SPONSORED CONTENT

MOVING FORWARD WITH ZERO TRUST: CHARTING AN OPTIMAL REMOTE ACCESS ROADMAP

FROM CLOUD CONNECTIVITY VPNs: LOCKDOWN LESSONS LEARNED

The global pandemic forced millions of enterprise employees to abandon their offices and do their jobs from home, putting intense pressure on IT professionals to support and secure a largely remote workforce. Since many of these employees likely will continue to work remotely well into the future, IT pros are well-advised to assess their organization's remote access capabilities and make any necessary changes to ensure long-term success.

Enterprise remote access challenges and options were explored in a recent CIO Virtual Roundtable titled "Moving Forward with Zero Trust: Charting an Optimal Remote Access Roadmap," which was sponsored by NetMotion Software.

IT leaders from a variety of industries joined the online session to discuss:

- VPNs (virtual private networks) and VPN alternatives such as ZTNA (zero trust network access)
- How cloud changes the network connection picture
- Lessons learned during the lockdown

VPNs are (mostly) holding up

Before the pandemic, most organizations relied on virtual private networks to provide secure remote access to employees. Over the past few months, their VPNs have stood up reasonably well under the crush of additional remote connections, roundtable participants said.

A principal security architect for a holding company specializing in the utilities, construction, and logistics industries said the pandemic tested the limits of the organization's VPN, which had been supporting roughly 1,500 remote and mobile employees.

"When COVID hit, we increased our remote workforce to 6,000 in about a week," he said. "The big challenge we had is we've never needed a wide area network (WAN) presence in our backbone. So, we've pushed our bandwidth limitations to the nth degree, but we learned a lot about bandwidth constraints."

Some participants reported performance bottlenecks not on the VPN side, but at the user level.

"Business has been normal," said the global director of IT for a company that provides intelligent solutions for thermal utilities. "Most of the complaints have been at the end point, the end user."

"There definitely have been bandwidth problems for some users," the global head of IT for an investment advisory firm said.

Speaking about those users

The main goal for all organizations in providing remote access is ensuring not just security, but ease of access, productivity, and a quality experience. Roundtable participants said they've faced obstacles to meeting those requirements.

"One of the things we're experiencing is Zoom burnout," said a cybersecurity and compliance leader for a non-profit research and technical services organization. "Now we're talking about blocking off times when there are no meetings."

An IT solution design expert in the roundtable said the rail transportation company he works for is "in the process of deploying more internet access points to improve performance and access for users. And we're looking at upgrading bandwidth."

One of the biggest obstacles to a quality user experience is lack of visibility, NetMotion CEO and President Chris Kenessey said.

"A lot of people who have moved to working remotely are using networks that aren't owned or managed by the business, so the business can't see what's going on in those networks," Kenessey said. "The other thing is you don't usually know who's having a bad experience working remotely until they call and complain. But there are a lot of people who don't want to bother calling to complain. They'd rather just suffer in silence, and it's hard to gain visibility into their device in real time."

Kenessey cited one humorous example of visibility challenges.

"We had an employee who called in the other day, and he didn't realize it, but he went and had a beer at his neighbor's house, and logged into the neighbor's wi-fi," he said. "So, he actually still was attached to the neighbor's wi-fi weeks later, and hence he was having miserable throughput."

Remote access roadmaps

Roundtable participants outlined several strategic avenues they're exploring to ensure their remote access plans reflect their respective organizations' vision of the future of work.

"It comes right back to Zero Trust," said the non-profit organization's cybersecurity and compliance leader. "We have to make sure we provide the capability for employees to work from anywhere using various devices. It's not always going to be a company device, but you have to allow people to securely authenticate and be identified regardless of what they're using."

"We're putting more emphasis on VDI (virtual desktop infrastructure)," said the rail transportation company's solution design expert. "The challenge is to create the right profiles, and it takes a long time to create profiles with the right application stack. That's why we're still stuck with a lot of VPN."

The non-profit education membership association director said "our most important commodity is our data. My primary responsibility is more data security than infrastructure. Data loss prevention, pattern matching, any enhancement in that space is something intriguing to me and something I'm looking at."

Keeping up with change

The new work paradigm presents IT leaders with a list of priorities to make the remote work experience productive and secure. They strive to ensure not just security, but also easy, reliable access, and productivity. Remote work has tested systems, from band-width, VPNs, to visibility. But it's also tested employees' patience as they navigate the sudden changes to where, how, with whom, and when they work. In many cases, it's fallen to IT to manage not just the technology, but the change itself in their quest to provide a quality remote work experience.

In the words of cybersecurity and compliance leader for a non-profit organization, "We're trying to shift the corporate culture, and that includes making employees more aware of security when they're working from home."

"A lot of people who have moved to working remotely are using networks that aren't owned or managed by the business, so the business can't see what's going on in those networks."

CHRIS KENESSEY
CEO AND PRESIDENT, NETMOTION

NETMOTION