Network Strategy Series

Autonomous Networks Lay The Foundation For Digital Transformation

LOPEZ RESEARCH

Digital Transformation Changes Network Requirements

Digital transformation (DX) isn't new, but the technologies and focus of a firm's transformation efforts change every few years. Market leaders will build hyper-adaptive businesses that continuously evolve to meet changing market demands.

These hyper-adaptive organizations deliver best-in-class customer and employee experiences by using technology to support a highly mobile workforce, remote workers and short-term contractors. The most successful companies will embrace new business models, such as moving to an as-a-service model, monetizing data from equipment and services, as well as adding third-party data to their offering to improve customer experiences. Meanwhile, market leaders also adopt different modes of application and service development such as DevOps, open source software and cloud computing to enable rapid service delivery.

These companies understand that a solid technology foundation underpins business success. In fact, 85%[1] of the companies Lopez Research interviewed believe better use of technology would help their company achieve competitive differentiation in 2019. Of course, digital transformation isn't without its challenges. IT and network administrators must deploy, manage and secure a rapidly changing landscape of devices, applications and cloud services. Today's digital transformation agenda differs from those that preceded it because it moves faster. IT must shorten the time it takes to adopt technology, deliver new insights and iterate on existing solutions.

IT must also evaluate and integrate multiple technologies into the organization simultaneously. Hyper-adaptive organizations will incorporate various technologies, such as mobile, cloud computing, autonomous networking and artificial intelligence, to create responsive infrastructure services. IT leaders must build a holistic roadmap that defines how these technologies will work together to create a flexible foundation for service delivery. For example, IT must design networking and cloud computing strategies to support mobile and the Internet of Things (IoT). Increasingly companies realize that an intelligent, autonomous network is the linchpin for growth or failure.

[1] All statistics are from the Lopez Research "Q1/19 Enterprise IT Benchmark Survey" report.

Autonomous Networking Enables New Experiences

The right networking foundation allows IT to support digital transformation by delivering Right-Time Experiences (RTEs). Lopez Research defines RTEs as a set of infrastructure and solutions that provide your employees, customers and business partners with the right information, at the right time on the person's device of choice. For example, hospitals want to improve patient care by connecting data from medical equipment into patient care applications in real-time.

Stadiums want to provide a new fan experience that allows high-speed connections, wayfinding and concessions delivery in the venue. Equipment manufacturers want to provide preventative maintenance services using sensor data and help field technicians resolve tickets faster with applications that use augmented reality. These are just a few of the examples of how companies are reinventing their business.

RTEs require a networking infrastructure that can deliver services that are contextual, adaptive, learning and predictive. Networking solutions deliver contextual experiences by collecting, analyzing and responding to new types of data such as mobile and IoT devices. Contextual information provides the basis for a company's applications to adapt to different performance and security characteristics.

Autonomous Networking Delivers 3 Main DX Benefits

With networking vendors embracing latest advances in artificial intelligence (AI) functions, such as machine learning (ML) and deep learning, companies can collect and analyze data from various sources to enable monitoring and management solutions that are learning, adaptive, predictive and automated.

Autonomous networking combines the latest advances in storage, big data processing and AI with networking to deliver new capabilities. Lopez Research defines autonomous networking as a network that runs with minimal to no human intervention. The software allows the system to configure, monitor, and maintain itself independently based on a set of business objectives orchestrated across a network through policies. These networks are also frequently called self-driving or intent-based. Autonomous networking services allow IT to anticipate issues, enable automation of specific tasks and optimize experiences. Embracing autonomous networks helps IT meet digital transformation demands by:

1. **Improving performance in a connected device world.** Mobility and the IoT devices have impacted networking requirements for years, but performance issues continue to increase over time as we add more devices to the network such as wearables, tablets and other IoT devices. These two trends impact networking by changing the volume of devices, the variety of devices and the mix of traffic that is on the network. Nearly two-thirds of the companies Lopez Research surveyed are experiencing network performance issues related to supporting the influx of mobile devices in the workplace. Additionally, new connected devices— from temperature sensors to MRI machines to smart lighting — have changed the definition of what administrators manage on the network.

2. **Minimizing security threats in a dynamic landscape.** The security threat landscape broadens as companies add new devices and bad actors create new types of attacks. More than 65% of the companies Lopez Research surveyed strongly agreed with the statement "Our organization struggles with the security and management challenges related to supporting a mobile workforce." Additionally, 75% of the IT leaders said security concerns stalled IoT deployment efforts. The autonomous network helps IT and security operations teams prevent security breaches by defining profiles of normal network behavior across a wide range of devices, detecting anomalous behaviors and taking actions to automatically remediate the issue. Many firms have already experienced a breach, but it can take almost a year for a company to detect and remediate a breach. Autonomous networking helps the networking and security operations team partner on finding and remediating an existing breach more rapidly.

3. **Eliminating mundane work.** To digitally transform a business, IT must move beyond merely replicating existing processes. Today's networking processes for configuration, optimization and troubleshooting require admins to perform mundane, repetitive work. Autonomous networks enable administrators to

work on higher-value tasks by automating repetitive tasks such as configuration management, RF optimization and troubleshooting.

What to Look For In Autonomous Networking

Organizations should no longer debate whether they should use autonomous networking technologies. Companies should be evaluating what type of networking technologies to use and how to deploy these services effectively. When assessing an autonomous network, IT should look for solutions that provide:

- **Integrated and adaptive management.** Autonomous systems offer a single management console that spans wired, wireless LAN and hooks into the WAN. The console unifies network provisioning, monitoring and troubleshooting. Companies need a networking system that can adapt to changing requirements without the need to rip and replace the infrastructure. A software-defined networking strategy allows IT teams to virtualize various aspects of infrastructure stack such as wireless controllers.

  Autonomous networks bridge the cloud and on-premise environments with the ability to configure and manage multiple types of networking functions in the cloud. For example, a company can control its WLAN entirely from the cloud, with access points remaining on location, allowing IT to manage multiple sites with fewer onsite resources easily.

  We've been on the Software-Defined Networking journey for some time, but vendors continue to improve the network analytics, visibility and automation. Autonomous networks enable IT to deliver the right capacity and performance to the right user and application at the right time. For example, the system can dynamically adapt to minimize congestion during peak times and support the proper quality of service based on whether the application is mission critical and the app performance requirements (e.g., low latency for video).

- **Insight created with the help of AI.** Visibility provides the foundation for any company's technology strategy. Autonomous networks use telemetry data, big data analytics and ML to analyze data, extract information from data and learn from it automatically, without being explicitly programmed. By combining these tools, IT can process and correlate massive amounts of data from different types of traffic and alerts. Networking vendors are leveraging ML to discover the behaviors of devices, users and network traffic at large.

Insight from network data helps IT detect patterns, create profiles and optimize network performance to support new applications. The autonomous network also helps IT move from reactive to proactive by pinpointing the root cause of current issues, predicting potential problems and suggesting the next best actions. Additionally, IT and security operations can use AI-driven insight to detect anomalies and remediate security issues faster.

- **Automation without loss of control.** Today's networks whether you call them intent-based, AI-enabled, autonomous or self-driving, all have one thing in common. These systems analyze data, provide recommendations and allow you to decide what actions to pursue. Autonomous networks deliver on the promise of self-provisioning, self-diagnosing, and self-healing. Autonomous systems enable IT to set parameters (sometimes called an intent) and allow the network to operate, self-heal and self-secure within those guidelines. Automation also reduces network performance issues and outages caused by human errors. While the network can run autonomously, admins can define the level of automation they want in the system.

  Automation doesn't replace jobs or create situations where IT is cut out of the loop. Autonomous networks help IT gain control through a better understanding of the overall network. As a result, IT can redeploy their resources to focus on higher return on investment task instead of managing basic network functions.

Conclusion

It's clear that IT and networking have never been a more critical part of the business. Thriving companies also understand that technology is not only about cost cutting or process efficiency. These nimble organizations embrace new technology to enable flexible work styles, new business models and rapid service delivery. Leading firms are treating autonomous networking as the foundation for creating hyper-adaptive organizations. With autonomous networking, IT will benefit from reduced complexity, better agility and security, operational efficiencies, and lower costs. The autonomous network increases productivity and improves the overall user experience by enabling IT to work better.

This report is reprinted from the Lopez Letter syndicated market research service. The opinion, analysis, and research results presented within the Lopez Letter syndicated services are drawn from research and analysis independently conducted and published by Lopez Research. For more information about Lopez Research reports, visit our web site at www.lopezresearch.com.