www.pipelinepub.com
Volume 19, Issue 7

Putting Network Resilience at the Heart of Digital Transformation

By: Joshua Currin

A resilient, robust, and always-on network is critical to business success in today's highly connected world. Such a network allows employees, engineers, and customers to work and perform essential day-to-day tasks. Any disruption to the network could result in a costly halt in business productivity and efficiency, not to mention untold damage to brand reputation. Nevertheless, many organizations pursuing digital transformation do not prioritize network resiliency. Research from Gartner shows that over 90 percent of businesses have some form of digital initiative, with 87 percent of senior business leaders stating that digitalization is a priority. Consequently, common technologies deployed during digital transformation include IoT, mobility, analytics and cloud solutions, all of which depend on a consistent network connection.

Moreover, as networks continue to grow in complexity, they also become more vulnerable to cyberattacks. While current numbers aren't as high as that initial surge during the pandemic, cyberattacks are still a significant danger. In the first half of 2022, there were an estimated 236.1 million ransomware attacks globally, representing 20 percent of all cybercrime in 2022. Similarly, malicious actors keep targeting vulnerable functionalities in software and networks. In fact, weaknesses got discovered in commonplace applications like SharePoint and OneDrive. Whether it's malware or phishing attacks, hackers constantly learn and evolve their techniques, becoming more sophisticated with each passing year. To make matters worse, any cybersecurity software available to the public can (and will) just as easily get obtained, analyzed, and dismantled by bad actors for future exploitation.

There is a clear correlation between the network, digital transformation, and cybersecurity—especially considering that so many cyberattacks often result in network outages or that the complexities stemming from digital initiatives open pathways for bad actors to access critical applications on networks. Our global study from 2020, which polled 500 CIOs and 500 network engineers from Western countries, found that 45 percent of surveyed CIOs saw security among their organization's greatest networking challenges post digital transformation. And although companies must deploy preventative measures to decrease the likelihood of a breach, the reality is that every enterprise pursuing digital transformation will inevitably experience a network outage. According to an analogous 2022 global report, which polled from a similar pool of participants as the first, the Mean Time To Recovery (MTTR), or the average time required to find and remediate a network outage, increased from 9.39 hours in 2020 to 11.2 hours in 2022.

The fact is that a resilient network—one that allows a business to maintain access to its critical assets and quickly (and remotely) recover from outages—is just as important to a company's overall security posture as the latest defensive solution. Indeed, security and network-focused digital transformation are not mutually exclusive but are two sides of the same coin. And because enterprises won't stop pushing digital transformation (nor should they), it's paramount that they place network resiliency at the heart of their digitization strategy to reduce the harmful consequences of downtime brought on by escalating cyberattacks.

Unifying network engineers and CIOs

Of course, putting the network at the heart of digital transformation to combat rising cybersecurity threats is easier said than done. One approach that organizations can take to move networks up the priority list is to promote collaboration between network engineers and CIOs. If anyone can drive network-focused digital transformation, it is these two roles. However, such cross-organizational collaboration is not as prolific as one might hope. Getting these two groups to work together cohesively is difficult because they face different challenges and responsibilities. According to the surveys above, 90 percent of digital transformation decision-making involves CIOs. Simultaneously, network engineers carry out the day-to-day processes needed to achieve said transformation. In other words, CIOs cast the vision for digital transformation, and the engineers determine how to execute that vision effectively. As a result, a disconnect emerges. To bring these two parties together and encourage effective investment in network security, it's crucial that businesses advocate for continuous communication to alleviate tension and more clearly illuminate objectives. CIOs can also deliver training for engineers to learn new network technologies and,

if necessary, allocate a larger budget to support implementation. Likewise, CIOs should find more opportunities to involve engineers, tapping into their expertise to ensure digital transformation remains networking-driven. While cooperation is essential for CIOs and network engineers, including alignment with their goals and needs, they are also uniquely positioned to bring about the most optimal change in their respective functions. Most notably, network engineers are ideally situated to suggest the right networking solutions to enhance cybersecurity. One such solution savvy engineers often recommend is out-of-band management.

Out-of-band management in network resilience

As companies increase their reliance on interconnected networks, virtualized cloud services and the edge, they, as mentioned above, become more susceptible to cyberattack-induced outages. In these situations, where the network is down, CIOs must avoid putting their engineers in scenarios where they have no option but to use the network to manage the network. While it may seem evident that such a method is inefficient, the truth is that many businesses' network configuration leaves them no choice, which exacerbates the cost and duration of downtime. In other words, too many companies rely on the traditional in-band network alone. When a disruption occurs, there is no way for engineers to access and remediate issues, as they become locked out of the primary network. Alternatively, CIOs should permit network engineers to leverage out-of-band management, which will allow them to separate and containerize the functions of the management plane from the data and control plane.

For some time, most businesses saw out-of-band configuration as reserved for “emergency only” use. However, with cyberattacks and outages on the rise, companies must use out-of-band management as it will help them keep the network central to their digital transformation strategy. An out-of-band network operates independently from the in-band network, enabling engineers to detect and resolve problems and access critical applications. Even if the primary network goes down, the out-of-band network is an alternative pathway that allows employees to perform their daily tasks and customers to access their profiles and use online applications. Indeed, out-of-band management creates a highly resilient network that can empower enterprises to maintain an acceptable level of service during faults to normal operations while also recovering rapidly from disruptions. Another invaluable benefit of out-of-band management is that it enables network engineers to manage network equipment and infrastructure remotely. Research shows that it can take a network engineer several days to go to a site and fix a problem, unnecessarily consuming time and resources. But, with out-of-band management, whenever there is an outage, the engineer or technician doesn’t need to travel physically to the site and manually remediate the issue.

Before utilizing out-of-band management to achieve network resiliency, CIOs and engineers must work together to complete an internal evaluation. During this assessment, both parties must assess how the network gets architected for remote access, automation, cellular connectivity, and scalability. This evaluation will assist engineers with day-one provisioning, emergency access and daily maintenance—in essence, every operation critical to keeping the network at the heart of digital transformation. For clarification, out-of-band management is not a substitute for cybersecurity. But, as the probability of network outages increases due to ongoing digital transformation initiatives, it is helpful that organizations also have a solution like out-of-band management to recover quickly from unavoidable downtime.

Finding an ideal vendor

CIOs should look for network solutions, like out-of-band management, that will allow their network engineers to remediate issues remotely, decrease the frequency of outages and provide critical services connectivity when the network is down. Likewise, they should prioritize finding a vendor whose capabilities aren’t limited to the worst days of the network’s lifecycle. Ideally, companies should search for network vendors that can minimize the worst days and are competent with first-day deployment and daily management. While network outages threaten businesses and digital transformation efforts, CIOs shouldn’t forgo the necessity of having a trusted partner to support those critical day-to-day operations. Ultimately, true digital transformation via a robust, resilient network must reduce downtime and bring value to the entire network lifecycle.