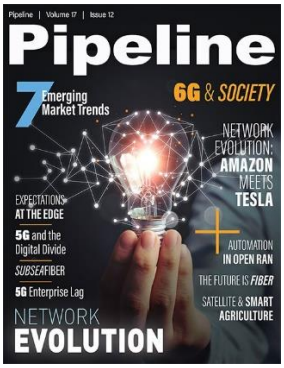
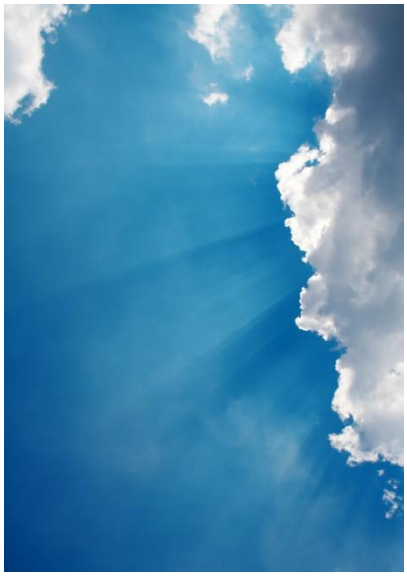


www.pipelinepub.com
Volume 17, Issue 12

7 Emerging Network Trends for Resiliency

By: Todd Rychecky



The network perimeter for businesses of every size all but dissolved due in large part to the events of the past 18 months. With millions having shifted to remote work and enterprises relying more heavily on a wide range of SaaS and cloud services to meet the requirements of a distributed workforce, the stakes suddenly increased. Some organizations were prepared for the transition, with policies already in place to some extent. Yet most were not prepared for the escalating cybercrime activity or network outages that occurred—not even the big tech giants. Google Services, for example, experienced a global outage that affected more than a million users of services including Gmail, Google Drive, Google Chat, Google Meet, Google Groups, Google Docs, Google Keep, and Google Voice. In the same month, Zoom, Slack and CenturyLink also suffered outages.

With experience comes perspective. Now it's clear that no single organization is immune to vulnerabilities. Experts now predict more than 60,000 organizations around the world may have been compromised, with more hackers joining the adversaries and more businesses at risk in the coming days and months. With the enterprise threat landscape increasingly more dynamic, expansive, and fluid, organizations must focus sharply on network management and security for more resilient networks.

To help businesses meet the challenges of 2021 and beyond, here are five emerging trends that will help create more robust infrastructures to protect them for years to come.

Increased investments in network resiliency

In 2020, many technology managers and C-level executives were forced to take measures to rapidly scale remote VPN services to keep operations going and employees connected. But even before the pandemic hit full force, a survey found that outages alone were costing 40 percent of US businesses more than $1 million annually. As technology evolves and network infrastructure becomes more geographically dispersed, organizations must adjust their strategies to prevent and recover from outages moving forward. Now, enterprises have more reason than ever to plan their budgets accordingly. By investing in network resilience solutions that can monitor, remediate, and configure equipment from any location, enterprises can drive more productivity and growth while defending against potential crises ahead.

A new virtual security paradigm for remote access

Recent surveys are revealing that people are adapting to the unprecedented changes, and so are many businesses. When it comes to work environments, a majority—44 percent of U.S. employees—would prefer to keep working from home compared to the 39 percent who would go back to the office. With videoconferencing technologies and collaboration platforms to keep people connected and engaged, it's understandable. But with millions more working from home, network boundaries are being pushed out. Add to this the high probability that many employees are using their personal computers for work and work computers for home tasks. IT departments have historically relied on location-based, physical security measures such as a secure floor in an office to protect certain equipment and digital assets, but with an ever-expanding perimeter, a more fortified management layer will become a necessity. Forward-thinking organizations are opting for an Out-of-Band connection to decouple network management from the primary production network that's processing hacker-prone user traffic. Or, they are implementing new security rules and gating mechanisms to protect data from being accessed remotely.

More secure, remote deployments

Advancements in technology are ramping up to ensure connectivity, which means enterprises must keep pace with upgrades, even if cost and social distancing make it impractical or impossible to get engineers onsite. To future-proof their infrastructure, organizations that are orchestrating new edge and data center deployments or cloud migrations are using tools like TPM chips, which prevent hardware tampering while enabling zero-touch provisioning capabilities. When it comes to re-provisioning equipment remotely, organizations are also utilizing new virtualized network functions to handle complex software stacks that need more troubleshooting or updates.

Smaller, distributed data centers and AI-powered management tools

With an exponential increase in data and tens of billions of IoT devices in use across the globe, the need for smaller distributed data centers is essential for supporting localized processing, which improves efficiency via network automation. These moregeographically disparate, edge-heavy networks, however, require smarter, more efficient management tools. In 2021, we've already seen an influx of increasingly must-have, smart AI-powered tools for self-healing and management functions, threat identification and recovery, low latency remote monitoring and provisioning, and much more.

With a need for efficiency to drive a hyper-automation mentality—dictating that everything that can be automated should be—leading-edge data centers are migrating from command line interface to NetOps automation to stay competitive and prepared for the future.

Increased focus on transparency

From unreported data breaches to deep fakes, there is a new level of distrust driving demand for greater transparency—and not just from consumers. The same week of the Association for Computing Machinery's fourth annual Conference on Fairness, Accountability and Transparency, the association removed Google as a sponsor in the wake of two female computer scientists calling out bias in artificial intelligence and within the company. When it comes to executives, Harvard Business Review Analytic Services reveals that 90 percent say increased business transparency leads to better-informed decision-making across the entire organization. This is good news for blockchain. Growing adoption and new implementation is occurring across industries ranging from entertainment services to healthcare. And with major organizations like PayPal, among others, embracing cryptocurrency, this trend will only gain more steam.

As blockchain-based applications quickly rise to prominence, they may present tempting targets to hackers seeking to capitalize on unprepared and less-resilient infrastructure tools, which is why some enterprises are turning to Smart Out-of-Band management, Failover to Cellular and NetOps automation to prevent outages and possible large-scale data breaches.

Rise in automation

As the escalating IoT market drives the need for smaller and disseminated data centers, the requirement for more efficient network management tools increases. All these changes will most likely lead to a trend toward hyper-automation. Businesses will have to adopt automation to be competitive in the future. As stated earlier, there will be an emerging desire to automate everything that can be automated to improve efficiencies, speed up processes and strengthen

business agility. Specifically, the first things to be automated will be legacy business procedures, along with a transition from the command-line interface to NetOps automation. Pivoting to remote work, enterprises that leverage automation will balance and secure the increasing distant connections. Likewise, local IT staff can use automation to augment service recovery and daily routine tasks. Still, the central purpose of automation is to enhance operational resilience to prepare businesses for any external factors that may cause further disruption from cyberattacks, outages, or other events. Automation will enable faster analysis, vulnerability testing and intervention in the event of a compromised network. In addition, it frees up engineers to put their energy and time into building other security and prevention strategies.

Accelerated transition to the cloud

There was a significant trend among businesses to move services and infrastructure to the cloud even before the pandemic. Files stored on cloud servers are encrypted and offer greater recovery and flexibility. Now, the cloud migration has gone into overdrive. No longer is the trend simply getting to the cloud, but instead a question of who can transition better, faster, and more securely. This massive acceleration into the cloud can be linked to the inundation of remote workers, causing providers to ramp up capacity. As nearly everyone shifts to the cloud, new cloud services will be the next key aspect of gaining a competitive edge, including AWS Network Firewall Services or those offered by major service providers. In terms of resiliency, the cloud will be at the core of every organization's future-proof strategy, as it permits quick recovery and continued operations despite equipment failure, power outages or cyberattack. Whether a business needs to scale up during periods of high traffic or scale down to lessen costs, a cloud computing solution will provide a higher level of security, which is why so many are making the switch.

There is no doubt about it: living in the Digital Age has provided new opportunities for businesses. But in the same way we could have never predicted a global pandemic, there is no telling what the future will bring. To improve the odds and outcomes in any future event, organizations can use these trends as a blueprint for success and take steps to prepare their networks.