 70% of SMBs with 5–9 employees prefer a single-provider solution
- 80% of SMBs with <100 employees prefer a single-provider solution
- 89% of SMBs with more than 100 employees prefer a single-provider solution.

This presents a sizeable opportunity for CSPs and voice providers who add UC offerings to their portfolios, especially because CSPs have a decisive advantage over OTT players.



SMBs view service providers as superior

When survey participants were asked to compare broadband providers with OTT VoIP providers on seven different product, company, and support capabilities, the respondents rated broadband providers as superior in all areas.

Respondents gave broadband providers higher ratings for support, voice quality, and service reliability. But most SMB decision makers also believe that broadband providers offer better pricing, innovation, and ease of use, which are key selling points for many OTT VoIP services.

Looking forward

Alianza's *2021 Cloud Communications Survey* revealed substantial opportunities for service providers. Digital transformation trends, accelerated by the global COVID-19 pandemic, have expedited the demand for service providers to offer cloud collaboration services. With voice services continuing to be indispensable to SMBs, and a clear preference for adding collaboration functionality to their existing voice solutions, service providers can gain key market advantages with the cloud.

Based on the survey data, we recommend service providers consider the following actions:

- Pursue cloud-based UC services for SMBs adopting work-from-home and hybrid work models. Fewer than half of SMBs said they are satisfied with their existing collaboration solutions.
- Emphasize the continued importance of voice for business-to-consumer interactions in marketing. 90% of SMBs consider voice services essential.
- Give customers a variety of endpoints to choose from, including desk phones and softphones, and be sure to have a UC application solution that supports both.

– Add business text messaging services to your portfolio to boost revenue and customer stickiness. SMBs overwhelmingly believe BTM can help streamline sales, marketing, and support interactions.
– Show customers the advantages of selecting a trusted service provider that can deliver superior customer support, service quality, and reliability. And leverage a communications platform that gives you innovation and ease of use advantages.

Hanna Miller *is Vice President of Marketing at Alianza*

Do you know what SMBs are looking for from their communication service providers? We do.

Offer customers a broad range of **voice, messaging, collaboration, and mobility solutions** while increasing ARPU and lowering OPEX with our Cloud Communications Platform.

www.alianza.com

ALIANZA™

CableLabs' Transparent Security more effectively mitigates DDoS attacks for operators

BY MATT VINCENT

Pixabay / pixel2013

As recently developed and promoted by CableLabs, Transparent Security is a cybersecurity solution aimed at cable operators and internet service providers that identifies distributed denial of service (DDoS) attack traffic — and the devices (e.g., internet of things [IoT] sensors) that are the source of those attacks — and mitigates the attack at the customer premises or in the access network. As fully described by a recent blog by CableLabs, "the Transparent Security architecture is enabled through a programmable data plane (e.g., "P4"-based) and uses in-band network telemetry (INT) technology for device identification and in-band mitigation, blocking attack traffic where it originates on the operator's network."

CableLabs notes that P4 is an open-source programming language that lets end users dictate how networking gear operates. In a discussion with *Broadband Technology Report* regarding the technology, Randy Levensalor, Principal Architect, Future Infrastructure Group, Office of the CTO at CableLabs, and co-author of the blog, explained, "Transparent Security, at the heart of it, is a project to create an in-band DDoS detection and mitigation solution for any service provider. We're targeting cable providers because we're CableLabs, but nothing in it is limited to just cable operators. It could be a telco, hyperscale provider, or even an enterprise could use this technology. We're primarily looking at source-based DDoS mitigation — trying to block the attack close to or at the source. It does also work for traditional inbound attacks; but really, the scale you need to do it on the outbound side is what the primary target of this project is."

The CableLabs blog points out that typical DDoS mitigation solutions are deployed only at the interconnection points with other networks, meaning that they do not protect the network from internal DDoS attacks, and that "they can allow networks to be weaponized." Alternatively, CableLabs observes that its Transparent Security solution "can monitor ingress and egress traffic at every point in the network, from the customer premises to the core of the network." The organization says this capability allows operators to quickly identify the local network from which attack traffic originates, instead of identifying a service area that could include hundreds of devices, which may or may not be impacted by the attack.

CableLabs initially released the Transparent Security architecture and open-source reference implementation in October 2019. Cox Communications and CableLabs conducted a proof-of-concept test of the Transparent Security solution in the Cox lab in late 2020.

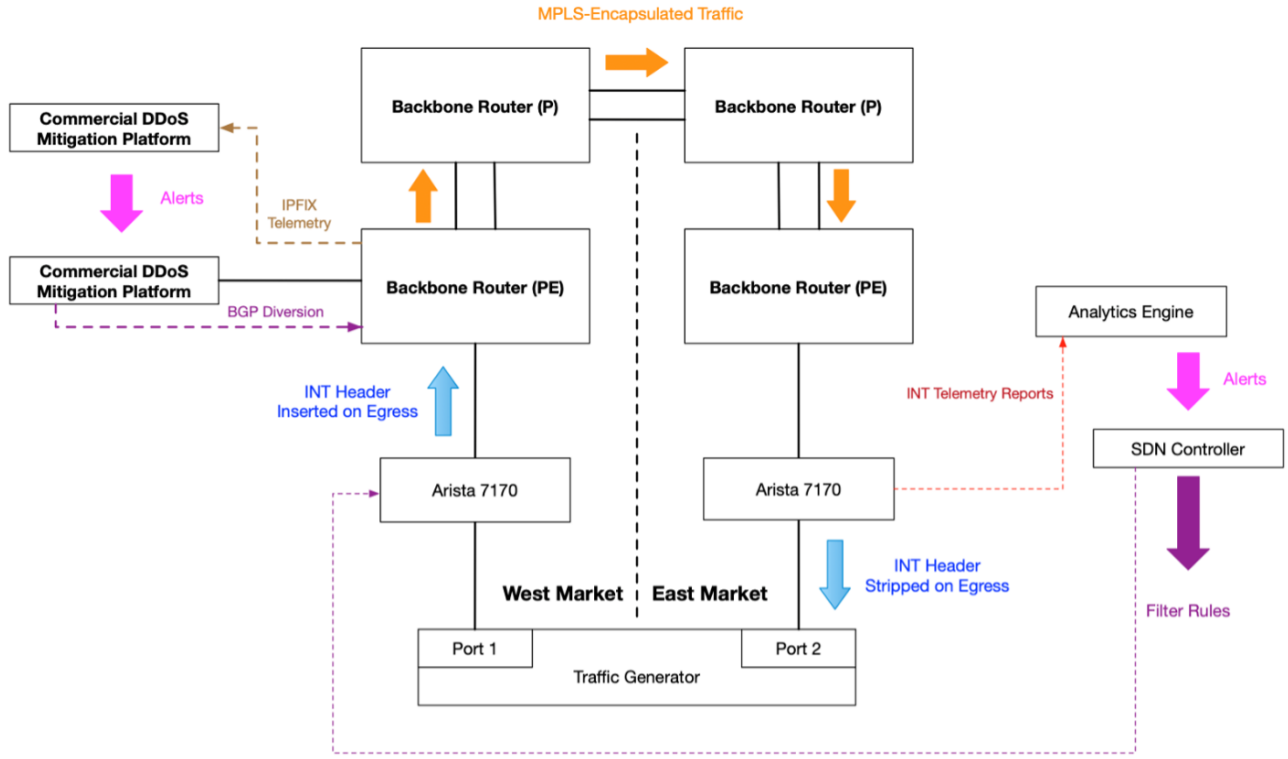
CableLabs' Levensalor noted, "Basically, we have a couple technologies in play here. To do a lot of this work we used P4, which is a programming language used to program networking devices. With NICs and switches, we can actually customize the behavior of the switch without having to wait for silicon to spin — that's how we were able to stand it up in our lab, and what we did with the test at Cox. It's open source, so our reference implementation, which really focuses on this in-band telemetry, the detection and mitigation function, is available now as an open source project on GitHub under the CableLabs namespace. So, you can actually go and download it today and run the exact code that we used for that for that trial."

CableLabs said that its Transparent Security trial with Cox with was primarily focused on several major objectives. Per the organization, these were: to compare and contrast performance of the Transparent Security solution against that of a leading commercially available DDoS mitigation solution; to validate that INT-encapsulated packets can be transported across an IPv4/IPv6/Multiprotocol Label Switching (MPLS) network without any adverse impact to network performance; and to validate that the Transparent Security solution can be readily implemented on commercially available programmable switches.

CableLabs' Levensalor added, "There's two implementations. One is how we're identifying where the threat came from — for that we're adding an in-band telemetry header to all the packets, basically as the packet enters the network. Eventually this will be implemented on the gateway on the customer premises, adding things such as the source Mac address and unique identifier for that gateway to the header. That way you can have that visibility, or transparency, if you will — that's where the name came from — across the network."

He continued, "Then, at each hop we add another identifier for that switch. To do that, we worked with the P4 application Working Group, which has an in-band telemetry specification. We worked with them to add a source-only metadata option to add that source of visibility into the switches that are able to do the in-band telemetry insertion; you can also add the Mac address of the device before it entered that controlled network."

CableLabs reported that its trial with Cox compared the effectiveness of Transparent Security with that of a leading DDoS mitigation



CableLabs

solution. CableLabs said that in the trial, "Transparent Security was able to identify and mitigate attacks in one second, as compared with one minute for the leading vendor." The organization noted that Transparent Security also validated that inserting and removing the INT header had no observable impact on network throughput or latency. The CableLabs blog stated that, when comparing and contrasting the performance of the Transparent Security solution against this commercially available DDoS mitigation solution, "the lab test results were very promising."

For the lab trial setup with Cox, CableLabs noted that the test environment was designed to simulate traffic originating from the access network, carried over the service provider's core backbone network, and targeting another endpoint on the service provider's access network in a different market (e.g., an "east-to-west" or "west-to-east" attack). The Transparent Security solution was implemented on commercially available programmable switches provided by Arista. "These switches are being deployed in networks today, and no changes to the Networking Operations System (NOS) were required to implement Transparent Security," added CableLabs. The diagram below provides a high-level overview of the lab test environment.

According to CableLabs, "In the lab trial, various types of DDoS traffic (UDP/TCP over IPv4/IPV6) were generated by the traffic generator and sent to the West Market Arista switch, which used a custom P4 profile to insert an INT header and metadata before sending the traffic to the West Market PE router. The traffic then traversed an MPLS label-switched path (LSP) to the East Market PE router, before being sent to the East Market Arista, which used a custom P4 profile to generate INT telemetry reports and to strip

the INT headers before sending the original IPv4/IPv6 packet back to the traffic generator."

"Detection of outbound attacks was rapid, taking approximately one second, and Transparent Security deployed the mitigation in five seconds," noted the CableLabs' blog, which added, "The commercial solution took 80 seconds to detect and mitigate the attack. These tests were run with randomized UDP floods; UDP reflection and TCP state exhaustion attacks were identified and mitigated by both solutions. In this trial, only packets related to the attack were dropped. Packets not related to the attack were not dropped."

CableLabs concluded that the tests validated that INT-encapsulated packets can be transported across an IPv4/IPv6/MPLS network without any adverse impact. According to the CableLabs blog, "There was no observable impact to throughput when adding INT headers, generating telemetry reports or mitigating the DDoS attacks. We validated that the traffic ran at line speed, with the INT headers increasing the packet size by an average 2.4 percent. Application response time showed no variance with or without enabling Transparent Security. This suggests that there will be no measurable impact to customer traffic when the solution is deployed in a production network."

As to why Cox was interested in deploying the solution, CableLabs points out that "although currently available DDoS mitigation solutions can monitor for outbound attacks, they're primarily focused on mitigating DDoS attacks directed at endpoints on the operator's network. These solutions use techniques such as BGP diversion and Flowspec to drop traffic as it comes into the network. However, mitigating outbound attacks using these techniques aren't effective because the malicious traffic will have already traversed the access network, where it has the greatest negative impact before the traffic can be diverted to a scrubber or dropped by a Flowspec rule."

Alternatively, CableLabs notes that "Transparent Security offers the promise of near-instantaneous detection of outbound attacks, as well as the ability to mitigate that attack at the source, on the customer premises equipment (CPE), thereby preventing that traffic from using upstream access network resources." CableLabs adds that, in addition to Transparent Security's DDoS mitigation capabilities, there are additional benefits to network performance/visibility in general.

"Implementation of Transparent Security on the CPE means that network operators can derive the specific device type associated with a given flow," explained the CableLabs blog. "This allows the operator to determine the type of IoT devices being leveraged in the attack. This also opens myriad other possibilities—for example, reducing truck rolls by enabling customer service personnel to determine that a customer's issue is with one specific device versus all the devices on the internal network. Another example would be the capability to track the path a given packet followed through the network by examining the INT metadata."

CableLabs contends that consumers will see a direct benefit from Transparent Security. The company says that, with the solution, once compromised devices are identified, the consumer can be notified to resolve the issue; or, alternatively, rules can be pushed to the CPE to isolate that device from the internet while allowing the consumer's other devices continued access. Such isolation mitigates the

additional harm coming from compromised devices, states the organization.

The CableLabs' blog notes that "this additional harm can take the form of degraded performance, exfiltration of private data, breaks in presumed confidentiality in communications, as well as the traffic consumed through DDoS. Less malicious traffic on the network provides for a better overall customer experience," adds the organization.

Why is the Transparent Security platform vital, and why is it being offered now? As explained by CableLabs, "As increasing numbers of devices connect to the network, there are more vulnerable points of attack for malicious actors. DDoS attacks cost the industry billions of dollars each year in malicious traffic delivery costs, traffic scrubbing and service downtime. The ability to quickly identify impacted devices and packets reduces malicious traffic delivery expenses for operators, service interruptions for consumers and costly mitigation efforts further in the packet lifecycle."

CableLabs' Levensalor concluded, "I think you know how bad DDoS attacks are, and we're predicting they're going to get worse with people buying more and more IoT devices, and a lot of them are not following the security standards and similar things that we're working on at CableLabs and in other industry forums. We're expecting that more IoT devices will probably be compromised, and other forms of DDoS attacks will arise. That trend has continued for a while, and we're hoping to hopefully curb that."

Comcast Business acquires SDN, cloud specialist Masergy

BY BTR STAFF

Comcast Business on Aug. 25 announced that it signed an agreement to acquire Masergy, a Plano, Texas-based expert in software-defined networking (SDN) and cloud platforms for global enterprises.

The acquisition stands to accelerate Comcast Business's increasing growth serving large and mid-size companies, particularly U.S.-based organizations with multi-site global operations, the company said in a statement.

"Masergy provides a perfect complement to our portfolio of enterprise services and solutions and will allow us to instantly and dramatically amplify our growth in the global enterprise market," said Bill Stemper, President, Comcast Business. "We're excited to welcome Masergy's employees and leadership to Comcast Business as we bring continued innovation and superior experience to our customers."

Comcast notes that, with over twenty years' experience and innovation in delivering managed network, cloud, and security services, Masergy has become a leading provider to companies worldwide, serving more than 1,400 customers in nearly 100 countries.

The combination of Comcast Business's advanced fiber network and Masergy's innovative services will enable Comcast Business customers to manage their international operations and networks more efficiently and securely, said the companies.

Masergy enables secure application performance across the network and the cloud with its Managed SD-WAN, Unified Communications as a Service (UCaaS), Call Center as a Service (CCaaS) and Managed Security offerings.

Notably, Masergy has been recognized for the past five years as a "Visionary" in Gartner's Magic Quadrant for Global Network Services.

Comcast Business's acquisition of Masergy is subject to regulatory approval and other customary conditions. Financial terms of the acquisition were not disclosed.

"On behalf of everyone at Masergy, we are thrilled to join the Comcast Business family and are extremely excited for the next chapter of Masergy. We are confident that together we can significantly enhance our service offerings to businesses of all sizes in their journey to the cloud," concluded Chris MacFarland, Chairman and CEO, Masergy.

Cox to acquire Segra's commercial enterprise and carrier fiber business

BY BTR STAFF

Cox Communications has entered into a definitive agreement to acquire Charlotte, N.C.-based Segra, one of the largest privately-held fiber infrastructure providers in the U.S.

Cox will acquire Segra's commercial services segment, which is a leading super-regional, fiber-based provider serving commercial enterprise and carrier customers in nine states in the Mid-Atlantic and Southeast. The company's dense metropolitan fiber network provides enhanced technology solutions and a commitment to a superior customer experience, it says.

As part of the transaction, EQT Infrastructure will retain ownership of Segra's fiber-to-the-premise (FTTP) residential and small- to medium-sized business segment in Virginia and North Carolina and accelerate the plan to expand broadband services to neighborhoods and markets throughout their regions.

"Cox is focused on buying and investing where it makes sense, and we believe that the demand for broadband infrastructure will continue to grow, making fiber an attractive area for long-term investment," commented Pat Esser, president and CEO, Cox Communications.

"Acquiring Segra's commercial services business is another key milestone in our pursuit of strategic infrastructure to ensure that we're providing the best products and services to our customers."

In the last few years, Cox network infrastructure investments have included EasyTel, EdgeConneX, InSite Wireless, StackPath, Unite Private Networks and ViaWest. The Segra acquisition supports that ongoing focus, says the operator.

"Our relationship with Cox will allow Segra to leverage expert resources, capabilities and strategic insights in order to scale up operations and accelerate long-term growth," said Timothy Biltz, CEO of Segra.

Blitz added, "Cox and Segra are equally devoted to the communities we serve. We will be even more strongly positioned to meet growing demand from carrier and enterprise customers for high-bandwidth fiber-infrastructure solutions. I would also like to thank EQT for its continued guidance and invaluable support as

we worked to grow the business over the last nearly four years."

Segra's existing management team will continue to lead the Segra enterprise and carrier organization following the acquisition, will retain the Segra brand and operate as a stand-alone business within the Cox family of companies.

The transaction is subject to customary regulatory approvals and closing conditions. Bank Street Group LLC and Goldman Sachs and Co. LLC acted as financial advisors and Simpson Thacher & Bartlett LLP acted as legal advisor to Segra in connection with the transaction.

For more information visit https://www.cox.com/business/home.html and www.segra.com.

Alianza delivers the only true cloud-native, carrier-grade communications platform built for service providers. Our proprietary full-stack cloud communications platform offers wholesale residential and business communications services, including voice, video conferencing, collaboration, text messaging, and standalone UC softphones. Our team of experts are passionate about transforming communications delivery and ensuring first-rate customer experiences for more than 200 service providers worldwide. As a result of the platform's exceptional quality and always-on availability, our service providers can innovate quickly and address the evolving demands of their end user customers in a way that is easy to manage, easy to consume, and highly profitable.

- Cloud Phone Systems: 9 Transformative Benefits for Service Providers
- Cloud VoIP Outsourcing Guide for Service Providers
- Service Provider Guide to SMB Communication Buying Trends
- Service Provider VoIP: Next-Gen is the Cloud
- Video: Alianza's Cloud Communications Platform for Service Providers