



Santhi Santhanakrishnan
Product Analyst, Site 24x7

LEVERAGING NETWORK MONITORING SOLUTIONS

While SMBs can choose between on-premises and cloud-based network monitoring tools, they should evaluate both pros and cons to make the right choice, writes Santhi Santhanakrishnan, Product Analyst, Site 24x7

As businesses grow, so do their networks and the challenges that come along with managing them. For small and medium-sized businesses (SMBs), however, tight budgets and fewer resources make it even more challenging for network admins to manually track and monitor all network elements. When network loads increase and issues begin to pile up, it starts to affect other IT elements, taking a toll on the entire business.

SMBs can use a comprehensive network management solution to ensure seamless functioning of not only IT, but the business as a whole. Without a proper tool in place, even simple issues like poor internet connectivity and network outages can bring down a service.

Here are four common network challenges SMBs face today and ways to leverage a network management solution to address them.

1. Security — the biggest question

Security, without a doubt, remains the biggest challenge in any IT environment. According to a recent cybersecurity report by Ponemon Institute, 58 percent of the surveyed SMBs experienced a cyberattack and data breach in 2018. 74 percent of SMBs list resource limitations as the main barrier when it comes to IT security. However, 55 percent of respondents blame their tight budget. In spite of cost and resource limitations, SMBs continue to strive to keep up with global security standards.

A network strategy with real-time per-

formance monitoring of all network devices, anomaly detection, and an instant alerting mechanism will help keep peripheral security threats in check. Keeping the budget constraints in mind, SMBs can adopt the freemium version of all-in-one monitoring solutions.

2. Visual documentation of the expanding network and its components

With network infrastructures growing at such a quick pace, keeping track of older devices can be particularly challenging. Just one device left unaccounted for can have negative ramifications that can ripple throughout the entire IT setup. Moreover, as the network expands, manually tracing out interconnections between devices becomes a Herculean task.

Without a proper map, it's nearly impossible to understand the network hierarchy. For example, if a switch loses its connection, without a network map, the network admin would first have to find the router to which the switch is connected, and then troubleshoot before fixing it, which can waste precious time. This is why a proper IP-based monitoring solution with a complete network map is essential to keep track of all resources.

3. Increased latency and packet loss

Annual global IP traffic will reach 4.8 ZB per year by 2022 according to research by Cisco. Higher volumes of traffic might present problems like increased latency and packet loss. Increases in latency affect the clarity of Voice over Internet Protocol (VoIP) calls, while packet loss can lead to data leaks. No one likes a slow network. Slow networks negatively affect the end-user experience and lead to loss of potential business.

A network monitoring tool with an

option to set thresholds on various performance metrics and send timely alerts could be a viable solution to track issues long before they affect the user experience.

4. Network congestion

Every network is prone to congestion at some point of time. Network congestion can be result of bandwidth hogs, higher volume of devices, incompatible hardware and more. An increase in incoming traffic isn't always a good sign. This could also be an indication of a distributed denial-of-service (DDoS) attack. DDoS attacks are on the rise; since last year Q4, DDoS attacks have increased by 84 percent according to Kaspersky's 2019 Q1 report. DDoS attacks can result in immediate and direct financial loss when potential customers are unable to reach the services while more long-term effects can include negative publicity and damage to brand name. Monitoring network bandwidth and traffic can keep networks secure from volumetric attacks.

While SMBs can choose between on-premises and cloud-based network monitoring tools, they should evaluate both pros and cons to make the right choice, keeping scalability in mind. As SMBs expand with multiple branch offices, spending on new monitoring resources and maintaining a private connection in each location might neither be feasible nor easy on their pockets. Cloud-based solutions bring in easier monitoring tool deployment architecture making it easy to access monitoring information on the move.

Beyond these day-to-day challenges, it's important for SMBs to build a sustainable and scalable network that they can manage from a single console. This is why, for growing networks, a comprehensive and customizable monitoring solution is less a perk and more a requirement.